AN ALGORITHM FOR MODULAR ELLIPTIC CURVES OVER REAL QUADRATIC FIELDS

LASSINA DEMBÉLÉ

Abstract. Let $F$ be a real quadratic field with narrow class number one, and \( f \) a Hilbert newform of weight 2 and level $n$ with rational Fourier coefficients, where $n$ is an integer 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 elliptic curve $E_f$. We give several illustrative examples which explain among other things how to compute modular elliptic curves with everywhere good reduction. Such curves do not admit any parametrization by Shimura curves, and so the Eichler-Shimura construction is still conjectural in this case.

Introduction

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

$$L(E, s) = \prod_{p|\text{cond}(E)} \left(1 - \frac{a_p(E)}{N(p)^s}\right)^{-1} \prod_{p|\text{cond}(E)} \left(1 - \frac{a_p(E)}{N(p)^s} + \frac{1}{N(p)^{2s-1}}\right)^{-1}.$$ 

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

**Conjecture 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 $X_0(n)$ and its Jacobian $\text{Jac}(X_0(n))$. In fact, by using the theory of modular symbols, one can make this construction very explicit. This is used in a very systematic way by Cremona [2] 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 generalized very well in this case as Hilbert-Blumenthal modular varieties prove not to be good substitutes for modular curves. As an alternative, the theory of Shimura curves has been exploited in order to prove many cases of the conjecture. This approach however needs to assume that the form $f$ satisfies certain restrictive conditions imposed by the use of the Jacquet-Langlands correspondence in this case. 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 [14] and references therein).

Although Hilbert-Blumenthal varieties are not good substitutes for modular curves, they provide the most natural approach to Conjecture 1. Indeed, the Eichler-Shimura construction can be phrased in the language of cohomology or motives, which is better suited for working in higher dimension. This was observed by Oda in the early 80s. In [9], he formulated a cohomological version of Conjecture 1 when $F$ is a real quadratic field. He later generalized this to totally real fields of arbitrary degree in [10]. From now on, we will restrict ourselves to the case where $F$ is a real quadratic field and recall the reformulation of Conjecture 1 by Oda. In order to do so, we need to introduce some notations. Let $X_0(n)/\mathbb{Q}$ be a compact arithmetic Hilbert modular surface of level $n$. (We recall that such compactifications exist thanks to Dimitrov [8]). Let $H^2_{\text{cusps}}(X_0(n), \mathbb{Q})$ be the middle degree cuspidal cohomology of the surface $X_0(n)$. The space $H^2_{\text{cusps}}(X_0(n), \mathbb{Q})$ comes equipped with a Hecke action provided by algebraic correspondences. Let $H^2_{\text{cusps}}(X_0(n), \mathbb{Q})_f$ 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 2** (Oda). Let $f$ be a Hilbert newform of weight 2 and level $n$ with integer Fourier coefficients. There exists an elliptic curve $E_f$ defined over $F$, with good reduction outside $n$, and an isomorphism of Hodge structures

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

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

In [9], Oda was able to construct the elliptic curve $E_f$ as a complex curve. However, he was able to prove that $E_f$ was defined over $F$ only when the newform $f$ was 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 provides some numerical evidence for Conjecture 1, but we think that it is the first algorithm which gives a way to systematically construct modular elliptic curves over real quadratic fields. One situation when our algorithm can be of special interest is 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 [11]. This curve is not a $\mathbb{Q}$-curve and so cannot be obtained by the method in Cremona [3].

The paper is organized as follows. In section 1, we present the strategy of our algorithm. In sections 2 and 3, we explain how to compute the periods of the curve $E_f$. In section 4, we present the algorithm, which is followed by several illustrative examples. As a final application of our algorithm, we explain in section 5 how to construct modular elliptic curves with everywhere good reduction.

**Acknowledgements.** I first lectured on the results in this paper at the MSRI Graduate Summer Workshop 2006 “Computing with modular forms”. 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.

1. 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 archimedian 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 [9] and the Weierstrass uniformization theorem in order to find an equation for $E_f$ over $F$. 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 $\omega_E$ be the Néron differential form of $E$ and $\Lambda_E$ the Néron lattice attached to $\omega_E$. Let $\Omega_E^+ \ (\text{resp. } \Omega_E^-)$ be the real period of $E$ (resp. $\bar{E}$), and $\Omega_E^+ \ (\text{resp. } \Omega_E^-)$ be the imaginary period of $E$ (resp. $\bar{E}$). We then define the period lattices $\Lambda_E^{ss} = \Omega_E^+ \Lambda_E$. Let $\mathfrak{H}$ be the Poincaré upper-half plane. We recall that the two involutions

$$\mathfrak{H} \overset{\varepsilon^2}{\rightarrow} \mathfrak{H},$$

$$(z_1, z_2) \overset{\varepsilon_1 z_1, \varepsilon_2 z_2},$$

$$(z_1, z_2) \overset{\varepsilon_1 \varepsilon_2 z_1, \varepsilon_1 z_2},$$

descend to the modular surface $X_0(n)$ and give the Hodge type decomposition

$$H^2_{\text{cusp}}(X_0(n), \mathbb{Q})_f = H^2_{\text{cusp}}(X_0(n), \mathbb{Q})_f^{++} \oplus H^2_{\text{cusp}}(X_0(n), \mathbb{Q})_f^{+-} \oplus H^2_{\text{cusp}}(X_0(n), \mathbb{Q})_f^{-+} \oplus H^2_{\text{cusp}}(X_0(n), \mathbb{Q})_f^{--}.$$ 

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

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

where $\Omega_f^{++}$ and $\Omega_f^{-+}$ are positive real numbers and $\Omega_f^{+-}$ and $\Omega_f^{--}$ are purely imaginary with positive imaginary parts. Concretely put, the Oda conjecture asserts that there are non-zero rational numbers $c_{ss'} \in \mathbb{Q}$ such that

$$c_{ss'} \Omega_f^{ss'} = \Omega_E^+ \Omega_E^{s'},$$

for all $s, s' \in \{-, +\}$.

This phenomenon illustrates the fact that the periods of the form $f$ are actually mixes 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 1.** Assume Conjecture 2, and let $\Lambda_f^+$ (resp. $\Lambda_f^-$) be the lattice given by $\Lambda_f^+ = (\Omega_f^{++}, \Omega_f^{+-})$ or $(2\Omega_f^{++}, \Omega_f^{+-} + \Omega_f^{-+})$ (resp. $\Lambda_f^- = (\Omega_f^{-+}, \Omega_f^{--})$ or $(2\Omega_f^{-+}, \Omega_f^{--} + \Omega_f^{++})$) 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 [9, Theorem 4.4]). The rest of the lemma follows by observing that the lattice \( \Lambda_f^+ \) is homothetic to a lattice contained in \( \Lambda_E \).

From Lemma 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 \( j(\tau) = \frac{\Omega_f^+}{\Omega_f^+} \) or \( \tau = \frac{1}{2} \left( 1 + \frac{\Omega_f^+}{\Omega_f^+} \right) \), 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 \( \Delta_E \), we can obtain \( c_4 \) if we know \( j(\tau) \) to enough 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-Laska’s algorithm.

2. Computing the period lattice: The Oda approach

In this section, we recall some results about the periods constructed by Oda in [9, sec. 16. 2]. His construction uses certain explicit 2-cycles that are reminiscent of the classical modular symbols. Let \( \chi : (\mathcal{O}_F/c)^\times \to \mathbb{C}^\times \) be a primitive quadratic character of conductor \( c = (\nu) \) that is prime to \( n \), where \( \nu \gg 0 \). Also let \( V \subseteq \mathcal{O}_F^{\times +} \) be a subgroup of finite index such that \( V \subseteq 1 + c \). We extend the character \( \chi \) to non-units in the obvious way. The twisted \( L \)-series of \( f \) by \( \chi \) is given by

\[
L(f, \chi, s) := \sum_{a \subseteq \mathcal{O}_F} \frac{\chi(a)c(a, f)}{N(a)^s},
\]

where \( c(a, f) \) is the Fourier coefficient of \( f \) at the ideal \( a \).

Proposition 1 (Oda). Let \( \Lambda_f \) be a period lattice in the isotypic component of \( f \) and let

\[
\Omega_{f, \chi, V}^{ss'} = -4\pi^2 \text{disc}(F)^{1/2} |\mathcal{O}_F^{\times +} : V| G(\chi)L(f, \chi, 1),
\]

where \( G(\chi) \) is the Gauss sum of the character \( \chi \), and \( \chi(\bar{\varepsilon}) = s \) and \( \chi(\varepsilon) = s' \). Then \( \Omega_{f, \chi, V}^{ss'} \) is a rational multiple of \( \Omega_f^{ss'} \) when \( \chi(-1) = ss' \).

Remark 1. We note that Proposition 1 is slightly different from [9, Theorem 16.3] because of the fact that the differential form we use is normalized.

By making use of Proposition 1, it is possible to compute the period lattice \( \Lambda_f \) 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 [1].

Conjecture 3. Let \( \chi : (\mathcal{O}_F/c)^\times \to \mathbb{C}^\times \) be a primitive quadratic character of conductor \( c = (\nu) \) that is prime to \( n \), where \( \nu \gg 0 \). Let

\[
\Omega_{f, \chi}^{ss'} = -4\pi^2 \text{disc}(F)^{1/2} G(\chi)L(f, \chi, 1),
\]

where \( G(\chi) \) is the Gauss sum of the character \( \chi \), and \( \chi(\bar{\varepsilon}) = s \) and \( \chi(\varepsilon) = s' \). Assume that Conjecture 2 is true. Then \( \Omega_{f, \chi}^{ss'} \) is an integer multiple of \( \Omega_{E, \chi}^{ss'} \) when \( \chi(-1) = ss' \).
We need to find a way to efficiently compute the periods we 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 \([2, \text{Propositions 2.11.1 and 2.11.2}]\).

Let \( W_N \) be the Atkin-Lehner involution given by

\[
W_N : z = (z_1, z_2) \mapsto (-\frac{1}{Nz_1}, -\frac{1}{Nz_2}),
\]

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

\[
f(z_1, z_2) = \sum_{\mu \in \mathfrak{O}_p^+} c((\mu)) \exp \left[ 2\pi i \text{Tr} \left( \frac{\varepsilon \mu z}{\sqrt{D}} \right) \right]
\]

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

\[
f_\chi(z_1, z_2) = \sum_{\mu \in \mathfrak{O}_p^+} c((\mu)) \chi(\mu) \exp \left[ 2\pi i \text{Tr} \left( \frac{\varepsilon \mu z}{\sqrt{D}} \right) \right]
\]

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 \( \chi \).

**Lemma 2.** Let \( f \in S_2(\mathfrak{n}) \) be an eigenform. If \( W_N f = -f \), then \( L(f, 1) = 0 \); otherwise

\[
L(f, 1) = -\frac{D}{2\pi^2} \sum_{\mu \in \mathfrak{O}_p^+} \frac{c((\mu))}{N(\mu)} \left[ 1 - \exp \left( -\frac{2\pi \varepsilon \mu}{\sqrt{DN}} \right) \right] \times
\]

\[
\exp \left[ \frac{2\pi}{\sqrt{D}} \left( \frac{\bar{\mu} \bar{\varepsilon}}{\sqrt{N}} - \frac{\mu}{\sqrt{N}} \right) \right].
\]

**Proof.** By definition,

\[
L(f, 1) = \int \int_{\mathfrak{O}_p^+ \setminus \mathbb{R}_+^2} f(iy_1, iy_2) dy_1 dy_2 = \int_{\tau_0}^{\tau_0} \int_{0}^{i\infty} f(z_1, z_2) dz_1 dz_2,
\]

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

\[
L(f, 1) = \int_{\tau_0}^{\tau_0} \int_{0}^{i\infty} f\|W_N(z_1, z_2) dz_1 dz_2
\]

\[
= \varepsilon_N L(f, 1).
\]
This gives the first part of the lemma. To get the second one, keeping the same choice of \( \tau_0 \) as before, we choose \( C \) on the imaginary axis and split the integral as

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

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

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

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 \( \tau_0 \) and \( C \) preserves the convergence rate under Atkin-Lehner involution and also ensures that both integrals have the same convergence rate. \( \square \)

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

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

By using the fact that every totally positive unit is of the form \( \epsilon^{2k}, k \in \mathbb{Z} \), this series can be rearranged as

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

3. **Computing the period lattice: The Darmon approach**

The Oda cycles provide a very efficient way to compute a period lattice \( \Lambda_f \) associated to the modular form \( f \). Unfortunately, in a way that is reminiscent of the classical setting, this method only gives the components \( \Omega_{j^+} \) and \( \Omega_{j^-} \), or \( \Omega_{j^+} \) and \( \Omega_{j^-} \), depending on wether \( \varepsilon_N = 1 \) or \( \varepsilon_N = -1 \), when the level \( n \) is a square. In order to circumvent that problem, we present a second approach that is based on a construction of Darmon [5, Chap. VIII]. His construction is a more down to earth reformulation of the Oda conjecture in the language of group cohomology. Although the primary goal of [5] 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 \( \Lambda_f^* \) and \( \Lambda_f^- \). We recall this construction along the lines of Darmon-Logan [6]. First, we define the differential forms

\[
\omega_f^\pm := -4\pi^2 \sqrt{D}^{-1} \left\{ f(z_1, z_2)dz_1dz_2 \pm f(-\varepsilon_1 \bar{z}_1, -\varepsilon_2 \bar{z}_2)d(\varepsilon_1 \bar{z}_1)d(\varepsilon_2 \bar{z}_2) \right\}.
\]
The differential forms $\omega_\pm^\pm$ are $\Gamma$-invariant, and so we have

$$\int_{\tau_1}^{\gamma_1} \int_{\tau_3}^{\gamma_3} \omega_\pm^\pm = \int_{\tau_1}^{\gamma_2} \int_{\tau_3}^{\gamma_3} \omega_\pm^\pm, \text{ for all } \gamma \in \Gamma.$$ 

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

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

with $I_\Gamma$ and take the module of coinvariants. This gives the exact sequence

$$0 \rightarrow K_\Gamma \rightarrow (I_\Gamma \otimes I_\Gamma) \rightarrow (\mathbb{Z}[\Gamma] \otimes I_\Gamma) \rightarrow I_{\Gamma} \rightarrow 0,$$

where $K_\Gamma$ is the kernel of the natural homomorphism $r$ and we use the canonical identification of $I_{\Gamma}/I_{\Gamma}^2$ with the abelianization $\Gamma_{ab}$ of $\Gamma$. We choose $\tau_1, \tau_2 \in \mathfrak{H}$ and put

$$I_{\tau_1, \tau_2} (\gamma_1 - \gamma_1', \gamma_2 - \gamma_2') := \int_{\tau_1}^{\gamma_1} \int_{\tau_2}^{\gamma_2} \omega_\pm^\pm, \text{ for all } \gamma_i, \gamma'_i \in \Gamma,$$

and extend it linearly to $(I_\Gamma \otimes I_\Gamma)$. This is possible because of the $\Gamma$-invariance of the forms $\omega_\pm^\pm$. The maps $I_{\tau_1, \tau_2} : (I_\Gamma \otimes I_\Gamma) \rightarrow \mathbb{C}$ are group homomorphisms whose restrictions to $K_\Gamma$ do not depend on the choices of $\tau_1$ and $\tau_2$, and so, the subgroups $\Lambda^\pm_\Gamma := I_{\tau_1, \tau_2} (K_\Gamma)$ only depend on the form $f$. The following conjecture is the combination of Conjecture 1.1. and Conjecture 2.1 in [6] and it is easy to see that it is a reformulation of Conjecture 2.

**Conjecture 4** (Darmon-Logan [6]). Let $f$ be a Hilbert modular form with rational Fourier coefficients. The subgroup $\Lambda^\pm_\Gamma$ (resp. $\Lambda^-_\Gamma$) is a lattice in $\mathbb{C}$ that is commensurable with the lattice $\Lambda^\pm_E$ (resp. $\Lambda^-_E$).

Let $e_\Gamma$ be the exponent of $\Gamma_{ab}$, which is finite by [6], and let $\tilde{\Lambda}^\pm_\Gamma = e_\Gamma^{-1} \Lambda^\pm_\Gamma$. The construction of Stark-Heegner points relies on the semi-definite integral

$$\mathfrak{H} \rightarrow C/\tilde{\Lambda}^\pm_\Gamma$$

$$(\tau, x, y) \mapsto \int_{x}^{y} \int_{\tau}^{y} \omega_\pm^\pm,$$

which enjoys the following crucial properties:

(i) $\int_{x}^{y} \int_{\tau}^{y} \omega_\pm^\pm + \int_{x}^{y} \int_{\tau}^{y} \omega_\pm^\pm = \int_{x}^{y} \int_{\tau}^{y} \omega_\pm^\pm.$

(ii) $\int_{x}^{y} \int_{\tau}^{y} \omega_\pm^\pm - \int_{x}^{y} \int_{\tau}^{y} \omega_\pm^\pm = \int_{x}^{y} \int_{\tau}^{y} \omega_\pm^\pm \in C/\Lambda^\pm_\Gamma.$

For more details on the construction of this semi-definite integral, we refer to [5, Chap. VIII] and [1, 6].

Let $K/F$ be a quadratic extension that is complex at $v_1$ and real at $v_2$, and let $O_K$ be the maximal order of $K$. An optimal embedding of $K$ into $M_2(F)$ is an $F$-algebra homomorphism $\Psi : K \rightarrow M_2(F)$ such that $\Psi(O_K) = \Psi(K) \cap M_2(O_F)$. By making use of the Dirichlet units theorem, it can be shown that $O_K^\times$ is a free rank one abelian group modulo $O_F^\times$. Let $\gamma$ be a generator of $\Psi(O_K) \cap \Gamma$. One can show that $\gamma$ has a unique fixed point $\tau \in v_1(K) \cap \mathfrak{H}$. Choose $x \in \mathfrak{H}$ and put

$$J^\pm_\Gamma := \int_{x}^{\gamma x} \int_{\tau}^{\gamma \tau} \omega_\pm^\pm.$$
It is shown in [5] that \( J_{v_1}^\pm \) 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 uniformisation attached to the lattice \( \Lambda_E^\pm \). We choose non-zero integers \( c^\pm \) such that \( c^\pm \Lambda_f^\pm \subseteq \Lambda_E^\pm \) and set
\[
P^\pm_\tau := t \cdot \eta^\pm(c^\pm \cdot J^\pm_\tau).
\]

Let \( H \) be the ring class field of \( K \), and \( H^+ \supseteq H \) the narrow ring class field. The Galois group \( \text{Gal}(H^+/H) \) has cardinality at most 2, and we let \( \sigma \) be its generator. We recall Conjecture 2.3 from [5].

**Conjecture 5 ([5]).** The local point \( P^+_\tau \) (resp. \( P^-_\tau \) in \( E(\mathbb{C}) \)) is a global point in \( E(H) \) (resp. in \( E(H^+) \)), and we have
\[
\sigma \cdot P^+_\tau = P^+_\tau \text{ and } \sigma \cdot P^-_\tau = -P^-_\tau.
\]

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 5 we can go round that problem. Indeed, Conjecture 5 suggests that when \( H^+ = H \), the point \( P^-_\tau \) is trivial, meaning that \( cJ^-_\tau \) is a period in \( \Lambda^-_f \) for some \( c \in \mathbb{Q} \). Thus, in favorable circumstances, we can use the following proposition in order to compute the period lattice \( \Lambda^-_f \).

**Proposition 2.** Let \( K \) be a quadratic extension of \( F \) that is complex at \( v_1 \) and real at \( v_2 \). Let \( \Psi : K \to M_2(F) \) be an optimal embedding. Let \( u \) be a generator of the rank one free group \( \mathcal{O}_K^\times \) and let \( \tau \) be the unique fixed point of \( v_1(\Psi(K^\times)) \) in \( \mathfrak{H} \). We assume that \( H^+ = H \) and that
\[
\gamma_\tau := \Psi(u) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}
\]
is such that \( a \in \mathcal{O}_E^\times \). Then
\[
J^-_\tau = \int_{\frac{a}{2} - \frac{1}{4}}^{\frac{a}{2} + \frac{1}{4}} \int_{\frac{b}{2} - \frac{1}{4}}^{\frac{b}{2} + \frac{1}{4}} \omega^-_f \text{ or } J^-_\tau = \int_{\frac{a}{2} - \frac{1}{4}}^{\frac{a}{2} + \frac{1}{4}} \int_{\frac{b}{2} - \frac{1}{4}}^{\frac{b}{2} + \frac{1}{4}} \omega^-_f
\]
depending on whether \( \varepsilon_N = 1 \) or \(-1 \). Assuming Conjecture 5, the period \( J^-_\tau \) belongs to \( \alpha \Lambda^-_f \) for some \( \alpha \in \mathbb{Q}^\times \).

**Proof.** Since \( H^+ = H \), Conjecture 5 implies that \( P^-_\tau \) 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 \( J^-_\tau \) is given by
\[
J^-_\tau = \int_{\frac{a}{2} - \frac{1}{4}}^{\frac{a}{2} + \frac{1}{4}} \int_{\frac{b}{2} - \frac{1}{4}}^{\frac{b}{2} + \frac{1}{4}} \omega^-_f = \int_{\frac{a}{2} - \frac{1}{4}}^{\frac{a}{2} + \frac{1}{4}} \int_{\frac{b}{2} - \frac{1}{4}}^{\frac{b}{2} + \frac{1}{4}} \omega^-_f = \int_{\frac{a}{2} - \frac{1}{4}}^{\frac{a}{2} + \frac{1}{4}} \int_{\frac{b}{2} - \frac{1}{4}}^{\frac{b}{2} + \frac{1}{4}} \omega^-_f.
\]
A similar argument gives the second identity when \( \varepsilon_N = 1 \) and this completes the proof of the proposition. \( \square \)
Remark 3. The aim of Conjecture 5 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 5 to compute lattice points in $\Lambda_f^-$ which correspond to the trivial point on $E(H)$.

4. Algorithm and examples

Given a Hilbert eigenform $f$ with integer Fourier coefficients, we need to find an elliptic curve $E$ which 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 $\Delta_E$ have the same set of prime divisors. Indeed, by incrementing the exponents of the prime divisors of $\text{cond}(E)$ in a convenient way, we will eventually reach the discriminant $\Delta_E$ and the algorithm will terminate.

Algorithm

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

Step 2. Knowing the signs of $v_1(\Delta_E)$ and $v_2(\Delta_E)$, compute the types of the period lattices $\Lambda_E$ and $\Lambda_{\bar{E}}$ and the pair $(\tau, \tau') \in \mathcal{H}$ 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, 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 $c_4^2 - \bar{c}_4^2 = 1728\Delta_E$ 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 Frobenius $a_p(E)$ agree with the Fourier coefficients of $f$ up to a convenient bound.

Remark 4. In Step (1), we sometimes use a trick of Cremona [2, Chap. II, sec. 11]. Namely, if $\chi_1$ and $\chi_2$ are two quadratic characters such that

$$\Omega^s, s'_{f, \chi_i} = c_i \Omega^s_E \Omega^s_{\bar{E}}, c_i \in \mathbb{Z},$$

then we can determine the ratio $c_2/c_1$ provided we compute it to enough precision. By trying several characters we can determine the primes that divides, say $c_1$, and then proceed as in [2]. 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 reconstruction from [7].

Example 1. Let $n = (5 + 2\omega)$ be one of the primes above 31 in $\mathbb{Q}(\sqrt{5})$, where $\omega = \frac{1 + \sqrt{5}}{2}$. In [7], we found that there is a normalized eigenform with rational Fourier coefficients of weight 2 and level $n$. We want to find an elliptic curve $E_f/F$ of conductor $n$. Let $c_1 = (3)$ be the unique prime above 3 and $\chi_1 : (\mathcal{O}_F/c_1)^\times \to \mathbb{C}^\times$ the
unique quadratic character such that \( \chi_1(\omega) = \chi_1(\bar{\omega}) = -1 \). Next, we let \( \epsilon_2 = (4-\omega) \) be one of the primes above 11 and \( \chi_2 : (\mathcal{O}_F/\epsilon_2)^\times \to \mathbb{C}^\times \) the quadratic character given by \( \chi_2(\bar{\omega}) = -1 = \chi_2(-1) \). Finally, let \( \epsilon_3 = (4) \) and \( \chi_3 : (\mathcal{O}_F/\epsilon_3)^\times \to \mathbb{C}^\times \) be the unique quadratic character such that \( \chi_3(\omega) = -1 \) and \( \chi_3(\bar{\omega}) = 1 \). By Conjecture 3, \( \Omega_{\omega, \chi_1}^- \), \( \Omega_{\omega, \chi_2}^+ \) and \( \Omega_{\omega, \chi_3}^- \) are integral multiples of \( \Omega_f^- \) (resp. \( \Omega_f^+ \) and \( \Omega_f^- \)). Using all the ideals \( \mathfrak{a} \) of norm up to 300, we get

\[
\Omega_{f, \chi_1}^- \approx 7.542829672311880211310427460
\]
\[
\Omega_{f, \chi_2}^+ \approx 20.24163256057813404243094417i
\]
\[
\Omega_{f, \chi_3}^- \approx 19.19485671379861563730661553i
\]

Letting
\[
\Omega_f^- = \Omega_{f, \chi_1}^-
\]
\[
\Omega_f^+ = \Omega_{f, \chi_2}^+
\]
\[
\Omega_f^+ \approx \Omega_{f, \chi_3}^- \approx 9.5974283568993078186533077658i,
\]
the Riemann-Hodge relations give
\[
\Omega_f^{++} \approx 25.75527047096714165922221002737.
\]

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
\[
\tau = 1.272390969151725829207221612644712687i,
\]
\[
\tau' = 0.500000000000000000000000000000 + 1.34177977231017506430258050599013i,
\]
we get the \( j \)-invariants
\[
j(\tau) \approx 3777.98500237062147734170399476212499969124
\]
\[
j(\tau') \approx -3883.4071179860670278426457091150886121120.
\]

From this, we obtain
\[
c_4 + \bar{c}_4 \approx 33.0062454618927078773801146693
\]
\[
c_4 - \bar{c}_4 \approx 8.00078626724441377191059137715.
\]

which indicates that \( c_4 = 25 + 8\omega \). 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
\[
j(E) = -54753 + 106208\omega.
\]

**Example 2.** Let \( n = (7) \) be the unique prime above 7 in \( \mathbb{Q}(\sqrt{5}) \). There is a unique normalized eigenform of weight 2 and level \( n \) 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
\[\Omega_{f, x_1}^{-} \approx 15.40250229889006031866355163263049,\]
\[\Omega_{f, x_2}^{-} \approx 20.640424670485092443756057304405i,\]
\[\Omega_{f, x_3}^{-} \approx 20.597768949371583380829878547368i.\]

Although we do not have enough precision, the values of \(\Omega_{f, x_2}^{-}+\) and \(\Omega_{f, x_3}^{-}+\) suggest that \(E\) and \(\bar{E}\) are isomorphic. Letting \(\Delta_E = -7\omega^6\) and
\[\Omega_f^{-} = \Omega_{f, x_1}^{-}, \quad \Omega_f^{+} = \Omega_{f, x_2}^{+}, \quad \text{and} \quad \Omega_f^{\pm} = \Omega_{f, x_3}^{\pm},\]
the Riemann-Hodge relations give
\[\Omega_f^{++} = -\frac{\Omega_f^{+} \Omega_f^{\pm}}{\Omega_f^{-}} \approx 26.13083300942127369020605631317278664.\]

Then letting
\[\tau = 0.50000000000000000000000000000000 + 0.651185648463821521543025019i\]
\[\tau' = 0.50000000000000000000000000000000 + 0.65132411856525621319280888i,\]
we get the approximate \(j\)-invariants
\[j(\tau) \approx 586.27333323579091250594341988173849743756738141,\]
\[j(\tau') \approx 585.16245084722668792737834819131243143882485,\]
and the approximates
\[\frac{c_4 + \bar{c}_4}{2} \approx -24.00220036102817748005777424316605240000,\]
\[\frac{c_4 - \bar{c}_4}{2\sqrt{5}} \approx 7.9992250613001254610458610579035703176250.\]

Then we determine that \(c_4 = -32 + 16\omega\) and \(c_6 = -280 + 160\omega\). The Kraus-Laska algorithm gives the minimal model \(E : y^2 + \omega xy + (1 + \omega)y = x^3 + (1 - \omega) x^2 - (1 + 2\omega) x - (1 + \omega)\).

**Example 3.** Let \(F = \mathbb{Q}(\sqrt{2}), \omega = \sqrt{2}, \varepsilon = 1 + \omega\) and \(n = (5 + 2\omega)\). 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. By using a similar argument as in Example 1, 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.** 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 [4] in order to determine \(E\) from \(j(E)\) and the prime divisors of \(\text{cond}(E)\). However, this approach requires a considerable amount of Fourier coefficients, and becomes quickly impractical even in the case when \(j(E)\) is an algebraic integer. For instance, in the simplest case of Example 1, this means using all the primes of norm up to 10000 in contrast to the 300 we did.
5. 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 reconstruction, they clearly demonstrate that the algorithm works in principle. Each of them is interesting in its own way as it explains how one can make the algorithm more efficient with some little variations depending on the situation in hand. To our knowledge, this is the first algorithm of its kind which 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 a 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 4. 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 [12]. 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 $c_1 = (3 + \omega)$ be one of the primes above 5 and $c_2 = (12 + 5\omega)$ be the unique prime above 29, and let $\chi_1$ (resp. $\chi_2$) be the unique quadratic character of conductor $c_1$ (resp. $c_2$) given by $\chi_1(\omega) = -1 = \chi_1(\bar{\omega})$, (resp. $\chi_2(\varepsilon) = -1 = \chi_2(\bar{\varepsilon})$). Then, by Conjecture 3, $\Omega_{+}^{++} f, \chi_1$ (resp. $\Omega_{-}^{--} f, \chi_2$) is an integer multiple of $\Omega_{E}^{+} \Omega_{E}^{+}$ (resp. $\Omega_{E}^{-} \Omega_{E}^{-}$). By using all ideals of norm up to 3000, we get

$$\Omega_{f, \chi_1}^{+} \approx 18.4047729449690593230209569437087470405583250$$

$$\Omega_{f, \chi_2}^{-} \approx 145.787495305353522804613478721693008625189704.$$ 

To compute the periods $\Omega_{f}^{+}$ and $\Omega_{f}^{-}$, we will use Conjecture 5. Let us consider the quadratic extension $K = F(\beta) = F(\sqrt{-1 + \omega})$. This is an extension that has been investigated in [5]. It has narrow class number one and a relative discriminant of norm $-7$. The group of units is generated by

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

Since the norm of $\varepsilon_K$ is not a square, we replace it by its square

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

In [5], it is shown that the embedding $\Psi : K \to M_2(F)$ that sends $\beta$ to the matrix

$$\begin{pmatrix} \omega & -4 \\ 2 & -\omega \end{pmatrix}$$

is an optimal embedding. The associated fixed point is

$$\tau \approx -1.09629120178362600781267762288 + 0.89338994895387814851284586494600i,$$

and we have

$$\gamma_\tau = \Psi(\varepsilon_K^2) = \begin{pmatrix} -1 & -2\omega - 2 \\ 1 + \omega & 5 + \omega \end{pmatrix}.$$
From this, we get the period
\[ J^-_\tau = \int_{\frac{1}{2} - \frac{1}{2} \tau}^{\frac{1}{2} + \frac{1}{2} \tau} \omega_f^- \approx 3.86090468002885037492721376436805387289324. \]

By Conjecture 5, \( J^-_\tau \) is a rational multiple of \( \Omega_E^- \Omega_E^+ \) 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
\[ \Omega_{f}^{++} = \Omega_{f, \chi_1}, \]
\[ \Omega_{f}^{--} = \Omega_{f, \chi_2} = \frac{11.58271404008655112478164129310416161867972524}{4}, \]
\[ \Omega_{f}^{-+} = 3J^-_\tau \approx 36.44687382633383807011533696804232521562974264, \]
the Riemann-Hodge relations give
\[ \Omega_{f}^{+} = \frac{1}{2} \Omega_{f}^{++} \Omega_{f}^{--} \Omega_{f}^{-+} \approx 57.913580099280209373800625897961006111331934244. \]

Letting
\[ \tau = 0.50000000000000000000000000000 + 0.314666040019056129827812167971421i, \]
\[ \tau' = 0.50000000000000000000000000000 + 1.57333046901594278787905615202387094i, \]
we get
\[ j(\tau) \approx 18.927148537157605478892686505143975711 + 5.7531634291693758484628202729673781084784990E - 149i, \]
\[ j(\tau') \approx -18909.9603232803393296978762603585016912E - 147i. \]

The approximates values
\[ \frac{j(\tau) + j(\tau')}{2} \approx -9445.516587315908621094178692667885, \]
\[ \frac{j(\tau) - j(\tau')}{2\sqrt{29}} \approx 1757.503080197255180934334374672918876, \]
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 \( \Delta_E \) is a unit. In fact, without loss of generality, we can assume that \( \Delta_E \in \mathcal{O}_F/(\mathcal{O}_F)^{12} \). 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 5.** Let \( F = \mathbb{Q}(\sqrt{37}) \), \( \omega = \frac{1 + \sqrt{37}}{2} \), 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
\[ \Omega_{f, \chi_1} \approx 40.896716499857408255292321685652645468633671446271. \]
From [5], we know that
\[
\int_0^\infty \int_{i\varepsilon}^{i\omega} \omega_f^2 = -2\ell_F^2 \Omega_f^{++} \\
\approx -5.4356127176615640089898722977525336010607204858210,
\]
where \( \ell_F = \frac{2}{\omega} \). To compute the period \( \Omega_f^{++} \), we use the quadratic extension \( K = F(\sqrt{\omega - 3}) \) in [5, Table 37.1]. This gives
\[
J_f \approx 5.27137134740499202551815570143616819076263476783850i.
\]
For the choices \( \Omega_f^{--} \approx \Omega_f^{--} \approx 10.22418835274925401000235971951991015757063 \),
\[
\Omega_f^{++} = \frac{5J_f}{2} \approx 13.17842836851248006379538925358782149017354i,
\]
the Riemann-Hodge relations give
\[
\Omega_f^{-+} \approx 13.17843227486942072481519660286609413879209178530i.
\]
The values of \( \Omega_f^{-+} \) and \( \Omega_f^{--} \) suggest that the curve \( E \) and its Galois conjugate have the same \( j \)-invariant, and so \( j(E) \in \mathbb{Z} \). Letting
\[
\tau = \frac{\Omega_f^{++}}{\Omega_f^{-+}} \approx 0.7758273624280973879843957726944777299414217i,
\]
we obtain
\[
j(\tau) \approx 4096.005494314602868984159585714736549576335866118539269.
\]
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.** 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 [11]. 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 [13] who also established Conjecture 1 in this case by using a result of Faltings and Serre. We want to explain how the computations in their paper could have been used in order to produce the curve \( E \). Using all the ideals of norm up to 50000, we compute
\[
\int_0^\infty \int_{i\varepsilon}^{i\omega} \omega_f^2 = -2\ell_F^2 \Omega_f^{++} \\
\approx -26.68782971866189788570328490568815717581329705382730,
\]
where \( \ell_F = 1 \). For the computations of the periods \( \Omega_f^{--} \) and \( \Omega_f^{++} \), 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 realtive 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 \( \beta \) to \( \begin{pmatrix} -13\omega - 137 & 166\omega + 1806 \\ -\omega - 11 & 13\omega + 139 \end{pmatrix} \). We replace \( \varepsilon_K \) by its square which gets sent to
\[
\gamma_\tau := \Psi(\varepsilon_K^2) = \begin{pmatrix} -67\omega - 716 & 332\omega + 3612 \\ -2\omega - 22 & -15\omega - 164 \end{pmatrix}.
\]
The class number and narrow class number are equal, \( h = h^+ = 10 \), so by Conjecture 5, the periods \( J^+_\tau \) up to rational multiples belong to \( \Lambda_f^- \). 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 \( \bar{f}_E \) that correspond to \( E \) and \( \bar{E} \) respectively, we get
\[
J^+_{E, \tau} \approx 61.70079138445727061529703480328731375115768i,
\]
\[
J^+_{\bar{E}, \tau} \approx 36.984361723493116902742772317960223959728i.
\]
Letting
\[
\Omega_f^+ = \frac{J^+_{E, \tau}}{10} \quad \text{and} \quad \Omega_f^{+-} = J^+_{E, \tau},
\]
we see that the curve \( E \) is given by one of the pairs \((\tau, \tau') \in \mathfrak{H}^2\), where
\[
\tau \approx 0.46238897680999509129648i \quad \text{or} \quad 0.50000000000000000000 + 0.23119448840499754564824082213i,
\]
\[
\tau' \approx 2.77162752560813905168849256982296i \quad \text{or} \quad 0.50000000000000000000 + 1.38581376280406952584424628i.
\]
For
\[
\tau = 0.46238897680999509129648i,
\]
\[
\tau' = 0.50000000000000000000 + 1.38581376280406952584424628i,
\]
we get the \( j \)-invariants
\[
j(\tau) \approx 797678.4966527060934982194441977726380067402453
\]
\[
j(\tau') \approx -5335.0178318045639741757323141642225253413742.
\]
By letting \( \Delta_E = \varepsilon \), we get
\[
\frac{c_4 + c_4}{2} \approx 452.711050645653766920618752468514
\]
\[
\frac{c_4 - c_4}{2\sqrt{509}} \approx 19.98657578270916698381220138644297.
\]
We then try all the closest integers or half-integers to these two values which give an algebraic integer. For \( c_4 = 433 + 40\omega \), we get \( c_6 = -12977 \) \(-1204\omega \). We recover the minimal model \( E \): \( y^2 + xy + y = x^3 - (1 + \omega)x^2 + 33x + 37 \) by using Kraus-Laska’s algorithm.

**Remark 6.** The recent algorithm developed by Cremona and Lingham [4] can be used in order 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.
References


Department of Mathematics and Statistics, University of Calgary, 2500 University Drive N.W., Calgary, AB, Canada T2N 1N4, e-mail: dembele@math.ucalgary.ca