Numerical Verification of a "Birch and Swinnerton-Dyer Type" Conjecture

François Séguin

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of Masters of Science

Under the supervision of
Prof. Henri Darmon

Department of Mathematics and Statistics
McGill University
Montréal

October 21 2014

Abstract

In [Dar92], Darmon gave a description of a "Birch and Swinnerton-Dyer" type conjecture attached to a modular elliptic curve E defined over the rational numbers and to a quadratic field. A theta object is constructed using Heegner points and cycles for those curves, and can be shown to interpolate special values of L-functions through formulas of Gross-Zagier and Waldspurger. The conjecture relates the "leading coefficient" of this theta object to the arithmetic data of the curve, in particular through a regulator given by a height pairing described by Mazur and Tate in [MT87]. In [Dar92], the leading coefficient for this theta element was calculated numerically for several cases, in particular for the modular curve of conductor 37 and many real quadratic number fields. Our goal is to compute the regulator in those cases in order to verify the conjecture. Along the way, we outline a procedure to calculate the Mazur-Tate height pairing in practice.

Résumé

Dans l'article [Dar92], Darmon donne une description d'une conjecture de "type Birch et Swinnerton-Dyer" reliée à une courbe elliptique E définie sur les nombres rationnels, et à un corps quadratique. Un objet thêta est ensuite construit via les points et cycles de Heegner sur ces courbes et peut interpoler les valeurs critiques des fonctions L associées grâce aux formules de Gross-Zagier et Waldspurger. La conjecture lie le "coefficient principal" de cet objet thêta avec les données arithmétiques des courbes à travers un régulateur défini par un accouplement de hauteur décrit par Mazur et Tate dans [MT87]. Dans [Dar92], le coefficient principal de cet élément theta a été calculé numériquement pour plusieurs cas, en particulier pour la courbe modulaire de conducteur 37 et plusieurs corps de nombres quadratiques réels. L'objectif de ce mémoire est de calculer le régulateur pour ces cas particuliers afin de vérifier la conjecture. Ce faisant, nous présenterons une procédure pour calculer l'accouplement de hauteur de Mazur-Tate concrètement.

Ackowledgements

I would like to thank my supervisor, prof. Henri Darmon, for his help and guidance with this thesis. I would like to thank the National Science and Engineering Research Council of Canada (NSERC), as well as the Fond de recherche du Québec - Nature et technologie (FQRNT) for their financial assistance that was key to completing this program. I would also like to thank the department of Mathematics and Statistics of McGill for their financial contribution. Finally, I would like to thank my family and my significant other for their unflagging support through rough times.

Contents

Introduction

In the article [Dar92], section 3.5 contains computational evidence for the conjecture on the order of vanishing of an analytic object constructed using Heegner cycles (Conjecture 3.2, see 1.2 in this thesis). Indeed, as the conjecture in question for positive discriminant is much harder to prove, we can only provide numerical verifications for the moment. As such, the leading coefficient for this theta was calculated by Darmon for several values of discriminant chosen to have the narrow class group $h^+(D)$ as large as possible. The conjecture concerning the order of vanishing of this theta was verified for these cases, and moreover was shown to be sharp.

A second conjecture of the “Birch and Swinnerton-Dyer type” was also stated in the article (conjecture 3.6, 1.3 in this thesis) relating this leading coefficient of theta to arithmetic values of curves. Darmon stated that it would be interesting to verify this second conjecture for the same cases, as the analytic part of the conjecture was already computed. The goal of this thesis is therefore to complete the article [Dar92] by giving numerical evidence of conjecture 3.6 (1.3 here).

This arithmetic data is given through a regulator R_D that is taken to be

$$R_D = \begin{vmatrix} \langle g_0, q_0 \rangle & \langle g_0, q_1 \rangle \\ \langle g_1, q_0 \rangle & \langle g_1, q_1 \rangle \end{vmatrix}$$

where the entries are the Mazur-Tate pairing between generators of the Mordell-Weil group and generators of a specific subgroup. As such, it was also interesting to describe the concrete procedure for computing the Mazur-Tate pairing in the specific case where the varieties are elliptic curves, with a non-empty set S of places (that we take here to be a single prime).

We restrict our attention here to the modular elliptic curve of conductor 37, given by the equation

$$y^2 - y = x^3 - x$$

over different real quadratic number fields of the same discriminants than those listed in Table 2 from [Dar92] (see Table 1 here). Because of computational complications, we only considered a subset of those discriminants that were originally considered in the original article.

1 Motivation

1.1 Heegner objects

We begin by recalling the context given by [Dar92] on the BSD type conjecture.

Elliptic curve

We keep all of the original notation. To be precise, let E be an elliptic curve defined over $\mathbb{Q}$ given by the Weierstrass equation

$$y^2 = 4x^3 - g_2 x - g_3.$$

For p prime, let $E_{ns}(\mathbb{F}_p)$ be the group of non singular points on E and N_p its order. Also let N denote the arithmetic conductor of E. For simplicity, assume N is odd. Define $a_p = p + \delta_p - N_p$ where δ_p is 1 if E has bad reduction at p and 0 otherwise. We then extend the definition to a_n for any composite n through the formal identity

$$\sum_{n \geq 0} a_n n^{-s} = \prod_p \left(1 - a_p p^{-s} + \delta_p p^{1-2s}\right)^{-1}.$$

Finally, we define the Fourier series

$$f_E(\tau) = \sum_{n=1}^{\infty} a_n \mathrm{e}^{2\pi i n \tau}$$

converging absolutely for $\mathrm{im}(\tau) > 0$, and so the differential

$$\omega_E = 2\pi i f_E(\tau)\, d\tau$$

is holomorphic on the upper half plane.

Binary quadratic forms

Let $D = D_0 f^2$ where D_0 is a fundamental discriminant and f a square-free integer prime to D_0. Let $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D_0})$ with $\mathcal{O}_K$ its ring of integers. The pair (E, D) is said to be *Heegner* if for all prime p dividing N, the Kronecker symbol $\left(\frac{D}{p}\right) = 1$.

Assume (E, D) is Heegner. Then, there exists $B_0 \in \mathbb{Z}$ such that $B_0^2 \equiv D_0 \pmod{4N}$. Fix such a B_0. A binary quadratic form $F = Ax^2 + Bxy + Cy^2$ of discriminant D is said to be *Heegner* if $N|A$ and $B \equiv B_0 f \pmod{2N}$. Let $\mathcal{F}$ denote the set of primitive binary quadratic forms of discriminant D, and $\mathcal{F}_N$ the subset of those which are Heegner.

The group $SL_2(\mathbb{Z})$ acts on $\mathcal{F}$ by change of variable. Also, we can notice that $\mathcal{F}_N$ is preserved under the action of the subgroup $\Gamma_0(N)$, the group of matrices of $SL_2(\mathbb{Z})$ whose lower left entry is divisible by N. Then, we can show that

$$G_D = \mathcal{F}_N / \Gamma_0(N) \cong \mathcal{F}/SL_2(\mathbb{Z})$$

with the Gaussian composition as the group law. Let $h^+(D)$ be the order of G_D.

The case $D > 0$

The following has a similar construction in the case $D < 0$, but we will restrict our attention here to cases where $D > 0$.

If F is a binary quadratic form of discriminant $D > 0$, it is preserved by an infinite abelian subgroup of $SL_2(\mathbb{Z})$ of rank 1. A generator M_F for this subgroup is called an *automorph* of F. Then, to this form we associate a point α_F on E in the following way.

$$\alpha_F = \int_z^{M_F z} \omega_E$$

which is independent of z, and is in Λ, the lattice associated to the elliptic curve E and the differential ω_E. Under the identification of Λ and $H_1(E(\mathbb{C}), \mathbb{Z})$, we denote $M_D = H_1(E(\mathbb{C}), \mathbb{Z})$ so that $\alpha_F \in M_D$. Then, define a $\mathbb{C}$-valued pairing in M_D

$$\langle \alpha_1, \alpha_2 \rangle_D = \int_{\alpha_1} \omega_E \int_{\alpha_2} \overline{\omega}_E.$$

Finally, given a complex character $\chi : G_D \longrightarrow \mathbb{C}^*$, we define

$$\alpha_\chi = \frac{1}{h^+(D)} \sum_{F \in G_D} \chi(F) \alpha_F \in M_D \otimes \mathbb{C}$$

and extend the pairing $\langle \cdot, \cdot \rangle_D$ to $M_D \otimes \mathbb{C}$ by the Hermitian property of the pairing. We have the following result of Waldspurger that really is the motivation behind this construction about the interpolation of special values of L-functions.

Theorem 1.1 (Waldpurger). *For $D = D_0$ a fundamental discriminant,*

$$\langle \alpha_\chi, \alpha_{\bar{\chi}} \rangle_D \doteq \sqrt{D} h^{-1} L(E/K, \chi, 1)$$

where $h = h^+(D)$ and $\doteq$ denote an equality up to an explicit factor of a power of 2.

1.2 θ_D and conjectures

Instead of working with α_χ, we can construct the following. Consider

$$\theta_D = \sum_{F \in G_D} \alpha_F \cdot F, \qquad \theta_D^* = \sum_{F \in G_D} \alpha_F \cdot F^{-1}$$

as formal elements in $M_D \otimes \mathbb{Z}[G_D]$. Then, let

$$L_D = \theta_D \cdot \theta_D^* \in M_D^{\otimes 2} \otimes \mathbb{Z}[G_D]$$

as a formal product. The pairing $\langle \cdot, \cdot \rangle_D$ can be viewed as a linear map from $M_D^{\otimes 2}$ to $\mathbb{C}$, and so we can extend it by linearity to a map $M_D^{\otimes 2} \otimes \mathbb{Z}[G_D]$ to $\mathbb{C}[G_D]$. Let $L_D^{\mathbb{C}}$ denote the image of L_D under this extended pairing. Then, we notice that $\chi(L_D^{\mathbb{C}}) = \langle \alpha_\chi, \alpha_{\bar{\chi}} \rangle_D$. Therefore, we can interpolate the special values of L-functions through the study of this element L_D. Darmon posed the following conjecture on L_D. Let I denote the augmentation ideal of the group ring $\mathbb{Z}[G_D]$ and r denote the rank of E.

Conjecture 1.1. *L_D belongs to the subgroup $M_D^{\otimes 2} \otimes I^r$ of $M_D^{\otimes 2} \otimes \mathbb{Z}[G_D]$.*

Furthermore, it might be interesting to consider the "square root" of this element, θ_D. As a matter of fact, Darmon established the following stronger conjecture concerning θ_D. Let r^+ (respectively r^-) be the rank of the plus (respectively minus) eigenspace of $E(K)$ under the involution in $\mathrm{Gal}(K/\mathbb{Q})$, and let $\rho = \max(r^+, r^-)$.

Conjecture 1.2. *θ_D belongs to the subgroup $M_D \otimes I^\rho$ of $M_D \otimes \mathbb{Z}[G_D]$.*

1.3 The leading coefficient

Assuming conjectures 1.1 and 1.2, we define the leading coefficient of θ_D, denoted $\tilde{\theta_D}$ as the projection of θ_D in $M_D \otimes (I^{\rho-1}/I^\rho)$. The main conjecture we are trying to verify is one about the interpretation of this leading coefficient in terms of arithmetic data of E. At the moment, this conjecture is formulated for the specific case where $r^+ = r^-$. Also, for simplicity reasons, we will assume that f is an odd prime, $r > 0$ and $E(K)$ is torsion free.

We use a pairing on abelian varieties given by Mazur and Tate in [MT87], which they call the S-pairing, that we will describe in greater details in the following sections. This pairing $\langle \cdot, \cdot \rangle$ is defined on $E(K) \times E_f(K)$ where $E_f(K)$ is a subgroup of $E(K)$ of finite index, and takes values in G_D, the ideal class group. Specifically, $E_f(K)$ is defined by the exact sequence

$$0 \longrightarrow E_f(K) \longrightarrow E(K) \longrightarrow E/E^0(K) \oplus E(k_f).$$

This definition is going to be explained in greater details in section 2.1. Then, if $\{P_1, \ldots, P_r\}$ and $\{Q_1, \ldots, Q_r\}$ denote integral bases for $E(K)$ and $E_f(K)$ respectively, define R_D to be the determinant of the matrix having $\langle P_i, Q_j \rangle$ as its ij-th coordinate. Under the natural identification between G_D and I^2/I (see [Sch75]), we obtain that R_D is an element of I^r/I^{r+1}. This R_D plays the role of the regulator in the following BSD type conjecture. We also define J_D to be the order of the cokernel of the right-hand map in the above exact sequence.

Conjecture 1.3.

$$\tilde{L}_D = \#\text{Ш}(E/K) \cdot R_D \cdot J_D \cdot \omega^+ \otimes \omega^+$$

where $\tilde{L}_D = (-1)^\rho \, \tilde{\theta}_D^2$, $\text{Ш}(E/K)$ is the Shafaravich Tate group for E/K, R_D and J_D is as above, and $\omega^+ \in \Lambda$ is the real period attached to E.

1.4 Statement of objectives

The main goal of this thesis is to verify conjecture 1.3 for a few very specific cases. In particular, let E be the elliptic curve given by

$$y^2 - y = x^3 - x.$$

We will restrict our attention exclusively to this elliptic curve. The conductor of E is 37, and E has rank 1 over $\mathbb{Q}$. Over the quadratic number fields K of discriminant below, we will see that E has rank 2 over K. We will verify that this is the case using 2-descent algorithms. Also, E is actually modular as it is the quotient of $X_0(37)$ by the Atkin-Lehner involution ω_{37}. Conjecture 1.2 predicts that $\theta_D \in M_D \otimes I$. In [Dar92], the leading coefficient of θ_D was

$D = D_0 f^2$	$h^+(D)$	Generators of G_D $(\sigma_1; \sigma_2)$	Leading term
$12 \cdot 607^2$	$38 \cdot 2$	$(-1034, 2066, 37)$; $(3, 2100, -949)$	$8(\sigma_1 - 1)$
$12 \cdot 2131^2$	$164 \cdot 2$	$(-3351, 6042, 1342)$; $(2, 7382, -1)$	$128(\sigma_1 - 1)$
$12 \cdot 3691^2$	$284 \cdot 2$	$(3489, 8136, -6971)$; $(3, 12780, -12781)$	$12(\sigma_1 - 1)$
$33 \cdot 151^2$	$38 \cdot 2$	$(-2, 867, 93)$; $(62, 867, -3)$	$26(\sigma_1 - 1)$
$44 \cdot 199^2$	$50 \cdot 2$	$(-10, 1318, 133)$; $(11, 1320, -1)$	$18(\sigma_1 - 1)$
$44 \cdot 379^2$	$76 \cdot 2$	$(-659, 1460, 1589)$; $(11, 2508, -685)$	$68(\sigma_1 - 1)$

Table 1: Extract of "Table 2" from [Dar92]

calculated for several values D to verify that it is not trivial in $M_D \otimes (I/I^2)$, i.e. that the conjecture is actually sharp on the order of vanishing of θ_D. Those leading terms were compiled in Table 2 of [Dar92], which is reproduced in Table 1.

Therefore, in order to verify Conjecture 1.3 for these cases, we need to compute the right hand side of the equation. Specifically, for every discriminant D listed, we need to find the value of :

- The regulator R_D,
- the order of the cokernel J_D, and
- the Tate-Shafarevich group $\#Ш(E/K)$.

The main goal of this thesis is to find the first of these three quantities, and it involves computing many Mazur-Tate pairings for the discriminants in Table 1. Fortunately, we can use explicit formulas for this S-pairing in the case of elliptic curves given in [MT87] in order to compute the latter. The pairing itself as well as detailed computations are described in detail in section 2.

2 The S-pairing

2.1 Formulas for elliptic curves

In order to compute the regulator R_D, we need to compute the S-pairing as described in [MT87] for several points on $E(K)$. We will now describe how such computations can be achieved.

Let A be an abelian variety over a field K, and let B denotes its dual. Let S be a finite set of nonarchimedean places of K, and S_m be the subset of S of the places at which A has split-multiplicative reduction. Then, in [MT87], Mazur and Tate define a pairing they call the (canonical) S-pairing as

$$\langle \cdot, \cdot \rangle_S : A_S \times B_S \to C_S$$

where the groups A_S and B_S are defined from the respective exact sequences

$$0 \longrightarrow \prod_{v \in S_m} Y_v \longrightarrow A_S \longrightarrow A(K) \longrightarrow 0 \tag{2.1}$$

$$0 \longrightarrow \prod_{v \in S_m} X_v \longrightarrow B_S \longrightarrow B(K) \longrightarrow \prod_{v \in S - S_m} B(k_v) \times \prod_{v \notin S} (B/B^0)(k_v). \tag{2.2}$$

Here, X_v (resp. Y_v) is the character group of the split torus $A^0_{/K}$ (resp. $B^0_{/K}$) at the place v, and k_v the residue field of K at v. A_S and B_S are called the *extended Mordell-Weil groups* and, in applications, they will usually be extensions of subgroups of finite index of the Mordell-Weil groups by free abelian groups of finite rank. From this point forward, we will assume that S_m is empty, which is the case for every computations we want to carry. This assumption simplifies the procedure. In particular, the extended Mordell-Weil groups will simply be the Mordell-Weil group or subgroup of finite index. Note that even though this implies that $S = S - S_m$, we will keep the latter notation for an easier comparison with the general case explained in [MT87].

The target group C_S of the pairing is defined as a quotient of the idèle class group, specifically

$$C_S = I \Big/ \left(K^* \prod_v U_v \right)$$

where

$$U_v = \begin{cases} K_v^* & \text{if } v \text{ is archimedean,} \\ \mathcal{O}_v^* & \text{if } v \text{ is non-archimedean, } v \notin S, \\ 1 + \mathfrak{m}_v & \text{if } v \in S - S_m. \end{cases}$$

We immediately notice that contrary to what was previously stated, this pairing does not immediately have for target the group of binary quadratic forms G_D. However, there is a way to make it so canonically. Indeed, given an idèle representing the class for a certain pairing, we can take the product of every coordinates as ideals to find an ideal, and then project the result in the narrow class group. Using the canonical isomorphism with the group of binary quadratic forms, we obtain what we want. Note however that such a technique works in the case where the discriminant $D = D_0$ is fundamental. If $D = D_0 f^2$, then the analysis is more complicated, and will be explored in details in a following section.

The pairing is defined for arbitrary abelian varieties, but [MT87] gives explicit description and formulas for the case where A is an elliptic curve. Since this is exactly the case in which we are interested, we use these formulas.

We give now an explicit formulation for computing $\langle P, Q \rangle_S$. Even though the pairing is defined on the extended Mordell-Weil group, we will be in the case here where those are subgroups of the Mordell-Weil group. Therefore, we can forget the extra structure of A_S and B_S and view P and Q as points on the elliptic curve $E(K)$.

We begin by making two assumptions. First, we assume that neither P or Q is zero. The case where one point is zero is explained in [MT87], but we won't need it for our specific cases. Next, we assume that there is a point P' on $E(K)$ such that none of the four points $P', P + P', Q + P', P + Q + P'$ is congruent to $0 \mod v$ for any $v \in S - S_m$. The assumption is usually satisfied in practice, and is not a problem for our purposes. Choose one such P'.

Then, the idèle $c = (c_v)$ represents the idèle class $\langle P, Q \rangle_S$ and is given by:

$$c_v = \text{arbitrary in } K_v^*, \text{ for } v \text{ archimedean} \tag{2.3}$$

$$c_v = \frac{t_v(P + P')t_v(Q + P')}{t_v(P')t_v(P + Q + P')} \bmod \mathcal{O}_v^*, \text{ for } v \text{ discrete, } v \notin S \tag{2.4}$$

where $t_v(P)$ denotes an element of K_v^* such that $t_v(P)^2$ is the denominator for the x-coordinate of P in a local minimal Weierstrass equation for A at v; and

$$c_v = 1 \bmod^{\times}(1+\mathfrak{m}_v), \text{ for } v \in S - S_m. \tag{2.5}$$

2.2 The case S empty

For the sake of understanding better how to carry out computations, we will assume for now that S is empty. In this case, it is easy to see from sequences 2.1 and 2.2 that the pairing is simply defined on the Mordell-Weil group, i.e. on $E(K) \times E(K)$. Let P, Q be non-zero points on $E(K)$. We wish to find $\langle P, Q\rangle$. First, notice that we can take P' to be zero, as S is empty.

We first calculate $P+Q$. Then, assuming we are given a Weierstrass form for $E(K)$, we calculate Δ, c_4 and c_6, and their prime factorization in K (as ideals). If there exists a prime $\mathfrak{p}$ in K such that $\nu_{\mathfrak{p}}(\Delta) \geq 12$, $\nu_{\mathfrak{p}}(c_4) \geq 4$ and $\nu_{\mathfrak{p}}(c_6) \geq 6$, then the given Weierstrass equation for $E(K_{\mathfrak{p}})$ might not be minimal. Since it is important to know a minimal equation for all the primes of K, the next step would be to find those missing minimal equations.

The next order of business is to find $t_{\mathfrak{p}}(P)$, $t_{\mathfrak{p}}(Q)$ and $t_{\mathfrak{p}}(P+Q)$ at all primes $\mathfrak{p}$ of K.

Fix one such prime $\mathfrak{p}$. Now suppose that for this prime the given equation of $E(K_{\mathfrak{p}})$ is minimal.

Fact 2.1. *Let P be a point on $E(K)$, then $x(P) = \frac{A}{C^2}$ and $y(P) = \frac{B}{C^3}$ for some A, B, C integral ideals of $\mathcal{O}_K$ such that both A and B are coprime with C.*

This is shown in [ST92, Section III.2] for rational coordinates, but notice that we can extend the proof to the number field K as the same argument works using ideals.

It should then be clear that when projected in $E(K_{\mathfrak{p}})$, such a point P would have $\mathfrak{p}^{2\nu_{\mathfrak{p}}(C)}$, as viewed in $K_{\mathfrak{p}}$, as a denominator of the x-coordinate, since all other factors of C^2 are invertible. It then follows that $t_{\mathfrak{p}}(P) = \mathfrak{p}^{\nu_{\mathfrak{p}}(C)}$.

Now for the case where the equation of $E(K_{\mathfrak{p}})$ is not minimal the analysis is sensibly different. In this case, we need to find a suitable change of variables making the equation minimal. Then, we use this change of variable on the point P, and then project in the local field to find which factors of the denominator remains. This analysis can be done, but was not of importance here since there is a globally minimal equation for the elliptic curve.

Call the primes $\mathfrak{p}$ for which the given equation of $E(K_{\mathfrak{p}})$ is minimal *good* primes, and the others *bad* primes. For these good primes, plugging the above values in equation 2.4, keeping in mind that we chose P' to be zero, we obtain

$$c_{\mathfrak{p}} = \frac{\mathfrak{p}^{\nu_{\mathfrak{p}}(C_P)}\mathfrak{p}^{\nu_{\mathfrak{p}}(C_Q)}}{\mathfrak{p}^{\nu_{\mathfrak{p}}(C_{P+Q})}} \bmod \mathcal{O}_K^*$$

where C_P, C_Q and C_{P+Q} represent C in fact 2.1 for P, Q and $P+Q$ respectively.

Obviously, for the archimedean places, the idèle is arbitrary, and since we supposed that S is empty, we have covered all places. As we are interested in the corresponding element from the class group, we need to consider the product of every ideal composing this idèle $c = (c_{\mathfrak{p}})$. This product becomes

$$\prod_{\mathfrak{p}\text{ good}} \frac{\mathfrak{p}^{\nu_{\mathfrak{p}}(C_P)}\mathfrak{p}^{\nu_{\mathfrak{p}}(C_Q)}}{\mathfrak{p}^{\nu_{\mathfrak{p}}(C_{P+Q})}} \times \prod_{\mathfrak{p}\text{ bad}} \frac{t_{\mathfrak{p}}(P)t_{\mathfrak{p}}(Q)}{t_{\mathfrak{p}}(P+Q)}.$$

Now if we have only good primes, this simplifies to

$$\prod_{\mathfrak{p}} \frac{\mathfrak{p}^{\nu_{\mathfrak{p}}(C_P)}\mathfrak{p}^{\nu_{\mathfrak{p}}(C_Q)}}{\mathfrak{p}^{\nu_{\mathfrak{p}}(C_{P+Q})}} = \frac{(C_P)(C_Q)}{(C_{P+Q})} \tag{2.6}$$

as a fractional ideal of $\mathcal{O}_K$.

At this point, to retrieve an element of G_D, it suffices to express the above ideal in its Hermite normal form, say (α, β), and then taking $\mathbf{N}(\alpha \cdot x + \beta \cdot y)$ gives a representative binary quadratic form in terms of x and y. Note that it might be necessary to apply reduction algorithms to get a reduced representative.

Example 2.1. Let E be the modular elliptic curve of conductor 37 $X_0(37)^+$, given by the equation $E : y^2 - y = x^3 - x$, and let $D = 12$. Then, $K = \mathbb{Q}(\sqrt{3})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$. Also, it is easy to find that $G_{12} \cong \{\pm 1\}$ with $1_{G_{12}} = [1, 2, -2]$ and $-1_{G_{12}} = [2, 2, -1]$. Now let $P = (-1, 1)$ and $Q = (\frac{\sqrt{3}}{2}, \frac{-\sqrt{3}+3}{4})$. Not only are those two points on $E(K)$, but they are the generators for $E(K)$, as $E(K)$ is of rank 2 and torsion free. We compute the point $P + Q = (-\sqrt{3} + 2, 2\sqrt{3} - 3)$.

Now, as it was hinted previously, the above equation for $E(K)$ is globally minimal. Indeed, $\Delta = 37 = (-2\sqrt{3}+7)(2\sqrt{3}+7)$, $c_4 = 48 = (\sqrt{3}+1)^8(\sqrt{3})^2$ and $c_6 = (\sqrt{3}+1)^6(\sqrt{3})^6$.

Notice a pitfall here that we must be very careful with. When trying to express the coordinates of Q as in Fact 2.1, we first notice that the denominator of the x-coordinate is 2. Here, since we work in $\mathbb{Q}(\sqrt{3})$, (2) is indeed a square as $(2) = (\sqrt{3}+1)^2$. However, when looking at the denominator of the y-coordinate, 4, we fail to express it as a cube, even when factoring in K, as $(4) = (\sqrt{3}+1)^4$. We resolve this problem by noticing that as element of $\mathcal{O}_K$, the fraction $\frac{-\sqrt{3}+3}{4}$ is not reduced as $(-\sqrt{3}+3) = (\sqrt{3})(\sqrt{3}+1)$. Therefore, the denominator ideal of the y-coordinate of Q truly is $(\sqrt{3}+1)^3$ and not (4). This is to show the importance of simplifying numerator and denominator *as ideals of* $\mathcal{O}_K$.

We then have for respective elements of equation 2.6, $C_Q = (\sqrt{3}+1)$, and obviously $C_P = C_{P+Q} = (1)$. Therefore, we conclude that the pairing, as a product of its idèle, is simply

$$\langle P, Q\rangle = (1+\sqrt{3}).$$

The $\mathbb{Z}$ basis of this ideal is $[2, 1+\sqrt{3}]$, and thus the associated binary quadratic form is

$$\begin{aligned}\left[\mathbf{N}(2x+(1+\sqrt{3})y)\right] &= \left[(2x+(1+\sqrt{3})y)(2x+(1-\sqrt{3})y)\right]\\ &= \left[4x^2+4xy-2y^2\right]\\ &= \left[2x^2+2xy-y^2\right]\\ &= -1_{G_{12}}.\end{aligned}$$

It was clear that this was going to be the case as we had a principal ideal to begin with. Although this example is a bit trivial, it is a good sanity check on our description of the procedure.

2.3 The case S non-empty

We will now try to describe what happens differently in the case where S is not empty. To be more specific, if we are working with determinant $D = D_0 f^2$, we want to have $S = \{f\}$. The following modifications will have to be respected from the above procedure.

1. The pairing is no longer defined on the whole Mordell-Weil group, but on $E(K) \times E_f(K)$, where $E_f(K)$ is a subgroup of finite index of $E(K)$.

2. The point P' can no longer be taken to be zero, as it (in particular) needs to be non-zero when reduced $\bmod f$. We therefore need to choose an appropriate P'.

3. The coordinate at f of the idèle is no longer determined by formula 2.4, but rather formula 2.5. In particular, if f divides the denominator of the x-coordinate of a point in formula 2.4, this factor is omitted when taking the product eventually, and is replaced by a factor determined by equation 2.5.

4. Finally, we cannot simply obtain with this idèle an element of the narrow class group, as the resulting binary quadratic form would have the same discriminant as K, i.e. D_0. Instead, we need a way to obtain an ideal of the order of conductor f of K, $\mathcal{O}_f$. This is to say that our ideal must be a locally free projective module in all places, including those dividing f. Then, the binary quadratic form obtained by taking $\mathbf{N}(\alpha x + \beta y)$ with $[\alpha, \beta]$ a $\mathbb{Z}$ basis, would indeed have discriminant $D_0 f^2$. We also need to make sure that this procedure is compatible with the canonical morphism $G_{D_0 f^2} \to G_{D_0}$ given by the composition with identity. This concept is detailed in [Bue89, Thm 7.9]

These modifications are explained in greater details in the following sections.

2.4 Finding $E_f(K)$

First of all, we notice that the Mazur Tate pairing is not defined on the full Mordell-Weil group, but on $E(K) \times E_f(K)$, where $E_f(K)$ is a subgroup of $E(K)$ of finite index in $E(K)$, defined through the following exact sequence modified from the sequence 2.2:

$$0 \longrightarrow E_f(K) \longrightarrow E(K) \longrightarrow E/E^0(K) \oplus E(k_f)$$

where k_f is the residue field of K at the prime f. What this concretely means is that $E_f(K)$ is a subgroup of the same rank as $E(K)$, consisting of elements that have nonsingular reduction at every primes of K, as well as being in the kernel of reduction at f. Since 0 is always a nonsingular point, this definition of $E_f(K)$ is well defined.

In our case, since we only consider torsion free curves of rank 2 over K, we know that $E_f(K)$ will also be torsion free of rank 2. Hence, we need to find two generators of this group. If we have $\{P_1, P_2\}$ a basis for $E(K)$, we start by computing the smallest multiple of P_1 and P_2 that are in $E_f(K)$, say $Q_1' = mP_1 \in E_f(K)$ and $Q_2' = nP_2 \in E_f(K)$.

We can simplify the situation by considering $E(K)$ as $\mathbb{Z}\times\mathbb{Z}$ to which it is isomorphic through the multiples of its two generators. Hence, by considering all possible structures for the subgroups of $\mathbb{Z}\times\mathbb{Z}$, we know that $E_f(K)$ will be of the form $\mathbb{Z}(a,b) \oplus \mathbb{Z}(0,c)$ for some $a, c > 0$ and b integers. Hence, without loss of generality, we can pick $(0,m)$ to be a generator of $E_f(K)$. If the second one is (a,b), we know that for some $\alpha, \beta \in \mathbb{Z}$,

$$\alpha(0,m) + \beta(a,b) = (n,0)$$

and so we have from the first coordinate that both a and β divide n, and from the second coordinate that $b = \frac{-\alpha m}{\beta}$. Hence, we know that b is both an integer and can be expressed as a multiple of m divided by a divisor of n. Finally, we also know that $b \leq m$ as we can always translate a generator by $\pm(0,m)$ to find another generator.

Putting all together, the candidates for the second generator of $E_f(K)$ are (a,b), where a ranges over all divisors of n, and b ranges over all multiples of $\frac{m}{\gcd(m,n)}$ up to m, as this cover all possibilities of $\frac{\text{multiple of } m}{\text{divisor of } n}$ being an integer. We then simply need to evaluate $aP_2 + bP_1$ for all such a, b, and figure out which are in $E_f(K)$. From all those in the subgroup, it should be fairly straightforward to determine which is the generator.

Notice also that $\Delta = 37$ for our elliptic curve, and so E has good reduction at all primes except those above (37) in K. Also, $c_4 = 48$ for the curve and thus, at those prime $\mathfrak{p}$, $\nu_{\mathfrak{p}}(c_4) = 0$, so E has multiplicative reduction at $\mathfrak{p}$ and by [Sil09, Thm VII.6.1], $E(K)/E^0(K)$ is cyclic of order $\nu_{\mathfrak{p}}(\Delta)$, i.e. 1 or 2 depending on whether 37 splits in K or not.

2.5 Computational complications

When we do compute the generators for $E_f(K)$, we find that they are points of very high height on the curve, most often at least several hundred times the generators of $E(K)$. As such, the denominator of the x-coordinate for those points can be several thousands digits long, which complicates the computations. We obviously cannot factor the denominator to find the primes at which $t_{\mathfrak{p}}$ is not trivial. However, by modifying the same reasoning leading to equation 2.6, we find that we don't need factoring as the product simply becomes

$$c = \frac{C_{P+P'}C_{Q+P'}}{C_{P'}C_{P+Q+P'}}(f)^{\epsilon} \cdot c_f \tag{2.7}$$

where $-2 \leq \epsilon \leq 2$ simply accounts for the fact that a factor of (f) may be present in any of the preceding ideals, but has to be removed according to point 3 of section 2.3. However, we notice that the requirement that $P', P+P', Q+P', P+Q+P'$ are not in the kernel of reduction of f specifically mean that

$$\prod_{v} \frac{t_v(P+P')t_v(Q+P')}{t_v(P')t_v(P+Q+P')} = \prod_{v \neq f} \frac{t_v(P+P')t_v(Q+P')}{t_v(P')t_v(P+Q+P')}$$

that is to say that $\epsilon = 0$ in equation 2.7.

We find that when we want to express each of these ideals in term of a binary quadratic form, the form given by the usual homomorphism is so large that any attempt at reduction fails computationally. We therefore need some way to simplify the data before translating it to binary quadratic forms.

We find that one way to do so is to take the above ideals of $\mathcal{O}_K$ and reduce them by f, in order to find an ideal of $(\mathcal{O}_K/(f))^*$.

This is also a way to tackle the last item of section 2.3. Indeed, the ideals that we compute in equation 2.7 are ideals of the maximal order $\mathcal{O}_K$. Were we to simply take its $\mathbb{Z}$ basis (as in the case where S is empty), we would have binary quadratic forms of discriminant D_0 instead of $D_0 f^2$.

2.6 Choice of P'

Another way to reduce the computation time is through the choice of P'. As it was previously discussed, as we don't have S empty anymore, we need P' to be non-trivial. One way to do so would be to pick P' a point of small order on $E(K)$, such that $C_{P'}$ would be trivial. This is the preferred technique in the cases where the generators of $E_f(K)$ are not so large. In particular, it can be easier to pick P' to be one of the generator of $E(K)$, specifically the generator that is defined over $\mathbb{Q}$. However, as generators of $E_f(K)$ grow larger, taking P' to be the inverse of half the multiples of the generators in play can speed up the computations significantly. For example, if P_1, P_2 are generators for $E(K)$ and $Q_1 = aP_1 + bP_2$ is a generator of $E_f(K)$, for the computation of $\langle P_2, Q_1 \rangle$ we might take $P' = -\left\lfloor \frac{a}{2} \right\rfloor P_1 - \left\lfloor \frac{b}{2} \right\rfloor P_2$. As such, we would not anymore be able to conclude that $C_{P_2+P'}$ and $C_{P'}$ are trivial (or really easy to compute) as with $P' = P_1$, but all four ideals involved in the computations would be much more manageable than $C_{Q_1+P_1}$ would be.

Also, notice that it is easy in either cases to verify that $P', P+P', Q+P'$, and $P+Q+P'$ are not in the kernel of reduction of f as, provided they are not trivial, they are smaller multiples of the generators of $E(K)$ and thus, were they in $E_f(K)$, they could be used to "generate" the generators of $E_f(K)$ that we found earlier.

2.7 When f is not prime

All these ways of reducing the computation time still have their limits. Indeed, we are still required for some cases to compute the coordinates to large multiples of generators of $E(K)$ before we can work modulo f. Usually, one indication that the multiples to compute are large is when f itself is large. It requires a larger prime to appear in the denominator of the point, hence we usually have larger multiples generating $E_f(K)$. Another problematic case that we have not discussed is when f is not prime in K. When f is split in K, going back to our more general definition of the S-pairing, we need to consider $S = \{\mathfrak{p}_1, \mathfrak{p}_2\}$ where $f = \mathfrak{p}_1\mathfrak{p}_2$. As such, going back to the exact sequence 2.2, which now reads

$$0 \longrightarrow E_f(K) \longrightarrow E(K) \longrightarrow E(k_{\mathfrak{p}_1}) \times E(k_{\mathfrak{p}_2}) \times \prod_{\mathfrak{p}\nmid f} (E/E_0)(k_{\mathfrak{p}}).$$

Therefore, for a point P to be in $E_f(K)$, it needs to be in the kernel of reduction of both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ which strengthens the conditions. Therefore, we can expect to have very large multiples of the generators of $E(K)$ as generators for $E_f(K)$ in these cases.

For these reasons, we did not get to compute the regulator for those cases with either very large f or where f ramifies. However, one way that we could go about solving those computation problems would be to come up with a recurrence formula for the denominator of the x-coordinate of a sum of points mod$f$. This way, we could easily compute the reduction of $\operatorname{Denom}(x(P)) \bmod f$, before taking the square root in $(\mathcal{O}_K/f)^*$ for P of any height.

2.8 Ideals of the order of conductor f

It is often useful to consider ideals in the number field as $\mathbb{Z}$-modules. As such, we want to be able to give a description of the ideals using a $\mathbb{Z}$-basis instead of a generator. We will do so by using the notation $I = [\alpha, \beta]$.

Those ideals we have considered so far are ideals of the ring of integers $\mathcal{O}_K$. We then need for the following to introduce the notion of an *order* of this ring.

Definition 2.1. The *order of conductor f* in $\mathcal{O}_K$ is the $\mathbb{Z}$ module with basis $[1, f\omega]$, where

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

and where d is a square free integer such that $K = \mathbb{Q}(\sqrt{d})$. It is denoted $\mathcal{O}_f$.

Notice that the orders are subrings of $\mathcal{O}_K$ and that the ring of integers $\mathcal{O}_K = \mathcal{O}_1$ is the order of conductor 1 by the definition of ω. We call it the maximal order, for obvious reasons.

We then want to consider ideals of an order of $\mathcal{O}_K$. Since we are going to be using the $\mathbb{Z}$ basis approach to those ideals, we need a way to recognize when such a module is in fact an ideal of $\mathcal{O}_f$.

Theorem 2.2. *Let I be an ideal of the order $\mathcal{O}_f$ of conductor f. Then I has a $\mathbb{Z}$ basis of the form $[a, b + cf\omega]$ with a, b, c integers such that $c|a$, $c|b$ and $ac|\,\boldsymbol{N}(b + cf\omega)$. Furthermore, any $\mathbb{Z}$ module with a basis of this form is an ideal of the order $\mathcal{O}_f$.*

See [Mol96] or [Sim14] for this result. We will call this form of basis the *Hermite normal form.* Notice that all ideals of $\mathcal{O}_K$ have such a basis as the ring of integers is an order as noted previously.

We then return to binary quadratic forms. We recall and detail the procedure to go from ideals to binary quadratic forms as it was detailed previously. Precisely, suppose the ideal I has a $\mathbb{Z}$ basis in Hermite normal form $[\alpha, \beta] = [a, b + c\omega]$. Then $\mathbf{N}(\alpha x + \beta y) = \alpha^2 x^2 + \alpha \operatorname{tr}(\beta) xy + \mathbf{N}(\beta) y^2$.

Now as $c|a$, clearly $ac|\alpha^2$. Also, as $\operatorname{tr}(\beta) = 2b$ or $2b + c$, and since $c|b$, we also have that $ac|\alpha \operatorname{tr}(\beta)$. Finally, as specified in theorem 2.2, $ac|\,\mathbf{N}(\beta)$. We must thus divide by the common factor ac to make the form primitive. The resulting form is $Q = \left[\frac{a}{c}, \frac{\operatorname{tr}(b+c\omega)}{c}, \frac{\mathbf{N}(b+c\omega)}{ac}\right]$. Then, notice that the discriminant of this form is

$$\begin{aligned}
\mathrm{D}(Q) &= \frac{1}{c^2}\left[(\operatorname{tr}(b+c\omega))^2 - 4a\frac{\mathbf{N}(b+c\omega)}{a}\right] && (2.8)\\
&= \frac{1}{c^2}\left[(2b+\operatorname{tr}(\omega)c)^2 - 4(b^2+\operatorname{tr}(\omega)bc + c^2\,\mathbf{N}(\omega))\right] && (2.9)\\
&= \begin{cases} \frac{1}{c^2}\left[(2b)^2 - 4(b^2-c^2d)\right] & \text{if } d \equiv 2,3 \pmod 4\\ \frac{1}{c^2}\left[(2b+c)^2 - 4\left(b^2+bc+c^2\frac{1-d}{4}\right)\right] & \text{if } d \equiv 1 \pmod 4\end{cases} && (2.10)\\
&= \begin{cases} 4d & \text{if } d \equiv 2,3 \pmod 4\\ d & \text{if } d \equiv 1 \pmod 4\end{cases} && (2.11)
\end{aligned}$$

which is exactly the discriminant of K, D_0. Working instead with an ideal having basis $[a, b+cf\omega]$ in Hermite normal form would yield a form of discriminant D_0f^2. We simply replace the occurrences of ω by $f\omega$ in equation 2.9 to arrive at this conclusion. It should therefore be clear that our next step consists in finding a way to go from an ideal in the maximal order $\mathcal{O}_K$ to one of the order of conductor f. From there, expressing it in Hermite normal form $[a, b+cf\omega]$ gives us the form

$$\frac{\mathbf{N}\left(ax-(b+cf\omega)y\right)}{ac} = \frac{a}{c}x^2 - \left(\frac{2b}{c} + f\operatorname{tr}(\omega)\right)xy + \frac{b^2+bcf\operatorname{tr}(\omega)+c^2f^2\,\mathbf{N}(\omega)}{ac}y^2 \tag{2.12}$$

2.9 The ideal $I(\alpha)$

Let $\alpha \in (\mathcal{O}_K/f)^*$ and I be an ideal of the maximal order $\mathcal{O}_K$. Then define

$$I(\alpha) = \{x \in I \,|\, \operatorname{tr}(x\cdot\alpha) \equiv 0 \pmod f\}.$$

Then, we want to show that $I(\alpha)$ is an ideal of $\mathcal{O}_f$. First, if $x, y \in I(\alpha)$, then $\operatorname{tr}((x+y)\alpha) = \operatorname{tr}(x\cdot\alpha) + \operatorname{tr}(y\cdot\alpha) \equiv 0 \bmod f$. Also, for any $z \in \mathcal{O}_f$, z can be written as $z_1 + z_2 f\omega$ and so

$$\operatorname{tr}(x\cdot z\cdot\alpha) = z_1\operatorname{tr}(x\cdot\alpha) + z_2 f\operatorname{tr}(x\cdot\alpha\cdot\omega) \equiv 0 \bmod f.$$

Therefore, $I(\alpha)$ is an ideal of $\mathcal{O}_f$ and thus has a basis in Hermite normal form as in Theorem 2.2. We now try to explicit this basis as it is needed for computations.

Let $\alpha = \alpha_1 + \alpha_2\omega$. Also, let $[a, b + c\omega]$ be the basis in Hermite normal form of I as above. Then, for any x in I, we can write $x = \gamma a + \delta(b + c\omega)$ with $\gamma, \delta \in \mathbb{Z}$. We have

$$\begin{aligned} \operatorname{tr}(x \cdot \alpha) &= \operatorname{tr}(\gamma a\alpha_1) + \operatorname{tr}(\gamma a\alpha_2\omega) + \operatorname{tr}(\delta(b + c\omega)\alpha_1) + \operatorname{tr}(\delta(b + c\omega)\alpha_2\omega) \\ &= 2(\gamma a\alpha_1 + \delta b\alpha_1) + \delta c\alpha_2 \operatorname{tr}(\omega^2) + (\gamma a\alpha_2 + \delta c\alpha_1 + \delta b\alpha_2) \operatorname{tr}(\omega) \end{aligned}$$

Notice that $\operatorname{tr}(\omega) = 0$ if $d = 2, 3 \pmod 4$ and 1 otherwise, and so the last part of the above equation is present only in the latter case. Since we require that the trace be 0 mod f, then for $d = 2, 3 \pmod 4$,

$$a\alpha_1\gamma \equiv -(b\alpha_1 + cd\alpha_2)\delta \pmod f \tag{2.13}$$

and for $d \equiv 1 \pmod 4$

$$a(2\alpha_1 + \alpha_2)\gamma \equiv -(b(2\alpha_1 + \alpha_2) + c\left(\alpha_1 + \frac{(1 + d)}{2}\alpha_2\right)\delta \pmod f. \tag{2.14}$$

In both cases, since $\alpha \in (\mathcal{O}_K/f)^*$, we can invert terms on either side to solve the equation. For simplicity, suppose that $\gamma \equiv l\delta \pmod f$. Then, that means that elements of $I(\alpha)$ are of the form $\kappa f \cdot a + \delta((b + la) + c\omega)$ for $\kappa, \delta \in \mathbb{Z}$. However, it is pretty clear at this stage that not all those elements are in $\mathcal{O}_f$. Since we obviously want our ideal to be included in $\mathcal{O}_f$, we can simply take its intersection with $\mathcal{O}_f$. That means that we should only take f multiples of the last element of the basis. Thus, the new Hermite normal form becomes $[af, f(b + la) + cf\omega]$. Also, since we knew $[a, b + c\omega]$ to be in Hermite normal form, $c|a$, $c|b$ and so $c|f(b + la)$. Finally, as

$$\mathbf{N}(f(b + la) + cf\omega) = f^2\left(\mathbf{N}(b + c\omega) + 2bla + l^2a^2 + lac\operatorname{tr}(\omega)\right)$$

and as ac divides every term in the sum, this basis satisfies the conditions of Theorem 2.2. Therefore, as described above, the binary quadratic form associated with this ideal is

$$\left[\frac{af}{c}, -2f\left(\frac{b + la}{c} + \operatorname{tr}(\omega)\right), \frac{f^2(b + la)^2 + f^2bc\operatorname{tr}(\omega) + f^2c^2\,\mathbf{N}(\omega)}{afc}\right].$$

However, notice that this form is not primitive, as it has the common factor f. Dividing through, the form becomes the one associated with the ideal $[a, b + la + c\omega]$ and has discriminant D_0.

2.10 Taking the intersection

Consider the ideal I of $\mathcal{O}_K$ with the $\mathbb{Z}$ basis $[a, b+c\omega]$ in Hermite normal form. Then, under the assumption that c and f are relatively prime, it is pretty clear that the intersection of I with $\mathcal{O}_f$ is given by the basis $[a, bf + cf\omega]$. It is already given that c divides a and b, and so bf too. Also, $\mathbf{N}(bf + cf\omega) = f^2\,\mathbf{N}(b+c\omega)$ which is divisible by ac. Therefore, the basis satisfies conditions of Theorem 2.2, and thus we conclude that $I \cap \mathcal{O}_f$ is an ideal of $\mathcal{O}_f$.

Also, we want to verify that the map $I \mapsto I \cap \mathcal{O}_f$ is compatible with the surjective homomorphism $G_{D_0 f^2} \to G_{D_0}$. Recall that this homomorphism is given by composing the binary quadratic form of $G_{D_0 f^2}$ with the identity of G_{D_0}. Since the composition of forms amounts to the multiplication of the associated ideals, we consider the ideal $(I \cap \mathcal{O}_f) \cdot (1)$.

Proposition 2.3. *Let $I = [a, b + c\omega]$ be an ideal of $\mathcal{O}_K$. Under the assumption that f does not divide a or c,*

$$(I \cap \mathcal{O}_f) \cdot (1) = I$$

Proof. We have,

$$[a, fb + fc\omega][1, \omega] = [a, fb + fc\omega, a\omega, fb\omega + fc\omega^2].$$

Now, assuming that $\gcd(fc, a) = c$, which is satisfied in practice, we use Bézout's identity to find u, v such that $ufc + va = c$. Then, $u(fb + fc\omega) - v(a\omega) = ufb + c\omega$. Furthermore, $(ufb + c\omega) + \frac{vb}{c}(a) = \frac{b}{c}(ufc + va) + c\omega = b + c\omega$. Now, it follows that we can harmlessly add $b + c\omega$ to the basis since it is obtained from other elements present. However, doing so, we can remove $fb + fc\omega$ as it is a multiple of this new element. The new basis is therefore

$$= [a, b + c\omega, a\omega, fb\omega + fc\omega^2]$$

Similarly, $u(fc\omega^2 + fb\omega) + v\omega^2 a = c\omega^2 + ufb\omega$. Here notice that $v\omega^2 a$ can be retrieved from the basis as if $\omega = \sqrt{d}$, $\omega^2 \in \mathbb{Z}$, and if $d \equiv 1 \bmod 4$, then $\omega^2 = \omega + \frac{d-1}{4}$. Also, $ufb\omega + v\frac{b}{c}a\omega = c\omega^2 + b\omega$. Again here, we can simply replace $fc\omega^2 + fb\omega$ by $c\omega^2 + b\omega$ in the basis. We have

$$= [a, b + c\omega, a\omega, b\omega + c\omega^2].$$

Then, we have that $a\omega = \frac{a}{c}(b + c\omega) - \frac{b}{c}a$. Therefore, this time we can simply remove $a\omega$ from the basis.

$$= [a, b + c\omega, fb\omega + fc\omega^2]$$

Finally, we modify the last element of the basis to get $(c\omega^2 + b\omega) - \frac{b}{c}(b + c\omega) = c\omega^2 - \frac{b^2}{c}$. We then obtain

$$= \left[a, b + c\omega, c\omega^2 - \frac{b^2}{c}\right]$$

Now, recall that $[a, b + c\omega]$ was a basis in Hermite normal form. Therefore, we have that $ac|\,\mathbf{N}(b + c\omega)$. First, suppose that $d \equiv 2, 3 \bmod 4$. Then, $\omega = \sqrt{d}$ and $\mathbf{N}(b + c\omega) = b^2 - c^2\omega^2$. Since $ac|b^2 - c^2\omega^2$, we also have $a|\frac{b^2}{c} - c\omega^2$, and we conclude that the last element of the basis is a multiple of a.

Now suppose that $d \equiv 1 \bmod 4$. Then, $c\omega^2 - \frac{b^2}{c} - (b + c\omega) = \frac{1}{c}\,\mathbf{N}(b + c\omega)$ and again $a|\frac{1}{c}\,\mathbf{N}(b + c\omega)$.

In either case, the last element is superfluous, and the basis is therefore simply

$$[a, fb + fc\omega][1, \omega] = [a, b + c\omega].$$

We recognize the basis for the original ideal I. What this means is that if we were to take the binary quadratic form associated with $I \cap \mathcal{O}_f$ and remove the square from the discriminant by composing with the identity, the form we would obtain is exactly the one associated with the ideal I. □

2.11 Binary quadratic forms

Let Φ_{IF} denote the map from ideals to binary quadratic forms. For details on this map see [Coh93, Section 5.2] and [Rob09, Section 25]. As we have the basis for our new ideal to be $[a, bf + cf\omega]$, formula 2.12 gives the form

$$\begin{aligned}\Phi_{IF}(I \cap \mathcal{O}_f) &= \left[\frac{a}{c}, \frac{\operatorname{tr}(bf + cf\omega)}{c}, \frac{\mathbf{N}(bf + cf\omega)}{c}\right] \\ &= \left[\frac{a}{c}, \frac{-2bf}{c} + f\operatorname{tr}(\omega), \frac{b^2f^2 + bcf^2\operatorname{tr}(\omega) + c^2f^2\,\mathbf{N}(\omega)}{ac}\right].\end{aligned} \tag{2.15}$$

Obviously, this is a binary quadratic form of positive discriminant ($D = D_0 f^2$). For such forms, we define the form to be *reduced* if

$$0 < \sqrt{D} - b < 2\,|a| < \sqrt{D} + b.$$

Under these conditions, the values of a and b are clearly bounded, and so there are only finitely many such form for a given discriminant. However, contrary to positive definite binary quadratic forms, there is no unique reduced form in an equivalence class of form, making harder to work with them.

The two forms $[a, b, c]$ and $[c, b', c']$ of discriminant D are *neighbours* if $b + b' \equiv 0 \pmod{2c}$. Notice that two neighbours are equivalent under the transformation $\begin{pmatrix} 0 & 1 \\ -1 & \frac{b+b'}{2c} \end{pmatrix}$. Given a form $Q = [a, b, c]$, we use Gauss's reduction algorithm to find its neighbour. This algorithm goes as follows:

1. Let b_0 be the center lift of $-b \pmod{2c}$, i.e. such that $|b_0| \leq c$.
2. If $|b_0| > \sqrt{D}$, then let $b' = b_0$.
3. If $|b_0| < \sqrt{D}$, then let b', choose k as large as possible such that $|b_0 + k\,|2c|| < \sqrt{D}$. Let $b' = b_0 + k\,|2c|$.
4. Take $c' = \frac{(b')^2 - D}{4c}$.
5. The form $[c, b', c']$ is the required neighbour of Q.

By repeating this process, we find a list of forms equivalent to Q such that the last coefficient of one is the first coefficient of the next one. Eventually, we end up retrieving the form Q and thus have a cycle, that we express as

$$a_0 \;{}^{b_0}\; a_1 \;{}^{b_1}\; a_2 \;{}^{b_2}\; a_3 \;\ldots\; a_n \;{}^{b_n}\; a_0$$

where the original form is $[a_0, b_0, a_1]$, its neighbour is $[a_1, b_1, a_2]$, and so on. Actually, all the possible reduced representatives of the form Q are listed in this cycle. For more details, see [Gra, Sec 4.6] and [BV07, Prop 6.10.3]. Thus, the cycle of reduced representatives for a form is an invariant of the equivalence class for that form. This is how we retrieve the factorization of a given form in terms of the generators for G_D.

Indeed, we see in table 1 the generators for the group G_D are listed along with their respective order (under $h^+(D)$). Given a binary quadratic form Q

from above formula 2.15, we begin by reducing it using the usual reduction algorithm, and then find its cycle of reduced forms. Comparing this list to the different multiples of σ_1 and σ_2, we can retrieve the factorization of Q in terms of those two generators.

2.12 Recapitulating

Given a discriminant $D = D_0 f^2$, let $K = \mathbb{Q}(\sqrt{D_0})$. We want to compute the pairings $\langle g_i, q_j \rangle$ where g_i are generators for the curve $E(K)$, and q_j are generators for $E_f(K)$, and where the pairing is taken for $S = \{f\}$.

1. The first step is to find $E_f(K)$. We know that $E_f(K)$ is a subgroup of $E(K)$ of rank 2. We are thus looking for the two generators. We do so following the algorithm given in section 2.4. Namely, we compute the smallest multiples of g_i that is in the kernel of reduction of f. Keeping one of them as a first generator for $E_f(K)$, we then compute several combinations of multiples of g_i as candidates for the second generator. We then verify which one is the smallest.

2. We then compute each $\langle g_i, q_j \rangle$ individually. To do so, we begin by choosing P' in $E(K)$ such that none of $P', P'+g_i, P'+q_j$ and $P'+g_i+q_j$ are zero mod$f$. Usually, we can choose $P' = g_i$, which makes the computations slightly easier. In any case, we need to verify that these listed points do not vanish in the reduction by f.

3. Then, we compute the ideals that we denoted by $C_{P'}, C_{P'+g_i}, C_{P'+q_j}$ and $C_{P'+g_i+q_j}$. During this computation, it might be necessary to reduce the denominator of the x-coordinate mod$f$ before being able to carry the computations, as some of these points tend to get very large.

4. We then express each of these ideals in Hermite normal form, so as to have a basis of the form $[a, b + c\omega]$. Then, we take the intersection of this ideal with $\mathcal{O}_f$ to find an ideal of the order of conductor f. Its basis should be $[a, bf + cf\omega]$.

5. The next step is to apply Φ_{IF} to this ideal. We do so by simply using formula 2.15. We can then apply reduction algorithms to this binary quadratic form to obtain a reduced form Q of discriminant $D_0 f^2$.

6. We use the algorithm described in section 2.11 to find the cycle of this form Q. We then compare this cycle to the list of all $\sigma_1^m \sigma_2^n$, where σ_1 and σ_2 are the generators for $G_{D_0 f^2}$ that are given in table 1, and m, n range over their respective orders. This list can be computed once and used throughout the computation for a fixed discriminant. We then have to intersect the different reduced forms from the cycle to those from the list to find a match.

7. Repeat steps 4 to 6 for all four ideals (possibly less if some are clearly trivial). Then multiply the corresponding forms (or their inverse) according to formula 2.7. The resulting binary quadratic form is $\langle g_i, q_j \rangle$.

3 The other factors

Now that we know how exactly to compute the pairings required to find R_D, the two factors that are left to find are J_D and $|Ш(E/K)|$.

3.1 J_D

Recall that J_D is defined as the order of the cokernel of the rightmost map φ in the exact sequence

$$0 \longrightarrow E_f(K) \longrightarrow E(K) \xrightarrow{\varphi} E/E^0(K) \oplus E(k_f)$$

specifically

$$J_D = \left| E/E^0(K) \oplus E(k_f) \ / \ \varphi(E(K)) \right|.$$

As it was pointed out in section 2.4, E has good reduction on all primes that does not divide $\Delta = 37$. As we here restricted our attention to cases were f is inert in K, we know that E will have good reduction at f. Also, we already explained that the component group $E/E^0(K)$ has order $\nu(\Delta)$. Thus, in the cases were 37 splits completely, we have that $E/E^0(K)$ is trivial, and consequently φ is surjective. Clearly then $J_D = 1$. We found that this was so in all cases that were studied, and so no further investigation was done.

3.2 The Tate-Shafarevich group $Ш(E/K)$

The last remaining factor present in conjecture 1.3 is $|Ш(E/K)|$. Recall that the Tate-Shafarevich group $Ш(E/K)$ is defined as the group of homogeneous spaces for E/K that has a K_ν rational point for every valuation ν of K. For more details we can refer to [Sil09, Section X.4]. We know that $Ш(E/K)$ is always a finite group, but in practice it might be very hard to compute. Unfortunately, it was not possible at this time to find a way to calculate $|Ш(E/K)|$ for all the number fields with which we worked. The only information included here concerning this group is $|Ш(E/\mathbb{Q})|$, which is listed in the tables of elliptic curves data of J.E. Cremona ([Cre, Table 4]). This value turns out to be 1 for our specific elliptic curve.

4 Illustrating example

We will start by carrying computations for the first case to check in a very explicit manner as to illustrate the process that we use throughout the different cases. This way, we will concentrate on complications encountered for all the other cases.

Let $D = D_0 \cdot f^2 = 12 \cdot 607^2$. Here, $K = \mathbb{Q}(\sqrt{3})$ and $\omega = \sqrt{3}$. We also know that $h(D) = 1$, $h^+(D) = 38 \cdot 2$ and that G_D is generated by the binary quadratic forms $(-1034, 2066, 37), (3, 2100, -949)$ denoted σ_1, σ_2 respectively.

As expected, the curve $X_0(37)^+$ has rank 2 in K (and is torsion free as we wanted), and we find using SAGE that the generators are $g_0 = (\frac{\sqrt{3}}{2}, \frac{-\sqrt{3}+3}{4})$ and $g_1 = (0, 1)$.

4.1 The S-pairing

4.1.1 $E_f(K)$

The first step to verify the conjecture for this case is to compute the subgroup $E_f(K)$ of $E(K)$. As explained in section 2.4, we start by computing multiples of g_0 and g_1 to see when they vanish modulo f. We find that the smallest such multiples are $256g_0$ and $640g_1$. We can take $640g_1$ as a generator for $E_f(K)$. Now we know that as $E_f(K)$ has rank 2 also, we need to find a second generator. The possible candidates here for such a second generator are $a \cdot g_0 + b \cdot g_1$ where a ranges over all divisors of

256, that is $\{1,2,4,8,16,32,64,128,256\}$ and b ranges over all multiples of $\frac{640}{\gcd(640,256)} = 5$ up to 640, that is $\{5n | 1 \leq n \leq 128\}$. We find that the smallest candidate that actually vanishes when reduced by 607 is $64g_0 + 160g_1$, which we take as our second generator. We have $E(K) = \langle g_0, g_1\rangle$ and $E_f(K) = \langle 64g_0 + 160g_1, 640g_1\rangle = \langle q_0, q_1\rangle$.

The next step is to compute the regulator expression for the right hand side of the equation in conjecture 1.3.

$$R_D = \begin{vmatrix} \langle g_0, q_0\rangle & \langle g_0, q_1\rangle \\ \langle g_1, q_0\rangle & \langle g_1, q_1\rangle \end{vmatrix} \tag{4.1}$$

We compute each pairing in the above matrix individually to later calculate the determinant. The first and easiest pairing to compute is $\langle g_1, q_1\rangle = \langle g_1, 640g_1\rangle$. Clearly this pairing is trivial. There are multiple ways to see this, but the easiest might be that the points appearing in the pairing are both defined on $E(\mathbb{Q})$ and we know that the pairing is trivial in $\mathbb{Q}$.

4.1.2 $\langle g_0, q_1\rangle$

Next up is the pairing $\langle g_0, q_1\rangle = \langle g_0, 640g_1\rangle$.

The first thing we need to do is to determine the point P' on E that is used during the computations. One way to do this that works in many cases and that somewhat simplifies the calculations is to pick $P' = g_1$. We know that $t_v(g_1)$ is trivial for all v, and specifically that the above conditions are satisfied for it. Similarly, it works better here to take $P' = -g_1 = (0,0)$, which does satisfy the same conditions as g_1. Also, it is easy to verify that $g_0 - g_1 = (-\sqrt{3}+2, 2\sqrt{3}-3)$ and thus we can say the same for this point. Finally, if $P_1 = 641g_1$ and $P_2 = 641g_1 + g_0$, we verify that $\tilde{P_1}, \tilde{P_2} \neq 0$ where $\tilde{P_i}$ indicates the reduction by f, and equation 2.7 simplifies to

$$c = \frac{C_{639g_1}}{C_{639g_1+g_0}} \cdot c_f.$$

We detail here the code from SAGE ([S$^+$14]) used to compute the result, that we break down to make it very understandable. The first thing to compute is C_{641g_1} or rather its reduction $\mathrm{mod}(f)$. Since g_1 has rational coordinates, so does any multiples of it. Therefore, we know that there is no further reduction to be done to find the truly reduced denominator (see example 2.1).

```
sage:  E = EllipticCurve([0,0,-1,-1,0]);
sage:  K.<sqrt3> = NumberField(x^2-3);
sage:  E  = E.change_ring(K); E
Elliptic Curve defined by y^2 + (-1)*y = x^3 + (-1)*x over
   Number Field in sqrt3 with defining polynomial x^2 - 3
sage:  [g0,g1] = E.gens(); [g0,g1]
[(1/2*sqrt3 : -1/4*sqrt3+3/4 : 1),(0 : 1 : 1)]
sage: f = K.ideal(607);
sage: D = denominator((639*g1)[0]);
sage: h = sqrt(D);
sage: f.reduce(h)
-92
```

We thus have that the projection of C_{639g_1} to $(\mathcal{O}_K/(f))^*$ is the ideal (-92) mod (f). Clearly, this ideal should map to the identity in G_D, but as a sanity check for our method, let's carry the computation anyways. The $\mathbb{Z}$ basis for this ideal is not hard to guess, it is simply $[-92, -92\sqrt{3}]$. The intersection with $\mathcal{O}_f$ is therefore given by $[-92, -607 \cdot 92\sqrt{3}]$. According to formula 2.15, the form associated is $[1, 0, -3 \cdot 607^2]$ which indeed, is the identity of G_D.

Things complicate slightly for the case of $C_{639g_1+g_0}$. Since the point has coordinates in K, we need to verify that the denominator of the x coordinate is reduced as an ideal of $\mathcal{O}_K$. To do so, we use the following SAGE code.

```
sage: M = K.ideal((639*g1+g0)[0]);
sage: D = denominator(M);
```

Here, the SAGE function `denominator`, when used on a number field fractional ideal I, returns an integral ideal D where $I = \frac{N}{D}$ for N an integral ideal relatively prime to D.

```
sage: gen = D.gens_reduced();
```

Here we need to use `.gens_reduced()` since we are in a principal ideal domain and we want the (single) generator of the ideal. Other functions may yield a basis of two generators.

```
sage: h = sqrt(gen);
sage: f.reduce(h)
161*sqrt3+335
```

So the reduction of $C_{639g_1+g_0}$ mod $(f) = (161\sqrt{3} + 335)$.

We then need to find the binary quadratic form associated to this ideal. First, we need to express it in Hermite normal form. Since the reduction algorithms for indefinite forms are already implemented in Pari ([PAR14]), we will use this software to carry out this part of the computation.

```
gp> K = nfinit(x^2-3);
gp> w = quadgen(12);
%2 = w
gp> idealhnf(K,[335;161])
%3 = [34462, 21193; 0, 1]
```

Here the Hermite normal form basis is represented as a matrix, specifically $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$. Thus, the basis here is actually $I = [34462, 21193 + \sqrt{3}]$. After verifying that $\gcd(34462, 607) = \gcd(21193, 607) = 1$, we have that the intersection of this ideal with the order of conductor 607 is $I' = [34462, 607 \cdot 21193 + 607\sqrt{3}]$. Then from formula 2.15, we find the form

$$\Phi_{IF}(I') = \left[34462, -2 \cdot 21193 \cdot 607, \frac{(21193 \cdot 607)^2 - 3 \cdot 607^2}{34462}\right].$$

We then find a reduced representative using

```
gp> Q = Qfb(34462,-2*21193*607,607^2*(21193^2-3)/34462)
%4 = Qfb(34462, -25728302, 4801995817, 0.E-28)
gp> qfbred(Q)
%5 = Qfb(433, 1294, -1586, 0.7455010895777085615427567231)
```

As for finding the cycle associated to this form, we use the following pari scripts.

```
qfbredcycle(a,b,c,D) =
{
        L = listcreate(1000);
        listput(L,a);
        listput(L,b);
        listput(L,c);
        while(L[1]!=L[length(L)],
                R = qfbredext(a,b,c,D);
                a = R[1];
                b = R[2];
                c = R[3];
                listput(L,b);
                listput(L,c);
                );
        return(L)
}
qfbredext(a,b,c,D)=
{
        b0 = centerlift(Mod(-b,2*c));
        if(abs(b0)>sqrt(D),
                bprime = b0,
                bprime = -b;
                while(abs(bprime+abs(2*c))<sqrt(D),bprime =
                   bprime+abs(2*c))
        );
        a = c;
        b = bprime;
        c = (b^2-D)/(4*a);
        return([a,b,c])
}
```

where `qfbredext(a,b,c,D)` finds the neighbour of form $[a, b, c]$ of discriminant D, and `qfbredcycle(a,b,c,D)` lists the cycle of this form. We then compute

```
gp> \r qfbredext.gp;
gp> \r qfbredcycle.gp;
gp> qfbredcycle(433,1294,-1586,12*607^2)
%8 = List([433, 1294, -1586, 1878, 141, 2070, -242, 1802,
    1213, 624, -831, 1038, 1006, 974, -863, 752, 1117, 1482,
    -498, 1506, 1081, 656, -923, 1190, 814,2066, -47, 2070,
    726, 834, -1283, 1732, 277, 1592, -1703, 1814, 166, 1838,
    -1571, 1304, 433])
```

So the cycle corresponding to our form is composed of 20 equivalent forms. Under our notation, it is

$$433\ {}^{1294}\ -1586\ {}^{1878}\ 141\ {}^{2070}\ -242\ {}^{1802}\ 1213\ {}^{624}\ -831\ {}^{1038}\ 1006\ {}^{974}\ -863\ {}^{752}$$
$$1117\ {}^{1482}\ -498\ {}^{1506}\ 1081\ {}^{656}\ -923\ {}^{1190}\ 814\ {}^{2066}\ -47\ {}^{2070}\ 726\ {}^{834}$$
$$-1283\ {}^{1732}\ 277\ {}^{1592}\ -1703\ {}^{1814}\ 166\ {}^{1838}\ -1571\ {}^{1304}\ 433$$

Now, by listing all the possible elements of G_D as $\sigma_1^i\sigma_2^j$ in Pari for $1 \leq i \leq 38$ and $j = 0, 1$, we find that $\sigma_1^{17} = [-47, 2070, 726]$. Notice that this form appears as the last on the second line in the above cycle. We conclude that $\Phi_{IF}(I') = \sigma_1^{17}$.

Putting the two result together, we find that the pairing actually maps to σ_1^{-17}, or equivalently

$$\langle g_0, q_1 \rangle = \sigma_1^{21}$$

as the first ideal C_{641g_1} maps to the identity, and $C_{641g_1+g_0}$ appeared in the denominator, so we need to take the inverse of the resulting form.

4.1.3 $\langle g_1, q_0 \rangle$

The next pairing to be calculated in the discriminant is $\langle g_1, q_0 \rangle = \langle g_1, 160g_1 + 64g_0 \rangle$.

Here we take $P' = g_1$ as it has the advantage of yielding $C_{g_1} = C_{2g_1} = (1)$ (as $2g_1 = (1, 1)$). Let $P_1 = 161g_1 + 64g_0$ and $P_2 = 162g_1 + 64g_0$, then

$$c = \frac{C_{P_1}}{C_{P_2}} \cdot c_f.$$

We can also easily verify that $\tilde{P}_1, \tilde{P}_2 \neq 0$ and so all the conditions are satisfied. We then use the SAGE to compute the following.

```
sage: M = K.ideal((161*g1+64*g0)[0]);
sage: D = denominator(M);
sage: gen = D.gens_reduced();
sage: gen.is_square()
False
```

Unfortunately here, even though we know that the ideal D is square, the generator that we are given with the `.gens_reduced()` command is not. We therefore use the following trick to obtain a square generator. The unit group of K here is isomorphic to $\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ where the fundamental unit is $u = \sqrt{3}-2$, and the roots of unity are simply $\{1, -1\}$. We then try multiplying the given generator of the ideal by a unit to obtain a square.

```
sage: UK = K.unit_group();
sage: u = UK.fundamental_units(); u
[sqrt3-2]
sage: (gen*(-u[0])).is_square()
True
sage: h = sqrt(gen*(-u[0]));
sage: f.reduce(h)
296*sqrt3+172
```

We therefore have that the reduction of C_{P_1} by (f) is $(296\sqrt{3} + 172)$. Now we use the same Pari code to obtain the binary quadratic form associated to this ideal. What we end up finding is that the Hermite normal form for the ideal is $[58316, 24432 + 4\sqrt{3}]$. Again, f is relatively prime with all those coefficients, and so we obtain using the same formulas and scripts as in previous case that $\Phi_{IF}(C_{P_1} \cap \mathcal{O}_f) = [-598, 1254, 1191]$.

As for C_{P_2}, we use the exact same code, with the exception that we need to multiply the given generator by u instead of $-u$ to obtain a square. The result we obtain is that the projection of C_{P_2} to $(\mathcal{O}_K/(f))^*$ is $(39\sqrt{3} + 26)$, and its Hermite normal form is $[299, 208+13\sqrt{3}]$. The binary quadratic form associated to this ideal is $[23, 2058, -2022]$ in reduced form.

Multiplying the first form with the inverse of the second yields the form $[-138, 2058, 337]$. Computing the cycle associated with this form and comparing with the list of elements of G_D, we find that $[-138, 2058, 337] = \sigma_1^{23}$. We thus have

$$\langle g_1, q_0\rangle = \sigma_1^{23}.$$

4.1.4 $\langle g_0, q_0\rangle$

The final pairing to calculate here is $\langle g_0, q_0\rangle = \langle g_0, 160g_1 + 64g_0\rangle$. Again here, we take $P' = g_1$ so that C_{g_1} and $C_{g_1+g_0}$ are trivial, as verified in previous cases. Let $P_1 = 161g_1 + 64g_0$ and $P_2 = 161g_1 + 65g_0$, then

$$c = \frac{C_{P_1}}{C_{P_2}} c_f$$

as before. However, here, we notice that P_1 was already studied in section 4.1.3. In particular, we have that C_{P_1} reduces to $(296\sqrt{3} + 172)$, and maps to the form $[-598, 1254, 1191]$.

We firstly verify that $\tilde{P_2} \neq 0$ to confirm our choice of P'. Then, we use the procedure defined in section 4.1.3 in SAGE to compute $C_{P_2} \bmod (f)$. In this specific case we needed to multiply the generator of D by the unit $-u$ to for it to be square. Taking the square root and reducing gives $(153\sqrt{3} - 191)$. The Hermite normal form of the basis associated with this ideal is $[33746, 881 + \sqrt{3}]$, and applying Φ_{IF} gives $[759, 1806, -382]$. Finally, multiplying the form $[-598, 1254, 1191]$ with the inverse of $[759, 1806, -382]$ yields the form $[-299, 1736, 1177]$. Verifying its cycle against the list of elements of G_D give that this pairing maps to

$$\langle g_0, q_0 \rangle = \sigma_1^{30}$$

in G_D.

4.2 The conjecture

4.2.1 The regulator R_D

Getting back to the regulator R_D, we input the binary quadratic forms corresponding to each pairing in equation 4.1, but by making sure to express them as elements of I/I^2.

$$\begin{aligned} R_D &= \begin{vmatrix} 30(\sigma_1 - 1) & 21(\sigma_1 - 1) \\ 23(\sigma_1 - 1) & (1-1) \end{vmatrix} \\ &= -21 \cdot 23(\sigma_1 - 1)^2 \end{aligned}$$

Also, in K, the ideal generated by 37 splits as $(37) = (7+2\sqrt{3})(7-2\sqrt{3})$. Therefore, as previously noted, we have $J_D = 1$. From Table 1, we know that the leading term $\tilde{\theta}_D$ for this discriminant is $8(\sigma_1 - 1) \cdot \omega^+$. Therefore, $\tilde{L}_D = -64(\sigma_1 - 1)^2 \cdot \omega^+ \otimes \omega^+$. Finally, if we let $n = |Ш(E/K)|$, the statement of conjecture 1.3 becomes

$$-64(\sigma_1 - 1)^2 \cdot \omega^+ \otimes \omega^+ = -n \cdot 483(\sigma_1 - 1)^2 \cdot \omega^+ \otimes \omega^+.$$

Although this might seem odd, we refer the reader to section 6 for explanation.

5 Results

5.1 Tables

The computations we carried out for a few selected discriminants are compiled in tables 2, 3 and 4.

The second row list the points used as generators of $E(K)$. $g_1 = (0, 1)$ is a known generator for the curve $E(\mathbb{Q})$, and thus is in every basis. The second point g_0 was given using a 2-descent algorithm (SAGE's `.simon_two_descent()`). We are assuming that the point given along with g_1 generate $E(K)$.

The third row lists the generators of $E_f(K)$ as found via the method described in section 2.4. They are described in terms of the linear combination of the generators of $E(K)$ as listed above them.

In the fourth row, we indicated the result for the pairings $\langle g_0, q_1\rangle$ and $\langle g_1, q_0\rangle$ individually, to show exactly how we got to the listed result of R_D. Notice that as per our convention to have g_1 a rational point (over $\mathbb{Q}$) and q_1 a multiple of g_1, the pairing $\langle g_1, q_1\rangle$ is always going to be trivial, hence 0 in I/I^2, making the pairing $\langle g_0, q_0\rangle$ irrelevant. Those two listed are thus the only pairing we need.

The fifth row contains the regulator element R_D. It is specifically calculated using the matrix

$$R_D = \begin{vmatrix} \langle g_0, q_0\rangle & \langle g_0, q_1\rangle \\ \langle g_1, q_0\rangle & \langle g_1, q_1\rangle \end{vmatrix}$$

The sixth row contains the information on J_D. As we have noted in section 3.1, provided that the ideal 37 splits completely in K, we have $J_D = 1$. It was the cases for all the discriminants we verified.

The last two rows list the leading terms $\tilde{\theta}_D$ as they appear in table 1, as well as the left hand side $\tilde{L}_D$ of conjecture 1.3. The factor ω^+ (the associated element of $M_D = H_1(E(\mathbb{C}), \mathbb{Z})$) that was present in all leading term was omitted, as well as the factor $\omega^+ \otimes \omega^+$ in $\tilde{L}_D$.

With those values calculated, the only missing value needed to verify the conjecture is $Ш(E/K)$.

6 Conclusion

We see from tables 2, 3 and 4 containing our results that there seems to be a discrepancy between the value we obtain for the arithmetical part of the

Table 2: Results for $D_0 = 12$

$D = D_0 f^2$	$12 \cdot 607^2$	$12 \cdot 2131^2$	$12 \cdot 3691^2$
Gens. of $E(K)$ $(g_0; g_1)$	$(\frac{\sqrt{3}}{2}, \frac{-\sqrt{3}+3}{4})$; $(0, 1)$		
Gens. of $E_f(K)$ $(q_0; q_1)$	$64g_0 + 160g_1$; $640g_1$	$86g_0 + 885g_1$; $1100g_1$	$946g_0 + 335g_1$; $1800g_1$
$\langle g_0, q_1\rangle$; $\langle g_1, q_0\rangle$	σ_1^{21}; σ_1^{23}	σ_1^{16}; σ_1^{108}	1; 1
R_D	$-483(\sigma_1 - 1)^2$	$-1728(\sigma_1 - 1)^2$	0
J_D	1	1	1
Leading Term	$8(\sigma_1 - 1)$	$128(\sigma_1 - 1)$	$12(\sigma_1 - 1)$
$\tilde{L}_D$	$64(\sigma_1 - 1)^2$	$16384(\sigma_1 - 1)^2$	$144(\sigma_1 - 1)^2$

Table 3: Results for $D_0 = 33$

$D = D_0 f^2$	$33 \cdot 151^2$
Gens. of $E(K)$ $(g_0; g_1)$	$(2\omega + 5, 7\omega + 17)$; $(0, 1)$
Gens. of $E_f(K)$ $(q_0; q_1)$	$28g_0 + 2g_1$; $68g_1$
$\langle g_0, q_1\rangle$; $\langle g_1, q_0\rangle$	$\sigma_1^{27}\sigma_2$; σ_1^{10}
R_D	$-270(\sigma_1 - 1)^2$ $+10(\sigma_1 - 1)(\sigma_2 - 1)$
J_D	1
Leading Term	$26(\sigma_1 - 1)$
$\tilde{L}_D$	$676(\sigma_1 - 1)^2$

conjecture and the calculated analytical part of the conjecture. For several reasons, we cannot conclude that the conjecture is false.

Firstly, it was not verified whether the points that were taken as generator for $E(K)$ truly generate the whole Mordell-Weil group. It might be the fact that we have a point of infinite order generating a subgroup of $E(K)$ of finite index. Although this would obviously skew the final results, it does not affect the procedure that was described in this thesis.

Also, as it was alluded to in section 3.2, it was not possible at this time to compute the order of the Tate-Shafarevich group for the specific number fields in which we worked. It might be the case that, when taken modulo the order of the elements of G_D, the resulting coefficients of $(\sigma_1 - 1)^2$ match.

Except for these reservations, it is hoped that the procedure for calculating the Mazur-Tate pairing described in this thesis lays the groundwork for successfully testing the Maxzur-Tate conjectures numerically, even if we fall short of doing so here.

Table 4: Results for $D_0 = 44$

$D = D_0 f^2$	$44 \cdot 199^2$	$44 \cdot 379^2$
Gens. of $E(K)$ $(g_0; g_1)$	$(\frac{33\sqrt{11}+193}{361}, \frac{-165\sqrt{11}+4089}{6859})$; $(0, 1)$	
Gens. of $E_f(K)$ $(q_0; q_1)$	$202g_0 + 93g_1$; $99g_1$	$395g_0 + 28g_1$; $73g_1$
$\langle g_0, q_1 \rangle$; $\langle g_1, q_0 \rangle$	$\sigma_1^{46}\sigma_2$; σ_1^8	$\sigma_1^{30}\sigma_2$; σ_1^{40}
R_D	$-368(\sigma_1 - 1)^2$ $+8(\sigma_1 - 1)(\sigma_2 - 1)$	$-1200(\sigma_1 - 1)^2$ $+40(\sigma_1 - 1)(\sigma_2 - 1)$
J_D	1	1
Leading term	$18(\sigma_1 - 1)$	$68(\sigma_1 - 1)$
$\tilde{L}_D$	$324(\sigma_1 - 1)^2$	$4624(\sigma_1 - 1)^2$

References

[Bue89] Duncan A. Buell. *Binary Quadratic Forms: Classical Theory and Modern Computations*. Springer-Verlag, 1989.

[BV07] Johannes Buchmann and Ulrich Vollmer. *Binary Quadratic Forms: An Algorithmic Approach*, volume 20 of *Algorithms and Computation in Mathematics*. Springer, 2007.

[Cal86] Gregory Scott Call. *Local heights on families of abelian varieties*. PhD thesis, Harvard University, 1986.

[Coh93] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Number 138 in Graduate Texts in Mathematics. Springer-Verlag, 1993.

[Cre] J. E. Cremona. Elliptic curve data. `http://homepages.warwick.ac.uk/ masgaj/ftp/data/`. Updated 12 May 2014.

[Dar92] Henri Darmon. Heegner points, Heegner cycles, and congruences. In H. Kisilevsky and M. Ram Murty, editors, *Elliptic curves and related topics*, volume 4 of *CRM proceedings and lecture notes*, 1992.

[Gra] Andrew Granville. Binary quadratic forms. Course notes for MAT6684: Prime numbers theory. Available at [`http://www.dms.umontreal.ca/ andrew/Courses/Chapter4.pdf`].

[Gro91] Benedict H. Gross. Kolyvagin's work on modular elliptic curves. In *L-functions and arithmetic*, number 153 in London Math. Soc. Lecture Note, pages 235–256. Cambridge Univ. Press, 1991.

[Mil13] J.S. Milne. Algebraic number theory. `http://www.jmilne.org/math/CourseNotes/ANT.pdf`, 2013. version 3.05.

[Mol96] Richard A. Mollin. *Quadratics*. CRC Press, 1996.

[MT87] B. Mazur and J. Tate. Refined conjecture of the "Birch and Swinnerton-Dyer type". *Duke mathematical journal*, 54(2), 1987.

[PAR14] The PARI Group, Bordeaux. *PARI/GP, Version 2.6.1*, 2014. available from http://pari.math.u-bordeaux.fr/.

[Rob09] John Robertson. Computing in quadratic orders. http://www.jpr2718.org/quadr.pdf, November 2009.

[S^+14] W. A. Stein et al. *Sage Mathematics Software (Version 6.3)*. The Sage Development Team, 2014. http://www.sagemath.org.

[Sch75] Brian K. Schmidt. Quotients of the augmentation ideal of a group ring by powers of itself. *Illinois journal of mathematics*, 19(1):18–26, 1975.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Number 106 in Graduate Texts in Mathematics. Springer, second edition, 2009.

[Sim14] Nicolas Simard. The mazur-tate pairing and explicit homomorphisms between mordell-weil groups of ellptic curves and ideal class groups. Master's thesis, McGill University, 2014.

[ST92] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer, 1992.