Models of curves : the birch and Swinnerton-Dyer conjecture & ordinary reduction

Bommel, R. van

Chapter 2

The BSD conjecture for an elliptic curve over $\mathbb{Q}(\sqrt[4]{5}\,)$

Abstract. In this chapter we show that the Birch and Swinnerton-Dyer conjecture for a certain elliptic curve over $\mathbb{Q}(\sqrt[4]{5}\,)$ is equivalent to the same conjecture for a certain pair of hyperelliptic curves of genus 2 over $\mathbb{Q}$. We numerically verify the conjecture for these hyperelliptic curves. Moreover, we explain the methods used to find this example, which turned out to be a bit more subtle than expected.

2.1 Introduction

The Birch and Swinnerton-Dyer conjecture ([BiSw65]) has been generalised by Tate ([Tate66]) to abelian varieties of higher dimension and over general number fields.

Conjecture 2.1.1 (BSD, [Gros86, Conj. 2.10, p. 224])**.** *Let A/K be an abelian variety of dimension d and algebraic rank r over a number field K of discriminant Δ. Let $L(s)$ be its L-function, $A^\vee$ its dual, R its regulator,* Ш *its Tate-Shafarevich group and Ω the product of its real and complex periods. For each prime $\mathfrak{p}$ of $\mathcal{O}_K$, let $c_\mathfrak{p}$ be the Tamagawa number of A at $\mathfrak{p}$. Then* Ш *is finite, $L(s)$ admits an analytic continuation to $\mathbb{C}$ having a zero of order r at $s = 1$, and*

$$\lim_{s\to 1} (s-1)^{-r} L(s) = \frac{\Omega \cdot R \cdot |\text{Ш}| \cdot \prod_\mathfrak{p} c_\mathfrak{p}}{|A(K)_{\text{tors}}| \cdot |A^\vee(K)_{\text{tors}}| \cdot |\Delta|^{d/2}}.$$

In 1989, Kolyvagin ([Koly89, Koly91]) proved equality of the analytic and algebraic rank for modular elliptic curves over $\mathbb{Q}$ of analytic rank at most 1. After the proof of the modularity theorem ([BCDT01]), this part of the conjecture is now known for all elliptic curves over $\mathbb{Q}$ of analytic rank at most 1.

For elliptic curves with complex multiplication more is known. In 1991, Rubin ([Rub91]) proved the correctness of the p-part of BSD for elliptic curves over an imaginary quadratic field K with complex multiplication by K, analytic rank equal to 0, and p coprime to $|\mathcal{O}_K^*|$.

Originally, the Birch and Swinnerton-Dyer conjecture has been conceived based on numerical calculations with elliptic curves. In Chapter 1, we numerically verified the conjecture for hundreds of hyperelliptic curves of genus 2 and 3 over $\mathbb{Q}$, extending the work of Flynn, Leprévost, Schaefer, Stein, Stoll and Wetherell ([FLSSSW01]), who numerically verified BSD for 32 modular hyperelliptic curves of genus 2 over $\mathbb{Q}$, using modularity.

This verification consists of two parts. First, we check that the analytic rank (established numerically) and the algebraic rank are equal. Then we numerically compute all terms in the BSD formula except for $|Ш|$ (to more than 20 digits precision), and by rearranging the formula we deduce a predicted value for $|Ш|$. This will a priori be some real number, but if the BSD conjecture is true then it should in fact be the square of a positive integer, cf. earlier results of Poonen and Stoll ([PoSt99]). So if our conjectural value of $|Ш|$ is indeed the square of a positive integer to high precision, then this provides strong numerical evidence for the conjecture.

After finishing this verification, a natural question that arose was if the numerical verification for genus 2 curves over $\mathbb{Q}$, could provide us with examples of elliptic curves E over quadratic number fields for which BSD numerically seems to hold. The Weil restriction of E to $\mathbb{Q}$ is an abelian variety of dimension 2 over $\mathbb{Q}$ and might have the chance of being the Jacobian of a genus 2 curve over $\mathbb{Q}$. As the Jacobi locus is dense in the moduli space, one might expect this to happen very often. This was not the case. While trying many examples, all seemed to fail.

However, this Weil restriction becomes a product of two elliptic curves, after base change. The product of two elliptic curves, taken with the associated product polarisation, does not lie in the Jacobi locus. The best we could hope for is the existence of another polarisation, which makes it isomorphic (as polarised abelian variety) to the Jacobian of a curve of genus 2. This is actually only possible in a few special cases. By trying other polarisations in these special cases, we found an example of an elliptic curve over $\mathbb{Q}(\sqrt{5})$, whose Weil restriction is isogenous to the Jacobian of a curve of genus 2 over $\mathbb{Q}$. However, the isogeny was only defined over $\mathbb{Q}(\sqrt[8]{5}, i)$. We applied some reduction steps to reduce the size of this field and arrive at the following theorem

Theorem 2.1.2. *Let E over $\mathbb{Q}(\sqrt[4]{5})$ be the elliptic curve given by*

$$y^2 = x^3 + \sqrt[4]{5} \cdot x^2 - \left(5 + 3\sqrt{5}\right) \cdot x + \sqrt[4]{5}\left(5 + \sqrt{5}\right).$$

Let H and H' over $\mathbb{Q}$ be the hyperelliptic curves given by $y^2 = x^5 - x^3 + \frac{1}{5} \cdot x$, and $y^2 = x^5 - 5 \cdot x^3 + 5 \cdot x$, respectively. Then the generalised Birch and Swinnerton-Dyer conjecture holds for E over $\mathbb{Q}(\sqrt[4]{5})$ if and only if it holds for the Jacobians $\operatorname{Jac} H$ *and* $\operatorname{Jac} H'$ *over $\mathbb{Q}$.*

Finally, because of this reduction of the size of the field, we were able to numerically verify the BSD conjecture for the mentioned hyperelliptic curves.

We could also phrase the problem we solved as a moduli problem. For fixed N, we consider the space $\mathcal{M}$ of quintuples $(E_1, E_2, A, \phi, \rho)$, where E_1 and E_2 are elliptic curves, (A, ϕ) is a principally polarised abelian surface, and $\rho : E_1 \times E_2 \to A$ is an isogeny of degree N. If $\iota : \mathcal{M} \to \mathcal{M}$ is the involution that swaps E_1 and E_2, then our problem is the finding of rational points of $\mathcal{M}/\iota$, for which (A, ϕ) is the Jacobian of a smooth genus-2 curve with its natural principal polarisation.

This moduli problem (or variations thereof) has been studied extensively by others. This started with Hayashida and Nishi in [HaNi65]. More recently, there is work of Rodriguez-Villegas ([Rodr00]), Lange ([Lan06]), and Kani ([Kani14], [Kani16]). However, as far as we are aware, none of these results gives a way to control the size of the field of definition for the isogeny ρ, which is needed for our verification of the BSD conjecture.

The organisation of this chapter is as follows. In the first section, the final results will be shown, the equivalence of BSD for a certain elliptic curve over a quartic field and BSD for a certain pair of hyperelliptic curves of genus 2 over $\mathbb{Q}$. In the second section, the methods used to find this example will be demonstrated. First we study which elliptic curves could have the potential to become isogenous to the Jacobian of a genus 2 curve after Weil restriction. Then we explain how the required isogenies, which are very easy to find analytically, were algebraised. Finally, we describe some steps that had to be taken to reduce the size of the number field over which these maps are defined, which was actually necessary to be able to complete the verification.

The author wishes to thank his supervisors David Holmes and Fabien Pazuki. Moreover Maarten Derickx is thanked for useful discussions that led to improvements of this chapter.

2.2 Verification for an elliptic curve over $\mathbb{Q}(\sqrt[4]{5})$

Throughout this section, let E be the elliptic curve over $\mathbb{Q}(\sqrt[4]{5})$ given by the Weierstraß equation

$$y^2 = x^3 + \sqrt[4]{5} \cdot x^2 - \left(5 + 3\sqrt{5}\right) \cdot x + \sqrt[4]{5}\left(5 + \sqrt{5}\right).$$

Even though it has j-invariant $282880\sqrt{5} + 632000$, it is not the base change of an elliptic curve over $\mathbb{Q}(\sqrt{5})$, which can be verified using the isomorphism criteria from [Silv09, Sect. III.1, p. 42–51]. Even though the following lemma is not strictly necessary for the proof, it does turn out to be an important property of E.

Lemma 2.2.1. *The elliptic curve E geometrically has complex multiplication by $\mathbb{Z}[\sqrt{-5}]$.*

Proof. The Hilbert class polynomial for discriminant -20 is

$$x^2 - 1264000 \cdot x - 681472000,$$

see for example [BLP16, Table 2, p. 400]. Its zeros are $632000 \pm 282880\sqrt{5}$. The j-invariant for E is $632000 + 282880\sqrt{5}$, which proves that E geometrically has complex multiplication by $\mathbb{Z}[\sqrt{-5}]$. □

Let H be the hyperelliptic curve of genus 2 over $\mathbb{Q}$ given by the Weierstraß equation $y^2 = x^5 - x^3 + \frac{1}{5} \cdot x$. Let $H' \colon y^2 = x^5 - 5 \cdot x^3 + 5 \cdot x$ over $\mathbb{Q}$ be the quadratic twist of H over $\mathbb{Q}(\sqrt{5})$.

The following propositions will be used to prove Theorem 2.1.2.

Proposition 2.2.2. *Let* $K = \mathbb{Q}(\sqrt[4]{5})$ *and*

$$\varphi \colon H_K \to E \colon (x : y : 1) \mapsto (\varphi_x : \varphi_y : 1), \quad \textit{with}$$

$$\varphi_x = \frac{\sqrt{5} \cdot x^2 - \sqrt[4]{5} \cdot x + 1}{x}, \qquad \varphi_y = \frac{-\sqrt[4]{5}^3 \cdot xy + \sqrt{5} \cdot y}{x^2}$$

Then the map $\psi \colon H_{\mathbb{Q}(\sqrt{5})} \to W := \operatorname{Res}^K_{\mathbb{Q}(\sqrt{5})} E$ *naturally induced by* φ *induces an isogeny* $\nu \colon \operatorname{Jac} H_{\mathbb{Q}(\sqrt{5})} \to W$ *over* $\mathbb{Q}(\sqrt{5})$.

Proof. For the Weil restriction we have

$$W_K = E \times E',$$

where E' over K is the pull-back of E under the automorphism $\sigma \colon \sqrt[4]{5} \mapsto -\sqrt[4]{5}$ of K over $\mathbb{Q}(\sqrt{5})$. Using this identification, after base change, the map ψ becomes

$$\psi_K \colon H_K \overset{(\varphi,\varphi^\sigma)}{\longrightarrow} E \times E'.$$

Suppose that the map ν_K induced by ψ_K is not an isogeny. Then the image of ν_K in $E \times E'$ is an elliptic curve F over K and we have the following diagram.

$$\begin{tikzcd}
 & & & E \\
H_K \arrow[r, "\geq 2"] \arrow[urrr, "{\varphi,2}"] \arrow[drrr, "{\varphi^\sigma,2}"'] & F \arrow[r] \arrow[urr, "1"] \arrow[drr, "1"'] & E \times E' \arrow[ur] \arrow[dr] & \\
 & & & E'
\end{tikzcd}$$

As the morphisms φ and φ^σ are of degree 2, and the morphism $H_K \to F = \nu(H_K)$ is of degree at least 2, the two morphisms $F \to E$ and $F \to E'$ are of degree 1 and defined over K. Hence, E and E' must be isomorphic over K. Even though E and E' are isomorphic over $\mathbb{Q}(i, \sqrt[4]{5})$, it is easily verified that they are not isomorphic over K. Therefore, ν_K must be an isogeny and hence also ν is an isogeny. □

Remark 2.2.3. The map $\varphi\colon H_K \to E$ is the quotient of H_K by the automorphism

$$H_K \to H_K\colon \quad x \mapsto \frac{1}{\sqrt{5} \cdot x}, \quad y \mapsto \frac{-y}{\sqrt[4]{5}^3 \cdot x^3}.$$

In fact, the geometric automorphism group of H is the dihedral group D_4 of order 8, and the Jacobian of any curve of genus 2 over $\mathbb{Q}$ whose automorphism group is non-abelian, is isogenous to the square of an elliptic curve, over a finite extension of $\mathbb{Q}$, cf. [CGLR99, Lem. 2.4, p. 42]. Note that this result does not give control on the degree of the field extension needed to define the isogeny.

Now let us generalise the notion of quadratic twists of elliptic curves to abelian varieties over number fields.

Definition 2.2.4. Let A be an abelian variety over a number field K, and let $K \subset L$ be an extension of degree 2. Then the *L-quadratic twist* of A over L is the twist of A corresponding to the cocycle $\mathrm{Gal}(L/K) \to \mathrm{Aut}_L(A)$ mapping the non-trivial element $\sigma \in \mathrm{Gal}(L/K)$ to the automorphism $-1\colon A \to A$.

Example 2.2.5. Let $E\colon y^2 = x^3 + x$ over $\mathbb{Q}$. Then its $\mathbb{Q}(i)$-quadratic twist can be determined using the following procedure. Let $G = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \langle\sigma\rangle$. Then we consider the cocycle $\rho\colon G \to \mathrm{Aut}_{\mathbb{Q}(i)}(E)$ mapping σ to -1.

Let $R = \mathbb{Q}(i)(x)[y]/(y^2 - x^3 - x)$ be the function field of E over $\mathbb{Q}(i)$. Then the group G already acts on $\mathbb{Q}(i)$. We extend this action to R by $g \cdot x = \rho(g)(x)$ and $g \cdot y = \rho(g)(y)$ for $g \in G$, i.e. G acts trivially on these coordinates except for $\sigma \cdot y = -y$.

Next, we compute $R^G = \mathbb{Q}(x, iy) \subset R$, and note that $R^G \cong \mathbb{Q}(x)[y]/(-y^2 - x^3 - x)$. Hence, the $\mathbb{Q}(\sqrt{-1})$-quadratic twist is $E'\colon -y^2 = x^3 + x$, as in the classical theory.

Note that E and E' are actually isomorphic over $\mathbb{Q}$ in this case. So, the quadratic twist does not have to be non-trivial. In fact, there is a non-trivial twist of E over $\mathbb{Q}(i)$, which is given by $E''\colon y^2 = x^3 - 4x$. It can be obtained by twisting using the cocycle $G \to \mathrm{Aut}_{\mathbb{Q}(i)}(E)$ mapping σ to the automorphism

$$E_{\mathbb{Q}(i)} \to E_{\mathbb{Q}(i)}\colon \quad x \mapsto -x, \quad y \mapsto iy.$$

The following proposition is probably well-known to the experts.

Proposition 2.2.6. *Let A be an abelian variety over a number field K, and let $K \subset L$ be an extension of degree 2. Then the Weil restriction $W := \mathrm{Res}_K^L A_L$ of the base change A_L to K is isogenous to the product $A \times A'$, where A' over K is the L-quadratic twist of A.*

Proof. Recall that $\operatorname{Hom}_K(T, W) = \operatorname{Hom}_L(T_L, A_L)$ for any scheme T over K. Consider the morphism $\nu\colon A \times A' \to W$, given by the morphism

$$\kappa\colon A_L \times A'_L \to A_L\colon (x, y) \mapsto x + \rho(y),$$

where the isomorphism $\rho : A'_L \cong A_L$ comes from the twist data. Then the map

$$\nu_L\colon A_L \times A'_L \to A_L \times A^\sigma_L$$

is given by κ on the first component and κ^σ on the second component, where $\sigma\colon L \to L$ is the non-trivial element of $\operatorname{Gal}(L/K)$. Then κ^σ is

$$A_L \times A'_L \to A^\sigma_L = A_L\colon (x, y) \mapsto \sigma(x) + \rho(\sigma(y)).$$

As $\rho(\sigma(y)) = -\sigma(\rho(y))$, by definition of the L-quadratic twist, we now find that the kernel of ν_L is finite and that ν is an isogeny. □

Example 2.2.7. For example, for an elliptic curve $E\colon y^2 = f(x)$ over K, the L-quadratic twist is the curve $E'\colon dy^2 = f(x)$ over K and the isomorphism ρ is given by $E'_L \to E_L\colon (x, y) \mapsto (x, y/\sqrt{d})$, and

$$\nu_L\colon E_L \times E'_L \to E_L \times E_L\colon (x, y) \mapsto (x + \rho(y), \sigma(x - \rho(y))).$$

The kernel of ν_L consists of the pairs $(x, \rho^{-1}(x))$ where $x \in E[2]$. Hence, the isogeny $E \times E' \to W$ has degree 4.

Proposition 2.2.8. *Let A and B be abelian varieties over a number field K, let $K \subset L$ be a finite extension of number fields and let C be an abelian variety over L. Then*

(1) BSD holds for $A \times B$ over K if and only if it holds for A and B over K;

(2) if A and B are isogenous over K, then BSD holds for A over K if and only if it holds for B over K;

(3) BSD holds for the Weil restriction $\operatorname{Res}^L_K C$ over K if and only if it holds for C over L;

(4) if L/K is quadratic, BSD holds for the base change A_L over L if and only if it holds for A over K and its L-quadratic twist A' over K.

Proof. For (1) and (2), see [Tate66, p. 422]. For (3), see [Mil72]. In the case L/K is a quadratic extension, $\operatorname{Res}^L_K A_L$ is isogenous over K to $A \times A'$, where A'/K is the L-quadratic twist of A, cf. Prop. 2.2.6 or [Kida95, Thm., p. 53]. Now (4) follows from (1), (2) and (3). □

Proof (Theorem 2.1.2). By Proposition 2.2.8 part (4), BSD holds for $\operatorname{Jac} H$ and $\operatorname{Jac} H'$ over $\mathbb{Q}$ if and only if it holds for $\operatorname{Jac} H_{\mathbb{Q}(\sqrt{5})}$ over $\mathbb{Q}(\sqrt{5})$. The latter is isogenous over $\mathbb{Q}(\sqrt{5})$ to $\operatorname{Res}^{\mathbb{Q}(\sqrt[4]{5})}_{\mathbb{Q}(\sqrt{5})} E$ by Proposition 2.2.2. Hence, by parts (2) and (3) of Proposition 2.2.8, BSD holds for $\operatorname{Jac} H_{\mathbb{Q}(\sqrt{5})}$ over $\mathbb{Q}(\sqrt{5})$ if and only if it holds for E over $\mathbb{Q}(\sqrt[4]{5})$. □

Using the methods in Chapter 1, we can numerically verify that the Birch and Swinnerton-Dyer conjecture holds for $\operatorname{Jac} H$ and $\operatorname{Jac} H'$ in the following sense. We numerically verified that the analytic and algebraic rank agree, and we computed all terms except for $|Ш|$, with more than 20 digits precision. Then we used the conjectural formula to predict the order of Ш. This predicted order, $|Ш_{\mathrm{an}}|$, appears to equal 1 in both cases. This gives strong evidence for the conjecture, especially since 1 is the square of an integer, which is to be expected according to [PoSt99].

In fact, we found the following values for the BSD-invariants:

	$\operatorname{Jac} H$	$\operatorname{Jac} H'$
r	1	1
$\lim_{s\to 1}(s-1)^{-r}L(s)$	4.54183774632835249986	4.54183774632835249986
R	4.70213971014416647713	0.94042794202883329543
Ω	1.93181743899697988452	9.65908719498489942260
$c_{\mathfrak{p}}$	$c_2 = 1,\ c_5 = 2$	$c_2 = 1,\ c_5 = 2$
$\lvert J_{\mathrm{tors}}\rvert$	2	2
$Ш_{\mathrm{an}}$	1.00000000000000000000	1.00000000000000000000

Remark 2.2.9. The values of these invariants suggest that $\operatorname{Jac} H$ and $\operatorname{Jac} H'$ are isogenous; they all seem to differ by an integer multiple. Since, the numerical verification succeeded for both curves, the author did not try to actually find an isogeny.

2.3 Methodology

In this section, I will try to answer the question how you find an elliptic curve E over a number field K, with $L \subset K$ of degree 2, such that its Weil restriction to L is isogenous as abelian variety (without fixed polarisation) to the base change of a Jacobian of a hyperelliptic curve of genus 2 defined over $\mathbb{Q}$.

2.3.1 Which elliptic curves?

The product of two elliptic curves over a number field, E and E', taken with the associated product polarisation, does not lie in the Jacobi locus in the moduli space of polarised abelian varieties, cf. [Weil57, Satz 2, p. 37]. However, in some cases it might happen that the abelian variety has another polarisation which makes it into the Jacobian of a smooth curve of genus 2. Heuristically, most polarised abelian varieties lie in the Jacobi locus, but also most polarised abelian varieties have only one polarisation, up to multiplication by an integer. So, heuristically it is not so clear whether such E and E' actually exist. Hence, we should be looking for elliptic curves E and E', such that $E \times E'$ contains a smooth curve of genus 2.

The work of Hayashida and Nishi, [HaNi65], contains sufficient conditions on E and E' for this situation to arise. In particular, [HaNi65, Thm., §4, p. 14] states: if E and E' have complex multiplication by the principal order of the imaginary quadratic field $\mathbb{Q}(\sqrt{-m})$ and m is not 1, 3, 7 or 15, then $E \times E'$ contains a smooth curve of genus 2.

2.3.2 Reconstruction of the hyperelliptic curve

Assume that E over K geometrically has complex multiplication by $\mathcal{O}_{-m} = \mathbb{Z}[\alpha_m]$, where

$$\alpha_m = \begin{cases} \sqrt{-m} & \text{if } m \not\equiv 3 \mod 4; \\ \frac{1}{2}(\sqrt{-m}+1) & \text{if } m \equiv 3 \mod 4. \end{cases}$$

Now consider the complexification $E_{\mathbb{C}}$ and fix an embedding of $\mathcal{O}_{-m}$ in $\mathbb{C}$. Then $E_{\mathbb{C}} \cong \mathbb{C}/\Lambda$, where Λ is a lattice of the form $\mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \frac{\beta}{\gamma}$ with β and $\gamma \neq 0$ generating, as $\mathbb{Z}$-module, an ideal of $\mathcal{O}_{-m}$. Moreover, $E_{\mathbb{C}}$ has a Hermitian form, whose imaginary part, without loss of generality, gives the standard antisymmetric form

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

on Λ, with respect to the basis just given.

The idea is now to consider the complex lattice $\mathbb{Z}\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) + \mathbb{Z}\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) + \mathbb{Z}\left(\begin{smallmatrix} \alpha_m \\ 0 \end{smallmatrix}\right) + \mathbb{Z}\left(\begin{smallmatrix} 0 \\ \alpha_m \end{smallmatrix}\right)$ inside $\mathbb{C}^2$. We try to put other antisymmetric forms on the lattice, and for each such a form, we choose a basis, such that the antisymmetric form with respect to this basis is of the standard form

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

After this, we apply a transformation in $\mathrm{GL}_2(\mathbb{C})$ to obtain a basis that is of the form $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} w_1 \\ w_2 \end{smallmatrix}\right)$, cf. [Sch89, §5]. If the antisymmetric form satisfies the Riemann relations, cf. [Lang82, Lem. 1.1 & 1.2, Chap. VII, §1, p. 132], then the matrix

$$M = \begin{pmatrix} v_1 & w_1 \\ v_2 & w_2 \end{pmatrix}$$

will be symmetric and its imaginary part will be positive definite, i.e. M has the potential to be the small period matrix of a hyperelliptic curve H of genus 2.

One can then evaluate the theta functions in M and use these to reconstruct the Igusa invariants of H. These Igusa invariants can only be computed numerically, up to a certain precision, but we expect them to be rational. If the precision is high enough, we can guess the rational values for the Igusa invariants. Then we can use Mestre's algorithm ([Mes91]) to construct a hyperelliptic curve with these Igusa invariants. This part of the reconstruction procedure is explained in more detail in [Weng03].

2.3.3 Constructing algebraic maps

Now we are in the situation that we found an elliptic curve E over K and a hyperelliptic curve H over $\mathbb{Q}$ (i.e. given with explicit equations in $\mathbb{P}^2$ over K and $\mathbb{Q}$, respectively), such that the base change of $E \times E$ and $J := \mathrm{Jac}(H)$ to $\mathbb{C}$ numerically seem to be isogenous. If such an isogeny exists, we know by GAGA that it is algebraisable and defined over a finite extension of K. The only problem that remains is to find such an algebraic isogeny explicitly.

It is possible to numerically construct an analytic isogeny $\tau\colon H_{\mathbb{C}} \to J_{\mathbb{C}} \to E_{\mathbb{C}} \times E_{\mathbb{C}}$. We consider the four composite maps

$$\begin{tikzcd} \tau_{1,x}, \tau_{1,y}, \tau_{2,x}, \tau_{2,y}\colon H_{\mathbb{C}} \arrow[r] & E_{\mathbb{C}} \times E_{\mathbb{C}} \arrow[r, shift left] \arrow[r, shift right] & E_{\mathbb{C}} \arrow[r, shift left, "x"] \arrow[r, shift right, "y"'] & \mathbb{P}^1_{\mathbb{C}} \end{tikzcd},$$

where the middle two maps are the two projections, and x and y are coordinate maps, and try to 'guess' them. We assume that the map $\tau_{1,x}\colon H_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ (and analogously for $\tau_{1,y}, \tau_{2,x}, \tau_{2,y}$) is of the shape

$$(x, y) \mapsto \frac{\sum_{i=0}^{N} \sum_{j=0}^{1} a_{i,j} x^i y^j}{\sum_{i=0}^{M} \sum_{j=0}^{1} b_{i,j} x^i y^j},$$

for certain $a_{i,j}, b_{i,j} \in \mathbb{C}$ and $N, M \in \mathbb{Z}_{\geq 0}$. We pick $R := 2N+2M$ complex-valued points $P_k := (\alpha_k, \beta_k) \in H_{\mathbb{C}}(\mathbb{C})$ for $k = 1, \ldots, R$ and numerically compute $Q_k := \tau_{1,x}(P_k)$. Each such point gives rise to a linear equation

$$\sum_{i=0}^{N} \sum_{j=0}^{1} a_{i,j} \alpha_k^i \beta_k^j - Q_k \cdot \sum_{i=0}^{M} \sum_{j=0}^{1} b_{i,j} \alpha_k^i \beta_k^j = 0$$

in the coefficients $a_{i,j}$ and $b_{i,j}$. Or, to phrase it in other words, the vector of coefficients $(a_{0,0}, \ldots, a_{N,1}, b_{0,0}, \ldots, b_{M,1})$ is in the kernel of the matrix

$$A = \begin{pmatrix} \alpha_1^0 \beta_1^0 & \cdots & \alpha_1^N \beta_1^1 & -Q_1 \alpha_1^0 \beta_1^0 & \cdots & -Q_1 \alpha_1^M \beta_1^0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_R^0 \beta_R^0 & \cdots & \alpha_R^N \beta_R^1 & -Q_R \alpha_R^0 \beta_R^0 & \cdots & -Q_R \alpha_R^M \beta_R^1 \end{pmatrix}.$$

We can compute this kernel numerically and choose N and M such that the kernel is 1-dimensional. In this way, we can be sure to find a basis vector, which is a $\mathbb{C}$-multiple of a vector with algebraic entries, instead of obtaining a random $\mathbb{C}$-linear combination of two or more.

We compute a generator for the kernel and rescale it to make one of the non-zero entries equal to 1. Then we use LLL to guess algebraic relations for the other entries. In this way, we found a solution $(a_{0,0}, \ldots, b_{M,1}) \in \overline{\mathbb{Q}}^R$ and, if M and N were chosen appropriately, it can be verified algebraically that these functions indeed define a morphism $\varphi\colon H_L \to E_L \times E_L$, where L is the field extension of K generated by all $a_{i,j}, b_{i,j}$, whose base change to $\mathbb{C}$ is $((\tau_{1,x}, \tau_{1,y}), (\tau_{2,x}, \tau_{2,y}))$.

2.3.4 Smaller fields

A priori, the field L might be way too big for a feasible numerical verification of BSD. For example, in our specific case, a priori the curve H and E were defined over $\mathbb{Q}$ and

$\mathbb{Q}(\sqrt{5}\,)$, respectively, but the maps φ and ψ were only defined over $L = \mathbb{Q}(\sqrt[8]{5}, i)$ and $\varphi\colon H \to E\colon (x : y : 1) \mapsto (\varphi_x : \varphi_y : 1)$ was given by

$$\varphi_x = \frac{\frac{1}{2}i\sqrt[4]{5}\cdot x^4 - x^3 - \frac{1}{2}i\left(\frac{4}{5}\sqrt[4]{5}^3 - \sqrt[4]{5}\right)\cdot x^2 + \frac{1}{5}\sqrt{5}\cdot x + \frac{1}{10}i\sqrt[4]{5}}{x^3 + \frac{2i}{5}\sqrt[4]{5}^3\cdot x^2 - \frac{1}{5}\sqrt{5}\cdot x},$$

$$\varphi_y = \frac{\frac{1}{4}\varepsilon\sqrt[8]{5}^3\cdot x^4y + \delta\sqrt[8]{5}\cdot x^3y - \frac{1}{4}\varepsilon\left(\frac{4}{5}\sqrt[8]{5}^7 + \sqrt[8]{5}^3\right)\cdot x^2y - \frac{\delta}{5}\sqrt[8]{5}^5\cdot xy + \frac{1}{20}\varepsilon\sqrt[8]{5}^3\cdot y}{x^5 + \frac{3i}{5}\sqrt[4]{5}^3\cdot x^4 - \frac{3}{5}\sqrt{5}\cdot x^3 - \frac{1}{5}i\sqrt[4]{5}\cdot x^2},$$

where $\varepsilon = 1 - i$ and $\delta = 1 + i$. Of course this still proves that $\operatorname{Jac} H_L$ and $E_L \times E_L$ are isogenous.

However, it is not feasible yet to numerically verify BSD for H_L. The situation is not as good as in Proposition 2.2.8 part (4). In the isogeny decomposition of the Weil restriction $\operatorname{Res}^L_{\mathbb{Q}(\sqrt{5})}\operatorname{Jac}(H_L)$, there will not only be twists of $\operatorname{Jac} H$ occuring, but also higher dimensional factors, see also [DiNa03]. Even if we are lucky, and all these factors are Jacobians of hyperelliptic curves over $\mathbb{Q}$, these curves will be of genus greater than 3. Numerical verification of BSD for such curves might take too much time.

In order to reduce the size of L and reduce to the case of a quadratic field extension, we performed some twists, for example on E by $\varepsilon\sqrt[8]{5}$ and on H by -1. We then repeated the procedure in the previous paragraph and even managed to find a map of smaller degree over the smaller field $\mathbb{Q}(\sqrt[4]{5})$.

Having found the appropriate map defined over $\mathbb{Q}(\sqrt[4]{5})$, we were able to get the result in Proposition 2.2.2 in order to finally prove Theorem 2.1.2.