Arch. Math. 114 (2020), 159–169

0003-889X/20/020159-11
published online October 3, 2019
https://doi.org/10.1007/s00013-019-01383-w

Archiv der Mathematik

The Birch and Swinnerton-Dyer conjecture for an elliptic curve over $\mathbb{Q}(\sqrt[4]{5})$

Raymond van Bommel

Abstract. In this paper, 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.

Mathematics Subject Classification. 11G40, 11G10, 11G30, 14H40, 14K02.

Keywords. Birch-Swinnerton-Dyer conjecture, Jacobians, Curves, Isogeny.

1. Introduction.

The Birch and Swinnerton-Dyer conjecture [1] has been generalised by Tate [22] to Abelian varieties of higher dimension and over general number fields.

Conjecture 1 (BSD, [6, 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*

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

In 1989, Kolyvagin [13,14] proved the 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 [2], 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 [19] 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 was conceived based on numerical calculations with elliptic curves. In [23], the author 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 [5], 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 [17]. 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. *Let E over $\mathbb{Q}\left(\sqrt[4]{5}\right)$ 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 $\mathbb{Q}\left(\sqrt[4]{5}\right)$ if and only if it holds for the Jacobians $\mathrm{Jac}H$ and $\mathrm{Jac}H'$ over $\mathbb{Q}$.

Finally, we were able to numerically verify the BSD conjecture for the aforementioned hyperelliptic curves. Note that most of the BSD-invariants of E could also be computed directly, but that the currently available methods to

compute the special value of the L-function do not finish in reasonable time: this computation did not finish within 100 h of CPU time. The main reason for this is that the norm of the conductor of E, 1 638 400, is still fairly large.

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 $\rho\colon E_1 \times E_2 \to A$ is an isogeny of degree N. If $\iota\colon \mathcal{M} \to \mathcal{M}$ 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 theorem) has been studied extensively by others. This started with Hayashida and Nishi in [7]. More recently, there is work of Rodriguez-Villegas [18], Lange [9], and Kani [10,11]. 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 article 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 Ph.D. supervisors David Holmes and Fabien Pazuki. He also thanks Maarten Derickx and an anonymous referee for useful discussions and comments that lead to improvements of this article.

2. Verification for an elliptic curve over $\mathbb{Q}\left(\sqrt[4]{5}\right)$. Throughout this section, let E be the elliptic curve over $\mathbb{Q}\left(\sqrt[4]{5}\right)$ 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 by comparing the c-invariants of both curves, as described in [21, Section III.1, pp. 42–51]. The curve 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.

Proposition 3. *Let* $K = \mathbb{Q}\big(\sqrt[4]{5}\big)$ *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 $\psi\colon H_{\mathbb{Q}(\sqrt{5})} \to W := \mathrm{Res}^K_{\mathbb{Q}(\sqrt{5})} E$ *naturally induced by* φ *induces an isogeny* $\nu\colon \mathrm{Jac}H_{\mathbb{Q}(\sqrt{5})} \to W$ *over* $\mathbb{Q}(\sqrt{5})$.

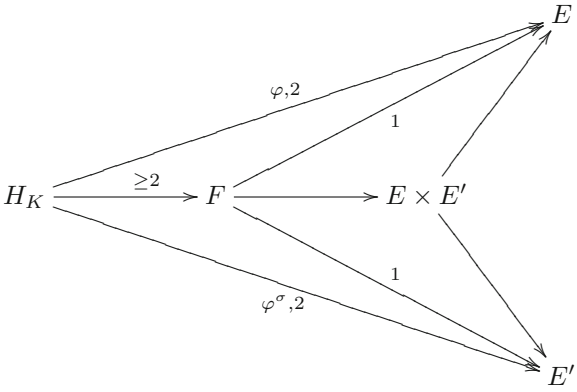
Proof. For the Weil restriction, we have

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

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

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

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.



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 $\mathbb{Q}\big(i, \sqrt[4]{5}\big)$, 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 4. 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. [3, Lemma 2.4, p. 42]. We remark 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 5. 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 $-1\colon A \to A$.

Proposition 6. *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 $\mathrm{Res}^L_K C$ 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 [22, p. 422]. For (3), see [16]. In the case that L/K is a quadratic extension, $\mathrm{Res}^L_K A_L$ is isogenous over K to $A \times A'$, where A'/K is the L-quadratic twist of A, cf. [12, Theorem, p. 53]. Now (4) follows from (1), (2), and (3). □

Proof of Theorem 2. By Proposition 6 part (4), BSD holds for $\mathrm{Jac}H$ and $\mathrm{Jac}H'$ over $\mathbb{Q}$ if and only if it holds for $\mathrm{Jac}H_{\mathbb{Q}(\sqrt{5})}$ over $\mathbb{Q}(\sqrt{5})$. The latter is isogenous over $\mathbb{Q}(\sqrt{5})$ to $\mathrm{Res}^{\mathbb{Q}(\sqrt[4]{5})}_{\mathbb{Q}(\sqrt{5})} E$ by Proposition 3. Hence, by parts (2) and (3) of Proposition 6, BSD holds for $\mathrm{Jac}H_{\mathbb{Q}(\sqrt{5})}$ over $\mathbb{Q}(\sqrt{5})$ if and only if it holds for E over $\mathbb{Q}\big(\sqrt[4]{5}\big)$. □

Using the methods in [23], we can numerically verify that the Birch and Swinnerton-Dyer conjecture holds for $\mathrm{Jac}H$ and $\mathrm{Jac}H'$ 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 [17] since both hyperelliptic curves have rational points.

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

	Jac$H$	JacH'	E
r	1	1	2
$\lim_{s\to 1}(s-1)^{-r}L(s)$	4.5418377463	4.5418377463	*did not finish*
R	4.7021397101	0.9404279420	1.1055058927
Ω	1.9318174390	9.6590871950	52.155148222
$c_{\mathfrak{p}}$	$c_2 = 1$, $c_5 = 2$	$c_2 = 1$, $c_5 = 2$	$c_{\mathfrak{p}_2} = 1$, $c_{\mathfrak{p}_5} = 2$
$\lvert J_{\mathrm{tors}}\rvert$	2	2	2
$Ш_{\mathrm{an}}$	1.0000000000	1.0000000000	

We included some of the BSD-invariants for E as well for completeness. Here $\mathfrak{p}_2$ and $\mathfrak{p}_5$ are the unique primes lying over 2 and 5, respectively, in $\mathcal{O}_{\mathbb{Q}(\sqrt[4]{5})}$.

Remark 7. The values of these invariants suggest that Jac$H$ and JacH' 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.

3. Methodology. In this section, we 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 to the Jacobian of a hyperelliptic curve of genus 2 defined over $\mathbb{Q}$ as Abelian varieties (without fixed polarisation).

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. [24, 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. In any case, 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 [7] contains sufficient conditions on E and E' for this situation to arise. In particular, [7, Theorem, §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.

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 Γ, 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 again 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. [20, §5]. If the antisymmetric form satisfies the Riemann relations, cf. [8, Lemma 1.1 & 1.2, Chapter 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 [15] to construct a hyperelliptic curve with these Igusa invariants. This part of the reconstruction procedure is explained in more detail in [25].

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 $\mathbb{Q}$, 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 $\tau : H_{\mathbb{C}} \to J_{\mathbb{C}} \to E_{\mathbb{C}} \times E_{\mathbb{C}}$. We consider two composite maps

$$\tau_1, \tau_2 : \; H_{\mathbb{C}} \longrightarrow E_{\mathbb{C}} \times E_{\mathbb{C}} \rightrightarrows E_{\mathbb{C}}$$

and try to 'guess' them. We assume that the map $\tau_1 : H_{\mathbb{C}} \to E_{\mathbb{C}}$ 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 $Q_k := \tau_1(P_k)$. 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 $\varphi{:}H_L \to E_L$, where $L = K(a_{0,0}, \ldots, b_{M,1})$, whose base change to $\mathbb{C}$ is τ_1.

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

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

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

where $\varepsilon = 1 - i$ and $\delta = 1 + i$. Of course this still proves that $\mathrm{Jac}H_L$ 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 6 part (4). In the isogeny decomposition of the Weil restriction $\mathrm{Res}^L_{\mathbb{Q}(\sqrt{5})}\mathrm{Jac}(H_L)$, there will not only be twists of $\mathrm{Jac}H$ occurring, but also higher dimensional factors, see also [4]. 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 extension of fields, 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 found 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 3 in order to finally prove Theorem 2.

References

[1] Birch, B.J., Swinnerton-Dyer, H.P.F.: Notes on elliptic curves. II. J. Reine Angew. Math. **218**, 79–108 (1965)

[2] Breuil, C., Conrad, B., Diamond, F., Taylor, R.: On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. J. Am. Math. Soc. **14**(4), 843–939 (2001)

[3] Cardona, G., González, J., Lario, J.C., Rio, A.: On curves of genus 2 with Jacobian of GL_2-type. Manuscr. Math. **98**(1), 37–54 (1999)

[4] Diem, C., Naumann, N.: On the structure of Weil restrictions of Abelian varieties. J. Ramanujan Math. Soc. **18**(2), 153–174 (2003)

[5] Flynn, E.V., Leprévost, F., Schaefer, E.F., Stein, W.A., Stoll, M., Wetherell, J.: Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves. Math. Comput. **70**(236), 1675–1697 (2001)

[6] Gross, B.H.: On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication. In: Koblitz, N. (ed.) Number Theory Related to Fermat's Last Theorem (Cambridge, MA, 1981). Progress in Mathematics, vol. 26, pp. 219–236. Birkhäuser, Boston, MA (1982)

[7] Hayashida, T., Nishi, M.: Existence of curves of genus two on a product of two elliptic curves. J. Math. Soc. Jpn. **17**, 1–16 (1965)

[8] Lang, S.: Introduction to Algebraic and Abelian Functions. Graduate Texts in Mathematics, vol. 89, 2nd edn. Springer, New York (1982)

[9] Lange, H.: Principal polarizations on products of elliptic curves. In: Porras, J.M.M., Popescu, S., Rodríguez, R.E. (eds.) The Geometry of Riemann Surfaces and Abelian Varieties. Contemporary Mathematics, vol. 397, pp. 153–162. American Mathematical Society, Providence, RI (2006)

[10] Kani, E.: Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms. J. Number Theory **139**, 138–174 (2014)

[11] Kani, E.: The moduli space of Jacobians isomorphic to a product of two elliptic curves. Collect. Math. **67**(1), 21–54 (2016)

[12] Kida, M.: Galois descent and twists of an Abelian variety. Acta Arith. **73**(1), 51–57 (1995)

[13] Kolyvagin, V.A.: Finiteness of $E(\mathbb{Q})$ and Ш$(E, \mathbb{Q})$ for a subclass of Weil curves. Math. **32**(3), 523–541 (1989)

[14] Kolyvagin, V.A.: On the Mordell–Weil group and the Shafarevich–Tate group of modular elliptic curves. In: International Congress of Mathematicians, vol. I, II (Kyoto, 1990), pp. 429–436. The Mathematical Society of Japan, Tokyo (1991)

[15] Mestre, J.-F.: Construction de courbes de genre 2 à partir de leurs modules. In: Mora, T., Traverso, C. (eds.) Effective Methods in Algebraic Geometry (Castiglioncello, 1990). Progress in Mathematics, vol. 94, pp. 313–334. Birkhäuser Boston, Boston, MA (1991)

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

[17] Poonen, B., Stoll, M.: The Cassels–Tate pairing on polarized Abelian varieties. Ann. Math. **150**(3), 1109–1149 (1999)

[18] Rodriguez-Villegas, F.: Explicit models of genus 2 curves with split CM. In: Bosma, W. (ed.) Algorithmic Number Theory (Leiden, 2000). Lecture Notes in Computer Science, vol. 1838, pp. 505–513. Springer, Berlin (2000)

[19] Rubin, K.: The "main conjectures" of Iwasawa theory for imaginary quadratic fields. Invent. Math. **103**(1), 25–68 (1991)

[20] Schlichenmaier, M.: An Introduction to Riemann Surfaces, Algebraic Curves and Moduli Spaces. Lecture Notes in Physics, vol. 322. Springer, Berlin (1989)

[21] Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, vol. 106, 2nd edn. Springer, Dordrecht (2009)

[22] Tate, J.: On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. Sém. Bourbaki **9**, 415–440 (1995)

[23] van Bommel, R.: Numerical verification of the Birch and Swinnerton-Dyer conjecture for hyperelliptic curves of higher genus over $\mathbb{Q}$ up to squares. ArXiv e-prints (2017). arXiv:1711.10409

[24] Weil, A.: Zum Beweis des Torellischen Satzes. Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa. **1957**, 33–53 (1957)

[25] Weng, A.: Constructing hyperelliptic curves of genus 2 suitable for cryptography. Math. Comput. **72**(241), 435–458 (2003)

Raymond van Bommel
Mathematisch Instituut
Universiteit Leiden
Niels Bohrweg 1
2333 CA Leiden
The Netherlands
e-mail: bommel@uni-mainz.de

Present Address
Raymond van Bommel
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
02139 Cambridge, MA
USA

Received: 2 May 2019