Comptes Rendus
Mathématique
Draft

Exact verification of the strong BSD conjecture for some absolutely simple abelian surfaces

Vérification exacte de la conjecture BSD forte pour certaines variétés abéliennes absolument simples

Timo Keller [a] **and Michael Stoll** [a]

[a] Lehrstuhl Mathematik II (Computeralgebra), Universität Bayreuth, Universitätsstraße 30, 95440 Bayreuth, Germany

E-mails: Timo.Keller@uni-bayreuth.de (T. Keller), Michael.Stoll@uni-bayreuth.de (M. Stoll)

Abstract. Let X be one of the 28 Atkin-Lehner quotients of a curve $X_0(N)$ such that X has genus 2 and its Jacobian variety J is absolutely simple. We show that the Shafarevich-Tate group $Ш(J/\mathbb{Q})$ is trivial. This verifies the strong BSD conjecture for J.

Résumé. Soit X un des 28 quotients d'Atkin-Lehner d'une courbe $X_0(N)$ tel que X est de genre 2 et sa jacobienne J est absolument simple. On démontre que le groupe de Shafarevich-Tate $Ш(J/\mathbb{Q})$ est trivial. Ceci vérifie la conjecture BSD forte pour J.

2020 Mathematics Subject Classification. 11G40 (11-04, 11G10, 11G30, 14G35).

Funding. This work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – Projektnummer STO 299/18-1, AOBJ: 667349.

This article is a draft (not yet accepted!)

1. Introduction

Let A be an abelian variety over $\mathbb{Q}$ and assume that its L-series $L(A,s)$ admits an analytic continuation to the whole complex plane. The *weak BSD conjecture* (or BSD rank conjecture) predicts that the Mordell-Weil rank $r = \operatorname{rk} A(\mathbb{Q})$ of A equals the analytic rank $r_{\text{an}} = \operatorname{ord}_{s=1} L(A,s)$. The *strong BSD conjecture* asserts that the Shafarevich-Tate group $Ш(A/\mathbb{Q})$ is finite and that its order equals the "analytic order of Sha",

$$\#Ш(A/\mathbb{Q})_{\text{an}} := \frac{\#A(\mathbb{Q})_{\text{tors}} \cdot \#A^\vee(\mathbb{Q})_{\text{tors}}}{\prod_v c_v} \cdot \frac{L^*(A,1)}{\Omega_A \operatorname{Reg}_{A/\mathbb{Q}}}. \tag{1}$$

Here $A^\vee$ is the dual abelian variety, $A(\mathbb{Q})_{\text{tors}}$ denotes the torsion subgroup of $A(\mathbb{Q})$, the product $\prod_v c_v$ runs over all finite places of $\mathbb{Q}$ and c_v is the Tamagawa number of A at v, $L^*(A,1)$ is the

ISSN (electronic) : 1778-3569

leading coefficient of the Taylor expansion of $L(A,s)$ at $s=1$, and Ω_A and $\mathrm{Reg}_{A/\mathbb{Q}}$ denote the volume of $A(\mathbb{R})$ and the regulator of $A(\mathbb{Q})$, respectively.

If A is *modular* in the sense that A is an isogeny factor of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$ for some N, then the analytic continuation of $L(A,s)$ is known. If A is in addition absolutely simple, then A is associated (up to isogeny) to a Galois orbit of size $\dim(A)$ of newforms of weight 2 and level N, such that $L(A,s)$ is the product of $L(f,s)$ with f running through these newforms. Such an abelian variety has *real multiplication*: its endomorphism ring over $\mathbb{Q}$ is an order in a totally real number field of degree $\dim(A)$. If, furthermore, $\mathrm{ord}_{s=1} L(f,s) \in \{0,1\}$ for one (equivalently, all) such f, then the weak BSD conjecture holds for A; see [13].

All elliptic curves over $\mathbb{Q}$ arise as one-dimensional modular abelian varieties [3, 21, 25] such that N is the conductor of A. For all elliptic curves of (analytic) rank ≤ 1 and $N < 5000$, the strong BSD conjecture has been verified [7, 10, 15].

In this note, we consider certain absolutely simple abelian *surfaces* and show that strong BSD holds for them. One class of such surfaces arises as the Jacobians of quotients X of $X_0(N)$ by a group of Atkin-Lehner operators. Hasegawa [12] has determined the complete list of such X of genus 2; 28 of them have absolutely simple Jacobian J. For most of these Jacobians (and those of further curves taken from [24]), it has been numerically verified in [1, 9] that $\#\text{Ш}(J/\mathbb{Q})_{\mathrm{an}}$ is very close to an integer, which equals $\#\text{Ш}(J/\mathbb{Q})[2]$ (= 1 in the cases considered here). We complete the verification of strong BSD for these Jacobians by showing that $\#\text{Ш}(J/\mathbb{Q})_{\mathrm{an}}$ is indeed an integer and $\text{Ш}(J/\mathbb{Q})$ is trivial.

2. Methods and algorithms

In the following, we denote the abelian surface under consideration by A; it is an absolutely simple isogeny quotient of $J_0(N)$, defined over $\mathbb{Q}$. We frequently use the fact that A can be obtained as the Jacobian variety of a curve X of genus 2. The algorithms described below have been implemented in Magma [2].

Recall that a *Heegner discriminant* for A is a fundamental discriminant $D < 0$ such that for $K = \mathbb{Q}(\sqrt{D})$, the analytic rank of A/K equals $\dim A = 2$ and all prime divisors of N split in K. Heegner discriminants exist by [4, 23]. Since Magma can determine whether $\mathrm{ord}_{s=1} L(f,s)$ is 0, 1, or larger (for a newform f as considered here), we can easily find one or several Heegner discriminants for A.

Associated to each Heegner discriminant D is a *Heegner point* $y_D \in A(K)$, unique up to sign and adding a torsion point. In particular, the *Heegner index* $I_D = (A(K) : \mathrm{End}(A)\cdot y_D)$ is well-defined.

Recall that $\mathscr{O} = \mathrm{End}(A) = \mathrm{End}_{\mathbb{Q}}(A)$ is an order in a real quadratic field. In all cases considered here, $\mathscr{O}$ equals the geometric endomorphism ring $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$ and is a maximal order and a principal ideal domain. For each prime ideal $\mathfrak{p}$ of $\mathscr{O}$, we have the residual Galois representation $\rho_{\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{Aut}(A[\mathfrak{p}]) \simeq \mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$, where $\mathbb{F}_{\mathfrak{p}} = \mathscr{O}/\mathfrak{p}$ denotes the residue class field.

We can use Magma's functionality for 2-descent on hyperelliptic Jacobians based on [20] to determine $\text{Ш}(A/\mathbb{Q})[2]$. In all cases considered here, this group is trivial, which implies that $\text{Ш}(A/\mathbb{Q})[2^\infty] = 0$. (In fact, this had already been done in [9] for most of the curves.) It is therefore sufficient to consider the p-primary parts of $\text{Ш}(A/\mathbb{Q})$ for odd p.

Theorem 1. *Let A be an abelian variety of GL_2-type over $\mathbb{Q}$. Assume that $\mathrm{ord}_{s=1} L(f,s) \in \{0,1\}$ for one (equivalently, all) newform associated to A.*

1. *If the level N of A is square-free, then $\mathrm{ord}_p(\#\text{Ш}(A/\mathbb{Q})_{\mathrm{an}}) = \mathrm{ord}_p(\#\text{Ш}(A/\mathbb{Q}))$ for all rational primes $p \ne 2$ such that $\rho_{\mathfrak{p}}$ is irreducible for all $\mathfrak{p} \mid p$.*
2. *If there exists a polarization $\lambda : A \to A^\vee$, then $\text{Ш}(A/\mathbb{Q})[\mathfrak{p}] = 0$ for all prime ideals $\mathfrak{p} \mid p \ne 2$ such that $\rho_{\mathfrak{p}}$ is irreducible and p does not divide $\deg\lambda$, and, for some Heegner field K with*

Heegner discriminant D, I_D and the order of the groups $\mathrm{H}^1(K_v^{\mathrm{nr}}|K_v, A)$ with v running through the places of K.

Proof. (1) is [5, Theorems C and D]. (2) is an explicit version of [13]. □

We have implemented the following algorithms.

(1) *Image of the residual Galois representations.* Extending the algorithm described in [8], which determines a finite small superset of the primes p with ρ_p reducible in the case that $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$, we obtain a finite small superset of the prime ideals $\mathfrak{p}$ of $\mathcal{O}$ such that $\rho_{\mathfrak{p}}$ is reducible. Building upon this and [6], we can also check whether $\rho_{\mathfrak{p}}$ has maximal possible image $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})^{\det \in \mathbb{F}_p^\times}$.

The irreducibility of $\rho_{\mathfrak{p}}$ for all $\mathfrak{p} \mid p$ is the crucial hypothesis in [5, Theorems C and D], and in [13].

(2) *Computation of the Heegner index.* We can compute the height of a Heegner point using the main theorem of [11]. By enumerating all points of that approximate height using [16], we can identify the Heegner point $y_D \in A(K)$ as a $\mathbb{Q}$-point on A, or on the quadratic twist A^K, depending on the analytic rank of $A/\mathbb{Q}$. An alternative implementation uses the j-invariant morphism $X_0(N) \to X_0(1)$ and takes the preimages of the j-invariants belonging to elliptic curves with CM by the order of discriminant D. A variant of this is based on approximating q-expansions of cusp forms analytically and finding the Heegner point as an algebraic approximation.

(3) *Determination of the (geometric) endomorphism ring of $A/\mathbb{Q}$ and its action on the Mordell-Weil group $A(\mathbb{Q})$.* Given the Heegner point y_D, this can be used to compute the Heegner index I_D. The endomorphism rings over $\mathbb{Q}$ and $\overline{\mathbb{Q}}$ agree for our examples; this can be seen by inspecting the LMFDB. The geometric endomorphism ring together with its action on the Mordell-Weil group is computed approximately from the analytic Jacobian, and we can verify the correctness of the result because we know that it equals the coefficient ring of f.

We can also compute the *kernel of a given endomorphism* as an abstract $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$-module together with explicit generators in $A(\overline{\mathbb{Q}})$. We apply this to find the characters corresponding to the constituents of $\rho_{\mathfrak{p}}$ when the representation is reducible.

(4) *Analytic order of* Ш. If the L-rank $\mathrm{ord}_{s=1} L(f,s)$ of $A/\mathbb{Q}$ is zero, then we can compute $\#Ш(A/\mathbb{Q})_{\mathrm{an}}$ exactly as a rational number using modular symbols via Magma's `LRatio` function, which gives $L(A,1)/\Omega_A^{-1} \in \mathbb{Q}_{>0}$, together with (1), since $\#A(\mathbb{Q})_{\mathrm{tors}} = \#A^\vee(\mathbb{Q})_{\mathrm{tors}}$ and the Tamagawa numbers c_v are known.

When the L-rank is 1, we can compute the analytic order of Ш from $\#Ш(A/K)_{\mathrm{an}} = \#Ш(A/\mathbb{Q})_{\mathrm{an}} \cdot \#Ш(A^K/\mathbb{Q})_{\mathrm{an}} \cdot 2^{(\text{bounded exponent})}$ and the formula

$$\#Ш(A/K)_{\mathrm{an}} = \frac{\#A(K)_{\mathrm{tors}} \#A^\vee(K)_{\mathrm{tors}}}{c_\pi^2 u_K^4 \prod_p c_p(A/\mathbb{Q})^2} \cdot \frac{\|\omega_f\|^2 \|\omega_{f^\sigma}\|^2}{\Omega_{A/K}} \cdot \frac{\hat{h}(y_{D,f})\hat{h}(y_{D,f^\sigma}) \operatorname{disc}\mathcal{O}}{\mathrm{Reg}_{A/K}}$$

deduced from [11]; here, the last two factors are integral. In the computation of $\#Ш(A^K/\mathbb{Q})_{\mathrm{an}}$, we use van Bommel's code to compute the Tamagawa numbers of $A/\mathbb{Q}$ and $A^K/\mathbb{Q}$ and the real period of $A^K/\mathbb{Q}$. In the one case where his code did not succeed, we used another Heegner discriminant.

(5) *Isogeny descent.* In the cases when $\mathfrak{p}$ is odd and $\rho_{\mathfrak{p}}$ is reducible, we determined characters χ_1 and χ_2 such that

$$\rho_{\mathfrak{p}} \cong \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix};$$

see (3) above. We then compute upper bounds for the $\mathbb{F}_p$-dimensions of the two Selmer groups associated to the corresponding two isogenies of degree p whose composition is

X	r	$\mathscr{O}$	$\#Ш_{\mathrm{an}}$	$\rho_{\mathfrak{p}}$ red.	c	(D, I_D)	$\#Ш$
$X_0(23)$	0	$\sqrt{5}$	1	11_1	11	$(-7, 11)$	11^0
$X_0(29)$	0	$\sqrt{2}$	1	7_1	7	$(-7, 7)$	7^0
$X_0(31)$	0	$\sqrt{5}$	1	$\sqrt{5}$	5	$(-11, 5)$	5^0
$X_0(35)/w_7$	0	$\sqrt{17}$	1	2_1	1	$(-19, 1)$	1
$X_0(39)/w_{13}$	0	$\sqrt{2}$	1	$\sqrt{2}$, 7_1	7	$(-23, 7)$	7^0
$X_0(67)^+$	2	$\sqrt{5}$	1		1	$(-7, 1)$	1
$X_0(73)^+$	2	$\sqrt{5}$	1		1	$(-19, 1)$	1
$X_0(85)^*$	2	$\sqrt{2}$	1	$\sqrt{2}$	1	$(-19, 1)$	1
$X_0(87)/w_{29}$	0	$\sqrt{5}$	1	$\sqrt{5}$	5	$(-23, 5)$	5^0
$X_0(93)^*$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(103)^+$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(107)^+$	2	$\sqrt{5}$	1		1	$(-7, 1)$	1
$X_0(115)^*$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(125)^+$	2	$\sqrt{5}$	1	$\sqrt{5}$	1	$(-11, 1)$	5^0
$X_0(133)^*$	2	$\sqrt{5}$	1		1	$(-31, 1)$	1
$X_0(147)^*$	2	$\sqrt{2}$	1	$\sqrt{2}$, 7_1	1	$(-47, 1)$	7^0
$X_0(161)^*$	2	$\sqrt{5}$	1		1	$(-19, 1)$	1
$X_0(165)^*$	2	$\sqrt{2}$	1	$\sqrt{2}$	1	$(-131, 1)$	1
$X_0(167)^+$	2	$\sqrt{5}$	1		1	$(-15, 1)$	1
$X_0(177)^*$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(191)^+$	2	$\sqrt{5}$	1		1	$(-7, 1)$	1
$X_0(205)^*$	2	$\sqrt{5}$	1		1	$(-31, 1)$	1
$X_0(209)^*$	2	$\sqrt{2}$	1		1	$(-51, 1)$	1
$X_0(213)^*$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(221)^*$	2	$\sqrt{5}$	1		1	$(-35, 1)$	1
$X_0(287)^*$	2	$\sqrt{5}$	1		1	$(-31, 1)$	1
$X_0(299)^*$	2	$\sqrt{5}$	1		1	$(-43, 1)$	1
$X_0(357)^*$	2	$\sqrt{2}$	1		1	$(-47, 1)$	1

Figure 1. BSD data for the absolutely simple modular Jacobians of Atkin-Lehner quotients of $X_0(N)$.

multiplication by a generator π of $\mathfrak{p}$ on A; see [17]. From this, we deduce an upper bound for the dimension of the π-Selmer group of A, which, in the cases considered here, is always ≤ 1. Using the known finiteness of $Ш(A/\mathbb{Q})$, which implies that $Ш(A/\mathbb{Q})[\mathfrak{p}]$ has even dimension, this shows that $Ш(A/\mathbb{Q})[\mathfrak{p}] = 0$.

(6) *Computation of the p-adic L-function.* We can also compute the p-adic L-functions of newforms of weight 2, trivial character and arbitrary coefficient ring for $p^2 \nmid N$. Computing $\operatorname{ord}_{\mathfrak{p}} \mathscr{L}^*_{\mathfrak{p}}(f, 0)$ and using the known results [18, 19] about the GL_2 Iwasawa Main Conjecture (IMC) with the hypotheses that $\rho_{\mathfrak{p}}$ is irreducible and there is a $q \| N$ with $\rho_{\mathfrak{p}}$ ramified at $q \neq p$ gives us information about the $\mathfrak{p}^\infty$-Selmer group.

3. Results

Our results are summarized in Figure 1. The first column gives the genus 2 curve X as a quotient of $X_0(N)$ by a subgroup of the Atkin-Lehner involutions. We denote the Atkin-Lehner involution

X	D_K	$\#Ш(A^K/\mathbb{Q})_{an}$	$\#Ш(A/K)_{an}$	$\#Ш(A/\mathbb{Q})_{an}$
$X_0(67)^+$	-7	4	1	1
$X_0(73)^+$	-19	4	1	1
$X_0(85)^*$	-19	4	1	1
$X_0(93)^*$	-11	1	1	1
$X_0(103)^+$	-11	4	1	1
$X_0(107)^+$	-7	4	1	1
$X_0(115)^*$	-11	1	1	1
$X_0(125)^+$	-11	4	1	1
$X_0(133)^*$	-31	4	1	1
$X_0(147)^*$	-47	4	1	1
$X_0(161)^*$	-19	1	1	1
$X_0(165)^*$	-131	16	4	1
$X_0(167)^+$	-15	4	1	1
$X_0(177)^*$	-11	4	1	1
$X_0(191)^+$	-7	4	1	1
$X_0(205)^*$	-31	4	1	1
$X_0(209)^*$	-79^*	2	1	1
$X_0(213)^*$	-11	4	1	1
$X_0(221)^*$	-35	4	1	1
$X_0(287)^*$	-21	4	1	1
$X_0(299)^*$	-43	4	1	1
$X_0(357)^*$	-47	2	1	1

Figure 2. Analytic order of Ш for the curves of L-rank 1. (A * means that we used a different Heegner discriminant than in Figure 1 in the case where van Bommel's `TamagawaNumber` did not succeed.)

associated to a divisor d of N such that d and N/d are coprime by w_d. We write $X_0(N)^+$ for $X_0(N)/w_N$ and $X_0(N)^*$ for the quotient of $X_0(N)$ by the full group of Atkin-Lehner operators. We are considering the Jacobian A of X.

The second column gives the algebraic rank of $A/\mathbb{Q}$, which is equal to its analytic rank by the combination of the main results of [11] and [13].

The third column specifies $\mathscr{O}$ as the maximal order in the number field obtained by adjoining the given square root to $\mathbb{Q}$.

The fourth column gives the analytic order of the Shafarevich-Tate group of A, defined as in the introduction. For the surfaces of L-rank 1, the intermediate results of our computation are contained in Figure 2.

The fifth column specifies the prime ideals $\mathfrak{p}$ of $\mathscr{O}$ such that $\rho_\mathfrak{p}$ is reducible. The notation p_1 means that p is split in $\mathscr{O}$ and $\rho_\mathfrak{p}$ is reducible for exactly one $\mathfrak{p} \mid p$. If p is ramified in $\mathscr{O}$, we write $\sqrt{p}$ for the unique prime ideal $\mathfrak{p} \mid p$.

The sixth column gives the odd part of $\operatorname{lcm}_p c_p(A/\mathbb{Q})$, which can be obtained from the LMFDB [22].

The seventh column gives a Heegner discriminant D for A together with the odd part of the Heegner index I_D. Our computation confirms that the Tamagawa product divides the Heegner index.

The last column contains the order of the Shafarevich-Tate group of $A/\mathbb{Q}$. An entry 1 means that it follows immediately from the previous columns, the computation of $\mathrm{Sel}_2(A/\mathbb{Q})$ and Theorem 1 that all p-primary components of $Ш(A/\mathbb{Q})$ vanish.

Otherwise, the order of $Ш(A/\mathbb{Q})$ is given as a product of powers of the odd primes p such that some $\rho_{\mathfrak{p}}$ with $\mathfrak{p} \mid p$ is reducible or p divides $c \cdot I_D$. (In each of these cases, there is exactly one such p.) We have to justify that the exponents are all zero. In the first three rows we use [14] to show that for the reducible odd $\mathfrak{p}$ on has $Ш(J_0(p)/\mathbb{Q})[\mathfrak{p}] = 0$; this is a consequence of these prime ideals being Eisenstein primes.

In the remaining cases, we used the approach described in item (5) in Section 2. For the rows with $A = \mathrm{Jac}(X_0(39)/w_{13})$ and $A = \mathrm{Jac}(X_0(87)/w_{29})$, one has non-split short exact sequences of Galois modules

$$0 \to \mathbb{Z}/p \to A[\mathfrak{p}] \to \mu_p \to 1$$

with $p = 7$ and 5, respectively. For the only two non-semistable abelian surfaces we found the following isomorphism and exact sequence.

$$J_0(125)^+[\sqrt{5}] \cong \mu_5^{\otimes 2} \oplus \mu_5^{\otimes 3}$$

$$1 \to \mu_7^{\otimes 4} \to \mathrm{Jac}(X_0(147)^*)[\mathfrak{p}] \to \mu_7^{\otimes 3} \to 1$$

In all cases, we find that $Ш(A/\mathbb{Q})[\mathfrak{p}] = 0$. Note that for the $\mathfrak{p} \mid 7$ for which $\rho_{\mathfrak{p}}$ is *irreducible*, $\mathrm{Jac}(X_0(147)^*)[\mathfrak{p}] = 0$ follows from [13] because I_{-43} is not divisible by 7. In the case of the square-free levels $N = 23, 29, 39$, we computed that the $\mathfrak{p}$-adic L-function is a unit for the $\mathfrak{p} \mid p$ with $\rho_{\mathfrak{p}}$ irreducible, so we can conclude that $\mathrm{Sel}_{\mathfrak{p}}(A/\mathbb{Q}) = 0$ and hence $\#Ш(A/\mathbb{Q})[\mathfrak{p}] = 0$ from the known cases of the GL_2 IMC. Note that our computation shows that in these cases, the image of $\rho_{\mathfrak{p}^\infty}$ is maximal, so it contains $\mathrm{SL}_2(\mathbb{Z}_p)$. This implies that the IMC holds *integrally*.

Details will be presented in a forthcoming article, where plan also to extend our computations to cover some two-dimensional absolutely simple isogeny factors of $J_0(N)$ that are not Jacobians of quotients of $X_0(N)$ by Atkin-Lehner involutions.

References

[1] R. van Bommel, "Numerical verification of the Birch and Swinnerton-Dyer conjecture for hyperelliptic curves of higher genus over $\mathbb{Q}$ up to squares", *Exp. Math.* (2019), p. 1–8.

[2] W. Bosma, J. Cannon, C. Playoust, "The Magma algebra system. I. The user language", *J. Symbolic Comput.* **24** (1997), no. 3–4, p. 235–265, Computational algebra and number theory (London, 1993).

[3] C. Breuil, B. Conrad, F. Diamond, R. Taylor, "On the modularity of elliptic curves over **Q**: wild 3-adic exercises", *J. Amer. Math. Soc.* **14** (2001), no. 4, p. 843–939.

[4] D. Bump, S. Friedberg, J. Hoffstein, "A nonvanishing theorem for derivatives of automorphic L-functions with applications to elliptic curves", *Bull. Amer. Math. Soc. (N.S.)* **21** (1989), no. 1, p. 89–93.

[5] F. Castella, M. Çiperiani, C. Skinner, F. Sprung, "On the Iwasawa main conjectures for modular forms at non-ordinary primes", 2018, Preprint, arXiv:1804.10993, https://arxiv.org/abs/arXiv:1804.10993.

[6] A. C. Cojocaru, "On the surjectivity of the Galois representations associated to non-CM elliptic curves", *Canad. Math. Bull.* **48** (2005), no. 1, p. 16–31, With an appendix by Ernst Kani.

[7] B. Creutz, R. L. Miller, "Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula", *J. Algebra* **372** (2012), p. 673–701.

[8] L. V. Dieulefait, "Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$", *Experiment. Math.* **11** (2002), no. 4, p. 503–512 (2003).

[9] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, J. L. Wetherell, "Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves", *Math. Comp.* **70** (2001), no. 236, p. 1675–1697.

[10] G. Grigorov, A. Jorza, S. Patrikis, W. A. Stein, C. Tarniţă, "Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves", *Math. Comp.* **78** (2009), no. 268, p. 2397–2425.

[11] B. H. Gross, D. B. Zagier, "Heegner points and derivatives of L-series", *Invent. Math.* **84** (1986), no. 2, p. 225–320.

[12] Y. Hasegawa, "Table of quotient curves of modular curves $X_0(N)$ with genus 2", *Proc. Japan Acad. Ser. A Math. Sci.* **71** (1995), no. 10, p. 235–239 (1996).

[13] V. A. Kolyvagin, D. Y. Logachëv, "Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties", *Algebra i Analiz* **1** (1989), no. 5 (Russian), p. 171–196.

[14] B. Mazur, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* (1977), no. 47, p. 33–186 (1978), With an appendix by Mazur and M. Rapoport.

[15] R. L. Miller, M. Stoll, "Explicit isogeny descent on elliptic curves", *Math. Comp.* **82** (2013), no. 281, p. 513–529.

[16] J. S. Müller, M. Stoll, "Canonical heights on genus-2 Jacobians", *Algebra Number Theory* **10** (2016), no. 10, p. 2153–2234.

[17] E. F. Schaefer, M. Stoll, "How to do a p-descent on an elliptic curve", *Trans. Amer. Math. Soc.* **356** (2004), no. 3, p. 1209–1231.

[18] C. Skinner, "Multiplicative reduction and the cyclotomic main conjecture for GL_2", *Pacific J. Math.* **283** (2016), no. 1, p. 171–200.

[19] C. Skinner, E. Urban, "The Iwasawa main conjectures for GL_2", *Invent. Math.* **195** (2014), no. 1, p. 1–277.

[20] M. Stoll, "Implementing 2-descent for Jacobians of hyperelliptic curves", *Acta Arith.* **98** (2001), no. 3, p. 245–277.

[21] R. Taylor, A. Wiles, "Ring-theoretic properties of certain Hecke algebras", *Ann. of Math. (2)* **141** (1995), no. 3, p. 553–572.

[22] The LMFDB collaboration, "L-functions and Modular Forms Database", https://www.lmfdb.org/Genus2Curve/Q/.

[23] J.-L. Waldspurger, "Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie", *Compositio Math.* **54** (1985), no. 2 (French), p. 173–242.

[24] X. D. Wang, "2-dimensional simple factors of $J_0(N)$", *Manuscripta Math.* **87** (1995), no. 2, p. 179–197.

[25] A. Wiles, "Modular elliptic curves and Fermat's last theorem", *Ann. of Math. (2)* **141** (1995), no. 3, p. 443–551.