Exact verification of the strong Birch–Swinnerton-Dyer conjecture for some absolutely simple modular abelian surfaces

Timo Keller, Michael Stoll
(Lehrstuhl Computeralgebra, Universität Bayreuth)

Timo.Keller@uni-bayreuth.de
Michael.Stoll@uni-bayreuth.de

Informal introduction

This article is on the *conjecture of Birch and Swinnerton-Dyer* (*BSD* for short) for abelian surfaces, originally formulated by Birch and Swinnerton-Dyer [1] in the 1960s for elliptic curves over $\mathbb{Q}$. Abelian surfaces are two-dimensional abelian varieties, and abelian varieties are higher-dimensional analogues of elliptic curves. An elliptic curve is an algebraic curve that carries a group structure. This means that we can add two points on the curve to get another point on the curve, and this addition has similar properties as the standard addition. Elliptic curves and abelian varieties are important in various contexts within mathematics, for example in the proof of Fermat's Last Theorem or in cryptography.

Using the numbers of points modulo each prime number on an abelian variety A that is defined over the rational numbers, one can construct a certain function, the L-function of A. The BSD conjecture for A proposes a surprising connection between the analytic behavior of the L-function of A and certain "global" invariants of A. These invariants include properties of the group of rational points on A on the one hand and the number of elements of the mysterious Shafarevich-Tate group $Ш(A)$ of A on the other hand. Since all other quantities that occur in the conjecture can be computed for given A, the conjecture can be expressed as "$Ш(A)$ is finite and has the expected number of elements".

Birch and Swinnerton-Dyer originally formulated their conjecture for elliptic curves. To prove this version is one of the seven "Millennium Problems" of the Clay Foundation.

For general elliptic curves and even more so for higher-dimensional abelian varieties, the conjecture is wide open. It is not even known that $Ш(A)$ is always finite. For so-called "modular" abelian varieties with additional properties, some parts of the conjecture are known, however, in particular the finiteness of $Ш(A)$. Every elliptic curve defined over the rational numbers is modular, and so it was possible to verify the BSD conjecture for many individual elliptic curves.

In this article, we report on our project with the goal to obtain the complete verification of the BSD conjecture also for many modular abelian surfaces. Except in cases that can be reduced to elliptic curves, this had not been done so far even for a single abelian surface. For the verification of the conjecture, we determined the size of $Ш(A)$. To this end, we used new ideas to generalize and improve the methods that have been successful for elliptic curves.

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

State of the art

We now give more detailed and also more technical description of the objects involved. The BSD conjecture consists of two parts, which we will explain for the case of an abelian variety A of dimension g over $\mathbb{Q}$.

One attaches to A its L-function $L(A, s)$, which is defined by an Euler product over all prime numbers p. If A is the Jacobian variety of a curve X of genus g, the Euler factor at p for a prime p of good reduction is determined by the number of $\mathbb{F}_{p^n}$-points on the mod p reduction of X for $n \leq g$. It follows from the Weil conjectures for varieties over finite fields that the Euler product converges for $\mathrm{Re}(s) > \frac{3}{2}$ to a holomorphic function. A standard conjecture predicts that $L(A, s)$ extends to an entire function; this is known when A is *modular*, i.e., occurs as an isogeny factor of the Jacobian $J_0(N)$ of one of the modular curves $X_0(N)$. By the Modularity Theorem of Wiles and others [28, 22, 3], this is always the case when A is an elliptic curve over $\mathbb{Q}$ (this is now a special case of Serre's Modularity Conjecture [11]).

We now introduce the relevant global invariants of A. By the Mordell-Weil Theorem, the abelian group $A(\mathbb{Q})$ of rational points on A is finitely generated, so it splits as

$$A(\mathbb{Q}) \cong A(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r,$$

where $A(\mathbb{Q})_{\text{tors}}$ is the finite *torsion subgroup* and r is a nonnegative integer, the *rank of* $A(\mathbb{Q})$. There is a natural positive definite quadratic form $\hat{h}$ on $A(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^r$, the *canonical height*, turning $A(\mathbb{Q})/A(\mathbb{Q})_{\text{tors}}$ into a lattice in a euclidean vector space. The squared covolume of this lattice (equivalently, the determinant of the Gram matrix of $\hat{h}$ with respect to a lattice basis) is the *regulator* Reg_A. The final global arithmetic invariant of A that

we need is the *Shafarevich-Tate group* $Ш(A)$. It can be defined as the localization kernel

$$Ш(A) = \ker\left(\mathrm{H}^1(\mathbb{Q}, A) \to \bigoplus_v \mathrm{H}^1(\mathbb{Q}_v, A)\right)$$

in Galois cohomology; here $\mathbb{Q}_v$ denotes the completion of $\mathbb{Q}$ with respect to a place v and the direct sum is over all places of $\mathbb{Q}$. Geometrically, $Ш(A)$ is the group of equivalence classes of everywhere locally trivial $A/\mathbb{Q}$-torsors. This group is conjectured to be finite, but this is completely open in general.

We also need some local invariants. To each prime p, one associates the *Tamagawa number* $c_p(A)$; this is the number of connected components of the special fiber at p of the Néron model $\mathcal{A}/\mathbb{Z}$ of A and equals 1 for all primes of good reduction. Let $(\omega_1, \ldots, \omega_g)$ be the pull-back to $\mathrm{H}^0(A, \Omega^1)$ of a basis of the free $\mathbb{Z}$-module $\mathrm{H}^0(\mathcal{A}, \Omega^1)$ of rank g. Then the *real period* of A is the volume of $A(\mathbb{R})$ measured using $|\omega_1 \wedge \cdots \wedge \omega_g|$:
$\Omega_A = \int_{A(\mathbb{R})} |\omega_1 \wedge \cdots \wedge \omega_g|$.

The *weak BSD* or *BSD rank conjecture* says that $L(A, s)$ has an analytic continuation to a neighborhood of $s = 1$ and

$$r_{\text{an}} := \operatorname{ord}_{s=1} L(A, s) = r\,.$$

The order of vanishing of $L(A, s)$ at $s = 1$ is also called the *analytic rank* of A.

The *strong BSD conjecture* says that in addition $Ш(A)$ is finite and

$$\begin{aligned} L^*(A, 1) &:= \lim_{s\to 1}(s-1)^{-r} L(A, s) \\ &= \frac{\Omega_A \prod_p c_p(A) \cdot \mathrm{Reg}_A \, \#Ш(A)}{\#A(\mathbb{Q})_{\text{tors}} \#A^\vee(\mathbb{Q})_{\text{tors}}}\,. \end{aligned}$$

Here $A^\vee$ is the dual abelian variety; it is isomorphic to A when A is a Jacobian, or, more generally, when A is principally polarized.

Since all the other invariants of A can (usually) be computed at least numerically, we define the *analytic order of Sha* to be

$$\#Ш(A)_{\text{an}} := \frac{L^*(A, 1)}{\Omega_A \, \mathrm{Reg}_A} \cdot \frac{\#A(\mathbb{Q})_{\text{tors}} \#A^\vee(\mathbb{Q})_{\text{tors}}}{\prod_p c_p(A)}\,.$$

Assuming the BSD rank conjecture, strong BSD can then be phrased as "$Ш(A)$ is finite and $\#Ш(A) = \#Ш(A)_{\text{an}}$."

Even the weak BSD conjecture for elliptic curves over $\mathbb{Q}$ is wide open in general (this is the Clay Millennium Problem mentioned above). However, the strong BSD conjecture has been verified for many "small" elliptic curves; see below. In our project we verified the strong BSD conjecture for the first time for a number of abelian surfaces A, in a situation where it cannot be reduced to BSD for some elliptic curves. Concretely, this means that A is absolutely simple.

Previously known results

Beside Serre's Modularity Conjecture, the two big theorems we use are the Gross–Zagier formula [9] and the Euler system of Heegner points of Kolyvagin–Logachev [12].

Assume that $A/\mathbb{Q}$ has real multiplication by an order $\mathcal{O}$ of a totally real number field of degree $g := \dim A$ over $\mathbb{Q}$, i.e. $\mathrm{End}_{\mathbb{Q}}(A) = \mathcal{O}$. By Serre's Modularity Conjecture and a result of Ribet [18], this is equivalent to the statement that A is an isogeny quotient of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$ for some N (which we can take such that N^g equals the conductor of A), or that there is a newform $f \in S_2(\Gamma_0(N), \mathcal{O})$ with

$$L(A/\mathbb{Q}, s) = \prod_{\sigma:\mathcal{O}\hookrightarrow\mathbb{R}} L(f^\sigma, s);$$

in particular $L(A/\mathbb{Q}, s)$ is holomorphic on $\mathbb{C}$. In the following, let A, g, $\mathcal{O}$, f and N be as in this paragraph.

The *Gross–Zagier formula* relates the first derivative $L'(f/K, 1)$ of the L-function of f base changed to a certain imaginary quadratic field K, called Heegner field and defined below, to the height of a Heegner point $y_K \in J(K)$. This is a step towards the rank conjecture because it says that $r_{\text{an}}(f/K) = 1$ implies $r(A/K) \geq \dim A$.

The *Euler system of Kolyvagin–Logachev* proves that a GL_2-type abelian variety A over $\mathbb{Q}$ with $r_{\text{an}}(A/K) = \dim A$ even satisfies $r(A/K) = \dim A$, $r(A/\mathbb{Q}) = r_{\text{an}}(A/\mathbb{Q})$ and that $Ш(A/\mathbb{Q})$ is finite. However, as it depends crucially on explicit open image theorems only available for elliptic curves in general, in contrast to the case of $\dim A = 1$, it does not give an explicit finite support of $Ш(A/\mathbb{Q})$. These theorems are not available for $\dim A > 1$ because the moduli space of g-dimensional principally polarized abelian varieties has dimension $\frac{g(g+1)}{2} > 1$ for $g > 1$. In our work, we therefore prove such open image theorems algorithmically only for a given modular abelian surface, and using this, we work out an explicit version of Kolyvagin–Logachev.

Regarding rank > 1, there is no single elliptic curve of analytic rank > 1 known for which we know that its Shafarevich-Tate group is finite.

Exact verification for elliptic curves

In the case of elliptic curves, the various ingredients mentioned above have been worked out, made explicit and been improved to an extent that it was possible to verify the strong BSD conjecture for all elliptic curves E over $\mathbb{Q}$ of rank ≤ 1 and conductor $N < 5000$; see [8, 14, 15, 4, 13].

Exact verification for modular abelian surfaces

We now specialize to the case $g = 2$, i.e., modular abelian surfaces $A/\mathbb{Q}$. We assume that $A = J$ is a Jacobian, in particular principally polarized, and absolutely

simple. The latter is to exclude cases where one can reduce strong BSD to elliptic curves over number fields (potentially larger than $\mathbb{Q}$).

Strong BSD has been verified *numerically* and *up to squares* for some Jacobians by van Bommel [25].

Our overall strategy is:

1. Classify the *image of the residual Galois representations* $\rho_{\mathfrak{p}} := \rho_{f,\mathfrak{p}}$ for almost all $\mathfrak{p}$: Show explicitly that almost all of them are irreducible and have maximal image $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})^{\det\in\mathbb{F}_p}$.

2. For at least one Heegner field K, compute the Heegner point $y_K \in J(K)$ (or rather $2y_K \in J^K(\mathbb{Q})$ or $J(\mathbb{Q})$ if the L-rank is 0 or 1, respectively). This gives the *Heegner index* $I_K = \mathrm{Ann}_{\mathcal{O}}(J(K)/\mathcal{O}y_K)$ as an $\mathcal{O}$-ideal.

3. Compute a *finite support* of $Ш(A/\mathbb{Q})$ with our explicit version of the Heegner point Euler system from the previous two steps.

4. For the finitely many remaining primes do one of the following:

   (a) If $\mathrm{SL}_2(\mathbb{F}_p) \subseteq \mathrm{im}\,\rho_{\mathfrak{p}}$ and p is a prime of good or multiplicative bad reduction, we can use the GL_2 Iwasawa Main Conjecture [21, 20] to get the p-valuation of the order of the $\mathfrak{p}$-Selmer group by *computing the p-adic L-function* using overconvergent modular symbols.

   (b) Perform a $\mathfrak{p}$-*descent*; if $\rho_{\mathfrak{p}}$ is reducible, determine the characters constituting the semisimplification $\rho_{\mathfrak{p}}^{\mathrm{ss}}$ and perform an isogeny descent.

5. Compute the *analytic order of* Ш using modular symbols if $L(f,1) \neq 0$ or from $\#Ш(A^K/\mathbb{Q})_{\mathrm{an}}$ and $\#Ш(A/K)_{\mathrm{an}}$ if the L-rank is 1. To compute $\#Ш(A/K)_{\mathrm{an}}$ exactly, we use the Gross–Zagier formula.

Our algorithms for 1 and 4 run very quickly. The most time-consuming part of 2 is the computation of the Mordell-Weil group. The last step 5 is very fast in the analytic rank 0 case and a bit slower for rank g. In general, the runtime is determined by the level N and the discriminant of the chosen Heegner field(s).

We now describe these substeps in more detail:

Classifying the images of the residual Galois representations

To prove $Ш(J/\mathbb{Q})[\mathfrak{p}] = 0$ for a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ using the Euler system (see below), one assumption we need to know is that the residual Galois representation

$$\rho_{\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{Aut}_{\mathcal{O}/\mathfrak{p}}(J[\mathfrak{p}](\overline{\mathbb{Q}}))$$

is irreducible or even has *maximal image* $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})^{\det\in\mathbb{F}_p}$. The restriction $\det \in \mathbb{F}_p$ comes from the fact that the determinant of $\rho_{\mathfrak{p}}$ is the mod-p cyclotomic character

$$\chi_p : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathbb{F}_p^\times$$

satisfying $\sigma(\zeta_p) = \zeta_p^{\chi_p(\sigma)}$ for a primitive p-th root of unity ζ_p. Another reason why we have to have information on $\rho_{\mathfrak{p}}$ is that we need to know the characters constituting its semisimplification if it is reducible when performing isogeny descents (see below).

We first determine a small finite set S of primes such that $\rho_{\mathfrak{p}}$ is irreducible for $\mathfrak{p} \notin S$: Assuming $\rho_{\mathfrak{p}}$ reducible, say

$$\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon\chi_p \oplus \varepsilon^{-1}$$

with a character

$$\varepsilon : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathbb{F}_{\mathfrak{p}}^\times,$$

we prove that the conductor d of ε satisfies $d^2 \mid N$ if $v_p(N) \leq 1$, with a more complicated condition if $p^2 \mid N$. This implies that $\varepsilon(\mathrm{Frob}_\ell)^{\mathrm{ord}_{\mathfrak{p}}\,\ell} = 1$ for $\ell \nmid pN$ with $\mathrm{ord}_{\mathfrak{p}}\,\ell$ the order of ℓ in $\mathbb{F}_{\mathfrak{p}}^\times$. Therefore p divides the gcd of the resultants

$$\mathrm{res}_{\mathbb{Z}[T]}\left(\det(T - \mathrm{Frob}_\ell \mid T_{\mathfrak{p}}J), T^{\mathrm{ord}_{\mathfrak{p}}\,\ell} - 1\right),$$

which is a non-zero integer which can be computed explicitly and very efficiently.

We can also exclude for all but finitely many p the possibility that the projectivized image is contained in $\mathbb{P}\mathrm{SL}_2(\mathbb{F}_p)$ if $\deg(\mathfrak{p}) = 2$.

Since $\rho_{\mathfrak{p}}$ always contains an element of order > 5 in its image if $p \geq 7$ (coming from the inertia subgroup at p), its projectivized image in $\mathrm{PSL}_2(\mathbb{F}_{\mathfrak{p}})$ is not exceptional, i.e., not contained in a subgroup isomorphic to A_4, S_4, or A_5.

By the classification of maximal subgroups of PSL_2 over a finite field, if $\rho_{\mathfrak{p}}$ for $p \geq 7$ is irreducible, not maximal and its projectivized image is not contained in $\mathbb{P}\mathrm{SL}_2(\mathbb{F}_p)$ if $\deg(\mathfrak{p}) = 2$, i.e., strictly contained in $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})^{\det\in\mathbb{F}_p}$, it is contained in the normalizer $N(C)$ of a Cartan subgroup C. One can show that the quadratic character given by modding out C from the image is unramified outside the level N. Using the Sturm bound and assuming that the newform f is non-CM, i.e., there is no imaginary quadratic field K with $a_p(f) = 0$ for all p inert in K, one can bound the p for which the image is contained in the normalizer of a Cartan. Hence we have established an explicit and small

finite set of primes outside of which $\rho_{\mathfrak{p}}$ is irreducible or even maximal.

To treat the finitely many remaining primes $\mathfrak{p}$, we compute $\Delta_{\mathfrak{p}}(\ell) = a_\ell(f)^2 - 4\ell \in \mathbb{F}_{\mathfrak{p}}$, the discriminant of the Euler factor at $\mathfrak{p}$ modulo $\mathfrak{p}$. If $\Delta_{\mathfrak{p}}(\ell) \neq 0$, $\rho_{\mathfrak{p}}(\mathrm{Frob}_\ell)$ has pairwise distinct eigenvalues, hence is contained in a unique Cartan subgroup. The latter is split iff $\Delta_{\mathfrak{p}}(\ell)$ is a square in $\mathbb{F}_{\mathfrak{p}}^\times$. If we can find an ℓ for a given $\mathfrak{p}$ such that $\rho_{\mathfrak{p}}(\mathrm{Frob}_\ell)$ is contained in a non-split Cartan subgroup, the image is reducible.

In practice and in all cases we considered, this procedure gives the set of reducible primes. To verify that $\rho_{\mathfrak{p}}$ is reducible, we compute $J[\mathfrak{p}](\overline{\mathbb{Q}})$ as a Galois module, see below.

Computing the Heegner point and Heegner index

Let K be an imaginary quadratic number fields in which all primes dividing the level N are split (in particular, unramified). This is called the *Heegner hypothesis*. It follows that there exists an ideal $\mathfrak{n}$ of the ring of integers $\mathcal{O}_K$ (this is *not* the endomorphism ring $\mathcal{O}$ of A!) of K with $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N$. Choose an ideal class $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_K)$. Every such $\mathfrak{n}$ as above defines a CM point $(\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}]) \in Y_0(N)(K)$: It is the point in the moduli space $Y_0(N)$ of elliptic curves with a cyclic isogeny of degree N corresponding to the elliptic curve $\mathbb{C}/\mathfrak{a}$ (a priori defined over $\mathbb{C}$) and the isogeny $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{n}^{-1}\mathfrak{a}$ and is defined over the ring class field $H_{\mathcal{O}_K}$ of $\mathcal{O}_K$ (which always contains the Hilbert class field of K and is equal to it if the order $\mathcal{O}$ is maximal) by the theory of complex multiplication. Summing over all $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_K)$, we get a cycle of degree $h_{\mathcal{O}_K}$, the class number of $\mathcal{O}_K$, on $Y_0(N)$. Subtracting $h_{\mathcal{O}_K}[\infty]$ with the cusp $\infty \in X_0(N)(\mathbb{Q}) \setminus Y_0(N)(\mathbb{Q})$, we get a 0-cycle on $X_0(N)$ defined over K. Its image in $J_0(N)(K)$ under the Abel-Jacobi morphism is called the *Heegner point* y_K. Mapping y_K to J under a modular parameterization $J_0(N) \to J$ gives the Heegner point on J. By abuse of notation, we denote it by y_K again.

The celebrated theorem of Gross–Zagier says that the height of $y_K \in J(K)$ is non-zero if and only if the order of vanishing of

$$L(f/K, s) = L(f, s)L(f \otimes \chi_K, s)$$

at $s = 1$ equals 1; here χ_K is the quadratic Dirichlet character attached to K. By a theorem of Waldspurger [26], for every newform f with $\mathrm{ord}_{s=1} L(f, s) \in \{0, 1\}$, there exist infinitely many K satisfying the Heegner hypothesis and the hypothesis on the order of vanishing of $L(f/K, s)$. Since a point is non-torsion if and only if its canonical height is non-zero, the Gross–Zagier formula establishes one inequality in the BSD rank conjecture: If $L(A/\mathbb{Q}, s)$ has order of vanishing $r_{\mathrm{an}} = g$, then $\mathrm{rk}\, A(\mathbb{Q}) \geq g$.

The Euler system of Kolyvagin (in the case of $g = 1$) and Kolyvagin-Logachev (for general real multiplication) not only proves the opposite inequality (and hence equality of the analytic and algebraic rank), but also the finiteness of the Shafarevich-Tate group:

Computing an explicit finite support of the Shafarevich-Tate group

This is a purely theoretical consideration, combining the results of the computation of $\mathcal{O}y_K \subseteq J(K)$ and the $\mathfrak{p} \subset \mathcal{O}$ with $\rho_{\mathfrak{p}}$ reducible.

It is crucial that the Heegner point

$$y_1 := y_K \in J(K[1])$$

with $K[1] = H_{\mathcal{O}_K}$ is the lowest level of a whole system $y_n \in J(K[n])$ with $K[n]$ the ring class field of the order $\mathcal{O}_{K,n} := \mathbb{Z} + n\mathcal{O}_K$. They satisfy a compatibility relation with respect to field norms in which the Euler factors of f occur; hence the name "Euler system".

Kolyvagin-Logachev define several constants $C_i(\mathfrak{p})$ for finitely many i, and show that they are equal to 0 for almost all $\mathfrak{p}$ and fixed i, such that $\mathfrak{p}^{\sum_i C_i(\mathfrak{p})} \mathrm{Sel}_{\mathfrak{p}^\infty}(J/\mathbb{Q}) = 0$. In particular, almost all $\mathrm{Sel}_{\mathfrak{p}}(J/\mathbb{Q})$ are 0 and all $\mathrm{Sel}_{\mathfrak{p}^\infty}(J/\mathbb{Q})$ are finite. The $C_i(\mathfrak{p})$ depend on the images of the Galois representations $\rho_{\mathfrak{p}^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{Aut}(T_{\mathfrak{p}}J)$ and $\rho_{\mathfrak{p}}$, the annihilator I_K of $J(K)/\mathcal{O}y_K$ as an $\mathcal{O}$-module (the so-called *Heegner index*), and the Tamagawa product $c(J/K) = \prod_v c_v(J/K)$ of J (conjecturally, all primes dividing $c(J/K)$ also divide I_K, so the latter would be redundant). There are additional complications for $\mathfrak{p} \mid 2$ as one often considers the space of Galois modules A where complex conjugation acts as $+1$ or -1, and A does not decompose as $A^+ \oplus A^-$ in general if $2 \mid \#A$. This is not a problem for us, since one can efficiently compute $\mathrm{Sel}_2(J/\mathbb{Q})$.

By making the argument of Kolyvagin-Logachev explicit enough, we show that $Ш(J/\mathbb{Q})[\mathfrak{p}] = 0$ if $\mathfrak{p} \nmid 2I_K c(J/K)$ and $\rho_{\mathfrak{p}}$ is irreducible. On the way, we prove that if $\rho_{\mathfrak{p}}$ is irreducible, its image contains a non-trivial homothety and one has

$$\mathrm{H}^1(\mathbb{Q}(J[\mathfrak{p}])|\mathbb{Q}, J[\mathfrak{p}](\overline{\mathbb{Q}})) = 0$$

using the classification of subgroups of $\mathrm{PSL}_2(\mathbb{F}_{\mathfrak{p}})$.

One can define Euler systems more generally for p-adic Galois representations ρ. In our case, this Galois representation is $T_{\mathfrak{p}}J$. The existence of a non-trivial Euler system together with "large image" results on ρ implies the finiteness of the Selmer group of ρ, and under some hypotheses one can even bound the size of the Selmer group via the "index" of its first level, which is the Heegner index in case of the Heegner point Euler system of Kolyvagin-Logachev. However, only a few Euler systems have been constructed, for example the Euler system of Heegner points for modular abelian varieties, the Euler system of elliptic units for CM elliptic curves, and the Euler system of cyclotomic units for the class group of cyclotomic field. Using the latter, one can give a more elementary, albeit not necessarily easier proof of the Main Conjecture of Iwasawa theory for cyclotomic extensions of $\mathbb{Q}$ compared with the first proof of Mazur and Wiles, which used arithmetic geometry of modular curves.

Computing the p-adic L-function and using the GL_2 Iwasawa Main Conjecture

We wrote a Magma [2] implementation of locally analytic distributions and distribution valued modular symbols together with their Hecke action. Building upon this, we implemented Greenberg's improvement [7] of the Pollack–Stevens algorithm [17] computing the p-adic L-function of a newform f of level divisible exactly by p, i.e., bad multiplicative reduction, as the evaluation at the path $\{\infty \to 0\}$ of the unique overconvergent lift of the modular symbol attached to f. If p does not divide the level, we compute the p-stabilization of the modular symbol; this currently only works if $a_p(f) \in \mathcal{O}_\mathfrak{p}^\times$.

Comparing with Magma's implementation of the p-adic L-function of an elliptic curve, our algorithm outperforms Magma's even for small p and precision $O(p^n)$, because the Magma implementation uses the naive "Riemann sum" approach, which has complexity exponential in $\log p$. Our algorithm also runs faster than the one implemented in SageMath [24], which only works for primes of degree 1. We verified that our algorithm produces the same output as SageMath with the same choice of a generator of the principal units using primes of degree 1.

In the cases where we use this, the p-adic L-function has vanishing order 0 and constant term a p-adic unit, and $\mathrm{im}(\rho_{\mathfrak{p}\infty})$ contains $\mathrm{SL}_2(\mathbb{Z}_p)$, so by the GL_2 Iwasawa Main Conjecture, $\mathrm{Sel}_\mathfrak{p}(J/\mathbb{Q}) = 0$ and hence $Ш(J/\mathbb{Q})[\mathfrak{p}] = 0$.

Performing isogeny descents

Let $\mathfrak{p} \mid p$ be an ideal of the endomorphism ring $\mathcal{O}$. We compute $J[\mathfrak{p}](\overline{\mathbb{Q}})$ as a $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$-module from a complex approximation on the analytic Jacobian $\mathbb{C}^g/\Lambda$, where $J[\pi](\mathbb{C}) = \frac{1}{\pi}\Lambda/\Lambda$ if $\mathfrak{p} = (\pi)$ is principal. (This is the case in all of our examples.) The computation is sped up significantly if we use Julia/Oscar [5]. If $\rho_\mathfrak{p}$ is also reducible, we can compute the (1-dimensional) characters constituting the semisimplification of $\rho_\mathfrak{p}$. We perform an isogeny descent on them, i.e., we compute an upper bound on the dimension of their Selmer groups $\mathrm{Sel}_\varphi(\mathbb{Q}, S)$ related to φ-eigenspaces of the unit group and the class group of $L = \mathbb{Q}(\varphi)$, the number field obtained by adjoining all values of φ. Here, S a finite set of primes v containing those dividing the level N such that $c_v(A/\mathbb{Q})$ is divisible by p. In all our examples with $\mathfrak{p} \nmid 2$, the sum of the dimensions of the Selmer group of φ and ψ is ≤ 1, hence $Ш(J/\mathbb{Q})[\mathfrak{p}] = 0$ since the existence of the perfect alternating Cassels-Tate pairing

$$Ш(J/\mathbb{Q}) \times Ш(J^\vee/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$$

(note that $Ш(J/\mathbb{Q})$ is known to be finite) implies that the dimension is even.

As the computation of the unit group and the class group is time-consuming even for moderately large values of $\#(\mathcal{O}/\mathfrak{p})$ and especially $[\mathbb{Q}(J[\mathfrak{p}]) : \mathbb{Q}]$, we use it only for small $\mathfrak{p}$ and reducible $\rho_\mathfrak{p}$.

Computing the analytic order of the Shafarevich-Tate group

Finally we have to compute $\#Ш(J/\mathbb{Q})_{\mathrm{an}}$. This is done by computing $\#Ш(J/K)_{\mathrm{an}}$ and $\#Ш(J^K/\mathbb{Q})_{\mathrm{an}}$ for a Heegner field K for $J/\mathbb{Q}$, where J^K is the quadratic twist of J by K. To compute $\#Ш(J/K)_{\mathrm{an}}$, we use the Gross–Zagier formula [9] for general abelian varieties of GL_2-type over $\mathbb{Q}$, using the Heegner point we computed above. To determine $\#Ш(J^K/\mathbb{Q})_{\mathrm{an}}$, we implemented a method that computes $L(J^K/\mathbb{Q}, 1)/\Omega_{J^K}$ with the twisted modular symbols of $J/\mathbb{Q}$, as directly computing $L(J^K/\mathbb{Q}, 1)/\Omega_{J^K}$ tends to be too slow, because the level of $J^K/\mathbb{Q}$ is ND_K^2 with D_K the discriminant of K, which can be fairly large; note that $J^K/\mathbb{Q}$ has analytic rank 0. With both analytic ranks at hand, we then use the equation $\#Ш(J/K)_{\mathrm{an}} = \#Ш(J/\mathbb{Q})_{\mathrm{an}} \cdot \#Ш(J^K/\mathbb{Q})_{\mathrm{an}}$ up to explicitly bounded powers of 2 and Dokchitser's code to compute the special L-value $L''(J/\mathbb{Q}, 1)$, van Bommel's code to compute the real period Ω_J and the Müller–Stoll code [16] to compute canonical heights on and the regulator $\mathrm{Reg}_{J/\mathbb{Q}}$ of a genus-2 Jacobian to compute the algebraic part $L''(J/\mathbb{Q}, 1)/(\Omega_J \mathrm{Reg}_{J/\mathbb{Q}})$ of the special L-value $L^*(J/\mathbb{Q}, 1)$. The remaining invariants needed to compute $Ш(J/\mathbb{Q})_{\mathrm{an}}$, namely the Tamagawa numbers and the torsion subgroup of $J(\mathbb{Q})$, can be obtained through existing Magma functions.

Verification of the conjecture for Atkin-Lehner quotients of modular curves

Using the above theory and algorithms, we managed to verify strong BSD exactly for all of the 28 genus-2 quotients $X_0(N)/W'(N)$ with $W'(N)$ a subgroup of the Atkin-Lehner operators such that the Jacobian is absolutely simple and of GL_2-type over $\mathbb{Q}$. We announced this result in [10] with the article giving full details to be published later.

Work in progress: more curves

There are curves of genus 2 whose Jacobians are isogeny factors of $J_0(N)$ for some N, but which are not (necessarily) Atkin-Lehner quotients of $X_0(N)$. We find such curves in the LMFDB [23] as curves of conductor N^2 whose Jacobians are absolutely simple and of GL_2-type over $\mathbb{Q}$. There are currently 97 such curves in the LMFDB (including some of the Atkin-Lehner quotients); these are curves with discriminant $\leq 10^6$ (which implies $N \leq 1000$). Recently, Andrew Sutherland has generated a much larger set of genus 2 curves that will eventually become part of the database; we will then apply our algorithms also to the curves from this set whose Jacobians are absolutely simple and of GL_2-type.

We plan to produce more curves of genus 2 whose Jacobians are isogeny factors of $J_0(N)$ for some $N \leq 1000$ (say) using the approach in [27] (which produces

numerical approximations to the curve up to a twist), enhanced by using the Sturm bound and point counting on the curve to determine the correct twist as sketched in [6]. To these curves, we will then apply our algorithms; we hope to be able to verify strong BSD for most of them. The LMFDB lists 1195 pairs of Galois conjugate newforms of level ≤ 1000, so that we can expect to find several hundred more examples in this way.

Our Magma code will be made available on `https://github.com/TimoKellerMath` as soon as we have finished our detailed article with more examples.

A challenge

The recent preprint [19] gives a recipe to construct absolutely simple modular abelian surfaces $A/\mathbb{Q}$ with odd primes p dividing $\#Ш(A/\mathbb{Q})$. In principle, our method can be used to verify strong BSD for them, but as the level of the quadratic twist A^D of A by the quadratic character with discriminant D equals ND^2, the computations quickly become infeasible. For example, all the 97 absolutely simple GL_2-type abelian surfaces listed in the LMFDB have analytic order of Ш approximately 1, 2 or 4. So we pose as a challenge to verify strong BSD for some $A/\mathbb{Q}$ with $Ш(A/\mathbb{Q})$ not a 2-group!

References

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

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3–4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over **Q**: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[4] Brendan Creutz and Robert L. Miller. Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula. *J. Algebra*, 372:673–701, 2012.

[5] Claus Fieker, William Hart, Tommy Hofmann, and Fredrik Johansson. Nemo/Hecke: Computer Algebra and Number Theory Packages for the Julia Programming Language. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, pages 157–164, New York, NY, USA, 2017. ACM.

[6] E. Victor Flynn, Franck Leprévost, Edward F. Schaefer, William A. Stein, Michael Stoll, and Joseph L. Wetherell. Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves. *Math. Comp.*, 70(236):1675–1697, 2001.

[7] Matthew Greenberg. Lifting modular symbols of non-critical slope. *Israel J. Math.*, 161:141–155, 2007.

[8] Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William A. Stein, and Corina Tarniţă. Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves. *Math. Comp.*, 78(268):2397–2425, 2009.

[9] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[10] Timo Keller and Michael Stoll. Exact verification of the strong BSD conjecture for some absolutely simple abelian surfaces, 2021. Preprint, arXiv:2107.00325, to appear in Comptes Rendus Mathématique.

[11] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. In *Proceedings of the International Congress of Mathematicians. Volume II*, page 280–293. Hindustan Book Agency, New Delhi, 2010.

[12] V. A. Kolyvagin and D. Yu. Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.

[13] Tyler Lawson and Christian Wuthrich. Vanishing of some Galois cohomology groups for elliptic curves. *Springer Proc. Math. Stat., vol. 188, Springer, Cham*, pages 373–399, 2016.

[14] Robert L. Miller. Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one. *LMS J. Comput. Math.*, 14:327–350, 2011.

[15] Robert L. Miller and Michael Stoll. Explicit isogeny descent on elliptic curves. *Math. Comp.*, 82(281):513–529, 2013.

[16] Jan Steffen Müller and Michael Stoll. Canonical heights on genus-2 Jacobians. *Algebra Number Theory*, 10(10):2153–2234, 2016.

[17] Robert Pollack and Glenn Stevens. Overconvergent modular symbols and p-adic L-functions. *Ann. Sci. Éc. Norm. Supér. (4)*, 44(1):1–42, 2011.

[18] Kenneth A. Ribet. Abelian varieties over **Q** and modular forms. *Modular curves and abelian varieties*, 224:241–261, 2004.

[19] Ari Shnidman and Ariel Weiss. Elements of prime order in Tate-Shafarevich groups of abelian varieties over $\mathbb{Q}$, 2021. Preprint, arXiv:2106.14096.

[20] Christopher Skinner. Multiplicative reduction and the cyclotomic main conjecture for GL_2. *Pacific J. Math.*, 283(1):171–200, 2016.

[21] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[22] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

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

[24] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.4)*, 2022. `https://www.sagemath.org`.

[25] Raymond 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.*, page 1–8, 2019.

[26] J.-L. Waldspurger. Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie. *Compositio Math.*, 54(2):173–242, 1985.

[27] Xiang Dong Wang. 2-dimensional simple factors of $J_0(N)$. *Manuscripta Math.*, 87(2):179–197, 1995.

[28] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Antrag auf Mitgliedschaft in der Fachgruppe Computeralgebra

Die Fachgruppe Computeralgebra sieht es als ihre Aufgabe an, Lehre, Forschung, Entwicklung, Anwendungen, Informationsaustausch und Zusammenarbeit auf dem Gebiet der Computeralgebra in Deutschland zu fördern.

Eine Mitgliedschaft in der Fachgruppe Computeralgebra gibt es bereits ab 7,50 € pro Jahr (für Mitglieder von DMV, GI oder GAMM; ansonsten 9 €).

Vorteile einer Mitgliedschaft:

- Sie fördern durch Ihren Beitrag die Workshops, Seminare, Tagungen und andere Aktivitäten auf dem Gebiet der Computeralgebra, die die Fachgruppe organisiert und unterstützt.
- Sie erhalten zweimal im Jahr den Computeralgebra-Rundbrief mit vielen interessanten Informationen rund um die Computeralgebra frei Haus.
- Sie verleihen unserer Stimme an Gewicht, die wir aktiv in Diskussionen um die Stellung der Computeralgebra in der Ausbildung in Schule und Hochschule einbringen.

Wir würden uns sehr über Ihre Unterstützung freuen. Die Mitgliedschaft in der Fachgruppe steht allen offen. Weiter Informationen zur Mitgliedschaft und einen Aufnahmeantrag finden Sie auf unserer Webseite unter folgender Adresse, oder scannen Sie einfach den QR-Code.

`https://fachgruppe-computeralgebra.de/aufnahmeantrag`

Fachgruppe Computeralgebra