Funded by
DFG Deutsche Forschungsgemeinschaft
German Research Foundation

Leibniz Universität Hannover

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

see arXiv:2107.00325 and forthcoming articles

Timo Keller

joint with Michael Stoll

Universität Hannover
(previously Universität Bayreuth)

July 21, 2022
PCMI Research Program
"Number Theory informed by Computation"

The BSD conjecture:
Why is it useful?

Fundamental problems

Let A be an abelian variety over $\mathbf{Q}$.

Problem 1

Compute $r := \operatorname{rk} A(\mathbf{Q})$, the *algebraic rank*.

For every $n > 1$, there is an n-descent exact sequence

$$0 \to A(\mathbf{Q})/n \to \mathrm{Sel}_n(A/\mathbf{Q}) \to Ш(A/\mathbf{Q})[n] \to 0$$

with the n-Selmer group $\mathrm{Sel}_n(A/\mathbf{Q})$ finite (and computable in principle).

Problem 2

Compute $Ш(A/\mathbf{Q})$, the *Shafarevich–Tate group*.

Fundamental problems

Let A be an abelian variety over $\mathbf{Q}$.

Problem 1

Compute $r := \operatorname{rk} A(\mathbf{Q})$, the *algebraic rank*.

For every $n > 1$, there is an n-descent exact sequence

$$0 \to A(\mathbf{Q})/n \to \mathrm{Sel}_n(A/\mathbf{Q}) \to Ш(A/\mathbf{Q})[n] \to 0$$

with the n-Selmer group $\mathrm{Sel}_n(A/\mathbf{Q})$ finite (and computable in principle).

Problem 2

Compute $Ш(A/\mathbf{Q})$, the *Shafarevich–Tate group*.

Statement of the BSD conjecture

Birch–Swinnerton-Dyer (rank) conjecture

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

For $A = E$ an elliptic curve:

- r_{an} well-defined by modularity of $E/\mathbf{Q}$.
- Yields "day-night algorithm" to compute r and hence $E(\mathbf{Q})$.
- Formulated based on computations in 1965.
- Proven if $r_{\mathrm{an}} \leq 1$.

strong BSD conjecture

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

Compare with the analytic class number formula!

Statement of the BSD conjecture

Birch–Swinnerton-Dyer (rank) conjecture

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

For $A = E$ an elliptic curve:

- r_{an} well-defined by modularity of $E/\mathbf{Q}$.
- Yields "day-night algorithm" to compute r and hence $E(\mathbf{Q})$.
- Formulated based on computations in 1965.
- Proven if $r_{\mathrm{an}} \leq 1$.

strong BSD conjecture

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

Compare with the analytic class number formula!

What are applications of the strong BSD conjecture?

Problem

Let $C/\mathbf{Q}$ be a curve of genus 1. Decide: $C(\mathbf{Q}) = \emptyset$? $\#C(\mathbf{Q}) = \infty$?

- Compute elliptic curve $E/\mathbf{Q}$ such that $[C] \in Ш(E/\mathbf{Q})$.
- If one can decide $C(\mathbf{Q}) \neq \emptyset$, one can decide $\#C(\mathbf{Q}) = \infty$ by deciding $L(E, 1) = 0$ (BSD rank conjecture).
- Compute $\#Ш(E/\mathbf{Q})$ using strong BSD.
- Enumerate representatives of $Ш(E/\mathbf{Q})$.
- Use the perfect Cassels–Tate pairing

$$\langle \cdot, \cdot \rangle : Ш(E/\mathbf{Q}) \times Ш(E/\mathbf{Q}) \to \mathbf{Q}/\mathbf{Z}$$

to decide existence of $[D] \in Ш(E/\mathbf{Q})$ with $\langle [C], [D] \rangle \neq 0$.

The BSD conjecture:
What is known?

What is already known about (strong) BSD?

Let A be a RM abelian variety over $\mathbf{Q}$ with associated newform f.

- Assume that $\mathrm{ord}_{s=1} L(f,s) \in \{0,1\}$ (hence $r_{\mathrm{an}} \in \{0, \dim A\}$).
- This implies by combining the Gross–Zagier formula with the Heegner point Euler system of Kolyvagin–Logachëv:

$$r = r_{\mathrm{an}}, \quad \text{(BSD rank conjecture)}$$
$$\#Ш(A/\mathbf{Q}) < \infty,$$
$$\#Ш(A/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}.$$

What is already known about (strong) BSD?

Let A be a RM abelian variety over $\mathbf{Q}$ with associated newform f.

- Assume that $\mathrm{ord}_{s=1} L(f,s) \in \{0,1\}$ (hence $r_{\mathrm{an}} \in \{0, \dim A\}$).
- This implies by combining the Gross–Zagier formula with the Heegner point Euler system of Kolyvagin–Logachëv:

$$\begin{aligned} r &= r_{\mathrm{an}}, \quad \text{(BSD rank conjecture)} \\ \#Ш(A/\mathbf{Q}) &< \infty, \\ \#Ш(A/\mathbf{Q})_{\mathrm{an}} &\in \mathbf{Q}_{>0}. \end{aligned}$$

- Unknown: $\#Ш(A/\mathbf{Q}) \stackrel{?}{=} \#Ш(A/\mathbf{Q})_{\mathrm{an}}$ (strong BSD)

What is already known about (strong) BSD?

Let A be a RM abelian variety over $\mathbf{Q}$ with associated newform f.

- Assume that $\mathrm{ord}_{s=1} L(f,s) \in \{0,1\}$ (hence $r_{\mathrm{an}} \in \{0, \dim A\}$).
- This implies by combining the Gross–Zagier formula with the Heegner point Euler system of Kolyvagin–Logachëv:

$$\begin{aligned} r &= r_{\mathrm{an}}, \quad \text{(BSD rank conjecture)} \\ \#Ш(A/\mathbf{Q}) &< \infty, \\ \#Ш(A/\mathbf{Q})_{\mathrm{an}} &\in \mathbf{Q}_{>0}. \end{aligned}$$

- Unknown: $\#Ш(A/\mathbf{Q}) \stackrel{?}{=} \#Ш(A/\mathbf{Q})_{\mathrm{an}}$ (strong BSD)

In which cases has strong BSD been verified?

- For elliptic curves with $r_{\text{an}} \leq 1$:
  - Strong BSD verified exactly for levels $N < 5000$ combining work of GRIGOROV–JORZA–PATRIKIS–STEIN–TARNIŢĂ (2009), MILLER (2011), MILLER–STOLL (2013, isogeny descent), CREUTZ–MILLER (2012, second isogeny descent), LAWSON–WUTHRICH (2016, use of p-adic L-functions).
- For RM abelian varieties of dimension > 1:
  - FLYNN–LEPRÉVOST–SCHAEFER–STEIN–STOLL–WETHERELL (2001): BSD for some Jacobians of dimension 2 numerically.
  - VAN BOMMEL (2019): BSD for some hyperelliptic Jacobians numerically up to squares.

In which cases has strong BSD been verified?

- For elliptic curves with $r_{\text{an}} \leq 1$:
  - Strong BSD verified exactly for levels $N < 5000$ combining work of Grigorov–Jorza–Patrikis–Stein–Tarniţă (2009), Miller (2011), Miller–Stoll (2013, isogeny descent), Creutz–Miller (2012, second isogeny descent), Lawson–Wuthrich (2016, use of p-adic L-functions).
- For RM abelian varieties of dimension > 1:
  - Flynn–Leprévost–Schaefer–Stein–Stoll–Wetherell (2001): BSD for some Jacobians of dimension 2 numerically.
  - van Bommel (2019): BSD for some hyperelliptic Jacobians numerically up to squares.
  - Skinner–Urban (2014): GL_2 Iwasawa Main Conjecture (IMC) for primes p of good ordinary reduction and ρ_p irreducible.
  - Skinner (2016): GL_2 IMC for primes p of bad multiplicative reduction and ρ_p irreducible.
  - Castella–Çiperiani–Skinner–Sprung (2019, preprint): $v_p(\#Ш(A/\mathbf{Q})) = v_p(\#Ш(A/\mathbf{Q})_{\text{an}})$ if N is square-free, $p \nmid N$, and ρ_p irreducible.

In which cases has strong BSD been verified?

- For elliptic curves with $r_{\mathrm{an}} \leq 1$:
  - Strong BSD verified exactly for levels $N < 5000$ combining work of Grigorov–Jorza–Patrikis–Stein–Tarniţă (2009), Miller (2011), Miller–Stoll (2013, isogeny descent), Creutz–Miller (2012, second isogeny descent), Lawson–Wuthrich (2016, use of p-adic L-functions).
- For RM abelian varieties of dimension > 1:
  - Flynn–Leprévost–Schaefer–Stein–Stoll–Wetherell (2001): BSD for some Jacobians of dimension 2 numerically.
  - van Bommel (2019): BSD for some hyperelliptic Jacobians numerically up to squares.
  - Skinner–Urban (2014): GL_2 Iwasawa Main Conjecture (IMC) for primes p of good ordinary reduction and ρ_p irreducible.
  - Skinner (2016): GL_2 IMC for primes p of bad multiplicative reduction and ρ_p irreducible.
  - Castella–Çiperiani–Skinner–Sprung (2019, preprint): $v_p(\#Ш(A/\mathbf{Q})) = v_p(\#Ш(A/\mathbf{Q})_{\mathrm{an}})$ if N is square-free, $p \nmid N$, and ρ_p irreducible.

What are our new results in dimension 2?

How to bound $\#Ш(A/\mathbf{Q})$?

There are two reasons why $Ш(A)$ could be infinite:

- "horizonal": $Ш(A)[p] \neq 0$ for infinitely many p.
- "vertical": $Ш(A)[p^\infty] \cong F \oplus (\mathbf{Q}_p/\mathbf{Z}_p)^n$ infinite for one p.

Solution to the "horizontal" problem:

Theorem (K.): explicit Euler system of Kolyvagin–Logachëv

Let A be a RM abelian variety over $\mathbf{Q}$. Denote $\mathcal{O} := \mathrm{End}_{\mathbf{Q}}(A)$.
One has $Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ for all $\mathfrak{p}$ with

- $\rho_{\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \longrightarrow \mathrm{Aut}_{\mathbf{F}_{\mathfrak{p}}}(A[\mathfrak{p}](\overline{\mathbf{Q}}))$ irreducible and
- $\mathfrak{p} \nmid 2 \cdot c \cdot \gcd_K(I_K)$ with Heegner indices I_K and the Tamagawa product c (both can be refined to $\mathcal{O}$-ideals).

How to bound $\#Ш(A/\mathbf{Q})$?

There are two reasons why $Ш(A)$ could be infinite:

- "horizonal": $Ш(A)[p] \neq 0$ for infinitely many p.
- "vertical": $Ш(A)[p^\infty] \cong F \oplus (\mathbf{Q}_p/\mathbf{Z}_p)^n$ infinite for one p.

Solution to the "horizontal" problem:

Theorem (K.): explicit Euler system of Kolyvagin–Logachëv

Let A be a RM abelian variety over $\mathbf{Q}$. Denote $\mathcal{O} := \mathrm{End}_{\mathbf{Q}}(A)$.
One has $Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ for all $\mathfrak{p}$ with

- $\rho_{\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \longrightarrow \mathrm{Aut}_{\mathbf{F}_{\mathfrak{p}}}(A[\mathfrak{p}](\overline{\mathbf{Q}}))$ irreducible and
- $\mathfrak{p} \nmid 2 \cdot c \cdot \gcd_K(I_K)$ with Heegner indices I_K and the Tamagawa product c (both can be refined to $\mathcal{O}$-ideals).

- These $\mathfrak{p}$ are explicitly computable and cover almost all $\mathfrak{p}$.
- In fact, $\mathfrak{p}^{2\,\mathrm{ord}_{\mathfrak{p}} I_K} Ш(A/\mathbf{Q})[\mathfrak{p}^\infty] = 0$ if $\rho_{\mathfrak{p}}$ irreducible and $\mathfrak{p} \nmid 2c$.
- We also have an explicit bound on $Ш(A/\mathbf{Q})[\mathfrak{p}^\infty]$ for *all* $\mathfrak{p}$.

How to bound $\#Ш(A/\mathbf{Q})$?

There are two reasons why $Ш(A)$ could be infinite:

- "horizonal": $Ш(A)[p] \neq 0$ for infinitely many p.
- "vertical": $Ш(A)[p^\infty] \cong F \oplus (\mathbf{Q}_p/\mathbf{Z}_p)^n$ infinite for one p.

Solution to the "horizontal" problem:

Theorem (K.): explicit Euler system of Kolyvagin–Logachëv

Let A be a RM abelian variety over $\mathbf{Q}$. Denote $\mathcal{O} := \mathrm{End}_{\mathbf{Q}}(A)$.
One has $Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ for all $\mathfrak{p}$ with

- $\rho_{\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{Aut}_{\mathbf{F}_{\mathfrak{p}}}(A[\mathfrak{p}](\overline{\mathbf{Q}}))$ irreducible and
- $\mathfrak{p} \nmid 2 \cdot c \cdot \gcd_K(I_K)$ with Heegner indices I_K and the Tamagawa product c (both can be refined to $\mathcal{O}$-ideals).

- These $\mathfrak{p}$ are explicitly computable and cover almost all $\mathfrak{p}$.
- In fact, $\mathfrak{p}^{2\,\mathrm{ord}_{\mathfrak{p}} I_K} Ш(A/\mathbf{Q})[\mathfrak{p}^\infty] = 0$ if $\rho_{\mathfrak{p}}$ irreducible and $\mathfrak{p} \nmid 2c$.
- We also have an explicit bound on $Ш(A/\mathbf{Q})[\mathfrak{p}^\infty]$ for *all* $\mathfrak{p}$.

What are the main obstacles in dimension > 1?

Problems when $\dim A > 1$ (necessary input for Euler system)

- We don't have an analog of Mazur's classification of rational isogenies of prime degree for *all* A: moduli spaces have dimension > 1.
- We have to compute Heegner points.

We solve the problems for concretely given $A = \mathrm{Jac}(C)$.

What are the main obstacles in dimension > 1?

Problems when $\dim A > 1$ (necessary input for Euler system)

- We don't have an analog of Mazur's classification of rational isogenies of prime degree for *all* A: moduli spaces have dimension > 1.
- We have to compute Heegner points.

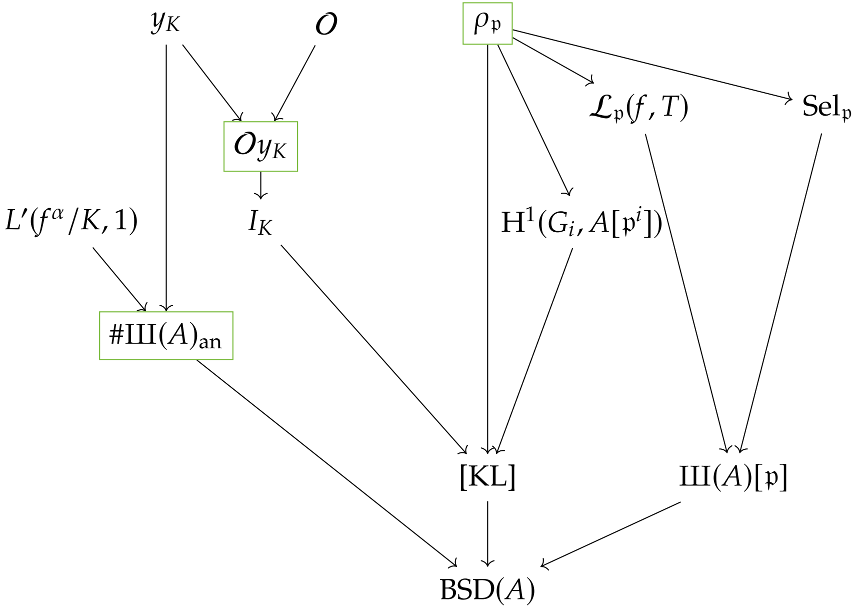
We solve the problems for concretely given $A = \mathrm{Jac}(C)$.

How to compute the remaining $Ш(A/\mathbf{Q})[\mathfrak{p}^\infty]$?

Two tools:

- Perform a $\mathfrak{p}^n$-descent to compute $\mathrm{Sel}_{\mathfrak{p}^n}(A/\mathbf{Q})$.
  - Works very well if $\rho_{\mathfrak{p}^n}$ is reducible.
  - Works for general $\mathfrak{p}^n$ in principle, but:
  - Infeasible if $\rho_{\mathfrak{p}^n}$ has large image,
    e.g., $\#\mathcal{O}/\mathfrak{p}^n > 7$ and $\rho_{\mathfrak{p}^n}$ irreducible, even assuming GRH.
- Compute the $\mathfrak{p}$-adic L-function and use the GL_2 IMC.
  - Can be computed very efficiently with overconvergent modular symbols using the Pollack–Stevens–Greenberg algorithm.
  - Requires $\rho_{\mathfrak{p}}$ to be irreducible.
    (But: work in progress joint with Castella)
  - Unclear for good non-ordinary and especially bad non-multiplicative reduction.
  - Requires the computation of the $\mathfrak{p}$-adic regulator if $r_{\mathrm{an}} > 0$ or if the reduction is split multiplicative.
    (work in progress by Kaya–Müller–van der Put)

How do we verify the conjecture?



Sketch of proofs

Almost all $\rho_{\mathfrak{p}}$ are irreducible

Theorem (K.)

Assume $v_p(N) \leq 1$.
If $\rho_{\mathfrak{p}}$ is reducible, $\rho_{\mathfrak{p}}^{ss} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with ε of conductor d with $d^2 \mid N$.
Hence: If $\rho_{\mathfrak{p}}$ is reducible as an $\mathbf{F}_{\mathfrak{p}}$-representation, then

$$\text{an eigenvalue of } \rho_{\mathfrak{p}}(\mathrm{Frob}_\ell) \text{ has order dividing } \operatorname{ord}(\bar{\ell} \in (\mathbf{Z}/d)^\times).$$

Hence:

for d maximal with $d^2 \mid N$.

Almost all $\rho_\mathfrak{p}$ are irreducible

Theorem (K.)

Assume $v_p(N) \leq 1$.
If $\rho_\mathfrak{p}$ is reducible, $\rho_\mathfrak{p}^{ss} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with ε of conductor d with $d^2 \mid N$.
Hence: If $\rho_\mathfrak{p}$ is reducible as an $\mathbf{F}_\mathfrak{p}$-representation, then

$$\text{an eigenvalue of } \rho_\mathfrak{p}(\mathrm{Frob}_\ell) \text{ has order dividing } \operatorname{ord}(\bar{\ell} \in (\mathbf{Z}/d)^\times).$$

Hence:

$$\mathfrak{p} \mid \operatorname{res}_{\mathcal{O}[X]}\left(\operatorname{charpol}_{\mathcal{O}[X]}(\rho_{\mathfrak{p}^\infty}(\mathrm{Frob}_\ell)), X^{\operatorname{ord}(\bar{\ell} \in (\mathbf{Z}/d)^\times)} - 1\right).$$

for d maximal with $d^2 \mid N$.

Almost all $\rho_{\mathfrak{p}}$ are irreducible

Theorem (K.)

Assume $v_p(N) \leq 1$.
If $\rho_{\mathfrak{p}}$ is reducible, $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with ε of conductor d with $d^2 \mid N$.
Hence: If $\rho_{\mathfrak{p}}$ is reducible as an $\mathbf{F}_{\mathfrak{p}}$-representation, then

$$\text{an eigenvalue of } \rho_{\mathfrak{p}}(\mathrm{Frob}_\ell) \text{ has order dividing } \operatorname{ord}(\bar{\ell} \in (\mathbf{Z}/d)^\times).$$

Hence:

$$\mathfrak{p} \mid \gcd_{\ell \nmid pN}\Big(\operatorname{res}_{\mathcal{O}[X]}\big(\operatorname{charpol}_{\mathcal{O}[X]}(\rho_{\mathfrak{p}^\infty}(\mathrm{Frob}_\ell)), X^{\operatorname{ord}(\bar{\ell}\in(\mathbf{Z}/d)^\times)} - 1\big)\Big).$$

for d maximal with $d^2 \mid N$.

- We can also treat the case $p^2 \mid N$.
- We can also do maximal image.
- Have upper bound on p depending on N.

Computing (a multiple of) the Heegner index I_K

Let $J = \mathrm{Jac}(X)$. There is an isogeny $\pi : J_0(N)/\mathrm{Ann}_{\mathbf{T}}(f) =: A_f \to J$.
Let K be a Heegner field for J.

$$\begin{array}{ccccc}
A_f(K) & \hookrightarrow & A_f(\mathbf{C}) & \xrightarrow{\sim} & \mathbf{C}^g/\Lambda_f \\
\downarrow & & \downarrow & & \downarrow \pi \\
J(K) & \hookrightarrow & J(\mathbf{C}) & \xrightarrow{\sim} & \mathbf{C}^g/\Lambda
\end{array}$$

1. Complex approximation of $y_K \in \mathbf{C}^g/\Lambda_f$ using integrals.
2. Compute the image of y_K under the isogeny $\pi : \mathbf{C}^g/\Lambda_f \to \mathbf{C}^g/\Lambda$.
3. Invert the Abel–Jacobi map $J(\mathbf{C}) \xrightarrow{\sim} \mathbf{C}^g/\Lambda$ using theta functions.
4. Approximate the Mumford representation in $J(K)$.
5. Prove correctness using $\hat{h}(y_K)$ from Gross–Zagier (reconstruct $\hat{h}_\vartheta$ on $J(K)$ from $\hat{h}_\iota$ on A_f with respect to isogeny $\iota : A_f^\vee \to A_f$).

Note that we use X hyperelliptic in steps 3 and 4.

How to compute $\#Ш(A/\mathbf{Q})_{\mathrm{an}}$ exactly?

- Compute $\frac{L(f,1)}{\Omega_f^+} \in \mathbf{Q}(f)$ exactly
  using modular symbols and Balakrishnan–Müller–Stein and van Bommel's code to compute Ω_A.
- If $L(A,1) \neq 0$, this gives $\#Ш(A/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ exactly.
- If $L(A,1) = 0$:
  - Choose a Heegner field K and compute $\frac{L(f_K,1)}{\mathrm{Reg}_{A/K}\,\Omega_{A/K}} \in \mathbf{Q}_{>0}$ exactly using Gross–Zagier, and hence compute $\#Ш(A/K)_{\mathrm{an}} \in \mathbf{Q}_{>0}$.
  - Compute $\#Ш(A^K/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ exactly.
  - Use $\#Ш(A/K)_{\mathrm{an}} = \#Ш(A/\mathbf{Q})_{\mathrm{an}} \cdot \#Ш(A^K/\mathbf{Q})_{\mathrm{an}}$ up to powers of 2 that can be explicitly bounded to compute $\#Ш(A/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ exactly.

How to compute $\#Ш(A/\mathbf{Q})_{\text{an}}$ exactly?

- Compute $\frac{L(f,1)}{\Omega_f^+} \in \mathbf{Q}(f)$ exactly using modular symbols and Balakrishnan–Müller–Stein and van Bommel's code to compute Ω_A.
- If $L(A,1) \neq 0$, this gives $\#Ш(A/\mathbf{Q})_{\text{an}} \in \mathbf{Q}_{>0}$ exactly.
- If $L(A,1) = 0$:
  - Choose a Heegner field K and compute $\frac{L(f_K,1)}{\text{Reg}_{A/K}\,\Omega_{A/K}} \in \mathbf{Q}_{>0}$ exactly using Gross–Zagier, and hence compute $\#Ш(A/K)_{\text{an}} \in \mathbf{Q}_{>0}$.
  - Compute $\#Ш(A^K/\mathbf{Q})_{\text{an}} \in \mathbf{Q}_{>0}$ exactly.
  - Use $\#Ш(A/K)_{\text{an}} = \#Ш(A/\mathbf{Q})_{\text{an}} \cdot \#Ш(A^K/\mathbf{Q})_{\text{an}}$ up to powers of 2 that can be explicitly bounded to compute $\#Ш(A/\mathbf{Q})_{\text{an}} \in \mathbf{Q}_{>0}$ exactly.

Examples in dimension 2

Can you give an example? $A = \mathrm{Jac}(X_0(39)/w_{13})$

- $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$
- $r = r_{\mathrm{an}} = 0$
- $\#Ш(A/\mathbf{Q})_{\mathrm{an}} = 1$
- $A(\mathbf{Q}) = A(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2 \times \mathbf{Z}/(2 \cdot 7)$
- $\rho_{\mathfrak{p}}$ is reducible exactly for $\mathfrak{p} = (\sqrt{2})$ and exactly one $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- [KL] with $I_{\mathbf{Q}(\sqrt{-23})} = 7$ gives $\#Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ for $\mathfrak{p} \nmid (\sqrt{2}), 7$.

Can you give an example? $A = \mathrm{Jac}(X_0(39)/w_{13})$

- $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$
- $r = r_{\mathrm{an}} = 0$
- $\#Ш(A/\mathbf{Q})_{\mathrm{an}} = 1$
- $A(\mathbf{Q}) = A(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2 \times \mathbf{Z}/(2 \cdot 7)$
- $\rho_{\mathfrak{p}}$ is reducible exactly for $\mathfrak{p} = (\sqrt{2})$ and exactly one $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- [KL] with $I_{\mathbf{Q}(\sqrt{-23})} = 7$ gives $\#Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ for $\mathfrak{p} \nmid (\sqrt{2}), 7$.
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})/2$ gives $Ш(A/\mathbf{Q})[2] = 0$.

Can you give an example? $A = \mathrm{Jac}(X_0(39)/w_{13})$

- $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$
- $r = r_{\mathrm{an}} = 0$
- $\#Ш(A/\mathbf{Q})_{\mathrm{an}} = 1$
- $A(\mathbf{Q}) = A(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2 \times \mathbf{Z}/(2 \cdot 7)$
- $\rho_{\mathfrak{p}}$ is reducible exactly for $\mathfrak{p} = (\sqrt{2})$ and exactly one $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- [KL] with $I_{\mathbf{Q}(\sqrt{-23})} = 7$ gives $\#Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ for $\mathfrak{p} \nmid (\sqrt{2}), 7$.
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})/2$ gives $Ш(A/\mathbf{Q})[2] = 0$.
- $\rho_{\mathfrak{p}}$ is reducible with

$$0 \longrightarrow \mathbf{Z}/7 \longrightarrow A[\mathfrak{p}] \longrightarrow \mu_7 \longrightarrow 1$$

  non-split exact, and $\mathrm{Sel}_{\mathfrak{p}}(A/\mathbf{Q}) \cong \mathbf{Z}/7 \cong A(\mathbf{Q})[7]$ by descent. Hence $Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$.

Can you give an example? $A = \mathrm{Jac}(X_0(39)/w_{13})$

- $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$
- $r = r_{\mathrm{an}} = 0$
- $\#Ш(A/\mathbf{Q})_{\mathrm{an}} = 1$
- $A(\mathbf{Q}) = A(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2 \times \mathbf{Z}/(2 \cdot 7)$
- $\rho_{\mathfrak{p}}$ is reducible exactly for $\mathfrak{p} = (\sqrt{2})$ and exactly one $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- [KL] with $I_{\mathbf{Q}(\sqrt{-23})} = 7$ gives $\#Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ for $\mathfrak{p} \nmid (\sqrt{2}), 7$.
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})/2$ gives $Ш(A/\mathbf{Q})[2] = 0$.
- $\rho_{\mathfrak{p}}$ is reducible with

$$0 \to \mathbf{Z}/7 \to A[\mathfrak{p}] \to \mu_7 \to 1$$

non-split exact, and $\mathrm{Sel}_{\mathfrak{p}}(A/\mathbf{Q}) \cong \mathbf{Z}/7 \cong A(\mathbf{Q})[7]$ by descent. Hence $Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$.
- The $\bar{\mathfrak{p}}$-adic L-function has constant term a unit in $\mathcal{O}_{\bar{\mathfrak{p}}} \simeq \mathbf{Z}_7$, hence the integral GL_2 IMC shows $\mathrm{Sel}_{\bar{\mathfrak{p}}}(A/\mathbf{Q}) = 0$ since $\rho_{\bar{\mathfrak{p}}}$ is irreducible.

Can you give an example? $A = \mathrm{Jac}(X_0(39)/w_{13})$

- $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$
- $r = r_{\mathrm{an}} = 0$
- $\#Ш(A/\mathbf{Q})_{\mathrm{an}} = 1$
- $A(\mathbf{Q}) = A(\mathbf{Q})_{\mathrm{tors}} \cong \mathbf{Z}/2 \times \mathbf{Z}/(2 \cdot 7)$
- $\rho_{\mathfrak{p}}$ is reducible exactly for $\mathfrak{p} = (\sqrt{2})$ and exactly one $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- [KL] with $I_{\mathbf{Q}(\sqrt{-23})} = 7$ gives $\#Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ for $\mathfrak{p} \nmid (\sqrt{2}), 7$.
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})/2$ gives $Ш(A/\mathbf{Q})[2] = 0$.
- $\rho_{\mathfrak{p}}$ is reducible with

  $$0 \longrightarrow \mathbf{Z}/7 \longrightarrow A[\mathfrak{p}] \longrightarrow \mu_7 \longrightarrow 1$$

  non-split exact, and $\mathrm{Sel}_{\mathfrak{p}}(A/\mathbf{Q}) \cong \mathbf{Z}/7 \cong A(\mathbf{Q})[7]$ by descent. Hence $Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$.
- The $\bar{\mathfrak{p}}$-adic L-function has constant term a unit in $\mathcal{O}_{\bar{\mathfrak{p}}} \simeq \mathbf{Z}_7$, hence the integral GL_2 IMC shows $\mathrm{Sel}_{\bar{\mathfrak{p}}}(A/\mathbf{Q}) = 0$ since $\rho_{\bar{\mathfrak{p}}}$ is irreducible.

All Atkin-Lehner quotients of genus 2 of our type (I)

X	r	$\mathcal{O}$	$\#Ш_{an}$	$\rho_{\mathfrak{p}}$ 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

All Atkin-Lehner quotients of genus 2 of our type (II)

X	r	$\mathcal{O}$	$\#Ш_{an}$	$\rho_{\mathfrak{p}}$ red.	c	(D, I_D)	$\#Ш$
$X_0(133)^*$	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

Outlook

What would be nice to achieve?

- Using Shnidman–Weiss[1], find examples of $A/\mathbf{Q}$ with

$$\#Ш(A/\mathbf{Q}) = \#Ш(A/\mathbf{Q})_{\mathrm{an}} \neq 2^i!$$

  Can have $p \in \{3, 5, 7, 11, (13?), \ldots, (31?), \ldots?\}$.
- Find $J/\mathbf{Q}$ and $\mathfrak{p} \mid p$ "large" with
  - $p^2 \mid N$ (no p-adic L-functions),
  - $\mathfrak{p} \mid c \cdot I_K$ ([KL] does not give $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$), and
  - $\rho_{\mathfrak{p}}$ irreducible ($\mathfrak{p}$-descent hard)!

[1] *Elements of prime order in Tate-Shafarevich groups of abelian varieties over* $\mathbb{Q}$, `arXiv:2106.14096`

What are the next steps and projects?

- Almost done: Verification for all 97 genus 2 curves with absolutely simple RM Jacobian from the LMFDB.
- Verification for (almost?) all ~ 1200 newforms of level ≤ 1000 with real-quadratic coefficients foreseeable.

What are the next steps and projects?

- Almost done: Verification for all 97 genus 2 curves with absolutely simple RM Jacobian from the LMFDB.
- Verification for (almost?) all ~ 1200 newforms of level ≤ 1000 with real-quadratic coefficients foreseeable.
- RM abelian threefolds: A generic curve of genus 3 is non-hyperelliptic, so we need an explicit theory of Jacobians and heights.
- Strong BSD over totally real fields.

What are the next steps and projects?

- Almost done: Verification for all 97 genus 2 curves with absolutely simple RM Jacobian from the LMFDB.
- Verification for (almost?) all ~ 1200 newforms of level ≤ 1000 with real-quadratic coefficients foreseeable.
- RM abelian threefolds: A generic curve of genus 3 is non-hyperelliptic, so we need an explicit theory of Jacobians and heights.
- Strong BSD over totally real fields.

Thank you!