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

see arXiv:2107.00325 and forthcoming articles

Timo Keller
joint with Michael Stoll

Universität Bayreuth

March 14, 2022
Outline

The BSD conjecture: motivation and overview

Computing the image of $\rho_p$

Computing the Heegner index $I_K$

Examples

Outlook
The BSD conjecture: motivation and overview
Motivating problem
Making the Mordell–Weil theorem explicit

Theorem of Mordell–Weil
Let $A$ be an abelian variety over $\mathbb{Q}$, e.g. $A = E$ an elliptic curve. Then the Mordell–Weil group $A(\mathbb{Q})$ is a finitely generated abelian group.

Proof (sketch).
For every $n > 1$, there is an $n$-descent exact sequence

$$0 \rightarrow A(\mathbb{Q})/n \rightarrow \text{Sel}_n(A/\mathbb{Q}) \rightarrow \text{III}(A/\mathbb{Q})[n] \rightarrow 0 \quad (1)$$

with the $n$-Selmer group $\text{Sel}_n(A/\mathbb{Q})$ finite (and computable in principle).
Motivating problem
Making the Mordell–Weil theorem explicit

Theorem of Mordell–Weil

Let $A$ be an abelian variety over $\mathbb{Q}$, e.g. $A = E$ an elliptic curve. Then the Mordell–Weil group $A(\mathbb{Q})$ is a finitely generated abelian group.

Proof (sketch).

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

$$0 \to A(\mathbb{Q})/n \to \text{Sel}_n(A/\mathbb{Q}) \to \text{III}(A/\mathbb{Q})[n] \to 0 \quad (1)$$

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

Now use the theory of heights to deduce finite generation of $A(\mathbb{Q})$ from that of $A(\mathbb{Q})/n$. \qed
Motivating problem
Making the Mordell–Weil theorem explicit

Theorem of Mordell–Weil

Let $A$ be an abelian variety over $\mathbb{Q}$, e.g. $A = E$ an elliptic curve. Then the Mordell–Weil group $A(\mathbb{Q})$ is a finitely generated abelian group.

Proof (sketch).
For every $n > 1$, there is an $n$-descent exact sequence

$$0 \rightarrow A(\mathbb{Q})/n \rightarrow \text{Sel}_n(A/\mathbb{Q}) \rightarrow \Sha(A/\mathbb{Q})[n] \rightarrow 0$$

(1)

with the $n$-Selmer group $\text{Sel}_n(A/\mathbb{Q})$ finite (and computable in principle). Now use the theory of heights to deduce finite generation of $A(\mathbb{Q})$ from that of $A(\mathbb{Q})/n$. 

Problem

Compute all three finite groups in (1)!
Motivating problem
Making the Mordell–Weil theorem explicit

Theorem of Mordell–Weil
Let $A$ be an abelian variety over $\mathbb{Q}$, e.g. $A = E$ an elliptic curve. Then the Mordell–Weil group $A(\mathbb{Q})$ is a finitely generated abelian group.

Proof (sketch).
For every $n > 1$, there is an $n$-descent exact sequence

$$0 \to A(\mathbb{Q})/n \to \text{Sel}_n(A/\mathbb{Q}) \to \text{III}(A/\mathbb{Q})[n] \to 0 \quad (1)$$

with the $n$-Selmer group $\text{Sel}_n(A/\mathbb{Q})$ finite (and computable in principle).
Now use the theory of heights to deduce finite generation of $A(\mathbb{Q})$ from that of $A(\mathbb{Q})/n$. □

Problem
Compute all three finite groups in (1)!
The Birch–Swinnerton-Dyer conjecture

**L-function of** $E$:

$$L(E, s) = \prod_{p \in S_{\text{good}}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \cdot \prod_{p \in S_{\text{bad}}} \frac{1}{1 - a_p p^{-s}}$$

with $a_p = p + 1 - \#E(F_p)$ for $p \in S_{\text{good}}$ (trace of $p$-Frobenius).

**Birch–Swinnerton-Dyer conjecture**

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

- Formulated based on computations in 1965.
- $r_{\text{an}}$ well-defined by modularity of $E/\mathbb{Q}$.
- Yields “day-night algorithm” to compute $E(\mathbb{Q})$.
- Proven if $r_{\text{an}} \leq 1$. 
The Birch–Swinnerton-Dyer conjecture

**L-function of E:**

\[ L(E, s) = \prod_{p \in S_{\text{good}}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \cdot \prod_{p \in S_{\text{bad}}} \frac{1}{1 - a_p p^{-s}} \]

with \( a_p = p + 1 - \#E(F_p) \) for \( p \in S_{\text{good}} \) (trace of \( p \)-Frobenius).

Birch–Swinnerton-Dyer conjecture

\[ r = r_{\text{an}} := \text{ord}_{s=1} L(E, s) \]

- Formulated based on computations in 1965.
- \( r_{\text{an}} \) well-defined by modularity of \( E/\mathbb{Q} \).
- Yields “day-night algorithm” to compute \( E(\mathbb{Q}) \).
- Proven if \( r_{\text{an}} \leq 1 \).
The Shafarevich–Tate group

The Shafarevich–Tate group

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

classifies everywhere locally \( A \)-torsors.

- \( \mathrm{Ш}(A/\mathbb{Q}) \) measures the failure of the local-global principle for principal homogeneous spaces for \( A/\mathbb{Q} \).
- Conjecture: finite!
The Shafarevich–Tate group

The Shafarevich–Tate group

$$\Sha(A/Q) := \ker \left( H^1(Q, A) \to \bigoplus_v H^1(Q_v, A) \right)$$

classifies everywhere locally $A$-torsors.

- $\Sha(A/Q)$ measures the failure of the local-global principle for principal homogeneous spaces for $A/Q$.
- Conjecture: finite!

**strong BSD conjecture**

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

Compare with the analytic class number formula!
The Shafarevich–Tate group

\[ \text{III}(A/\mathbb{Q}) := \ker \left( H^1(\mathbb{Q}, A) \to \bigoplus_v H^1(\mathbb{Q}_v, A) \right) \]

classifies everywhere locally \( A \)-torsors.

- \( \text{III}(A/\mathbb{Q}) \) measures the failure of the local-global principle for principal homogeneous spaces for \( A/\mathbb{Q} \).
- Conjecture: finite!

strong BSD conjecture

\[ \#\text{III}(A/\mathbb{Q}) = \#\text{III}(A/\mathbb{Q})_{\text{an}} : = \frac{\# A(\mathbb{Q})_{\text{tors}} \cdot \# A^\vee(\mathbb{Q})_{\text{tors}}}{\prod_p c_p} \cdot \frac{L^*(A, 1)}{\Omega_A \text{Reg}_A} \]

Compare with the analytic class number formula!
An example for the Shafarevich–Tate group

The Selmer cubic

\[ C : 3x^3 + 4y^3 + 5z^3 = 0 \]

is a non-trivial element of \( \Sha(E/\Q)[3] \) with the elliptic curve

\[ E : x^3 + y^3 + 3 \cdot 4 \cdot 5 \cdot z^3 = 0 \]

with \( r = r_{\text{an}} = 0 \).

Proof (sketch).

\( C(\Q_v) \neq \emptyset \): Weil conjectures or \( H^1(F_p, E) = 0 \) and Hensel’s lemma.
\( C(\Q) = \emptyset \): Cassels: Non-trivial point gives point in \( E(\Q) \) with \( z \neq 0 \), but \( E(\Q) = \{[1 : -1 : 0]\} \).
An example for the Shafarevich–Tate group

The Selmer cubic

\[ C : 3x^3 + 4y^3 + 5z^3 = 0 \]

is a non-trivial element of \( \Sha(E/Q)[3] \) with the elliptic curve

\[ E : x^3 + y^3 + 3 \cdot 4 \cdot 5 \cdot z^3 = 0 \]

with \( r = r_{\text{an}} = 0 \).

Proof (sketch).

\( C(\mathbb{Q}_v) \neq \emptyset \): Weil conjectures or \( H^1(F_p, E) = 0 \) and Hensel’s lemma.
\( C(\mathbb{Q}) = \emptyset \): Cassels: Non-trivial point gives point in \( E(\mathbb{Q}) \) with \( z \neq 0 \), but \( E(\mathbb{Q}) = \{[1 : -1 : 0]\} \).

Assuming strong BSD, one has

\( \Sha(E/Q) \cong (\mathbb{Z}/3)^2 \).
An example for the Shafarevich–Tate group

The Selmer cubic

\[ C : 3x^3 + 4y^3 + 5z^3 = 0 \]

is a non-trivial element of \( \Sha(E/Q)[3] \) with the elliptic curve

\[ E : x^3 + y^3 + 3 \cdot 4 \cdot 5 \cdot z^3 = 0 \]

with \( r = r_{\text{an}} = 0 \).

**Proof (sketch).**

\( C(Q_v) \neq \emptyset \): Weil conjectures or \( H^1(F_p, E) = 0 \) and Hensel’s lemma.

\( C(Q) = \emptyset \): Cassels: Non-trivial point gives point in \( E(Q) \) with \( z \neq 0 \), but \( E(Q) = \{[1 : -1 : 0]\} \).

Assuming strong BSD, one has

\[ \Sha(E/Q) \cong (\mathbb{Z}/3)^2. \]
Application of the strong BSD conjecture

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

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

$$\langle \cdot, \cdot \rangle : \Sha(E/\mathbb{Q}) \times \Sha(E/\mathbb{Q}) \rightarrow \mathbb{Q}/\mathbb{Z}$$

to find $[D] \in \Sha(E/\mathbb{Q})$ or not with $\langle [C], [D] \rangle \neq 0$. 
State of the art: some history

- **Birch–Swinnerton-Dyer (1965):** formulation of BSD.
- **Coates–Wiles (1977):** $r_{an} = 0 \implies r = 0$ for $E$ CM.
State of the art: some history

- **Birch–Swinnerton-Dyer (1965):** formulation of BSD.
- **Coates–Wiles (1977):** \( r_{\text{an}} = 0 \implies r = 0 \) for \( E \) CM.
- **Gross–Zagier (1986):** \( r_{\text{an}} = 1 \implies r \geq 1 \) for \( E \) modular
  (and for \( A_f/\mathbb{Q} \) modular: \( r_{\text{an}}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f \)).
State of the art: some history

- **Birch–Swinnerton-Dyer** (1965): formulation of BSD.
- **Coates–Wiles** (1977): $r_{an} = 0 \implies r = 0$ for $E$ CM.
- **Gross–Zagier** (1986): $r_{an} = 1 \implies r \geq 1$ for $E$ modular (and for $A_f/Q$ modular: $r_{an}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f$).
- **Rubin** (1987): $r_{an} = 0 \implies \Sha(E/K)$ finite for $E/K$ CM.
State of the art: some history

- **Birch–Swinnerton-Dyer (1965):** formulation of BSD.
- **Coates–Wiles (1977):** \( r_{an} = 0 \implies r = 0 \) for \( E \) CM.
- **Gross–Zagier (1986):** \( r_{an} = 1 \implies r \geq 1 \) for \( E \) modular (and for \( A_f/\mathbb{Q} \) modular: \( r_{an}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f \)).
- **Rubin (1987):** \( r_{an} = 0 \implies \text{III}(E/K) \) finite for \( E/K \) CM.
- **Kolyvagin (1988):** \( r_{an} \leq 1 \implies r = r_{an} \) and III finite for \( E/\mathbb{Q} \).
State of the art: some history

- **Birch–Swinnerton-Dyer** (1965): formulation of BSD.
- **Coates–Wiles** (1977): $r_{\text{an}} = 0 \implies r = 0$ for $E$ CM.
- **Gross–Zagier** (1986): $r_{\text{an}} = 1 \implies r \geq 1$ for $E$ modular (and for $A_f/\mathbb{Q}$ modular: $r_{\text{an}}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f$).
- **Rubin** (1987): $r_{\text{an}} = 0 \implies \text{III}(E/K)$ finite for $E/K$ CM.
- **Kolyvagin** (1988): $r_{\text{an}} \leq 1 \implies r = r_{\text{an}}$ and III finite for $E/\mathbb{Q}$.
- **Kolyvagin–Logachëv** (1989) [KL]: $r_{\text{an}}(f) \leq 1 \implies r = r_{\text{an}}$ and III finite for $A_f/\mathbb{Q}$ modular.
State of the art: some history

- **Birch–Swinnerton-Dyer (1965):** formulation of BSD.
- **Coates–Wiles (1977):** $r_{an} = 0 \implies r = 0$ for $E$ CM.
- **Gross–Zagier (1986):** $r_{an} = 1 \implies r \geq 1$ for $E$ modular
  (and for $A_f/\mathbb{Q}$ modular: $r_{an}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f$).
- **Rubin (1987):** $r_{an} = 0 \implies \text{III}(E/K)$ finite for $E/K$ CM.
- **Kolyvagin (1988):** $r_{an} \leq 1 \implies r = r_{an}$ and III finite for $E/\mathbb{Q}$.
- **Kolyvagin–Logachëv (1989) [KL]:** $r_{an}(f) \leq 1 \implies r = r_{an}$
  and III finite for $A_f/\mathbb{Q}$ modular.
- **Wiles, Taylor–Wiles (1994):** every $E/\mathbb{Q}$ semistable is modular.
State of the art: some history

- **Birch–Swinnerton-Dyer** (1965): formulation of BSD.
- **Coates–Wiles** (1977): $r_{\text{an}} = 0 \implies r = 0$ for $E$ CM.
- **Gross–Zagier** (1986): $r_{\text{an}} = 1 \implies r \geq 1$ for $E$ modular (and for $A_f/Q$ modular: $r_{\text{an}}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f$).
- **Rubin** (1987): $r_{\text{an}} = 0 \implies \text{III}(E/K)$ finite for $E/K$ CM.
- **Kolyvagin** (1988): $r_{\text{an}} \leq 1 \implies r = r_{\text{an}}$ and III finite for $E/Q$.
- **Kolyvagin–Logachëv** (1989) [KL]: $r_{\text{an}}(f) \leq 1 \implies r = r_{\text{an}}$ and III finite for $A_f/Q$ modular.
State of the art: some history

- **Birch–Swinnerton-Dyer** (1965): formulation of BSD.
- **Coates–Wiles** (1977): \( r_{\text{an}} = 0 \implies r = 0 \) for \( E \) CM.
- **Gross–Zagier** (1986): \( r_{\text{an}} = 1 \implies r \geq 1 \) for \( E \) modular (and for \( A_f/\mathbb{Q} \) modular: \( r_{\text{an}}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f \)).
- **Rubin** (1987): \( r_{\text{an}} = 0 \implies \text{III}(E/K) \) finite for \( E/K \) CM.
- **Kolyvagin** (1988): \( r_{\text{an}} \leq 1 \implies r = r_{\text{an}} \) and III finite for \( E/\mathbb{Q} \).
- **Kolyvagin–Logachëv** (1989) [KL]: \( r_{\text{an}}(f) \leq 1 \implies r = r_{\text{an}} \) and III finite for \( A_f/\mathbb{Q} \) modular.
- **Wiles, Taylor–Wiles** (1994): every \( E/\mathbb{Q} \) semistable is modular.
- **Ribet** (2004): Serre’s modularity conjecture \( \implies \) every \( A/\mathbb{Q} \) with RM is modular.
State of the art: some history

- **Birch–Swinnerton-Dyer (1965)**: formulation of BSD.
- **Coates–Wiles (1977)**: $r_{an} = 0 \implies r = 0$ for $E$ CM.
- **Gross–Zagier (1986)**: $r_{an} = 1 \implies r \geq 1$ for $E$ modular (and for $A_f/Q$ modular: $r_{an}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f$).
- **Rubin (1987)**: $r_{an} = 0 \implies \Sha(E/K)$ finite for $E/K$ CM.
- **Kolyvagin (1988)**: $r_{an} \leq 1 \implies r = r_{an}$ and $\Sha$ finite for $E/Q$.
- **Kolyvagin–Logachëv (1989) [KL]**: $r_{an}(f) \leq 1 \implies r = r_{an}$ and $\Sha$ finite for $A_f/Q$ modular.
- **Wiles, Taylor–Wiles (1994)**: every $E/Q$ semistable is modular.
- **Ribet (2004)**: Serre’s modularity conjecture $\implies$ every $A/Q$ with RM is modular.
- **Khare–Kisin–Wintenberger (2010)**: Serre’s modularity conjecture holds.
Birch–Swinnerton-Dyer (1965): formulation of BSD.

Coates–Wiles (1977): $r_{an} = 0 \implies r = 0$ for $E$ CM.

Gross–Zagier (1986): $r_{an} = 1 \implies r \geq 1$ for $E$ modular (and for $A_f/\mathbb{Q}$ modular: $r_{an}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f$).

Rubin (1987): $r_{an} = 0 \implies \Sha(E/K)$ finite for $E/K$ CM.

Kolyvagin (1988): $r_{an} \leq 1 \implies r = r_{an}$ and $\Sha$ finite for $E/\mathbb{Q}$.

Kolyvagin–Logachëv (1989) [KL]: $r_{an}(f) \leq 1 \implies r = r_{an}$ and $\Sha$ finite for $A_f/\mathbb{Q}$ modular.

Wiles, Taylor–Wiles (1994): every $E/\mathbb{Q}$ semistable is modular.


Ribet (2004): Serre’s modularity conjecture $\implies$ every $A/\mathbb{Q}$ with RM is modular.

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

- Assume that the $L$-rank $\text{ord}_{s=1} L(f, s)$ equals 0 or 1.
- This implies by the Gross–Zagier formula:

  $$ r \geq r_{\text{an}}, \quad \# \text{III}(A/\mathbb{Q})_{\text{an}} \in \mathbb{Q}_{>0}, $$

  and by the Heegner point Euler system of Kolyvagin–Logachëv:

  $$ r = r_{\text{an}}, \quad \# \text{III}(A/\mathbb{Q}) < \infty. $$
Let $A$ be a modular abelian variety over $\mathbb{Q}$ with associated newform $f$.

- Assume that the $L$-rank $\operatorname{ord}_{s=1} L(f, s)$ equals 0 or 1.
- This implies by the Gross–Zagier formula:

  $$r \geq r_{\text{an}}, \quad \# \Sha(A/\mathbb{Q})_{\text{an}} \in \mathbb{Q}_{>0},$$

  and by the Heegner point Euler system of Kolyvagin–Logachëv:

  $$r = r_{\text{an}}, \quad \# \Sha(A/\mathbb{Q}) < \infty.$$
Let $A$ be a modular abelian variety over $\mathbb{Q}$ with associated newform $f$.

- Assume that the $L$-rank $\text{ord}_{s=1} L(f, s)$ equals 0 or 1.
- This implies by the Gross–Zagier formula:

\[
    r \geq r_{\text{an}}, \quad \#\Sha(A/\mathbb{Q})_{\text{an}} \in \mathbb{Q}_{>0},
\]

and by the Heegner point Euler system of Kolyvagin–Logachëv:

\[
    r = r_{\text{an}}, \quad \#\Sha(A/\mathbb{Q}) < \infty.
\]

- **Unknown:** $\#\Sha(A/\mathbb{Q}) \neq \#\Sha(A/\mathbb{Q})_{\text{an}}$ (strong BSD)
Previous work on the verification

- For elliptic curves:

- In dimension $> 1$:
Previous work on the verification

- For elliptic curves:

- In dimension $> 1$:
  - Skinner–Urban (2014): $GL_2$ Iwasawa Main Conjecture (IMC) for primes $p$ of good ordinary reduction and $\rho_p$ irreducible.
  - Skinner (2016): $GL_2$ IMC for primes $p$ of bad multiplicative reduction and $\rho_p$ irreducible.
Previous work on the verification

- For elliptic curves:

- In dimension $> 1$:
  - Skinner–Urban (2014): GL$_2$ Iwasawa Main Conjecture (IMC) for primes $p$ of good ordinary reduction and $\rho_p$ irreducible.
  - Skinner (2016): GL$_2$ IMC for primes $p$ of bad multiplicative reduction and $\rho_p$ irreducible.
  - van Bommel (2019): BSD for some hyperelliptic Jacobians numerically up to squares.
Previous work on the verification

- For elliptic curves:

- In dimension $> 1$:
  - Skinner–Urban (2014): $\text{GL}_2$ Iwasawa Main Conjecture (IMC) for primes $p$ of good ordinary reduction and $\rho_p$ irreducible.
  - Skinner (2016): $\text{GL}_2$ IMC for primes $p$ of bad multiplicative reduction and $\rho_p$ irreducible.
  - van Bommel (2019): BSD for some hyperelliptic Jacobians numerically up to squares.
    \[ v_p(\#\overline{\text{III}}(A/\mathbb{Q})) = v_p(\#\overline{\text{III}}(A/\mathbb{Q})_{\text{an}}) \]
    if $N$ is square-free, $p \nmid N$, and $\rho_p$ irreducible.
Previous work on the verification

▶ For elliptic curves:

▶ In dimension $> 1$:
- Skinner–Urban (2014): $GL_2$ Iwasawa Main Conjecture (IMC) for primes $p$ of good ordinary reduction and $\rho_p$ irreducible.
- Skinner (2016): $GL_2$ IMC for primes $p$ of bad multiplicative reduction and $\rho_p$ irreducible.
- van Bommel (2019): BSD for some hyperelliptic Jacobians numerically up to squares.
- Castella–Çiperiani–Skinner–Sprung (2019, preprint): $\nu_p(#\Sha(A/\mathbb{Q})) = \nu_p(#\Sha(A/\mathbb{Q})_{an})$ if $N$ is square-free, $p \nmid N$, and $\rho_p$ irreducible.
Theorem (consequence of Serre’s Modularity Conjecture)

Let $A/\mathbb{Q}$ be an absolutely simple abelian variety. The following are equivalent:

- $A/\mathbb{Q}$ has real multiplication,
- $A$ is an isogeny quotient of $J_0(N)$ for some $N$, 

If this is the case, we call $A/\mathbb{Q}$ modular, and then $N \dim A$ is the conductor of $A/\mathbb{Q}$ and $\mathcal{O} = \text{End}_{\mathbb{Q}}(A)$, and $A$ is of GL$_2$-type over $\mathbb{Q}$: $\dim \text{End}(A) \otimes \mathbb{Q} \ell V_\ell A = 2$. 


Modularity in dimension > 1

**Theorem (consequence of Serre’s Modularity Conjecture)**

Let \( A/\mathbb{Q} \) be an absolutely simple abelian variety. The following are equivalent:

- \( A/\mathbb{Q} \) has **real multiplication**, 
- \( A \) is an isogeny quotient of \( J_0(N) \) for some \( N \), 
- \( L(A/\mathbb{Q}, s) = \prod_{\alpha: \mathcal{O} \to \mathbb{C}} L(f^\alpha, s) \) for a newform \( f \in S_2(\Gamma_0(N), \mathcal{O}) \).

\[
L(A/\mathbb{Q}, s) = \prod_p \frac{1}{\det(1 - \text{Frob}_p p^{-s} | (V_\ell A)^I_p)}
\]

\[
L(f, s) = \prod_{p \nmid N} \frac{1}{1 - a_p(f) p^{-s} + p^{1-2s}} \cdot \prod_{p | N} \frac{1}{1 - a_p(f) p^{-s}}
\]
Theorem (consequence of Serre’s Modularity Conjecture)

Let \( A/\mathbb{Q} \) be an absolutely simple abelian variety. The following are equivalent:

- \( A/\mathbb{Q} \) has **real multiplication**, 
- \( A \) is an isogeny quotient of \( J_0(N) \) for some \( N \), 
- \( L(A/\mathbb{Q}, s) = \prod_{\alpha: \mathcal{O} \to \mathbb{C}} L(f^\alpha, s) \) for a newform \( f \in S_2(\Gamma_0(N), \mathcal{O}) \).

\[
L(A/\mathbb{Q}, s) = \prod_p \frac{1}{\det(1 - \text{Frob}_p p^{-s} | (V_\ell A)^{I_p})}
\]

\[
L(f, s) = \prod_{p \nmid N} \frac{1}{1 - a_p(f) p^{-s} + p^{1-2s}} \cdot \prod_{p | N} \frac{1}{1 - a_p(f) p^{-s}}
\]

If this is the case, we call \( A/\mathbb{Q} \) **modular**, and then \( N^{\dim A} \) is the conductor of \( A/\mathbb{Q} \) and \( \mathcal{O} \cong \text{End}_{\mathbb{Q}}(A) \), and \( A \) is of **GL\(2\)**-type over \( \mathbb{Q} \): \( \dim_{\text{End}(A) \otimes \mathbb{Q}_\ell} V_\ell A = 2 \).
Theorem (consequence of Serre’s Modularity Conjecture)

Let $A/\mathbb{Q}$ be an absolutely simple abelian variety. The following are equivalent:

- $A/\mathbb{Q}$ has **real multiplication**, 
- $A$ is an isogeny quotient of $J_0(N)$ for some $N$, 
- $L(A/\mathbb{Q}, s) = \prod_{\alpha:\mathcal{O} \to \mathbb{C}} L(f^\alpha, s)$ for a newform $f \in S_2(\Gamma_0(N), \mathcal{O})$.

If this is the case, we call $A/\mathbb{Q}$ **modular**, and then $N^{\text{dim} A}$ is the conductor of $A/\mathbb{Q}$ and $\mathcal{O} \cong \text{End}_{\mathbb{Q}}(A)$, and $A$ is of **GL$_2$-type** over $\mathbb{Q}$: $\text{dim}_{\text{End}(A) \otimes \mathbb{Q}_\ell} V_\ell A = 2$. 

$$L(A/\mathbb{Q}, s) = \prod_p \frac{1}{\det(1 - \text{Frob}_p p^{-s} | (V_\ell A)^{I_p})}$$

$$L(f, s) = \prod_{p \nmid N} \frac{1}{1 - a_p(f) p^{-s} + p^{1-2s}} \cdot \prod_{p | N} \frac{1}{1 - a_p(f) p^{-s}}$$
Main technical problems
concerning the mod-$p$ and $p$-adic Galois representations of $A/Q$

Problems if $\dim A > 1$

- We don’t have an analog of Mazur’s classification of rational isogenies of prime degree for all $A$: $\dim \mathcal{A}_2 = 3 \cdot 2 - 3 = 3$
- We don’t have an explicit Serre’s open image theorem for $\rho_{p^\infty} : \text{Gal}(\overline{Q}|Q) \rightarrow \text{GL}_2(\mathcal{O}_p)$. 

$\mathcal{A}_2$
Main technical problems
concerning the mod-$p$ and $p$-adic Galois representations of $A/\mathbb{Q}$

Problems if $\dim A > 1$

- We don’t have an analog of Mazur’s classification of rational isogenies of prime degree for all $A$: $\dim \mathcal{A}_2 = 3 \cdot 2 - 3 = 3$
- We don’t have an explicit Serre’s open image theorem for $\rho_p^\infty : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \text{GL}_2(\mathcal{O}_p)$.

In this talk, for a given modular abelian surface $A$, we …

- … explicitly prove that almost all $\rho_p$ are irreducible and maximal,
Main technical problems
concerning the mod-\(p\) and \(p\)-adic Galois representations of \(A/\mathbb{Q}\)

Problems if \(\dim A > 1\)

- We don’t have an analog of Mazur’s classification of rational isogenies of prime degree for all \(A\): \(\dim \mathcal{A}_2 = 3 \cdot 2 - 3 = 3\)
- We don’t have an explicit Serre’s open image theorem for \(\rho_{p^{\infty}} : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \text{GL}_2(\mathcal{O}_p)\).

In this talk, for a given modular abelian surface \(A\), we ...

- ... explicitly prove that almost all \(\rho_p\) are irreducible and maximal,
- ... compute the Heegner index \(I_K = [A(K) : \mathcal{O}_y K]\),
- and use this to compute \(#\text{III}(A/\mathbb{Q}) \in \mathbb{Z}_{\geq 1}\) and \(#\text{III}(A/\mathbb{Q})_{\text{an}} \in \mathbb{Q}_{>0}\) exactly.
Main technical problems
concerning the mod-$p$ and $p$-adic Galois representations of $A/\mathbb{Q}$

Problems if dim $A > 1$

- We don’t have an analog of Mazur’s classification of rational isogenies of prime degree for all $A$: $\dim \mathcal{A}_2 = 3 \cdot 2 - 3 = 3$
- We don’t have an explicit Serre’s open image theorem for $\rho_{p\infty} : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \rightarrow \text{GL}_2(O_p)$.

In this talk, for a given modular abelian surface $A$, we ...

- ... explicitly prove that almost all $\rho_p$ are irreducible and maximal,
- ... compute the Heegner index $I_K = [A(K) : \mathcal{O}y_K]$,
- and use this to compute $\#\text{III}(A/\mathbb{Q}) \in \mathbb{Z}_{\geq 1}$ and $\#\text{III}(A/\mathbb{Q})_{an} \in \mathbb{Q}_{>0}$ exactly.
An explicit Euler system

**Theorem (K.): explicit finite support of \( \Sha(A/\mathbb{Q}) \)**

Let \( A \) be a modular abelian variety over \( \mathbb{Q} \).
One has \( \Sha(A/\mathbb{Q})[\mathfrak{p}] = 0 \) for all \( \mathfrak{p} \) with

- \( \rho_\mathfrak{p} : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \text{Aut}_{F_\mathfrak{p}}(A[\mathfrak{p}](\overline{\mathbb{Q}})) \) 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.
An explicit Euler system

Theorem (K.): explicit finite support of $\Sha(A/\mathbb{Q})$

Let $A$ be a modular abelian variety over $\mathbb{Q}$. One has $\Sha(A/\mathbb{Q})[p] = 0$ for all $p$ with

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

These $p$ are explicitly computable.
Computation of $\Sha(A/Q)[p^\infty]$ for given $p$

Two tools:

- Perform a $p^n$-descent to compute $\text{Sel}_{p^n}(A/Q)$.
  - Works very well if $\rho_{p^n}$ is reducible.
  - Works for general $p^n$ in principle, but:
    - Infeasible if $\rho_{p^n}$ has large image, e.g., $\#O/p^n > 7$ and $\rho_{p^n}$ irreducible, even assuming GRH.

- Compute the $p$-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 $\rho_p$ 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 $p$-adic regulator if $r_{an} > 0$ or if the reduction is split multiplicative.
    (work in progress by Kaya–Müller–van der Put)
Computation of $\Sha(A/Q)[p^\infty]$ for given $p$

Two tools:

- Perform a $p^n$-descent to compute $\text{Sel}_{p^n}(A/Q)$.
  - Works very well if $\rho_{p^n}$ is reducible.
  - Works for general $p^n$ in principle, but:
    - Infeasible if $\rho_{p^n}$ has large image,
      e.g., $#\mathcal{O}/p^n > 7$ and $\rho_{p^n}$ irreducible, even assuming GRH.
- Compute the $p$-adic $L$-function and use the $\text{GL}_2$ IMC.
  - Can be computed very efficiently with overconvergent modular symbols using the Pollack–Stevens–Greenberg algorithm.
  - Requires $\rho_p$ 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 $p$-adic regulator if $r_{an} > 0$ or if the reduction is split multiplicative.
    (work in progress by Kaya–Müller–van der Put)
Structure and dependencies of the project

\[ L'(f^\alpha / K, 1) \]

\[ y_K \]

\[ \mathcal{O}y_K \]

\[ \mathcal{O} \]

\[ \rho_p \]

\[ \mathcal{L}_p(f, T) \]

\[ \text{Sel}_p \]

\[ H^1(G_i, A[p^j]) \]

\[ \#\text{III}(A)_{\text{an}} \]

\[ [\text{KL}] \]

\[ \text{BSD}(A) \]

\[ \text{III}(A)[p] \]
Computing the image of $\rho_p$
Definitions: residual Galois representations

- Let $\mathfrak{p} | p$ be a regular prime ideal of $\mathcal{O}$ with residue field $F_p$.
- We use the following Galois representations:
  - $\chi_p : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to F_p^\times$ the mod-$p$ cyclotomic character,
  - the mod-$p$ Galois representation $\rho_p : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \text{Aut}_{\mathbb{Z}/p}(A[p](\overline{\mathbb{Q}})) \cong \text{GL}_4(F_p),$
  - the mod-$\mathfrak{p}$ Galois representation $\rho_{\mathfrak{p}} : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \text{Aut}_{\mathcal{O}/\mathfrak{p}}(A[p](\overline{\mathbb{Q}})) \cong \text{GL}_2(F_p)$. 


Let $\mathfrak{p} | p$ be a regular prime ideal of $\mathcal{O}$ with residue field $\mathbb{F}_p$.

We use the following Galois representations:

- $\chi_p : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathbb{F}_p^\times$ the mod-$p$ cyclotomic character,
- the mod-$p$ Galois representation $\rho_p : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \text{Aut}_{\mathbb{Z}/p}(A[p](\overline{\mathbb{Q}})) \cong \text{GL}_4(\mathbb{F}_p)$,
- the mod-$\mathfrak{p}$ Galois representation $\rho_{\mathfrak{p}} : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \text{Aut}_{\mathcal{O}/\mathfrak{p}}(A[\mathfrak{p}](\overline{\mathbb{Q}})) \cong \text{GL}_2(\mathbb{F}_p)$. 

Definitions: residual Galois representations
Excursion: Group theory of finite groups of Lie type

Maximal subgroups of $\text{PSL}_2(\mathbb{F}_p)$

Assume $p \nmid 2$. Every subgroup of $\text{PSL}_2(\mathbb{F}_p) := \ker(\text{det} : \text{PGL}_2(\mathbb{F}_p) \to \mathbb{F}_p^\times / 2)$ is (up to conjugacy) contained in one of the following maximal subgroups:

- Borel subgroup $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ (reducible image as $\mathbb{F}_p$-representation)
- $\text{PSL}_2(p)$ (reducible image as $\mathbb{F}_p$-representation, only for $\mathbb{F}_p \supseteq \mathbb{F}_p$)
- Normalizer of a split/non-split Cartan subgroup $C_s/C_{ns}$:
  
  $N_s = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} 0 & b \\ a & 0 \end{pmatrix} \right\}$; $N_{ns} = \left\{ \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix}, \begin{pmatrix} a & \varepsilon b \\ -b & -a \end{pmatrix} \right\}$ (dihedral)

  with $\varepsilon \in \mathbb{F}_p \setminus \mathbb{F}_p^\square$

- $A_4$, $S_4$ or $A_5$ (exceptional image)
Irreducibility for almost all $p$

- Raynaud’s classification of simple factors of $\rho_p|_{I_p}^{ss}$ and CFT:
  
  If $\rho_p$ is reducible, $\rho_p^{ss} \cong \varepsilon \oplus \varepsilon^{-1} \chi_p$ with $\varepsilon$ of conductor $d$ with $d^2 | N$, or $\rho_p^{ss} \cong \varepsilon \chi_p^n \oplus \varepsilon^{-1} \chi_p^{1-n}$ if $p^2 | N$.

- Hence: $\rho_p$ is irreducible as an $F_p$-representation for all $p | p$ if

\[
p \nmid \gcd_{\ell \nmid pN} \left( \text{res}_{\mathbb{Z}[X]} \left( \text{charpol}_{\mathbb{Z}[X]}(\rho_{p \infty}(\text{Frob}_\ell)) \right), X^{\text{ord}(\ell \in (\mathbb{Z}/d)^\times)} - 1 \right).
\]

for $d = d_{\text{max}}$ maximal such that $d_{\text{max}}^2 | N$, or $d = p \cdot d_{\text{max}}$ if $p^2 | N$.

Bounding the resultant using the Weil conjectures gives a small finite set of primes $p$ containing all $p$ with $\rho_p$ reducible for all $p | p$.

Can be refined to $p \nmid \text{ord}(\ell \in (\mathbb{Z}/d)^\times)$.
Irreducibility for almost all \( p \)

- Raynaud’s classification of simple factors of \( \rho_p|_{I_p}^{ss} \) and CFT:
  If \( \rho_p \) is reducible, \( \rho_p^{ss} \cong \epsilon \oplus \epsilon^{-1} \chi_p \) with \( \epsilon \) of conductor \( d \) with \( d^2 \mid N \), or \( \rho_p^{ss} \cong \epsilon \chi_p^n \oplus \epsilon^{-1} \chi_p^{1-n} \) if \( p^2 \mid N \).
  Hence: \( \rho_p \) is irreducible as an \( F_p \)-representation for all \( p \mid p \) if
  \[
  p \nmid \gcd_{\ell \mid pN} \left( \text{res}_{\mathbb{Z}[X]} \left( \text{charpol}_{\mathbb{Z}[X]}(\rho_{p^\infty}(\text{Frob}_\ell)), X^{\text{ord}(\bar{\ell} \in (\mathbb{Z}/d^\times)) - 1} \right) \right).
  \]
  for \( d = d_{\text{max}} \) maximal such that \( d_{\text{max}}^2 \mid N \),
  or \( d = p \cdot d_{\text{max}} \) if \( p^2 \mid N \).

- Bounding the resultant using the Weil conjectures gives a small finite set of primes \( p \) containing all \( p \) with \( \rho_p \) reducible for all \( p \mid p \).
Irreducibility for almost all $p$

- Raynaud’s classification of simple factors of $\rho_p\big|_{I_p}^{ss}$ and CFT:
  If $\rho_p$ is reducible, $\rho_p^{ss} \cong \epsilon \oplus \epsilon^{-1} \chi_p$ with $\epsilon$ of conductor $d$ with $d^2 \mid N$, or $\rho_p^{ss} \cong \epsilon \chi_p^n \oplus \epsilon^{-1} \chi_p^{1-n}$ if $p^2 \mid N$.

- Hence: $\rho_p$ is irreducible as an $F_p$-representation for all $p \mid p$ if

\[
p \nmid \gcd_{\ell \mid pN} \left( \text{res}_{Z[X]} \left( \text{charpol}_{Z[X]}(\rho_p^\infty(\text{Frob}_\ell)), X^{\text{ord}(\bar{\ell} \in (Z/d)\times)} - 1 \right) \right).
\]

for $d = d_{\text{max}}$ maximal such that $d_{\text{max}}^2 \mid N$,
or $d = p \cdot d_{\text{max}}$ if $p^2 \mid N$.

- Bounding the resultant using the Weil conjectures gives a small finite set of primes $p$ containing all $p$ with $\rho_p$ reducible for all $p \mid p$.

- Can be refined to $p \prec O$. 


Irreducibility for almost all \( p \)

- Raynaud’s classification of simple factors of \( \rho_p|_{I_p}^{ss} \) and CFT:
  If \( \rho_p \) is reducible, \( \rho_p^{ss} \cong \varepsilon \oplus \varepsilon^{-1} \chi_p \) with \( \varepsilon \) of conductor \( d \) with \( d^2 \mid N \), or \( \rho_p^{ss} \cong \varepsilon \chi_p^n \oplus \varepsilon^{-1} \chi_p^{1-n} \) if \( p^2 \mid N \).
  - Hence: \( \rho_p \) is irreducible as an \( F_p \)-representation for all \( p \mid p \) if
    \[
    p \nmid \gcd \left( \text{res}_{\mathbb{Z}[X]} \left( \text{charpol}_{\mathbb{Z}[X]}(\rho_{p^\infty}(\text{Frob}_\ell)), X^{\text{ord}(\ell \in (\mathbb{Z}/d)^\times)} - 1 \right) \right).
    \]
    for \( d = d_{\text{max}} \) maximal such that \( d_{\text{max}}^2 \mid N \),
    or \( d = p \cdot d_{\text{max}} \) if \( p^2 \mid N \).
  - Bounding the resultant using the Weil conjectures gives a small finite set of primes \( p \) containing all \( p \) with \( \rho_p \) reducible for all \( p \mid p \).
  - Can be refined to \( p \nmid \mathcal{O} \).
Maximal image for almost all \( p \)

- If \( \rho_p \) is irreducible as an \( \mathbb{F}_p \)-representation, but reducible as an \( \mathbb{F}_p \)-representation,

\[
p \mid \gcd_{\ell \nmid pN} \left( \frac{a_\ell - \bar{a}_\ell}{2} \right).
\]

- If \( p > 5 \), \( \rho_p \) does not have exceptional image.
- If \( p > C(N, \deg p) \), then the image of \( \rho_p \) is not contained in the normalizer of a Cartan subgroup.
Computing the Heegner index $I_K$
We can determine \( x \in \mathbb{Q} \) exactly if we know an explicit \( N \in \mathbb{Z} \) such that \( x \in \frac{1}{N} \mathbb{Z} \) and if we can approximate \( x \in \mathbb{C} \) up to an arbitrary precision.

(We can determine \( x \in \overline{\mathbb{Q}} \) exactly if we know an explicit \( N \in \mathbb{Z} \) such that \( x \in \frac{1}{N} \overline{\mathbb{Z}} \) and \([\mathbb{Q}(x) : \mathbb{Q}] \leq d\) and if we can approximate \( x \in \mathbb{C} \) up to an arbitrary precision.)
The Gross–Zagier formula

Let $K/Q$ be an imaginary quadratic Heegner field such that

- all primes $\ell \mid N$ split in $K$,
- i.e., there is a fractional ideal $\frak{n} \triangleleft \mathcal{O}_K$ with $\mathcal{O}_K/\frak{n} \cong \mathbb{Z}/N$,
- $L'(f/K, 1) \neq 0$.

(By results of Waldspurger et al., there are infinitely many such $K$.)

Gross–Zagier formula, 1986

For an isogeny quotient $\pi : J_0(N) \to A_f$ with Manin constant $c_\pi$ and Heegner point $y_K \in A_f(K)$,

$$L'(f/K, 1) = \frac{\|\omega_f\|^2}{c_\pi^2 u_K^2 \sqrt{\mid \text{disc}_K \mid}} \hat{h}(y_K) \in \mathbb{R}_{\geq 0}.$$
The Gross–Zagier formula

Let \( K/\mathbb{Q} \) be an imaginary quadratic Heegner field such that
- all primes \( \ell \mid N \) split in \( K \),
  i.e., there is a fractional ideal \( \mathfrak{n} \triangleleft \mathcal{O}_K \) with \( \mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N \),
- \( L'(f/K, 1) \neq 0 \).

(By results of Waldspurger et al., there are infinitely many such \( K \).)

**Gross–Zagier formula, 1986**

For an isogeny quotient \( \pi : J_0(N) \to A_f \) with Manin constant \( c_\pi \) and Heegner point \( y_K \in A_f(K) \),

\[
L'(f/K, 1) = \frac{\|\omega_f\|^2}{c_\pi^2 u_K^2 \sqrt{|\text{disc}_K|}} \hat{h}(y_K) \in \mathbb{R}_{\geq 0}.
\]
Computing the Heegner index $I_K$

- We need to work on a Jacobian in the isogeny class of $A_f := J_0(N)/\text{Ann}_T(f)$.
- Compute an isogeny $\pi : A_f \to J := \text{Jac}(X)$ using the big period matrices of $A_f$ and $J$.
- Compute the $h_K$ Heegner forms $Ax^2 + Bx + C$ for $(N, \text{disc}_K)$.
- Compute the zeros $\tau$ of the Heegner forms with $\text{Im}(\tau) > 0$.
- Approximate $\int_{q_{\tau}}^{i\infty} f(q) dq, \int_{q_{\tau}}^{i\infty} f^\alpha(q) dq$ with $q_{\tau} := \exp(2\pi i \tau)$ and map the points via $\pi : \mathbb{C}^2/\Lambda_f \to J(\mathbb{C})$ ($X$ hyperelliptic!) and sum over all $\tau$ to get a $\mathbb{C}$-approximation of $\pi(y_K)$.
- Find a $K$-approximation to $\pi(y_K) \in J(K)$.

Note that $\text{Ann}_\mathcal{O}(J(K)/\mathcal{O}\pi(y_K))$ can be a multiple of $I_K := \text{Ann}_\mathcal{O}(A_f(K) : \mathcal{O}y_K)$ if $[J(K) : \pi(A_f(K))] > 1$. 
Computing the Heegner index $I_K$

- We need to work on a Jacobian in the isogeny class of $A_f := J_0(N)/\text{Ann}_T(f)$.
- Compute an isogeny $\pi : A_f \to J := \text{Jac}(X)$ using the big period matrices of $A_f$ and $J$.
- Compute the $h_K$ Heegner forms $Ax^2 + Bx + C$ for $(N, \text{disc}_K)$.
- Compute the zeros $\tau$ of the Heegner forms with $\text{Im}(\tau) > 0$.
- Approximate $\int_{q_\tau}^{i\infty} f(q)dq, \int_{q_\tau}^{i\infty} f^\alpha(q)dq$ with $q_\tau := \exp(2\pi i \tau)$ and map the points via $\pi : \mathbb{C}^2/\Lambda_f \to J(\mathbb{C})$ ($X$ hyperelliptic!) and sum over all $\tau$ to get a $\mathbb{C}$-approximation of $\pi(y_K)$.
- Find a $K$-approximation to $\pi(y_K) \in J(K)$.

Note that $\text{Ann}_\mathcal{O}(J(K)/\mathcal{O} \pi(y_K))$ can be a multiple of $I_K := \text{Ann}_\mathcal{O}(A_f(K) : \mathcal{O} y_K)$ if $[J(K) : \pi(A_f(K))] > 1$. 
Proving the correctness of $O_{\pi}(y_K)$

- **Problem:** The set of points of $J(K)$ near to some $y \in J(\mathbb{C})$ is dense!
- **Idea:** Use the Northcott property of heights $\hat{h}_L : J(K) \to \mathbb{R}_{\geq 0}$ and assume that $\hat{h}_{2\varphi}$ is injective on $J(K)$ up to sign and torsion.
Proving the correctness of $O \pi (y_K)$

- **Problem:** The set of points of $J(K)$ near to some $y \in J(\mathbb{C})$ is dense!
- **Idea:** Use the Northcott property of heights $\hat{h}_L : J(K) \to \mathbb{R}_{\geq 0}$ and assume that $\hat{h}_{2\varphi}$ is injective on $J(K)$ up to sign and torsion.
- Use the Gross–Zagier formula to compute $\hat{h}_{\varphi}(y_K)$ with $y_K \in A_f(K)$.
Proving the correctness of $O\pi(y_K)$

- **Problem:** The set of points of $J(K)$ near to some $y \in J(\mathbb{C})$ is dense!
- **Idea:** Use the Northcott property of heights $\hat{h}_\mathcal{L} : J(K) \rightarrow \mathbb{R}_{\geq 0}$ and assume that $\hat{h}_{2\mathcal{G}}$ is injective on $J(K)$ up to sign and torsion.
- Use the Gross–Zagier formula to compute $\hat{h}_\mathcal{G}(y_K)$ with $y_K \in A_f(K)$.
- Compute the degree of the polarization

\[
A_f^\vee \rightarrow J_0(N)^\vee \xrightarrow{\sim} J_0(N) \rightarrow A_f.
\]

- Compute the degree of the isogeny $\pi : A_f \rightarrow J$.
- Reconstruct the height pairing matrix on $A_f$.
- Approximate the canonical height of $\pi(y_K) \in J(K)$ w.r.t. $2\mathcal{G}$.
- There is exactly one $y \in J(K)$ (up to sign and torsion) with height sufficiently close to that.
- We get $O_x^y$, hence $I_K$ exactly up to a divisor of $\deg(\pi)$. 

21 / 27
Proving the correctness of $O\pi(y_K)$

- Problem: The set of points of $J(K)$ near to some $y \in J(\mathbb{C})$ is dense!
- Idea: Use the Northcott property of heights $\hat{h}_L : J(K) \to \mathbb{R}_{\geq 0}$ and assume that $\hat{h}_{2\delta}$ is injective on $J(K)$ up to sign and torsion.
- Use the Gross–Zagier formula to compute $\hat{h}_{\delta}(y_K)$ with $y_K \in A_f(K)$.
- Compute the degree of the polarization
  \[ A_f^\vee \to J_0(N)^\vee \sim J_0(N) \to A_f. \]
- Compute the degree of the isogeny $\pi : A_f \to J$.
- Reconstruct the height pairing matrix on $A_f$.
- Approximate the canonical height of $\pi(y_K) \in J(K)$ w.r.t. $2\delta$.
- There is exactly one $y \in J(K)$ (up to sign and torsion) with height sufficiently close to that.
- We get $O^x y$, hence $I_K$ exactly up to a divisor of $\deg(\pi)$. 

21 / 27
Computing $\#\Sha(A/\mathbb{Q})_{\text{an}}$ exactly

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

- Compute $\frac{L(f,1)}{\Omega_f^+} \in \Q(f)$ exactly using modular symbols and Balakrishnan–Müller–Stein and van Bommel’s code to compute $\Omega_A$.
- If $L(A,1) \neq 0$, this gives $\#\Sha(A/\Q)_{an} \in \Q_{>0}$ exactly.
- If $L(A,1) = 0$, ... 
  - choose a Heegner field $K$ and compute $\frac{L(f_K,1)}{\Reg_{A/K} \Omega_{A/K}} \in \Q_{>0}$ exactly using Gross–Zagier, and hence compute $\#\Sha(A/K)_{an} \in \Q_{>0}$.
  - Compute $\#\Sha(A^K/\Q)_{an} \in \Q_{>0}$ exactly.
  - Use $\#\Sha(A/K)_{an} = \#\Sha(A/\Q)_{an} \cdot \#\Sha(A^K/\Q)_{an}$ up to powers of 2 that can be explicitly bounded to compute $\#\Sha(A/\Q)_{an} \in \Q_{>0}$ exactly.
Examples
Example: $A = \text{Jac}(X_0(39)/\mathcal{W}_{13})$

- $O = \mathbb{Z}[\sqrt{2}]$
- $r = r_{\text{an}} = 0$
- $\#\text{III}(A/\mathbb{Q})_{\text{an}} = 1$
- $A(\mathbb{Q}) = A(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2 \times \mathbb{Z}/(2 \cdot 7)$
- $\rho_p$ is reducible exactly for $p = (\sqrt{2})$ and exactly one $p\bar{p} = 7$.
- $c = 7$
Example: $A = \text{Jac}(X_0(39)/w_{13})$

- $O = \mathbb{Z}[\sqrt{2}]$
- $r = r_{\text{an}} = 0$
- $\#\text{III}(A/\mathbb{Q})_{\text{an}} = 1$
- $A(\mathbb{Q}) = A(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2 \times \mathbb{Z}/(2 \cdot 7)$
- $\rho_p$ is reducible exactly for $p = (\sqrt{2})$ and exactly one $p\bar{p} = 7$.
- $c = 7$
- $\text{Sel}_2(A/\mathbb{Q}) \cong (\mathbb{Z}/2)^2 \cong A(\mathbb{Q})/2$ gives $\text{III}(A/\mathbb{Q})[2] = 0$. 

- $\rho_p$ is reducible exactly for $p = (\sqrt{2})$ and exactly one $p\bar{p} = 7$. 
- $c = 7$
- $\text{Sel}_2(A/\mathbb{Q}) \cong (\mathbb{Z}/2)^2 \cong A(\mathbb{Q})/2$ gives $\text{III}(A/\mathbb{Q})[2] = 0$. 

Hence $X(A/\mathbb{Q})[\bar{p}] = 0$. 

- The $\bar{p}$-adic $L$-function has constant term a unit in $\mathcal{O}_{\bar{p}} \cong \mathbb{Z}/7$, hence the integral $\text{GL}_2\text{IMC}$ shows $\text{Sel}_{\bar{p}}(A/\mathbb{Q}) = 0$ since $\rho_{\bar{p}}$ is irreducible. 

23 / 27
Example: $A = \text{Jac}(X_0(39)/\mathcal{O}_{13})$

- $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$
- $r = r_{\text{an}} = 0$
- $\#\Pi(A/\mathbb{Q})_{\text{an}} = 1$
- $A(\mathbb{Q}) = A(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2 \times \mathbb{Z}/(2 \cdot 7)$
- $\rho_p$ is reducible exactly for $p = (\sqrt{2})$ and exactly one $p \bar{p} = 7$.
- $c = 7$
- $\text{Sel}_2(A/\mathbb{Q}) \cong (\mathbb{Z}/2)^2 \cong A(\mathbb{Q})/2$ gives $\Pi(A/\mathbb{Q})[2] = 0$.
- $[\text{KL}]$ with $I_{\mathbb{Q}(\sqrt{-23})} = 7$ gives $\#\Pi(A/\mathbb{Q})[p] = 0$ for $p \nmid (\sqrt{2}), 7$. 
Example: $A = \text{Jac}(X_0(39)/\mathcal{O}_{13})$

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

\[
0 \to \mathbb{Z}/7 \to A[p] \to \mu_7 \to 1
\]

non-split exact, and $\text{Sel}_p(A/\mathbb{Q}) \cong \mathbb{Z}/7 \cong A(\mathbb{Q})[7]$ by descent. Hence $\Sha(A/\mathbb{Q})[p] = 0$. 
Example: $A = \text{Jac}(X_0(39)/\mathcal{O}_{w_{13}})$

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

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

non-split exact, and $\text{Sel}_p(A/\mathbb{Q}) \cong \mathbb{Z}/7 \cong A(\mathbb{Q})[7]$ by descent. Hence $\text{III}(A/\mathbb{Q})[p] = 0$.

- The $\bar{p}$-adic $L$-function has constant term a unit in $O_{\bar{p}} \cong \mathbb{Z}_7$, hence the integral $\text{GL}_2$ IMC shows $\text{Sel}_{\bar{p}}(A/\mathbb{Q}) = 0$ since $\rho_{\bar{p}}$ is irreducible.
Example: $A = \text{Jac}(X_0(39)/\mathcal{O}_{13})$

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

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

non-split exact, and $\text{Sel}_p(A/\mathbb{Q}) \cong \mathbb{Z}/7 \cong A(\mathbb{Q})[7]$ by descent. Hence $\text{III}(A/\mathbb{Q})[p] = 0$.

- The $\bar{p}$-adic $L$-function has constant term a unit in $\mathcal{O}_{\bar{p}} \cong \mathbb{Z}_7$, hence the integral $\text{GL}_2$ IMC shows $\text{Sel}_{\bar{p}}(A/\mathbb{Q}) = 0$ since $\rho_{\bar{p}}$ is irreducible.
### All Atkin-Lehner quotients of genus 2 of our type (I)

<table>
<thead>
<tr>
<th>$X$</th>
<th>$r$</th>
<th>$O$</th>
<th>$#\text{III}_{\text{an}}$</th>
<th>$\rho_p$ red.</th>
<th>$c$</th>
<th>$(D, I_D)$</th>
<th>$#\text{III}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_0(23)$</td>
<td>0</td>
<td>$\sqrt{5}$</td>
<td>1</td>
<td>$11_1$</td>
<td>11</td>
<td>$(-7, 11)$</td>
<td>$11^0$</td>
</tr>
<tr>
<td>$X_0(29)$</td>
<td>0</td>
<td>$\sqrt{2}$</td>
<td>1</td>
<td>$7_1$</td>
<td>7</td>
<td>$(-7, 7)$</td>
<td>$7^0$</td>
</tr>
<tr>
<td>$X_0(31)$</td>
<td>0</td>
<td>$\sqrt{5}$</td>
<td>1</td>
<td>$\sqrt{5}$</td>
<td>5</td>
<td>$(-11, 5)$</td>
<td>$5^0$</td>
</tr>
<tr>
<td>$X_0(35)/w_7$</td>
<td>0</td>
<td>$\sqrt{17}$</td>
<td>1</td>
<td>$2_1$</td>
<td>1</td>
<td>$(-19, 1)$</td>
<td>$1$</td>
</tr>
<tr>
<td>$X_0(39)/w_{13}$</td>
<td>0</td>
<td>$\sqrt{2}$</td>
<td>1</td>
<td>$\sqrt{2}, 7_1$</td>
<td>7</td>
<td>$(-23, 7)$</td>
<td>$7^0$</td>
</tr>
<tr>
<td>$X_0(67)^+$</td>
<td>2</td>
<td>$\sqrt{5}$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$(-7, 1)$</td>
<td>$1$</td>
</tr>
<tr>
<td>$X_0(73)^+$</td>
<td>2</td>
<td>$\sqrt{5}$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$(-19, 1)$</td>
<td>$1$</td>
</tr>
<tr>
<td>$X_0(85)^*$</td>
<td>2</td>
<td>$\sqrt{2}$</td>
<td>1</td>
<td>$\sqrt{2}$</td>
<td>1</td>
<td>$(-19, 1)$</td>
<td>$1$</td>
</tr>
<tr>
<td>$X_0(87)/w_{29}$</td>
<td>0</td>
<td>$\sqrt{5}$</td>
<td>1</td>
<td>$\sqrt{5}$</td>
<td>5</td>
<td>$(-23, 5)$</td>
<td>$5^0$</td>
</tr>
<tr>
<td>$X_0(93)^*$</td>
<td>2</td>
<td>$\sqrt{5}$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$(-11, 1)$</td>
<td>$1$</td>
</tr>
<tr>
<td>$X_0(103)^+$</td>
<td>2</td>
<td>$\sqrt{5}$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$(-11, 1)$</td>
<td>$1$</td>
</tr>
<tr>
<td>$X_0(107)^+$</td>
<td>2</td>
<td>$\sqrt{5}$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$(-7, 1)$</td>
<td>$1$</td>
</tr>
<tr>
<td>$X_0(115)^*$</td>
<td>2</td>
<td>$\sqrt{5}$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$(-11, 1)$</td>
<td>$1$</td>
</tr>
<tr>
<td>$X_0(125)^+$</td>
<td>2</td>
<td>$\sqrt{5}$</td>
<td>1</td>
<td>$\sqrt{5}$</td>
<td>1</td>
<td>$(-11, 1)$</td>
<td>$5^0$</td>
</tr>
</tbody>
</table>
All Atkin-Lehner quotients of genus 2 of our type (II)

<table>
<thead>
<tr>
<th>X</th>
<th>r</th>
<th>O</th>
<th>#\text{III}_{\text{an}}</th>
<th>\rho_{\psi} \text{ red.}</th>
<th>c</th>
<th>(D, I_D)</th>
<th>#III</th>
</tr>
</thead>
<tbody>
<tr>
<td>X_0(133)^*</td>
<td>2</td>
<td>\sqrt{5}</td>
<td>1</td>
<td>\sqrt{2}, 7_1</td>
<td>1</td>
<td>(-31, 1)</td>
<td>1</td>
</tr>
<tr>
<td>X_0(147)^*</td>
<td>2</td>
<td>\sqrt{2}</td>
<td>1</td>
<td></td>
<td>1</td>
<td>(-47, 1)</td>
<td>7^0</td>
</tr>
<tr>
<td>X_0(161)^*</td>
<td>2</td>
<td>\sqrt{5}</td>
<td>1</td>
<td>\sqrt{2}</td>
<td>1</td>
<td>(-19, 1)</td>
<td>1</td>
</tr>
<tr>
<td>X_0(165)^*</td>
<td>2</td>
<td>\sqrt{2}</td>
<td>1</td>
<td>\sqrt{2}</td>
<td>1</td>
<td>(-131, 1)</td>
<td>1</td>
</tr>
<tr>
<td>X_0(167)^+</td>
<td>2</td>
<td>\sqrt{5}</td>
<td>1</td>
<td></td>
<td>1</td>
<td>(-15, 1)</td>
<td>1</td>
</tr>
<tr>
<td>X_0(177)^*</td>
<td>2</td>
<td>\sqrt{5}</td>
<td>1</td>
<td></td>
<td>1</td>
<td>(-11, 1)</td>
<td>1</td>
</tr>
<tr>
<td>X_0(191)^+</td>
<td>2</td>
<td>\sqrt{5}</td>
<td>1</td>
<td></td>
<td>1</td>
<td>(-7, 1)</td>
<td>1</td>
</tr>
<tr>
<td>X_0(205)^*</td>
<td>2</td>
<td>\sqrt{5}</td>
<td>1</td>
<td></td>
<td>1</td>
<td>(-31, 1)</td>
<td>1</td>
</tr>
<tr>
<td>X_0(209)^*</td>
<td>2</td>
<td>\sqrt{2}</td>
<td>1</td>
<td></td>
<td>1</td>
<td>(-51, 1)</td>
<td>1</td>
</tr>
<tr>
<td>X_0(213)^*</td>
<td>2</td>
<td>\sqrt{5}</td>
<td>1</td>
<td></td>
<td>1</td>
<td>(-11, 1)</td>
<td>1</td>
</tr>
<tr>
<td>X_0(221)^*</td>
<td>2</td>
<td>\sqrt{5}</td>
<td>1</td>
<td></td>
<td>1</td>
<td>(-35, 1)</td>
<td>1</td>
</tr>
<tr>
<td>X_0(227)^*</td>
<td>2</td>
<td>\sqrt{5}</td>
<td>1</td>
<td></td>
<td>1</td>
<td>(-31, 1)</td>
<td>1</td>
</tr>
<tr>
<td>X_0(287)^*</td>
<td>2</td>
<td>\sqrt{5}</td>
<td>1</td>
<td></td>
<td>1</td>
<td>(-43, 1)</td>
<td>1</td>
</tr>
<tr>
<td>X_0(357)^*</td>
<td>2</td>
<td>\sqrt{2}</td>
<td>1</td>
<td></td>
<td>1</td>
<td>(-47, 1)</td>
<td>1</td>
</tr>
</tbody>
</table>
Outlook
Using Shnidman–Weiss\(^1\), find examples of \(A/\mathbb{Q}\) with

\[
\#\Sha(A/\mathbb{Q}) = \#\Sha(A/\mathbb{Q})_{\text{an}} \neq 2^i!
\]

Can have \(p \in \{3, 5, 7, 11, (13?), \ldots, (31?), \ldots\}\).

Find \(J/\mathbb{Q}\) and \(\mathfrak{p} | p\) “large” with

- \(p^2 \mid N\) (no \(p\)-adic \(L\)-functions),
- \(\mathfrak{p} \mid c \cdot I_K ([KL] does not give \(\Sha(J/\mathbb{Q})[\mathfrak{p}] = 0\), 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
Future work

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

- Almost done: Verification for all 97 genus 2 curves with absolutely simple modular Jacobian from the LMFDB.
- Verification for (almost?) all ~ 1200 newforms of \( \text{level} \leq 1000 \) with real-quadratic coefficients foreseeable.
- Modular 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.
Outlook

Future work

▶ Almost done: Verification for all 97 genus 2 curves with absolutely simple modular Jacobian from the LMFDB.
▶ Verification for (almost?) all $\sim 1200$ newforms of level $\leq 1000$ with real-quadratic coefficients foreseeable.
▶ Modular 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!