Funded by
DFG Deutsche Forschungsgemeinschaft
German Research Foundation

Leibniz Universität Hannover

# 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 Hannover
(previously Universität Bayreuth)

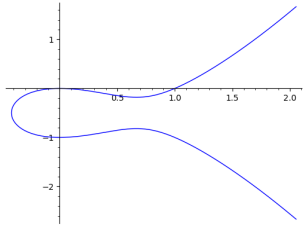
July 5, 2022

# The BSD conjecture: Why is it useful?

# Introduction:
# How to compute the $\mathbf{Q}$-points of a given genus 1 curve?

- Consider

$$E : y^2 + y = x^3 - x^2 \quad \text{(model of } X_1(11)\text{, 11a3)}$$



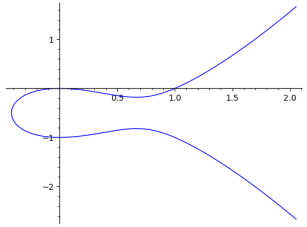

One has $E(\mathbf{Q}) = \{\infty, (0,0), (0,-1), (1,0), (1,-1)\}$ finite.

*Proof:* $L(E,1) \neq 0$.

# Introduction:
# How to compute the $\mathbf{Q}$-points of a given genus 1 curve?

- Consider

$$E : y^2 + y = x^3 - x^2 \quad \text{(model of } X_1(11)\text{, 11a3)}$$

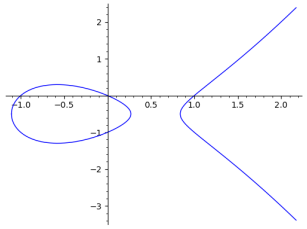


One has $E(\mathbf{Q}) = \{\infty, (0,0), (0,-1), (1,0), (1,-1)\}$ finite.

*Proof:* $L(E,1) \neq 0$.

- Consider

$$E : y^2 + y = x^3 - x \quad \text{(model of } X_0(37)^+\text{, 37a1)}$$

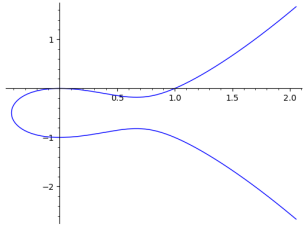


One has $E(\mathbf{Q}) \cong \mathbf{Z} \cdot (0,0)$ infinite.

# Introduction:
# How to compute the $\mathbf{Q}$-points of a given genus 1 curve?

- Consider

$$E : y^2 + y = x^3 - x^2 \quad \text{(model of } X_1(11)\text{, 11a3)}$$

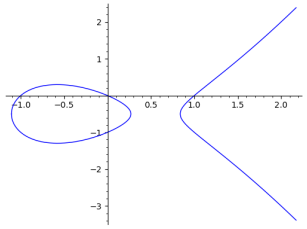


One has $E(\mathbf{Q}) = \{\infty, (0,0), (0,-1), (1,0), (1,-1)\}$ finite.

*Proof:* $L(E,1) \neq 0$.

- Consider

$$E : y^2 + y = x^3 - x \quad \text{(model of } X_0(37)^+\text{, 37a1)}$$



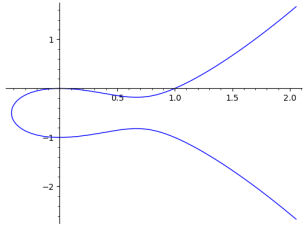
One has $E(\mathbf{Q}) \cong \mathbf{Z} \cdot (0,0)$ infinite.

*Proof:* $L(E,1) = 0, L'(E,1) \neq 0$.

# Introduction:
# How to compute the $\mathbf{Q}$-points of a given genus 1 curve?

- Consider

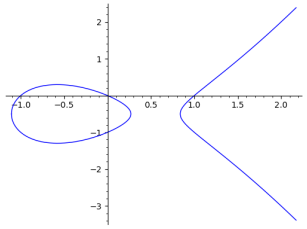
$$E : y^2 + y = x^3 - x^2 \quad \text{(model of } X_1(11)\text{, 11a3)}$$



One has $E(\mathbf{Q}) = \{\infty, (0,0), (0,-1), (1,0), (1,-1)\}$ finite.
*Proof:* $L(E,1) \neq 0$.

- Consider

$$E : y^2 + y = x^3 - x \quad \text{(model of } X_0(37)^+\text{, 37a1)}$$

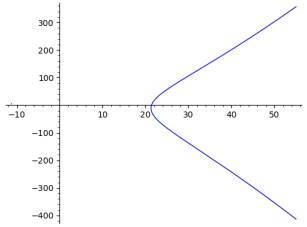


One has $E(\mathbf{Q}) \cong \mathbf{Z} \cdot (0,0)$ infinite.
*Proof:* $L(E,1) = 0, L'(E,1) \neq 0$.

- Consider

$$C : y^2 = 8x^4 + 65x^2 + 132.$$

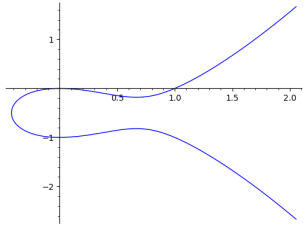
One has $g(C) = 1$, $C(\mathbf{Q}) = \emptyset$, but $C(\mathbf{Q}_v) \neq \emptyset$, and
$C \otimes \overline{\mathbf{Q}} \cong E : y^2 + xy + y = x^3 + x^2 - 352x - 2689$ (66b3).
(failure of the local-global principle)



# Introduction:
# How to compute the $\mathbf{Q}$-points of a given genus 1 curve?

- Consider

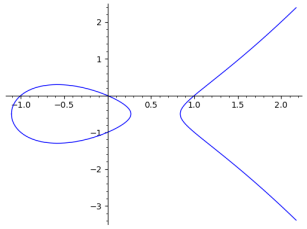
$$E : y^2 + y = x^3 - x^2 \quad \text{(model of } X_1(11)\text{, 11a3)}$$



One has $E(\mathbf{Q}) = \{\infty, (0,0), (0,-1), (1,0), (1,-1)\}$ finite.
*Proof:* $L(E,1) \neq 0$.

- Consider

$$E : y^2 + y = x^3 - x \quad \text{(model of } X_0(37)^+\text{, 37a1)}$$

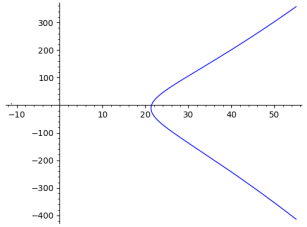


One has $E(\mathbf{Q}) \cong \mathbf{Z} \cdot (0,0)$ infinite.
*Proof:* $L(E,1) = 0, L'(E,1) \neq 0$.

- Consider

$$C : y^2 = 8x^4 + 65x^2 + 132.$$

One has $g(C) = 1$, $C(\mathbf{Q}) = \emptyset$, but $C(\mathbf{Q}_v) \neq \emptyset$, and
$C \otimes \overline{\mathbf{Q}} \cong E : y^2 + xy + y = x^3 + x^2 - 352x - 2689$ (66b3).
(failure of the local-global principle)

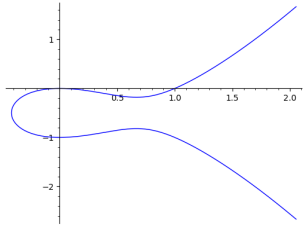


How many such curves are there (up to isomorphism)?

# Introduction:
# How to compute the $\mathbf{Q}$-points of a given genus 1 curve?

- Consider

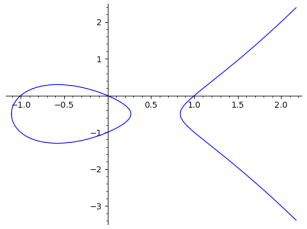
$$E : y^2 + y = x^3 - x^2 \quad \text{(model of } X_1(11)\text{, 11a3)}$$



One has $E(\mathbf{Q}) = \{\infty, (0,0), (0,-1), (1,0), (1,-1)\}$ finite.
*Proof:* $L(E,1) \neq 0$.

- Consider

$$E : y^2 + y = x^3 - x \quad \text{(model of } X_0(37)^+\text{, 37a1)}$$

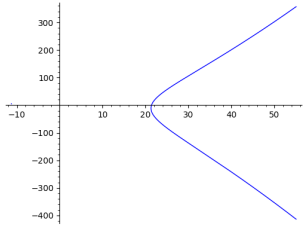


One has $E(\mathbf{Q}) \cong \mathbf{Z} \cdot (0,0)$ infinite.
*Proof:* $L(E,1) = 0, L'(E,1) \neq 0$.

- Consider

$$C : y^2 = 8x^4 + 65x^2 + 132.$$

One has $g(C) = 1$, $C(\mathbf{Q}) = \emptyset$, but $C(\mathbf{Q}_v) \neq \emptyset$, and
$C \otimes \overline{\mathbf{Q}} \cong E : y^2 + xy + y = x^3 + x^2 - 352x - 2689$ (66b3).
(failure of the local-global principle)

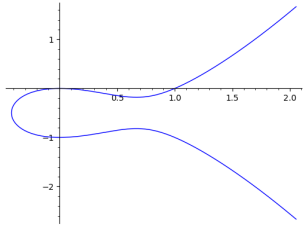


How many such curves are there (up to isomorphism)? Here: 4.

# Introduction:
# How to compute the $\mathbf{Q}$-points of a given genus 1 curve?

- Consider

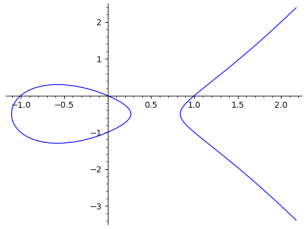
$$E : y^2 + y = x^3 - x^2 \quad \text{(model of } X_1(11)\text{, 11a3)}$$



One has $E(\mathbf{Q}) = \{\infty, (0,0), (0,-1), (1,0), (1,-1)\}$ finite.
*Proof:* $L(E,1) \neq 0$.

- Consider

$$E : y^2 + y = x^3 - x \quad \text{(model of } X_0(37)^+\text{, 37a1)}$$

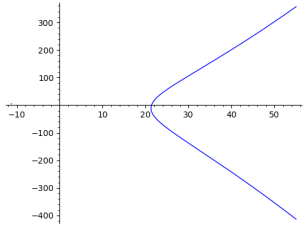


One has $E(\mathbf{Q}) \cong \mathbf{Z} \cdot (0,0)$ infinite.
*Proof:* $L(E,1) = 0, L'(E,1) \neq 0$.

- Consider

$$C : y^2 = 8x^4 + 65x^2 + 132.$$

One has $g(C) = 1$, $C(\mathbf{Q}) = \emptyset$, but $C(\mathbf{Q}_v) \neq \emptyset$, and
$C \otimes \overline{\mathbf{Q}} \cong E : y^2 + xy + y = x^3 + x^2 - 352x - 2689$ (66b3).
(failure of the local-global principle)



How many such curves are there (up to isomorphism)? Here: 4.

# How to compute the rank?

**Theorem of Mordell–Weil**

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

**Proof (sketch).**

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

$$0 \to A(\mathbf{Q})/n \to \mathrm{Sel}_n(A/\mathbf{Q}) \to Ш(A/\mathbf{Q})[n] \to 0 \tag{1}$$

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

# How to compute the rank?

## Theorem of Mordell–Weil

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

## Proof (sketch).

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

$$0 \to A(\mathbf{Q})/n \to \mathrm{Sel}_n(A/\mathbf{Q}) \to Ш(A/\mathbf{Q})[n] \to 0 \tag{1}$$

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

Now use the theory of heights
to deduce finite generation of $A(\mathbf{Q})$ from that of $A(\mathbf{Q})/n$. □

# How to compute the rank?

## Theorem of Mordell–Weil

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

## Proof (sketch).

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

$$0 \to A(\mathbf{Q})/n \to \mathrm{Sel}_n(A/\mathbf{Q}) \to Ш(A/\mathbf{Q})[n] \to 0 \tag{1}$$

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

Now use the theory of heights
to deduce finite generation of $A(\mathbf{Q})$ from that of $A(\mathbf{Q})/n$. □

## Two open problems

- Compute $r := \mathrm{rk}\, A(\mathbf{Q})$, the *algebraic rank*.
- Compute $Ш(A/\mathbf{Q})$, the *Shafarevich–Tate group*.

# How to compute the rank?

## Theorem of Mordell–Weil

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

## Proof (sketch).

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

$$0 \to A(\mathbf{Q})/n \to \mathrm{Sel}_n(A/\mathbf{Q}) \to Ш(A/\mathbf{Q})[n] \to 0 \tag{1}$$

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

Now use the theory of heights
to deduce finite generation of $A(\mathbf{Q})$ from that of $A(\mathbf{Q})/n$. □

## Two open problems

- Compute $r := \mathrm{rk}\, A(\mathbf{Q})$, the *algebraic rank*.
- Compute $Ш(A/\mathbf{Q})$, the *Shafarevich–Tate group*.

# How do you solve the problem conjecturally?

$L$-function of $E$:

$$L(E,s) := \prod_{p \in S_{\text{good}}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \cdot \prod_{p \in S_{\text{bad}}} \frac{1}{1 - a_p p^{-s}}, \quad \mathrm{Re}(s) > \tfrac{3}{2}$$

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

**Birch–Swinnerton-Dyer (rank) conjecture**

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

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

# How do you solve the problem conjecturally?

$L$-function of $E$:

$$L(E,s) := \prod_{p \in S_{\text{good}}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \cdot \prod_{p \in S_{\text{bad}}} \frac{1}{1 - a_p p^{-s}}, \quad \mathrm{Re}(s) > \tfrac{3}{2}$$

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

**Birch–Swinnerton-Dyer (rank) conjecture**

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

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

# What is the Shafarevich–Tate group?

The Shafarevich–Tate group

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

classifies everywhere locally trivial $A$-torsors.

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

# What is the Shafarevich–Tate group?

The Shafarevich–Tate group

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

classifies everywhere locally trivial $A$-torsors.

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

**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 is the Shafarevich–Tate group?

The Shafarevich–Tate group

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

classifies everywhere locally trivial $A$-torsors.

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

**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!

# Can you give a non-trivial example for Ш?

The Selmer cubic

$$C : 3x^3 + 4y^3 + 5z^3 = 0$$

is a non-trivial element of $Ш(E/\mathbf{Q})[3]$ for the elliptic curve

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

with $r = r_{\mathrm{an}} = 0$.

**Proof (sketch).**

- $C(\mathbf{Q}_v) \neq \emptyset$: Weil conjectures or $\mathrm{H}^1(\mathbf{F}_p, E) = 0$ and Hensel's lemma.
- $C(\mathbf{Q}) = \emptyset$: Cassels: Non-trivial point gives point in $E(\mathbf{Q})$ with $z \neq 0$, but $E(\mathbf{Q}) = \{[1 : -1 : 0]\}$. □

# Can you give a non-trivial example for Ш?

The Selmer cubic

$$C : 3x^3 + 4y^3 + 5z^3 = 0$$

is a non-trivial element of $Ш(E/\mathbf{Q})[3]$ for the elliptic curve

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

with $r = r_{\mathrm{an}} = 0$.

**Proof (sketch).**

- $C(\mathbf{Q}_v) \neq \emptyset$: Weil conjectures or $\mathrm{H}^1(\mathbf{F}_p, E) = 0$ and Hensel's lemma.
- $C(\mathbf{Q}) = \emptyset$: Cassels: Non-trivial point gives point in $E(\mathbf{Q})$ with $z \neq 0$, but $E(\mathbf{Q}) = \{[1 : -1 : 0]\}$. □

Assuming strong BSD, one has

$$Ш(E/\mathbf{Q}) \cong (\mathbf{Z}/3)^2.$$

# Can you give a non-trivial example for Ш?

The Selmer cubic

$$C : 3x^3 + 4y^3 + 5z^3 = 0$$

is a non-trivial element of $Ш(E/\mathbf{Q})[3]$ for the elliptic curve

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

with $r = r_{\mathrm{an}} = 0$.

**Proof (sketch).**

- $C(\mathbf{Q}_v) \neq \emptyset$: Weil conjectures or $\mathrm{H}^1(\mathbf{F}_p, E) = 0$ and Hensel's lemma.
- $C(\mathbf{Q}) = \emptyset$: Cassels: Non-trivial point gives point in $E(\mathbf{Q})$ with $z \neq 0$, but $E(\mathbf{Q}) = \{[1 : -1 : 0]\}$. □

Assuming strong BSD, one has

$$Ш(E/\mathbf{Q}) \cong (\mathbf{Z}/3)^2.$$

# 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 $\langle [C], [D] \rangle \neq 0$.

Questions?

# The BSD conjecture: What is known?

# What is an isogeny?
# How is it related to Galois representations?

**Definition**

An isogeny of abelian varieties is a finite surjective morphism.

- For $p$ prime, one has an isogeny $[p] : A \to A$.
- $A[p]$ is a finite flat $p$-torsion group scheme of order $p^{2\dim A}$.
- Sometimes $[p]$ can be factorized. This holds if and only if there is a non-trivial subgroup scheme of $A[p]$. In this case,

$$\rho_p : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{Aut}(A[p])$$

  is reducible and vice versa.
- If $A = E$ is an elliptic curve, reducible $\rho_p$ look like:

$$\rho_p \sim \begin{pmatrix} \varphi & * \\ 0 & \psi \end{pmatrix}, \quad \varphi, \psi : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathbf{F}_p^\times$$

- The expectation is that there are only finitely many reducible $\rho_p$.

# What is an isogeny?
# How is it related to Galois representations?

**Definition**

An isogeny of abelian varieties is a finite surjective morphism.

- For $p$ prime, one has an isogeny $[p] : A \to A$.
- $A[p]$ is a finite flat $p$-torsion group scheme of order $p^{2\dim A}$.
- Sometimes $[p]$ can be factorized. This holds if and only if there is a non-trivial subgroup scheme of $A[p]$. In this case,

$$\rho_p : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{Aut}(A[p])$$

  is reducible and vice versa.
- If $A = E$ is an elliptic curve, reducible $\rho_p$ look like:

$$\rho_p \sim \begin{pmatrix} \varphi & * \\ 0 & \psi \end{pmatrix}, \quad \varphi, \psi : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathbf{F}_p^\times$$

- The expectation is that there are only finitely many reducible $\rho_p$.

# What is a modular form?

## Definition

- The functor representing (generalized) elliptic curves with a cyclic $N$-isogeny (up to twist) is representable by a nice curve, called $X_0(N)$.
- Its Jacobian is denoted by $J_0(N)$.
- The space $S_2(\Gamma_0(N))$ of cusp forms is $\mathrm{H}^0(X_0(N), \Omega^1)$.

# What is a modular form?

## Definition

- The functor representing (generalized) elliptic curves with a cyclic $N$-isogeny (up to twist) is representable by a nice curve, called $X_0(N)$.
- Its Jacobian is denoted by $J_0(N)$.
- The space $S_2(\Gamma_0(N))$ of cusp forms is $\mathrm{H}^0(X_0(N), \Omega^1)$.

- $\dim_{\mathbf{C}} S_2(\Gamma_0(N)) = g(X_0(N)) < \infty$
- There is an injective $q$-expansion morphism $S_2(\Gamma_0(N)) \hookrightarrow \mathbf{C}[\![q]\!], f \mapsto \sum_{n\geq 1} a_n(f) q^n$.
- Example: $S_2(\Gamma_0(11)) = \mathbf{C} \cdot (\Delta(z)\Delta(11z))^{\frac{1}{12}}$ with

$$\Delta(z) := (2\pi)^{12} \cdot q \prod_{n\geq 1} (1 - q^n)^{24}, \quad q = e^{2\pi i z}.$$

# What is a modular form?

## Definition

- The functor representing (generalized) elliptic curves with a cyclic $N$-isogeny (up to twist) is representable by a nice curve, called $X_0(N)$.
- Its Jacobian is denoted by $J_0(N)$.
- The space $S_2(\Gamma_0(N))$ of cusp forms is $\mathrm{H}^0(X_0(N), \Omega^1)$.

- $\dim_{\mathbf{C}} S_2(\Gamma_0(N)) = g(X_0(N)) < \infty$
- There is an injective $q$-expansion morphism $S_2(\Gamma_0(N)) \hookrightarrow \mathbf{C}[\![q]\!], f \mapsto \sum_{n\geq 1} a_n(f) q^n$.
- Example: $S_2(\Gamma_0(11)) = \mathbf{C} \cdot (\Delta(z)\Delta(11z))^{\frac{1}{12}}$ with

$$\Delta(z) := (2\pi)^{12} \cdot q \prod_{n\geq 1} (1 - q^n)^{24}, \quad q = e^{2\pi i z}.$$

# What is a newform?

- Newforms $f$ are special cusp forms.
- There are only finitely many for each $N$.
- One can associate a system of $\ell$-adic Galois representations to $f$, denoted by $\rho_{f,\ell^\infty}$.
- $A$ is called modular if $\rho_{A,\ell^\infty} \cong \rho_{f,\ell^\infty}$.
- One can transfer results about $A$ to $f$ and vice versa.

# What is a newform?

- Newforms $f$ are special cusp forms.
- There are only finitely many for each $N$.
- One can associate a system of $\ell$-adic Galois representations to $f$, denoted by $\rho_{f,\ell^\infty}$.
- $A$ is called modular if $\rho_{A,\ell^\infty} \cong \rho_{f,\ell^\infty}$.
- One can transfer results about $A$ to $f$ and vice versa.

# What is a modular abelian variety?

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

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

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

# What is a modular abelian variety?

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

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

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

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

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

# What is a modular abelian variety?

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

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

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

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

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

If this is the case, $A/\mathbf{Q}$ is modular,
$\mathbf{Q}(f) \simeq \mathrm{End}^0_{\mathbf{Q}}(A)$,
and $A$ is of $\mathrm{GL}_2$-type over $\mathbf{Q}$: $\dim_{\mathrm{End}(A)\otimes\mathbf{Q}_\ell} V_\ell A = 2$.

# What is a modular abelian variety?

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

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

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

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

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

If this is the case, $A/\mathbf{Q}$ is modular,
$\mathbf{Q}(f) \simeq \mathrm{End}^0_{\mathbf{Q}}(A)$,
and $A$ is of $\mathrm{GL}_2$-type over $\mathbf{Q}$: $\dim_{\mathrm{End}(A)\otimes\mathbf{Q}_\ell} V_\ell A = 2$.

# What is already known about (strong) BSD?

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

# What is already known about (strong) BSD?

- Birch–Swinnerton-Dyer (1965): formulation of BSD.
- Coates–Wiles (1977): $r_{\mathrm{an}} = 0 \implies r = 0$ for $E$ CM.
- Gross–Zagier (1986): $r_{\mathrm{an}} = 1 \implies r \geq 1$ for $E$ modular (and for $A_f/\mathbf{Q}$ modular: $r_{\mathrm{an}}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f$).

# What is already known about (strong) BSD?

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

# What is already known about (strong) BSD?

- Birch–Swinnerton-Dyer (1965): formulation of BSD.
- Coates–Wiles (1977): $r_{\mathrm{an}} = 0 \implies r = 0$ for $E$ CM.
- Gross–Zagier (1986): $r_{\mathrm{an}} = 1 \implies r \geq 1$ for $E$ modular (and for $A_f/\mathbf{Q}$ modular: $r_{\mathrm{an}}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f$).
- Rubin (1987): $r_{\mathrm{an}} = 0 \implies Ш(E/K)$ finite for $E/K$ CM.
- Kolyvagin (1988): $r_{\mathrm{an}} \leq 1 \implies r = r_{\mathrm{an}}$ and Ш finite for $E/\mathbf{Q}$.
- Kolyvagin–Logachëv (1989) [KL]: $r_{\mathrm{an}}(f) \leq 1 \implies r = r_{\mathrm{an}}$ and Ш finite for $A_f/\mathbf{Q}$ modular.
- Wiles, Taylor–Wiles (1994): every $E/\mathbf{Q}$ semistable is modular.
- Breuil–Conrad–Diamond–Taylor (2001): every $E/\mathbf{Q}$ is modular.

# What is already known about (strong) BSD?

- Birch–Swinnerton-Dyer (1965): formulation of BSD.
- Coates–Wiles (1977): $r_{\mathrm{an}} = 0 \implies r = 0$ for $E$ CM.
- Gross–Zagier (1986): $r_{\mathrm{an}} = 1 \implies r \geq 1$ for $E$ modular (and for $A_f/\mathbf{Q}$ modular: $r_{\mathrm{an}}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f$).
- Rubin (1987): $r_{\mathrm{an}} = 0 \implies Ш(E/K)$ finite for $E/K$ CM.
- Kolyvagin (1988): $r_{\mathrm{an}} \leq 1 \implies r = r_{\mathrm{an}}$ and Ш finite for $E/\mathbf{Q}$.
- Kolyvagin–Logachëv (1989) [KL]: $r_{\mathrm{an}}(f) \leq 1 \implies r = r_{\mathrm{an}}$ and Ш finite for $A_f/\mathbf{Q}$ modular.
- Wiles, Taylor–Wiles (1994): every $E/\mathbf{Q}$ semistable is modular.
- Breuil–Conrad–Diamond–Taylor (2001): every $E/\mathbf{Q}$ is modular.
- Ribet (2004): Serre's modularity conjecture $\implies$ every $A/\mathbf{Q}$ with RM is modular.
- Khare–Kisin–Wintenberger (2010): Serre's modularity conjecture holds.

# What is already known about (strong) BSD?

- Birch–Swinnerton-Dyer (1965): formulation of BSD.
- Coates–Wiles (1977): $r_{\mathrm{an}} = 0 \implies r = 0$ for $E$ CM.
- Gross–Zagier (1986): $r_{\mathrm{an}} = 1 \implies r \geq 1$ for $E$ modular (and for $A_f/\mathbf{Q}$ modular: $r_{\mathrm{an}}(f) \geq 1 \implies r(A_f/K) \geq \dim A_f$).
- Rubin (1987): $r_{\mathrm{an}} = 0 \implies Ш(E/K)$ finite for $E/K$ CM.
- Kolyvagin (1988): $r_{\mathrm{an}} \leq 1 \implies r = r_{\mathrm{an}}$ and Ш finite for $E/\mathbf{Q}$.
- Kolyvagin–Logachëv (1989) [KL]: $r_{\mathrm{an}}(f) \leq 1 \implies r = r_{\mathrm{an}}$ and Ш finite for $A_f/\mathbf{Q}$ modular.
- Wiles, Taylor–Wiles (1994): every $E/\mathbf{Q}$ semistable is modular.
- Breuil–Conrad–Diamond–Taylor (2001): every $E/\mathbf{Q}$ is modular.
- Ribet (2004): Serre's modularity conjecture $\implies$ every $A/\mathbf{Q}$ with RM is modular.
- Khare–Kisin–Wintenberger (2010): Serre's modularity conjecture holds.

# What is important to remember for this talk?

Let $A$ be a modular abelian variety[1] 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:

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

[1]Note that a generic abelian variety of dimension $> 1$ is *not* modular in this sense!

# What is important to remember for this talk?

Let $A$ be a modular abelian variety[1] 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:

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

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

[1] Note that a generic abelian variety of dimension $> 1$ is *not* modular in this sense!

# What is important to remember for this talk?

Let $A$ be a modular abelian variety[1] 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)

[1] Note that a generic abelian variety of dimension $> 1$ is *not* modular in this sense!

# 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 modular 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 $r_{\mathrm{an}} \leq 1$:
  - 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 modular 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): $\mathrm{GL}_2$ Iwasawa Main Conjecture (IMC) for primes $p$ of good ordinary reduction and $\rho_p$ irreducible.
  - Skinner (2016): $\mathrm{GL}_2$ IMC for primes $p$ of bad multiplicative reduction and $\rho_p$ 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 $\rho_p$ 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 modular 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): $\mathrm{GL}_2$ Iwasawa Main Conjecture (IMC) for primes $p$ of good ordinary reduction and $\rho_p$ irreducible.
  - Skinner (2016): $\mathrm{GL}_2$ IMC for primes $p$ of bad multiplicative reduction and $\rho_p$ 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 $\rho_p$ irreducible.

Questions?

# 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 modular 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).

# 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 modular 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* $\mathfrak{p}$.

# 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 modular 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.

# 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.

## For a *given* modular abelian surface $A$, we . . .

- . . . explicitly prove that almost all $\rho_{\mathfrak{p}}$ are irreducible and maximal,

# 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.

## For a *given* modular abelian surface $A$, we . . .

- . . . explicitly prove that almost all $\rho_{\mathfrak{p}}$ are irreducible and maximal,
- . . . compute Heegner indices $I_K := [A(K) : \mathcal{O}y_K]$,
- . . . and use this to compute
  - $\#Ш(A/\mathbf{Q})$ and
  - $\#Ш(A/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ exactly.

# 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.

## For a *given* modular abelian surface $A$, we . . .

- . . . explicitly prove that almost all $\rho_{\mathfrak{p}}$ are irreducible and maximal,
- . . . compute Heegner indices $I_K := [A(K) : \mathcal{O}y_K]$,
- . . . and use this to compute
  - $\#Ш(A/\mathbf{Q})$ and
  - $\#Ш(A/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ exactly.

# 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 $\mathrm{GL}_2$ 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 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 $\mathrm{GL}_2$ 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?

$$
\begin{tikzcd}
 & \boxed{y_K} \arrow[dr] \arrow[ddd] & & \mathcal{O} \arrow[dl] & & \boxed{\rho_{\mathfrak{p}}} \arrow[dr] \arrow[drr] \arrow[ddd] & & \mathcal{L}_{\mathfrak{p}}(f,T) \arrow[dddl] & \mathrm{Sel}_{\mathfrak{p}} \arrow[dddl] \\
 & & \mathcal{O}y_K \arrow[d] & & & & H^1(G_i, A[\mathfrak{p}^i]) \arrow[ddl] & & \\
L'(f^{\alpha}/K,1) \arrow[dr] & & I_K \arrow[ddr] & & & & & & \\
 & \#Ш(A)_{\mathrm{an}} \arrow[ddrr] & & & & [\mathrm{KL}] \arrow[d] & & Ш(A)[\mathfrak{p}] \arrow[dl] & \\
 & & & & & \mathrm{BSD}(A) & & &
\end{tikzcd}
$$

Questions?

How to compute $\rho_{\mathfrak{p}}$?

# Which Galois representations are we interested in?

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

# Which Galois representations are we interested in?

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

# Excursion: Group theory of finite groups of Lie type

Assume $\mathfrak{p} \nmid 2$. Every subgroup of
$\mathrm{PSL}_2(\mathfrak{p}) := \mathbf{ker}\big(\overline{\det} : \mathrm{PGL}_2(\mathbf{F}_\mathfrak{p}) \twoheadrightarrow \mathbf{F}_\mathfrak{p}^\times/2\big)$ is (up to conjugacy)
contained in one of the following maximal subgroups:

- Borel subgroup $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ (reducible image as $\mathbf{F}_\mathfrak{p}$-representation)
- $\mathrm{PSL}_2(p)$ (reducible image as $\mathbf{F}_p$-representation, only for $\mathbf{F}_\mathfrak{p} \supsetneq \mathbf{F}_p$)
- 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 $\varepsilon \in \mathbf{F}_\mathfrak{p} \setminus \mathbf{F}_\mathfrak{p}^\square$
- $A_4$, $S_4$ or $A_5$ (exceptional image)

# How to prove almost all $\rho_{\mathfrak{p}}$ are irreducible?

- Raynaud's classification of simple factors of $\rho_p|_{I_p}^{\mathrm{ss}}$ and CFT:

  If $\rho_{\mathfrak{p}}$ is reducible, $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with $\varepsilon$ of conductor $d$ with $d^2 \mid N$, or $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon\chi_p^n \oplus \varepsilon^{-1}\chi_p^{1-n}$ if $p^2 \mid N$.
- Hence: If $\rho_{\mathfrak{p}}$ is reducible as an $\mathbf{F}_{\mathfrak{p}}$-representation for all $\mathfrak{p} \mid p$, then

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

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

# How to prove almost all $\rho_{\mathfrak{p}}$ are irreducible?

- Raynaud's classification of simple factors of $\rho_p|_{I_p}^{\mathrm{ss}}$ and CFT:

  If $\rho_{\mathfrak{p}}$ is reducible, $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with $\varepsilon$ of conductor $d$ with $d^2 \mid N$,
  or $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon\chi_p^n \oplus \varepsilon^{-1}\chi_p^{1-n}$ if $p^2 \mid N$.
- Hence: If $\rho_{\mathfrak{p}}$ is reducible as an $\mathbf{F}_{\mathfrak{p}}$-representation for all $\mathfrak{p} \mid p$, then

  an eigenvalue of $\rho_p(\mathrm{Frob}_\ell)$ has order dividing $\mathrm{ord}(\overline{\ell} \in (\mathbf{Z}/d)^\times)$.

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

# How to prove almost all $\rho_{\mathfrak{p}}$ are irreducible?

- Raynaud's classification of simple factors of $\rho_p|_{I_p}^{\mathrm{ss}}$ and CFT:

  If $\rho_{\mathfrak{p}}$ is reducible, $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with $\varepsilon$ of conductor $d$ with $d^2 \mid N$,
  or $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon\chi_p^n \oplus \varepsilon^{-1}\chi_p^{1-n}$ if $p^2 \mid N$.
- Hence: If $\rho_{\mathfrak{p}}$ is reducible as an $\mathbf{F}_{\mathfrak{p}}$-representation for all $\mathfrak{p} \mid p$, then

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

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

# How to prove almost all $\rho_{\mathfrak{p}}$ are irreducible?

- Raynaud's classification of simple factors of $\rho_p|_{I_p}^{\mathrm{ss}}$ and CFT:

  If $\rho_{\mathfrak{p}}$ is reducible, $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with $\varepsilon$ of conductor $d$ with $d^2 \mid N$,
  or $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon\chi_p^n \oplus \varepsilon^{-1}\chi_p^{1-n}$ if $p^2 \mid N$.
- Hence: If $\rho_{\mathfrak{p}}$ is reducible as an $\mathbf{F}_{\mathfrak{p}}$-representation for all $\mathfrak{p} \mid p$, then

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

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

# How to prove almost all $\rho_{\mathfrak{p}}$ are irreducible?

- Raynaud's classification of simple factors of $\rho_p|_{I_p}^{\mathrm{ss}}$ and CFT:
  If $\rho_{\mathfrak{p}}$ is reducible, $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with $\varepsilon$ of conductor $d$ with $d^2 \mid N$,
  or $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon\chi_p^n \oplus \varepsilon^{-1}\chi_p^{1-n}$ if $p^2 \mid N$.
- Hence: If $\rho_{\mathfrak{p}}$ is reducible as an $\mathbf{F}_{\mathfrak{p}}$-representation for all $\mathfrak{p} \mid p$, then

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

  for $d = d_{\max}$ maximal such that $d_{\max}^2 \mid N$,
  or $d = p \cdot d_{\max}$ if $p^2 \mid N$.
- Bounding the resultant using the Weil conjectures gives a small finite set of primes $p$ containing all $p$ with $\rho_{\mathfrak{p}}$ reducible for all $\mathfrak{p} \mid p$.

# How to prove almost all $\rho_{\mathfrak{p}}$ are irreducible?

- Raynaud's classification of simple factors of $\rho_p|_{I_p}^{\mathrm{ss}}$ and CFT:
  If $\rho_{\mathfrak{p}}$ is reducible, $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with $\varepsilon$ of conductor $d$ with $d^2 \mid N$,
  or $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon\chi_p^n \oplus \varepsilon^{-1}\chi_p^{1-n}$ if $p^2 \mid N$.
- Hence: If $\rho_{\mathfrak{p}}$ is reducible as an $\mathbf{F}_{\mathfrak{p}}$-representation for all $\mathfrak{p} \mid p$, then

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

  for $d = d_{\max}$ maximal such that $d_{\max}^2 \mid N$,
  or $d = p \cdot d_{\max}$ if $p^2 \mid N$.
- Bounding the resultant using the Weil conjectures gives a small finite set of primes $p$ containing all $p$ with $\rho_{\mathfrak{p}}$ reducible for all $\mathfrak{p} \mid p$.
- Can be refined to $\mathfrak{p} \triangleleft \mathcal{O}$.

# How to prove almost all $\rho_{\mathfrak{p}}$ are maximal?

- If $\rho_{\mathfrak{p}}$ is irreducible as an $\mathbf{F}_{\mathfrak{p}}$-representation, but reducible as an $\mathbf{F}_p$-representation,

$$p \mid \gcd_{\substack{\ell \nmid pN \\ \ell \equiv 1 \pmod{d}}} \left( \frac{a_\ell - \overline{a_\ell}}{2} \right).$$

- If $p > 5$, $\rho_{\mathfrak{p}}$ does not have exceptional image.
- If $p > C(N, \deg \mathfrak{p})$, then the image of $\rho_{\mathfrak{p}}$ is not contained in the normalizer of a Cartan subgroup.

Questions?

# How to compute the Heegner index?

# How to compute a rational number exactly?

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

# How to go from the analytic rank to the algebraic rank?

Let $K/\mathbf{Q}$ 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 $\mathcal{O}_K/\mathfrak{n} \cong \mathbf{Z}/N$,
- $L'(f/K, 1) \neq 0$.

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

**Gross–Zagier formula, 1986**

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

$$L'(f/K, 1) = \frac{\|\omega_f\|^2}{c_\pi^2 u_K^2 \sqrt{|\operatorname{disc}_K|}} \hat{h}(y_K) \in \mathbf{R}_{\geq 0}.$$

# How to go from the analytic rank to the algebraic rank?

Let $K/\mathbf{Q}$ 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 $\mathcal{O}_K/\mathfrak{n} \cong \mathbf{Z}/N$,
- $L'(f/K, 1) \neq 0$.

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

## Gross–Zagier formula, 1986

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

$$L'(f/K, 1) = \frac{\|\omega_f\|^2}{c_\pi^2 u_K^2 \sqrt{|\operatorname{disc}_K|}} \hat{h}(y_K) \in \mathbf{R}_{\geq 0}.$$

# How to compute the Heegner index $I_K$?

- We need to work on a Jacobian in the isogeny class of $A_f := J_0(N)/\mathrm{Ann}_{\mathbf{T}}(f)$.
- Compute an isogeny $\pi : A_f \to J := \mathrm{Jac}(X)$ using the big period matrices of $A_f$ and $J$.
- Compute the $h_K$ Heegner forms $Ax^2 + Bx + C$ for $(N, \mathrm{disc}_K)$.
- Compute the zeros $\tau$ of the Heegner forms with $\mathrm{Im}(\tau) > 0$.
- 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 $\pi : \mathbf{C}^2/\Lambda_f \to J(\mathbf{C})$ ($X$ hyperelliptic!) and sum over all $\tau$ to get a $\mathbf{C}$-approximation of $\pi(y_K)$.
- Find a $K$-approximation to $\pi(y_K) \in J(K)$.

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

# How to compute the Heegner index $I_K$?

- We need to work on a Jacobian in the isogeny class of $A_f := J_0(N)/\mathrm{Ann}_{\mathbf{T}}(f)$.
- Compute an isogeny $\pi : A_f \to J := \mathrm{Jac}(X)$ using the big period matrices of $A_f$ and $J$.
- Compute the $h_K$ Heegner forms $Ax^2 + Bx + C$ for $(N, \mathrm{disc}_K)$.
- Compute the zeros $\tau$ of the Heegner forms with $\mathrm{Im}(\tau) > 0$.
- 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 $\pi : \mathbf{C}^2/\Lambda_f \to J(\mathbf{C})$ ($X$ hyperelliptic!) and sum over all $\tau$ to get a $\mathbf{C}$-approximation of $\pi(y_K)$.
- Find a $K$-approximation to $\pi(y_K) \in J(K)$.

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

# How to prove that our $\mathcal{O}\pi(y_K)$ is correct?

- Problem: The set of points of $J(K)$ near to some $y \in J(\mathbf{C})$ is dense!
- Idea: Use the Northcott property of heights $\hat{h}_{\mathscr{L}} : J(K) \to \mathbf{R}_{\geq 0}$ and assume that $\hat{h}_{2\vartheta}$ is injective on $J(K)$ up to sign and torsion.

# How to prove that our $\mathcal{O}\pi(y_K)$ is correct?

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

# How to prove that our $\mathcal{O}\pi(y_K)$ is correct?

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

$$A_f^\vee \to J_0(N)^\vee \xrightarrow{\sim} J_0(N) \to A_f.$$

- 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. $2\vartheta$.
- There is exactly one $y \in J(K)$ (up to sign and torsion) with height sufficiently close to that.
- We get $\mathcal{O}^\times y$, hence $I_K$ exactly up to a divisor of $\deg(\pi)$.

# How to prove that our $\mathcal{O}\pi(y_K)$ is correct?

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

$$A_f^\vee \to J_0(N)^\vee \xrightarrow{\sim} J_0(N) \to A_f.$$

- 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. $2\vartheta$.
- There is exactly one $y \in J(K)$ (up to sign and torsion) with height sufficiently close to that.
- We get $\mathcal{O}^\times y$, hence $I_K$ exactly up to a divisor of $\deg(\pi)$.

# 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 $\Omega_A$.
- 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 $\#Ш(A/\mathbf{Q})_{\mathrm{an}}$ 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 $\Omega_A$.
- 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.

Questions?

# 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 $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$

# 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 $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})/2$ 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 $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})/2$ gives $Ш(A/\mathbf{Q})[2] = 0$.
- [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 $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})/2$ gives $Ш(A/\mathbf{Q})[2] = 0$.
- [KL] with $I_{\mathbf{Q}(\sqrt{-23})} = 7$ gives $\#Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ for $\mathfrak{p} \nmid (\sqrt{2}), 7$.
- $\rho_{\mathfrak{p}}$ 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 $Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$.

# 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 $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})/2$ gives $Ш(A/\mathbf{Q})[2] = 0$.
- [KL] with $I_{\mathbf{Q}(\sqrt{-23})} = 7$ gives $\#Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ for $\mathfrak{p} \nmid (\sqrt{2}), 7$.
- $\rho_{\mathfrak{p}}$ 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 $\mathrm{GL}_2$ 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 $\mathfrak{p}\bar{\mathfrak{p}} = 7$.
- $c = 7$
- $\mathrm{Sel}_2(A/\mathbf{Q}) \cong (\mathbf{Z}/2)^2 \cong A(\mathbf{Q})/2$ gives $Ш(A/\mathbf{Q})[2] = 0$.
- [KL] with $I_{\mathbf{Q}(\sqrt{-23})} = 7$ gives $\#Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$ for $\mathfrak{p} \nmid (\sqrt{2}), 7$.
- $\rho_{\mathfrak{p}}$ 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 $\mathrm{GL}_2$ 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 |

Questions?

# What is left to do?

# What would be nice to achieve?

- Using Shnidman–Weiss[2], 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)!

[2] *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 modular Jacobian from the LMFDB.
- Verification for (almost?) all $\sim 1200$ newforms of level $\leq 1000$ with real-quadratic coefficients foreseeable.

# What are the next steps and projects?

- Almost done: Verification for all 97 genus 2 curves with absolutely simple 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.

# What are the next steps and projects?

- 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!