

Funded by



Deutsche  
Forschungsgemeinschaft  
German Research Foundation



UNIVERSITÄT  
BAYREUTH

# 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  $\mathbf{Q}$ , 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

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

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

# Motivating problem

Making the Mordell–Weil theorem explicit

## Theorem of Mordell–Weil

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

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

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

Now use the theory of **heights**

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

# Motivating problem

Making the Mordell–Weil theorem explicit

## 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

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

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

Now use the theory of **heights**

to deduce finite generation of  $A(\mathbf{Q})$  from that of  $A(\mathbf{Q})/n$ .  $\square$

## 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  $\mathbf{Q}$ , 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

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

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

Now use the theory of **heights**

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

## 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  $a_p = p + 1 - \#E(\mathbf{F}_p)$  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  $E/\mathbf{Q}$ .
- ▶ Yields “day-night algorithm” to compute  $E(\mathbf{Q})$ .
- ▶ 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  $a_p = p + 1 - \#E(\mathbf{F}_p)$  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  $E/\mathbf{Q}$ .
- ▶ Yields “day-night algorithm” to compute  $E(\mathbf{Q})$ .
- ▶ Proven if  $r_{\text{an}} \leq 1$ .

# The Shafarevich–Tate group

## The Shafarevich–Tate group

$$\text{III}(A/\mathbf{Q}) := \ker \left( H^1(\mathbf{Q}, A) \rightarrow \bigoplus_v H^1(\mathbf{Q}_v, A) \right)$$

classifies everywhere locally  $A$ -torsors.

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

# The Shafarevich–Tate group

## The Shafarevich–Tate group

$$\text{III}(A/\mathbf{Q}) := \ker \left( H^1(\mathbf{Q}, A) \rightarrow \bigoplus_v H^1(\mathbf{Q}_v, A) \right)$$

classifies everywhere locally  $A$ -torsors.

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

strong BSD conjecture

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

Compare with the analytic class number formula!

# The Shafarevich–Tate group

## The Shafarevich–Tate group

$$\text{III}(A/\mathbf{Q}) := \ker \left( H^1(\mathbf{Q}, A) \rightarrow \bigoplus_v H^1(\mathbf{Q}_v, A) \right)$$

classifies everywhere locally  $A$ -torsors.

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

## strong BSD conjecture

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

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  $\text{III}(E/\mathbf{Q})[3]$  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).

$C(\mathbf{Q}_v) \neq \emptyset$ : Weil conjectures or  $H^1(\mathbf{F}_p, E) = 0$  and Hensel's lemma.

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

# An example for the Shafarevich–Tate group

The Selmer cubic

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

is a non-trivial element of  $\text{III}(E/\mathbf{Q})[3]$  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).

$C(\mathbf{Q}_v) \neq \emptyset$ : Weil conjectures or  $H^1(\mathbf{F}_p, E) = 0$  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

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

# An example for the Shafarevich–Tate group

The Selmer cubic

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

is a non-trivial element of  $\text{III}(E/\mathbf{Q})[3]$  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).

$C(\mathbf{Q}_v) \neq \emptyset$ : Weil conjectures or  $H^1(\mathbf{F}_p, E) = 0$  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

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

# Application of the strong BSD conjecture

## Problem

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

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

$$\langle \cdot, \cdot \rangle : \text{III}(E/\mathbf{Q}) \times \text{III}(E/\mathbf{Q}) \rightarrow \mathbf{Q}/\mathbf{Z}$$

to find  $[D] \in \text{III}(E/\mathbf{Q})$  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):  $r_{\text{an}} = 0 \implies r = 0$  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):  $r_{\text{an}} = 0 \implies r = 0$  for  $E$  CM.
- ▶ GROSS–ZAGIER (1986):  $r_{\text{an}} = 1 \implies r \geq 1$  for  $E$  modular  
(and for  $A_f/\mathbf{Q}$  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.

## 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  $A_f/\mathbf{Q}$  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  $\text{III}$  finite for  $E/\mathbf{Q}$ .

## 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  $A_f/\mathbf{Q}$  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  $\text{III}$  finite for  $E/\mathbf{Q}$ .
- ▶ KOLYVAGIN–LOGACHËV (1989) [KL]:  $r_{\text{an}}(f) \leq 1 \implies r = r_{\text{an}}$   
and  $\text{III}$  finite for  $A_f/\mathbf{Q}$  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  $A_f/\mathbf{Q}$  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  $\text{III}$  finite for  $E/\mathbf{Q}$ .
- ▶ KOLYVAGIN–LOGACHËV (1989) [KL]:  $r_{\text{an}}(f) \leq 1 \implies r = r_{\text{an}}$  and  $\text{III}$  finite for  $A_f/\mathbf{Q}$  modular.
- ▶ WILES, TAYLOR–WILES (1994): every  $E/\mathbf{Q}$  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  $A_f/\mathbf{Q}$  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  $\text{III}$  finite for  $E/\mathbf{Q}$ .
- ▶ KOLYVAGIN–LOGACHËV (1989) [KL]:  $r_{\text{an}}(f) \leq 1 \implies r = r_{\text{an}}$  and  $\text{III}$  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.

## 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  $A_f/\mathbf{Q}$  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  $\text{III}$  finite for  $E/\mathbf{Q}$ .
- ▶ KOLYVAGIN–LOGACHËV (1989) [KL]:  $r_{\text{an}}(f) \leq 1 \implies r = r_{\text{an}}$  and  $\text{III}$  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.



## 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  $A_f/\mathbf{Q}$  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  $\text{III}$  finite for  $E/\mathbf{Q}$ .
- ▶ KOLYVAGIN–LOGACHËV (1989) [KL]:  $r_{\text{an}}(f) \leq 1 \implies r = r_{\text{an}}$  and  $\text{III}$  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.

## 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  $A_f/\mathbf{Q}$  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  $\text{III}$  finite for  $E/\mathbf{Q}$ .
- ▶ KOLYVAGIN–LOGACHËV (1989) [KL]:  $r_{\text{an}}(f) \leq 1 \implies r = r_{\text{an}}$  and  $\text{III}$  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.

# State of the art: summary

The strong BSD conjecture for abelian varieties of  $GL_2$ -type and  $L$ -rank 0 or 1 over  $\mathbf{Q}$

Let  $A$  be a modular abelian variety over  $\mathbf{Q}$  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:

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

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

$$r = r_{\text{an}}, \quad \#\text{III}(A/\mathbf{Q}) < \infty.$$

# State of the art: summary

The strong BSD conjecture for abelian varieties of  $GL_2$ -type and  $L$ -rank 0 or 1 over  $\mathbf{Q}$

Let  $A$  be a modular abelian variety over  $\mathbf{Q}$  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:

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

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

$$r = r_{\text{an}}, \quad \#\text{III}(A/\mathbf{Q}) < \infty.$$

- ▶ **Unknown:**  $\#\text{III}(A/\mathbf{Q}) \stackrel{?}{=} \#\text{III}(A/\mathbf{Q})_{\text{an}}$  (strong BSD)

# State of the art: summary

The strong BSD conjecture for abelian varieties of  $GL_2$ -type and  $L$ -rank 0 or 1 over  $\mathbf{Q}$

Let  $A$  be a modular abelian variety over  $\mathbf{Q}$  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:

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

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

$$r = r_{\text{an}}, \quad \#\text{III}(A/\mathbf{Q}) < \infty.$$

- ▶ **Unknown:**  $\#\text{III}(A/\mathbf{Q}) \stackrel{?}{=} \#\text{III}(A/\mathbf{Q})_{\text{an}}$  (strong BSD)

## Previous work on the verification

- ▶ For elliptic curves:
  - Strong BSD verified exactly for levels  $N < 5000$  combining work of GRIGOROV–JORZA–PATRIKIS–STEIN–TARNIȚĂ (2009), MILLER (2011), MILLER–STOLL (2013, isogeny descent), CREUTZ–MILLER (2012, second isogeny descent), LAWSON–WUTHRICH (2016, use of  $p$ -adic  $L$ -functions).
- ▶ In dimension  $> 1$ :
  - FLYNN–LEPRÉVOST–SCHAEFER–STEIN–STOLL–WETHERELL (2001): BSD for some Jacobians of dimension 2 numerically.

## Previous work on the verification

- ▶ For elliptic curves:
  - Strong BSD verified exactly for levels  $N < 5000$  combining work of GRIGOROV–JORZA–PATRIKIS–STEIN–TARNIȚĂ (2009), MILLER (2011), MILLER–STOLL (2013, isogeny descent), CREUTZ–MILLER (2012, second isogeny descent), LAWSON–WUTHRICH (2016, use of  $p$ -adic  $L$ -functions).
- ▶ In dimension  $> 1$ :
  - FLYNN–LEPRÉVOST–SCHAEFER–STEIN–STOLL–WETHERELL (2001): BSD for some Jacobians of dimension 2 **numerically**.
  - 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:
  - Strong BSD verified exactly for levels  $N < 5000$  combining work of GRIGOROV–JORZA–PATRIKIS–STEIN–TARNIȚĂ (2009), MILLER (2011), MILLER–STOLL (2013, isogeny descent), CREUTZ–MILLER (2012, second isogeny descent), LAWSON–WUTHRICH (2016, use of  $p$ -adic  $L$ -functions).
- ▶ In dimension  $> 1$ :
  - FLYNN–LEPRÉVOST–SCHAEFER–STEIN–STOLL–WETHERELL (2001): BSD for some Jacobians of dimension 2 **numerically**.
  - 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:
  - Strong BSD verified exactly for levels  $N < 5000$  combining work of GRIGOROV–JORZA–PATRIKIS–STEIN–TARNIȚĂ (2009), MILLER (2011), MILLER–STOLL (2013, isogeny descent), CREUTZ–MILLER (2012, second isogeny descent), LAWSON–WUTHRICH (2016, use of  $p$ -adic  $L$ -functions).
- ▶ In dimension  $> 1$ :
  - FLYNN–LEPRÉVOST–SCHAEFER–STEIN–STOLL–WETHERELL (2001): BSD for some Jacobians of dimension 2 **numerically**.
  - 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):  
 $v_p(\#\text{III}(A/\mathbb{Q})) = v_p(\#\text{III}(A/\mathbb{Q})_{\text{an}})$   
if  $N$  is **square-free**,  $p \nmid N$ , and  $\rho_p$  irreducible.

## Previous work on the verification

- ▶ For elliptic curves:
  - Strong BSD verified exactly for levels  $N < 5000$  combining work of GRIGOROV–JORZA–PATRIKIS–STEIN–TARNIȚĂ (2009), MILLER (2011), MILLER–STOLL (2013, isogeny descent), CREUTZ–MILLER (2012, second isogeny descent), LAWSON–WUTHRICH (2016, use of  $p$ -adic  $L$ -functions).
- ▶ In dimension  $> 1$ :
  - FLYNN–LEPRÉVOST–SCHAEFER–STEIN–STOLL–WETHERELL (2001): BSD for some Jacobians of dimension 2 **numerically**.
  - 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):  
$$v_p(\#\text{III}(A/\mathbf{Q})) = v_p(\#\text{III}(A/\mathbf{Q})_{\text{an}})$$
if  $N$  is **square-free**,  $p \nmid N$ , and  $\rho_p$  irreducible.

# Modularity in dimension $> 1$

## 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  $N$ ,

# Modularity in dimension $> 1$

## 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  $N$ ,
- ▶  $L(A/\mathbf{Q}, s) = \prod_{\alpha: \mathcal{O} \rightarrow \mathbf{C}} L(f^\alpha, s)$  for a newform  $f \in S_2(\Gamma_0(N), \mathcal{O})$ .

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

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

# Modularity in dimension $> 1$

## 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  $N$ ,
- ▶  $L(A/\mathbf{Q}, s) = \prod_{\alpha: \mathcal{O} \hookrightarrow \mathbf{C}} L(f^\alpha, s)$  for a newform  $f \in S_2(\Gamma_0(N), \mathcal{O})$ .

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

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

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

# Modularity in dimension $> 1$

## 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  $N$ ,
- ▶  $L(A/\mathbf{Q}, s) = \prod_{\alpha: \mathcal{O} \hookrightarrow \mathbf{C}} L(f^\alpha, s)$  for a newform  $f \in S_2(\Gamma_0(N), \mathcal{O})$ .

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

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

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

# 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  $\rho_{p^\infty} : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \rightarrow \text{GL}_2(\mathcal{O}_p)$ .

# 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  $\rho_{p^\infty} : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \rightarrow \text{GL}_2(\mathcal{O}_p)$ .

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  $A/\mathbf{Q}$

## 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  $\rho_{p^\infty} : \text{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \rightarrow \text{GL}_2(\mathcal{O}_p)$ .

## 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  $\#\text{III}(A/\mathbf{Q}) \in \mathbf{Z}_{\geq 1}$  and  $\#\text{III}(A/\mathbf{Q})_{\text{an}} \in \mathbf{Q}_{>0}$  exactly.

# Main technical problems

concerning the mod- $p$  and  $p$ -adic Galois representations of  $A/\mathbf{Q}$

## 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  $\rho_{p^\infty} : \text{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \rightarrow \text{GL}_2(\mathcal{O}_p)$ .

## 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  $\#\text{III}(A/\mathbf{Q}) \in \mathbf{Z}_{\geq 1}$  and  $\#\text{III}(A/\mathbf{Q})_{\text{an}} \in \mathbf{Q}_{>0}$  exactly.

# An explicit Euler system

## Theorem (K.): explicit finite support of $\text{III}(A/\mathbf{Q})$

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

One has  $\text{III}(A/\mathbf{Q})[\mathfrak{p}] = 0$  for all  $\mathfrak{p}$  with

- ▶  $\rho_{\mathfrak{p}} : \text{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \rightarrow \text{Aut}_{\mathbf{F}_p}(A[\mathfrak{p}](\overline{\mathbf{Q}}))$  irreducible und
- ▶  $\mathfrak{p} \nmid 2 \cdot c \cdot \text{gcd}_K(I_K)$  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 $\text{III}(A/\mathbf{Q})$

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

One has  $\text{III}(A/\mathbf{Q})[\mathfrak{p}] = 0$  for all  $\mathfrak{p}$  with

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

These  $\mathfrak{p}$  are explicitly **computable**.

# Computation of $\text{III}(A/\mathbb{Q})[p^\infty]$ for given $p$

Two tools:

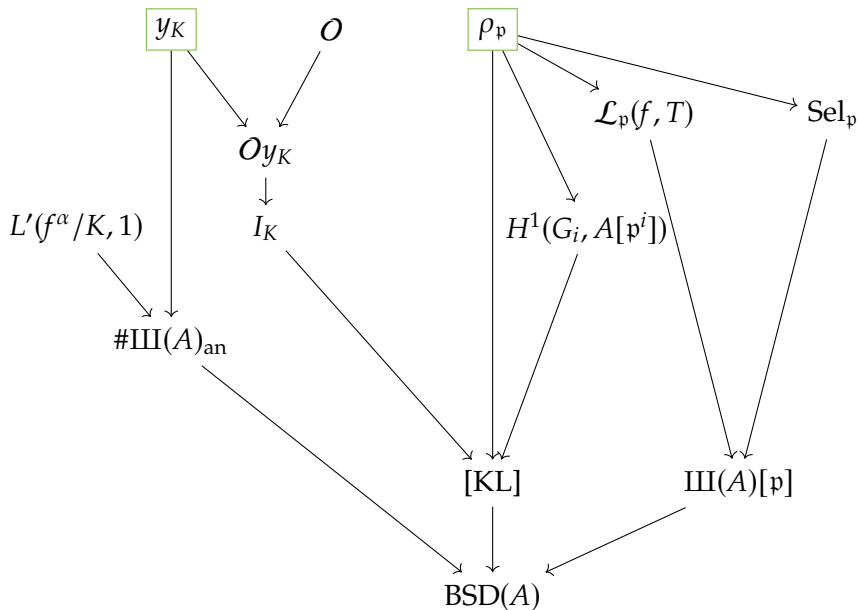
- ▶ Perform a  $p^n$ -descent to compute  $\text{Sel}_{p^n}(A/\mathbb{Q})$ .
  - Works very well if  $\rho_{p^n}$  is reducible.
  - Works for general  $p^n$  in principle, but:
  - Infeasible if  $\rho_{p^n}$  has large image, e.g.,  $\#O/p^n > 7$  and  $\rho_{p^n}$  irreducible, even assuming GRH.
- ▶ Compute the  $p$ -adic  $L$ -function and use the  $\text{GL}_2$  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  $r_{\text{an}} > 0$  or if the reduction is split multiplicative.  
(work in progress by KAYA–MÜLLER–VAN DER PUT)

# Computation of $\text{III}(A/\mathbb{Q})[p^\infty]$ for given $p$

Two tools:

- ▶ Perform a  $p^n$ -descent to compute  $\text{Sel}_{p^n}(A/\mathbb{Q})$ .
  - 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  $\text{GL}_2$  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  $r_{\text{an}} > 0$  or if the reduction is split multiplicative.  
(work in progress by KAYA–MÜLLER–VAN DER PUT)

# Structure and dependencies of the project



Computing the image of  $\rho_p$



# Definitions: residual Galois representations

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

# Definitions: residual Galois representations

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

# Excursion: Group theory of finite groups of Lie type

## Maximal subgroups of $\mathrm{PSL}_2(p)$

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

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

# Irreducibility for almost all $p$

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

If  $\rho_p$  is reducible,  $\rho_p^{\text{ss}} \cong \varepsilon \oplus \varepsilon^{-1} \chi_p$  with  $\varepsilon$  of conductor  $d$  with  $d^2 \mid N$ ,  
or  $\rho_p^{\text{ss}} \cong \varepsilon \chi_p^n \oplus \varepsilon^{-1} \chi_p^{1-n}$  if  $p^2 \mid N$ .

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

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

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

# Irreducibility for almost all $p$

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

If  $\rho_p$  is reducible,  $\rho_p^{\text{ss}} \cong \varepsilon \oplus \varepsilon^{-1} \chi_p$  with  $\varepsilon$  of conductor  $d$  with  $d^2 \mid N$ ,  
or  $\rho_p^{\text{ss}} \cong \varepsilon \chi_p^n \oplus \varepsilon^{-1} \chi_p^{1-n}$  if  $p^2 \mid N$ .

- ▶ Hence:  $\rho_p$  is **irreducible** as an  $\mathbf{F}_p$ -representation for all  $p \mid p$  if

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

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  $\rho_p$  **reducible** for all  $p \mid p$ .

# Irreducibility for almost all $p$

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

If  $\rho_p$  is reducible,  $\rho_p^{\text{ss}} \cong \varepsilon \oplus \varepsilon^{-1} \chi_p$  with  $\varepsilon$  of conductor  $d$  with  $d^2 \mid N$ ,  
or  $\rho_p^{\text{ss}} \cong \varepsilon \chi_p^n \oplus \varepsilon^{-1} \chi_p^{1-n}$  if  $p^2 \mid N$ .

- ▶ Hence:  $\rho_p$  is **irreducible** as an  $\mathbf{F}_p$ -representation for all  $p \mid p$  if

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

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  $\rho_p$  **reducible** for all  $p \mid p$ .
- ▶ Can be refined to  $p \ll O$ .

# Irreducibility for almost all $p$

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

If  $\rho_p$  is reducible,  $\rho_p^{\text{ss}} \cong \varepsilon \oplus \varepsilon^{-1} \chi_p$  with  $\varepsilon$  of conductor  $d$  with  $d^2 \mid N$ ,  
or  $\rho_p^{\text{ss}} \cong \varepsilon \chi_p^n \oplus \varepsilon^{-1} \chi_p^{1-n}$  if  $p^2 \mid N$ .

- ▶ Hence:  $\rho_p$  is **irreducible** as an  $\mathbf{F}_p$ -representation for all  $p \mid p$  if

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

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  $\rho_p$  **reducible** for all  $p \mid p$ .
- ▶ Can be refined to  $p \ll \mathcal{O}$ .

## Maximal image for almost all $p$

- ▶ If  $\rho_p$  is irreducible as an  $\mathbf{F}_p$ -representation, but **reducible as an  $\mathbf{F}_p$ -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  $p > C(N, \deg \rho)$ , then the image of  $\rho_p$  is not contained in the **normalizer of a Cartan subgroup**.



Computing the Heegner index  $I_K$

# Basic principle

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.)

# The Gross–Zagier formula

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  $\pi : J_0(N) \rightarrow A_f$  with Manin constant  $c_\pi$  and Heegner point  $y_K \in A_f(K)$ ,

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

# The Gross–Zagier formula

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  $\pi : J_0(N) \rightarrow A_f$  with Manin constant  $c_\pi$  and Heegner point  $y_K \in A_f(K)$ ,

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

# 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  $\pi : A_f \rightarrow J := \text{Jac}(X)$  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  $\pi : \mathbf{C}^2/\Lambda_f \rightarrow J(\mathbf{C})$  ( $X$  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  $\text{Ann}_O(J(K)/O\pi(y_K))$  can be a multiple of  $I_K := \text{Ann}_O(A_f(K) : O y_K)$  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  $\pi : A_f \rightarrow J := \text{Jac}(X)$  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  $\pi : \mathbf{C}^2/\Lambda_f \rightarrow J(\mathbf{C})$  ( $X$  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  $\text{Ann}_O(J(K)/O\pi(y_K))$  can be a multiple of  $I_K := \text{Ann}_O(A_f(K) : O y_K)$  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  $y \in J(\mathbf{C})$  is dense!
- ▶ **Idea:** Use the Northcott property of heights  $\hat{h}_{\mathcal{L}} : J(K) \rightarrow \mathbf{R}_{\geq 0}$  and assume that  $\hat{h}_{2\mathfrak{g}}$  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  $y \in J(\mathbf{C})$  is dense!
- ▶ Idea: Use the Northcott property of heights  $\hat{h}_{\mathcal{L}} : J(K) \rightarrow \mathbf{R}_{\geq 0}$  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  $y_K \in A_f(K)$ .



## Proving the correctness of $O\pi(y_K)$

- ▶ 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  $\hat{h}_{\mathcal{L}} : J(K) \rightarrow \mathbf{R}_{\geq 0}$  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

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

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

## Proving the correctness of $O\pi(y_K)$

- ▶ 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  $\hat{h}_{\mathcal{L}} : J(K) \rightarrow \mathbf{R}_{\geq 0}$  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

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

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

# Computing $\text{III}(A/\mathbf{Q})_{\text{an}}$ exactly

- ▶ Compute  $\frac{L(f,1)}{\Omega_f^+} \in \mathbf{Q}(f)$  exactly  
using modular symbols and BALAKRISHNAN–MÜLLER–STEIN  
and VAN BOMMEL'S code to compute  $\Omega_A$ .
- ▶ If  $L(A, 1) \neq 0$ , this gives  $\#\text{III}(A/\mathbf{Q})_{\text{an}} \in \mathbf{Q}_{>0}$  exactly.
- ▶ If  $L(A, 1) = 0, \dots$ 
  - choose a Heegner field  $K$  and compute  $\frac{L(f_K,1)}{\text{Reg}_{A/K} \Omega_{A/K}} \in \mathbf{Q}_{>0}$  exactly  
using Gross–Zagier, and hence compute  $\#\text{III}(A/K)_{\text{an}} \in \mathbf{Q}_{>0}$ .
  - Compute  $\#\text{III}(A^K/\mathbf{Q})_{\text{an}} \in \mathbf{Q}_{>0}$  exactly.
  - Use  $\#\text{III}(A/K)_{\text{an}} = \#\text{III}(A/\mathbf{Q})_{\text{an}} \cdot \#\text{III}(A^K/\mathbf{Q})_{\text{an}}$  up to powers of 2 that  
can be explicitly bounded to compute  $\#\text{III}(A/\mathbf{Q})_{\text{an}} \in \mathbf{Q}_{>0}$  exactly.

# Computing $\text{III}(A/\mathbf{Q})_{\text{an}}$ exactly

- ▶ Compute  $\frac{L(f,1)}{\Omega_f^+} \in \mathbf{Q}(f)$  exactly  
using modular symbols and BALAKRISHNAN–MÜLLER–STEIN  
and VAN BOMMEL'S code to compute  $\Omega_A$ .
- ▶ If  $L(A, 1) \neq 0$ , this gives  $\#\text{III}(A/\mathbf{Q})_{\text{an}} \in \mathbf{Q}_{>0}$  exactly.
- ▶ If  $L(A, 1) = 0, \dots$ 
  - choose a Heegner field  $K$  and compute  $\frac{L(f_K,1)}{\text{Reg}_{A/K} \Omega_{A/K}} \in \mathbf{Q}_{>0}$  exactly  
using Gross–Zagier, and hence compute  $\#\text{III}(A/K)_{\text{an}} \in \mathbf{Q}_{>0}$ .
  - Compute  $\#\text{III}(A^K/\mathbf{Q})_{\text{an}} \in \mathbf{Q}_{>0}$  exactly.
  - Use  $\#\text{III}(A/K)_{\text{an}} = \#\text{III}(A/\mathbf{Q})_{\text{an}} \cdot \#\text{III}(A^K/\mathbf{Q})_{\text{an}}$  up to powers of 2 that  
can be explicitly bounded to compute  $\#\text{III}(A/\mathbf{Q})_{\text{an}} \in \mathbf{Q}_{>0}$  exactly.

Examples

## Example: $A = \text{Jac}(X_0(39)/w_{13})$

- ▶  $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$
- ▶  $r = r_{\text{an}} = 0$
- ▶  $\#\text{III}(A/\mathbf{Q})_{\text{an}} = 1$
- ▶  $A(\mathbf{Q}) = A(\mathbf{Q})_{\text{tors}} \cong \mathbf{Z}/2 \times \mathbf{Z}/(2 \cdot 7)$
- ▶  $\rho_{\mathfrak{p}}$  is reducible exactly for  $\mathfrak{p} = (\sqrt{2})$  and exactly one  $\mathfrak{p}\bar{\mathfrak{p}} = 7$ .
- ▶  $c = 7$

## Example: $A = \text{Jac}(X_0(39)/w_{13})$

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

## Example: $A = \text{Jac}(X_0(39)/w_{13})$

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



## Example: $A = \text{Jac}(X_0(39)/w_{13})$

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

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

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

## Example: $A = \text{Jac}(X_0(39)/w_{13})$

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

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

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

- ▶ The  $\bar{p}$ -adic  $L$ -function has constant term a unit in  $\mathcal{O}_{\bar{p}} \simeq \mathbf{Z}_7$ , hence the integral  $\text{GL}_2$  IMC shows  $\text{Sel}_{\bar{p}}(A/\mathbf{Q}) = 0$  since  $\rho_{\bar{p}}$  is irreducible.

## Example: $A = \text{Jac}(X_0(39)/w_{13})$

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

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

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

- ▶ The  $\bar{p}$ -adic  $L$ -function has constant term a unit in  $\mathcal{O}_{\bar{p}} \simeq \mathbf{Z}_7$ , hence the integral  $\text{GL}_2$  IMC shows  $\text{Sel}_{\bar{p}}(A/\mathbf{Q}) = 0$  since  $\rho_{\bar{p}}$  is irreducible.

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

$X$	$r$	$O$	$\#\text{III}_{\text{an}}$	$\rho_p$ red.	$c$	$(D, I_D)$	$\#\text{III}$
$X_0(23)$	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)

$X$	$r$	$O$	#III <sub>an</sub>	$\rho_p$ red.	$c$	$(D, I_D)$	#III
$X_0(133)^*$	2	$\sqrt{5}$	1		1	$(-31, 1)$	1
$X_0(147)^*$	2	$\sqrt{2}$	1	$\sqrt{2}, 7_1$	1	$(-47, 1)$	$7^0$
$X_0(161)^*$	2	$\sqrt{5}$	1		1	$(-19, 1)$	1
$X_0(165)^*$	2	$\sqrt{2}$	1	$\sqrt{2}$	1	$(-131, 1)$	1
$X_0(167)^+$	2	$\sqrt{5}$	1		1	$(-15, 1)$	1
$X_0(177)^*$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(191)^+$	2	$\sqrt{5}$	1		1	$(-7, 1)$	1
$X_0(205)^*$	2	$\sqrt{5}$	1		1	$(-31, 1)$	1
$X_0(209)^*$	2	$\sqrt{2}$	1		1	$(-51, 1)$	1
$X_0(213)^*$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(221)^*$	2	$\sqrt{5}$	1		1	$(-35, 1)$	1
$X_0(287)^*$	2	$\sqrt{5}$	1		1	$(-31, 1)$	1
$X_0(299)^*$	2	$\sqrt{5}$	1		1	$(-43, 1)$	1
$X_0(357)^*$	2	$\sqrt{2}$	1		1	$(-47, 1)$	1

Outlook

# Challenge

- ▶ Using SHNIDMAN–WEISS<sup>1</sup>, find examples of  $A/\mathbf{Q}$  with

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

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

- ▶ 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  $\text{III}(J/\mathbf{Q})[\mathfrak{p}] = 0$ ), and
  - $\rho_{\mathfrak{p}}$  irreducible ( $p$ -descent hard)!

---

<sup>1</sup>Elements of prime order in Tate-Shafarevich groups of abelian varieties over  $\mathbf{Q}$ ,  
arXiv:2106.14096

# 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.



# 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.

# 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!