Funded by
Deutsche Forschungsgemeinschaft
German Research Foundation

UNIVERSITÄT BAYREUTH

Verification of the strong BSD conjecture for abelian surfaces over $\mathbf{Q}$

see arXiv:2107.00325 and forthcoming articles

Timo Keller

joint with Michael Stoll

Universität Bayreuth

March 28, 2022

Outline

The BSD conjecture: state of the art

State of the art: some history

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

State of the art: some history

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

State of the art: some history

- 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.

State of the art: some history

- 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.

State of the art: some history

- 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.

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

$$r \geq r_{\mathrm{an}}, \qquad \#Ш(A/\mathbf{Q})_{\mathrm{an}} \qquad \in \mathbf{Q}_{>0},$$

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

$$r = r_{\mathrm{an}}, \qquad \#Ш(A/\mathbf{Q}) \qquad < \infty.$$

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

$$r \geq r_{\mathrm{an}}, \qquad \#Ш(A/\mathbf{Q})_{\mathrm{an}} \qquad \in \mathbf{Q}_{>0},$$

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

$$r = r_{\mathrm{an}}, \qquad \#Ш(A/\mathbf{Q}) \qquad < \infty.$$

- Unknown: $\#Ш(A/\mathbf{Q}) \stackrel{?}{=} \#Ш(A/\mathbf{Q})_{\mathrm{an}}$ (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 $\mathrm{ord}_{s=1} L(f, s)$ equals 0 or 1.
- This implies by the Gross–Zagier formula:

$$r \geq r_{\mathrm{an}}, \qquad \#Ш(A/\mathbf{Q})_{\mathrm{an}} \qquad \in \mathbf{Q}_{>0},$$

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

$$r = r_{\mathrm{an}}, \qquad \#Ш(A/\mathbf{Q}) \qquad < \infty.$$

- Unknown: $\#Ш(A/\mathbf{Q}) \stackrel{?}{=} \#Ш(A/\mathbf{Q})_{\mathrm{an}}$ (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–Tarniţă (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–Tarniţă (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 ρ_p irreducible.
  - Skinner (2016): GL_2 IMC for primes p of bad multiplicative reduction and ρ_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–Tarniţă (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 ρ_p irreducible.
  - Skinner (2016): GL_2 IMC for primes p of bad multiplicative reduction and ρ_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–Tarniţă (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 ρ_p irreducible.
  - Skinner (2016): GL_2 IMC for primes p of bad multiplicative reduction and ρ_p irreducible.
  - van Bommel (2019): BSD for some hyperelliptic Jacobians numerically up to squares.
  - Castella–Çiperiani–Skinner–Sprung (2019, preprint): $v_p(\#Ш(A/\mathbf{Q})) = v_p(\#Ш(A/\mathbf{Q})_{\mathrm{an}})$ if N is square-free, $p \nmid N$, and ρ_p irreducible.

Previous work on the verification

- For elliptic curves:
  - 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).
- 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 ρ_p irreducible.
  - Skinner (2016): GL_2 IMC for primes p of bad multiplicative reduction and ρ_p irreducible.
  - van Bommel (2019): BSD for some hyperelliptic Jacobians numerically up to squares.
  - Castella–Çiperiani–Skinner–Sprung (2019, preprint): $v_p(\#Ш(A/\mathbf{Q})) = v_p(\#Ш(A/\mathbf{Q})_{\mathrm{an}})$ if N is square-free, $p \nmid N$, and ρ_p irreducible.

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

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

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

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 $f \in S_2(\Gamma_0(N), \mathcal{O})$.

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

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

If this is the case, we call $A/\mathbf{Q}$ modular,
and then $N^{\dim A}$ is the conductor of $A/\mathbf{Q}$, $\mathcal{O} \cong \mathrm{End}_{\mathbf{Q}}(A)$,
and A is of GL_2-type over $\mathbf{Q}$: $\dim_{\mathrm{End}(A)\otimes\mathbf{Q}_\ell} V_\ell A = 2$.

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 $f \in S_2(\Gamma_0(N), \mathcal{O})$.

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

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

If this is the case, we call $A/\mathbf{Q}$ modular,
and then $N^{\dim A}$ is the conductor of $A/\mathbf{Q}$, $\mathcal{O} \cong \mathrm{End}_{\mathbf{Q}}(A)$,
and A is of GL_2-type over $\mathbf{Q}$: $\dim_{\mathrm{End}(A)\otimes\mathbf{Q}_\ell} V_\ell A = 2$.

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 $\rho_{\mathfrak{p}^\infty} : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{GL}_2(\mathcal{O}_\mathfrak{p})$.

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 $\rho_{\mathfrak{p}^\infty} : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$.

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

- . . . explicitly prove that almost all $\rho_{\mathfrak{p}}$ 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 $\rho_{\mathfrak{p}^\infty} : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$.

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

- . . . explicitly prove that almost all $\rho_{\mathfrak{p}}$ are irreducible and maximal,
- . . . compute the Heegner index $I_K = [A(K) : \mathcal{O}y_K]$,
- and use this to compute $\#Ш(A/\mathbf{Q}) \in \mathbf{Z}_{\geq 1}$ and $\#Ш(A/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ 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 $\rho_{\mathfrak{p}^\infty} : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$.

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

- . . . explicitly prove that almost all $\rho_{\mathfrak{p}}$ are irreducible and maximal,
- . . . compute the Heegner index $I_K = [A(K) : \mathcal{O}y_K]$,
- and use this to compute $\#Ш(A/\mathbf{Q}) \in \mathbf{Z}_{\geq 1}$ and $\#Ш(A/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ exactly.

An explicit Euler system

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

Let A be a modular abelian variety over $\mathbf{Q}$.
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 und
- $\mathfrak{p} \nmid 2 \cdot c \cdot \gcd_K(I_K)$ with Heegner indices I_K and the Tamagawa product c (both can be refined to $\mathcal{O}$-ideals).

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

An explicit Euler system

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

Let A be a modular abelian variety over $\mathbf{Q}$.
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 und
- $\mathfrak{p} \nmid 2 \cdot c \cdot \gcd_K(I_K)$ with Heegner indices I_K and the Tamagawa product c (both can be refined to $\mathcal{O}$-ideals).

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

Computation of $Ш(A/\mathbf{Q})[\mathfrak{p}^\infty]$ for given $\mathfrak{p}$

Two methods:

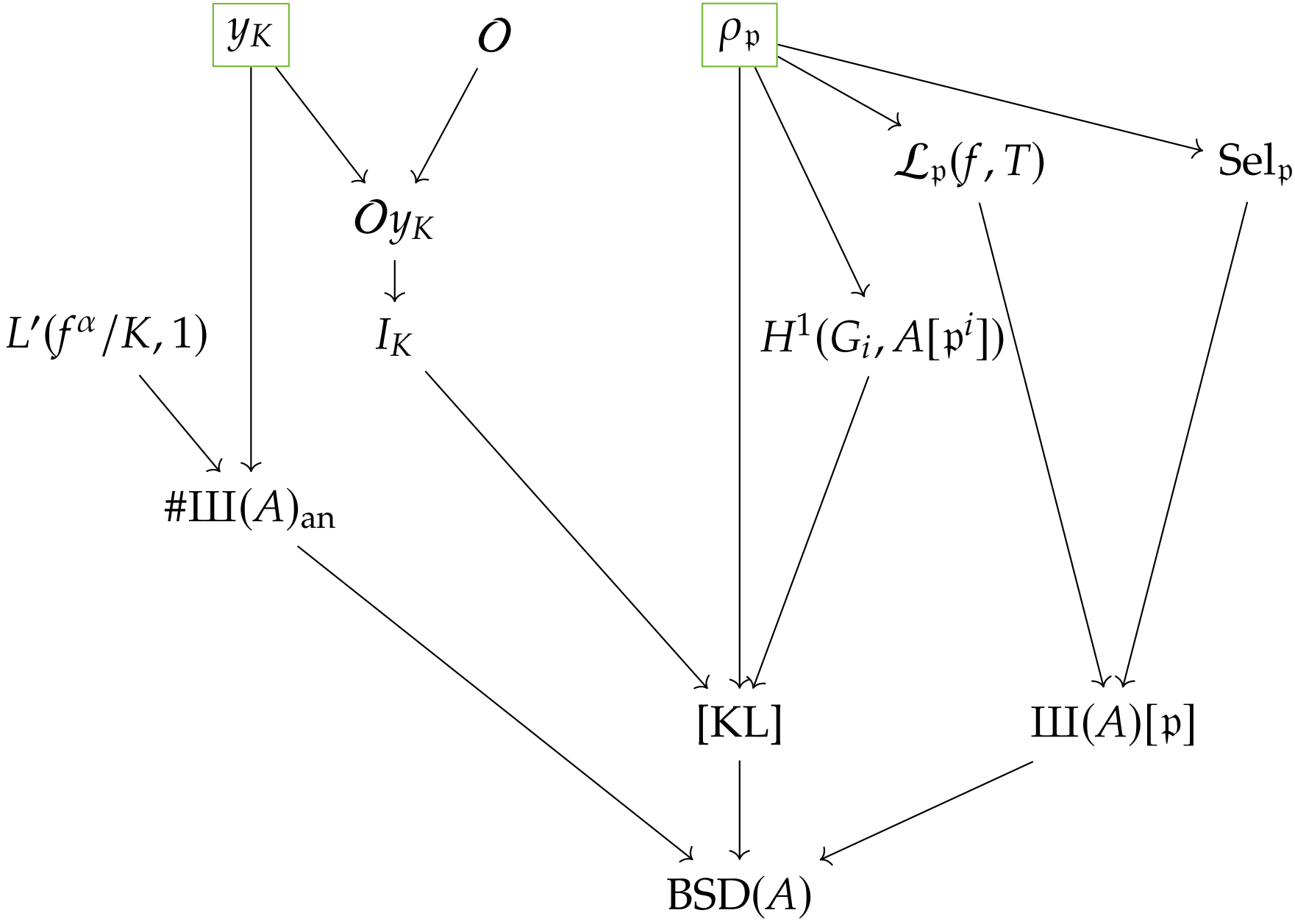
- Perform a $\mathfrak{p}^n$-descent to compute $\mathrm{Sel}_{\mathfrak{p}^n}(A/\mathbf{Q})$.
  - Works very well if $\rho_{\mathfrak{p}^n}$ is reducible.
  - Works for general $\mathfrak{p}^n$ in principle, but:
  - Infeasible if $\rho_{\mathfrak{p}^n}$ has large image,
    e.g., $\#\mathcal{O}/\mathfrak{p}^n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

Computation of $Ш(A/\mathbf{Q})[\mathfrak{p}^\infty]$ for given $\mathfrak{p}$

Two methods:

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

Structure and dependencies of the project



Computing the image of $\rho_{\mathfrak{p}}$

Excursion: Group theory of finite groups of Lie type

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

Assume $\mathfrak{p} \nmid 2$. Every subgroup of
$\mathrm{PSL}_2(\mathfrak{p}) := \mathbf{ker}\left(\overline{\det} : \mathrm{PGL}_2(\mathbf{F}_\mathfrak{p}) \twoheadrightarrow \mathbf{F}_\mathfrak{p}^\times/2\right)$ 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)

Irreducibility for almost all $\mathfrak{p}$

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

  If $\rho_{\mathfrak{p}}$ is reducible, $\rho_{\mathfrak{p}}^{ss} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with ε of conductor d with $d^2 \mid N$, or $\rho_{\mathfrak{p}}^{ss} \cong \varepsilon\chi_p^n \oplus \varepsilon^{-1}\chi_p^{1-n}$ 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

  the eigenvalues of $\rho_p(\mathrm{Frob}_\ell)$ have 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 $p^2 \mid N$.

Irreducibility for almost all $\mathfrak{p}$

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

  If $\rho_{\mathfrak{p}}$ is reducible, $\rho^{\mathrm{ss}}_{\mathfrak{p}} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with ε of conductor d with $d^2 \mid N$,
  or $\rho^{\mathrm{ss}}_{\mathfrak{p}} \cong \varepsilon\chi_p^n \oplus \varepsilon^{-1}\chi_p^{1-n}$ 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

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

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

Irreducibility for almost all $\mathfrak{p}$

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

  If $\rho_{\mathfrak{p}}$ is reducible, $\rho^{\mathrm{ss}}_{\mathfrak{p}} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with ε of conductor d with $d^2 \mid N$, or $\rho^{\mathrm{ss}}_{\mathfrak{p}} \cong \varepsilon\chi_p^n \oplus \varepsilon^{-1}\chi_p^{1-n}$ 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 $p^2 \mid N$.

Irreducibility for almost all $\mathfrak{p}$

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

  If $\rho_{\mathfrak{p}}$ is reducible, $\rho^{\mathrm{ss}}_{\mathfrak{p}} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with ε of conductor d with $d^2 \mid N$, or $\rho^{\mathrm{ss}}_{\mathfrak{p}} \cong \varepsilon\chi_p^n \oplus \varepsilon^{-1}\chi_p^{1-n}$ 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

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

  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 $\mathfrak{p}$

- 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 ε 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

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

  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 $\rho_{\mathfrak{p}}$ reducible for all $\mathfrak{p} \mid p$.

Irreducibility for almost all $\mathfrak{p}$

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

  If $\rho_{\mathfrak{p}}$ is reducible, $\rho^{\mathrm{ss}}_{\mathfrak{p}} \cong \varepsilon \oplus \varepsilon^{-1}\chi_p$ with ε of conductor d with $d^2 \mid N$, or $\rho^{\mathrm{ss}}_{\mathfrak{p}} \cong \varepsilon\chi_p^n \oplus \varepsilon^{-1}\chi_p^{1-n}$ 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

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

  for $d = d_{\max}$ maximal such that $d^2_{\max} \mid N$, 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 $\mathfrak{p} \triangleleft \mathcal{O}$.

Maximal image for almost all p

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

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

- If $p > 5$, then $\rho_{\mathfrak{p}}$ 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.

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 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 $\mathcal{O}_K/\mathfrak{n} \cong \mathbf{Z}/N$,
- $\operatorname{ord}_{s=1} L(f/K, s) = 1$.

(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_π and Heegner point $y_K \in A_f(K)$,

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

The Gross–Zagier formula

Let K 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 $\mathcal{O}_K/\mathfrak{n} \cong \mathbf{Z}/N$,
- $\operatorname{ord}_{s=1} L(f/K, s) = 1$.

(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_π and Heegner point $y_K \in A_f(K)$,

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

Computing 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, disc_K).
- Compute the zeros τ 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 τ 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 $[J(K) : \pi(A_f(K))] > 1$.

Computing 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, disc_K).
- Compute the zeros τ 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 τ 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 $[J(K) : \pi(A_f(K))] > 1$.

Proving the correctness of $\mathcal{O}\pi(y_K)$

- 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 $\hat{h}_{\mathscr{L}} : J(K) \to \mathbf{R}_{\geq 0}$ and assume that $\hat{h}_{2\vartheta}$ is injective on $J(K)$ up to sign and torsion.

Proving the correctness of $\mathcal{O}\pi(y_K)$

- 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 $\hat{h}_{\mathscr{L}} : J(K) \to \mathbf{R}_{\geq 0}$ and assume that $\hat{h}_{2\vartheta}$ is injective on $J(K)$ up to sign and torsion.
- Compute the kernel of the polarization

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

- Use the Gross–Zagier formula to compute $\hat{h}_\iota(y_K)$ with $y_K \in A_f(K)$.

Proving the correctness of $\mathcal{O}\pi(y_K)$

- 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 $\hat{h}_{\mathscr{L}} : J(K) \to \mathbf{R}_{\geq 0}$ and assume that $\hat{h}_{2\vartheta}$ is injective on $J(K)$ up to sign and torsion.
- Compute the kernel of the polarization

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

- Use the Gross–Zagier formula to compute $\hat{h}_\iota(y_K)$ with $y_K \in A_f(K)$.
- Compute the kernel 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. 2ϑ.
- 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 $\deg(\pi)$.

Proving the correctness of $\mathcal{O}\pi(y_K)$

- 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 $\hat{h}_{\mathscr{L}} : J(K) \to \mathbf{R}_{\geq 0}$ and assume that $\hat{h}_{2\vartheta}$ is injective on $J(K)$ up to sign and torsion.
- Compute the kernel of the polarization

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

- Use the Gross–Zagier formula to compute $\hat{h}_\iota(y_K)$ with $y_K \in A_f(K)$.
- Compute the kernel 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. 2ϑ.
- 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 $\deg(\pi)$.

Computing $Ш(A/\mathbf{Q})_{\mathrm{an}}$ exactly

- Compute $\frac{L(f,1)}{\Omega_f^+} \in \mathbf{Q}(f)$ exactly
  using modular symbols and Balakrishnan–Müller–Stein and van Bommel's code to compute Ω_A.
- If $L(A,1) \neq 0$, this gives $\#Ш(A/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ exactly.
- If $L(A,1) = 0, \ldots$
  - 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.

Computing $Ш(A/\mathbf{Q})_{\mathrm{an}}$ exactly

- Compute $\frac{L(f,1)}{\Omega_f^+} \in \mathbf{Q}(f)$ exactly
  using modular symbols and Balakrishnan–Müller–Stein and van Bommel's code to compute Ω_A.
- If $L(A,1) \neq 0$, this gives $\#Ш(A/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ exactly.
- If $L(A,1) = 0, \ldots$
  - 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.

Examples

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

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 $Ш(A/\mathbf{Q})[2] = 0$.

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 $\mathfrak{p} \nmid (\sqrt{2}), 7$.

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 $Ш(A/\mathbf{Q})[\mathfrak{p}] = 0$.

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 GL_2 IMC shows $\mathrm{Sel}_{\bar{\mathfrak{p}}}(A/\mathbf{Q}) = 0$ since $\rho_{\bar{\mathfrak{p}}}$ is irreducible.

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 GL_2 IMC shows $\mathrm{Sel}_{\bar{\mathfrak{p}}}(A/\mathbf{Q}) = 0$ since $\rho_{\bar{\mathfrak{p}}}$ is irreducible.

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

X	r	$\mathcal{O}$	$\#Ш_{an}$	$\rho_{\mathfrak{p}}$ red.	c	(D, I_D)	$\#Ш$
$X_0(23)$	0	$\sqrt{5}$	1	11_1	11	$(-7, 11)$	11^0
$X_0(29)$	0	$\sqrt{2}$	1	7_1	7	$(-7, 7)$	7^0
$X_0(31)$	0	$\sqrt{5}$	1	$\sqrt{5}$	5	$(-11, 5)$	5^0
$X_0(35)/w_7$	0	$\sqrt{17}$	1	2_1	1	$(-19, 1)$	1
$X_0(39)/w_{13}$	0	$\sqrt{2}$	1	$\sqrt{2}, 7_1$	7	$(-23, 7)$	7^0
$X_0(67)^+$	2	$\sqrt{5}$	1		1	$(-7, 1)$	1
$X_0(73)^+$	2	$\sqrt{5}$	1		1	$(-19, 1)$	1
$X_0(85)^*$	2	$\sqrt{2}$	1	$\sqrt{2}$	1	$(-19, 1)$	1
$X_0(87)/w_{29}$	0	$\sqrt{5}$	1	$\sqrt{5}$	5	$(-23, 5)$	5^0
$X_0(93)^*$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(103)^+$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(107)^+$	2	$\sqrt{5}$	1		1	$(-7, 1)$	1
$X_0(115)^*$	2	$\sqrt{5}$	1		1	$(-11, 1)$	1
$X_0(125)^+$	2	$\sqrt{5}$	1	$\sqrt{5}$	1	$(-11, 1)$	5^0

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

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

Outlook

Challenge

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

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

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

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

Outlook

Future work

- Almost done: Verification for all 97 genus 2 curves with absolutely simple modular Jacobian from the LMFDB.
- Verification for (almost?) all 1195 newforms of level ≤ 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 1195 newforms of level ≤ 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 1195 newforms of level ≤ 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!