Quadratic Chabauty and L-functions

Samuel Le Fourn (joint work with Samir Siksek)
ENS de Lyon

May 24, 2018

Plan of the talk

Motivation: rational points on modular curves

- Finding rational points on curves
- Images of Galois representations associated to elliptic curves
- Chabauty method in the context of modular curves

The new input of "quadratic Chabauty"

- What is the "quadratic Chabauty" method ?
- Applying the method to families of modular curves

Nonvanishing of derivatives of modular L-functions

- Notations for modular L-functions
- Weighted sums: exact expression and asymptotic values
- Improving the estimates to get a computable range

Hypotheses and notations

- A *curve* C is a smooth, projective, geometrically integral algebraic curve over $\mathbb{Q}$, of genus g and Jacobian J.

Hypotheses and notations

- A *curve* C is a smooth, projective, geometrically integral algebraic curve over $\mathbb{Q}$, of genus g and Jacobian J.
- For $O \in C(\mathbb{Q})$ fixed, $\iota : C \to J$ is the Albanese morphism sending O to 0.

Hypotheses and notations

- A *curve* C is a smooth, projective, geometrically integral algebraic curve over $\mathbb{Q}$, of genus g and Jacobian J.
- For $O \in C(\mathbb{Q})$ fixed, $\iota : C \to J$ is the Albanese morphism sending O to 0.
- We assume $g \geq 2$ so that $C(\mathbb{Q})$ is *finite* by Faltings theorem.

Determining rational points on curves

Determining rational points on curves

Problem

Faltings theorem and does not say how to figure out $C(\mathbb{Q})$ explicitly.

Determining rational points on curves

Problem

Faltings theorem and does not say how to figure out $C(\mathbb{Q})$ explicitly.

Chabauty's idea

Consider, for a prime p, the following commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \overset{\iota}{\hookrightarrow} & J(\mathbb{Q}) \\ \downarrow & & \downarrow \\ C(\mathbb{Q}_p) & \overset{\iota}{\hookrightarrow} & J(\mathbb{Q}_p) \end{array}$$

In the p-adic variety $J(\mathbb{Q}_p)$,

$$C(\mathbb{Q}) \subset C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}.$$

If $\operatorname{codim} \overline{J(\mathbb{Q})} \geq 1$, this should enable to prove finiteness !

Chabauty theorem...

Chabauty theorem...

By p-adic Lie group theory, there is a logarithm

$$\log : J(\mathbb{Q}_p) \to T_0 J_{\mathbb{Q}_p} \cong \mathbb{Q}_p^g$$

with image isomorphic to $\mathbb{Z}_p^g$.

Chabauty theorem...

By p-adic Lie group theory, there is a logarithm

$$\log : J(\mathbb{Q}_p) \to T_0 J_{\mathbb{Q}_p} \cong \mathbb{Q}_p^g$$

with image isomorphic to $\mathbb{Z}_p^g$. Then,

$$\log \overline{J(\mathbb{Q})} \subset \overline{\log J(\mathbb{Q})} \subset \mathbb{Z}_p \log J(\mathbb{Q}),$$

Chabauty theorem...

By p-adic Lie group theory, there is a logarithm

$$\log : J(\mathbb{Q}_p) \to T_0 J_{\mathbb{Q}_p} \cong \mathbb{Q}_p^g$$

with image isomorphic to $\mathbb{Z}_p^g$. Then,

$$\log \overline{J(\mathbb{Q})} \subset \overline{\log J(\mathbb{Q})} \subset \mathbb{Z}_p \log J(\mathbb{Q}),$$

in particular it is included in a hyperplane of $T_0 J_{\mathbb{Q}_p}$ if

$$r = \operatorname{rank} J(\mathbb{Q}) < g.$$

Chabauty theorem...

By p-adic Lie group theory, there is a logarithm

$$\log : J(\mathbb{Q}_p) \to T_0 J_{\mathbb{Q}_p} \cong \mathbb{Q}_p^g$$

with image isomorphic to $\mathbb{Z}_p^g$. Then,

$$\log \overline{J(\mathbb{Q})} \subset \overline{\log J(\mathbb{Q})} \subset \mathbb{Z}_p \log J(\mathbb{Q}),$$

in particular it is included in a hyperplane of $T_0 J_{\mathbb{Q}_p}$ if

$$r = \operatorname{rank} J(\mathbb{Q}) < g.$$

Proposition (Chabauty)

For any nonempty open subset $U \subset C(\mathbb{Q}_p)$, $\operatorname{Vect}_{\mathbb{Q}_p} \log(\iota(U)) = T_0 J_{\mathbb{Q}_p}$.

Chabauty theorem...

By p-adic Lie group theory, there is a logarithm

$$\log : J(\mathbb{Q}_p) \to T_0 J_{\mathbb{Q}_p} \cong \mathbb{Q}_p^g$$

with image isomorphic to $\mathbb{Z}_p^g$. Then,

$$\log \overline{J(\mathbb{Q})} \subset \overline{\log J(\mathbb{Q})} \subset \mathbb{Z}_p \log J(\mathbb{Q}),$$

in particular it is included in a hyperplane of $T_0 J_{\mathbb{Q}_p}$ if

$$r = \operatorname{rank} J(\mathbb{Q}) < g.$$

Proposition (Chabauty)

For any nonempty open subset $U \subset C(\mathbb{Q}_p)$, $\mathrm{Vect}_{\mathbb{Q}_p} \log(\iota(U)) = T_0 J_{\mathbb{Q}_p}$.

Theorem (Chabauty)

If $r < g$ (Chabauty condition), then $C(\mathbb{Q})$ is finite.

...made more effective by Coleman...

...made more effective by Coleman...

Recall the canonical identifications and pairing

$$(T_0 J_{\mathbb{Q}_p})^* \cong H^0(J_{\mathbb{Q}_p}, \Omega^1) \cong H^0(C_{\mathbb{Q}_p}, \Omega^1), \quad \langle \cdot, \cdot \rangle : T_0 J_{\mathbb{Q}_p} \times (T_0 J_{\mathbb{Q}_p})^*. \to \mathbb{Q}_p$$

...made more effective by Coleman...

Recall the canonical identifications and pairing

$$(T_0 J_{\mathbb{Q}_p})^* \cong H^0(J_{\mathbb{Q}_p}, \Omega^1) \cong H^0(C_{\mathbb{Q}_p}, \Omega^1), \quad \langle \cdot, \cdot \rangle : T_0 J_{\mathbb{Q}_p} \times (T_0 J_{\mathbb{Q}_p})^*. \to \mathbb{Q}_p$$

Definition (p-adic integration)

There is an analytic integration pairing

$$\begin{array}{ccc} J(\mathbb{Q}_p) \times H^0(C_{\mathbb{Q}_p}, \Omega^1) & \longrightarrow & \mathbb{Q}_p \\ (D, \omega) & \longmapsto & \int_D \omega := \langle \log D, \omega \rangle \end{array} .$$

...made more effective by Coleman...

Recall the canonical identifications and pairing

$$(T_0 J_{\mathbb{Q}_p})^* \cong H^0(J_{\mathbb{Q}_p}, \Omega^1) \cong H^0(C_{\mathbb{Q}_p}, \Omega^1), \quad \langle \cdot, \cdot \rangle : T_0 J_{\mathbb{Q}_p} \times (T_0 J_{\mathbb{Q}_p})^*. \to \mathbb{Q}_p$$

Definition (p-adic integration)

There is an analytic integration pairing

$$\begin{array}{ccc} J(\mathbb{Q}_p) \times H^0(C_{\mathbb{Q}_p}, \Omega^1) & \longrightarrow & \mathbb{Q}_p \\ (D, \omega) & \longmapsto & \int_D \omega := \langle \log D, \omega \rangle \end{array} .$$

If C has a good reduction $C_{\mathbb{F}_p}$ at p and z is a well-chosen parameter at O, for $\omega = (\sum_{n \geq 0} a_n z^n) dz$ and any P reducing to O modulo p,

$$\int_O^P \omega := \int_{\iota(P)} \omega = \sum_{n=0}^{+\infty} \frac{a_n}{n+1} z(P)^{n+1}.$$

...made more effective by Coleman...

Recall the canonical identifications and pairing

$$(T_0 J_{\mathbb{Q}_p})^* \cong H^0(J_{\mathbb{Q}_p}, \Omega^1) \cong H^0(C_{\mathbb{Q}_p}, \Omega^1), \quad \langle \cdot, \cdot \rangle : T_0 J_{\mathbb{Q}_p} \times (T_0 J_{\mathbb{Q}_p})^*. \to \mathbb{Q}_p$$

Definition (p-adic integration)

There is an analytic integration pairing

$$\begin{array}{ccc} J(\mathbb{Q}_p) \times H^0(C_{\mathbb{Q}_p}, \Omega^1) & \longrightarrow & \mathbb{Q}_p \\ (D, \omega) & \longmapsto & \int_D \omega := \langle \log D, \omega \rangle \end{array} .$$

If C has a good reduction $C_{\mathbb{F}_p}$ at p and z is a well-chosen parameter at O, for $\omega = (\sum_{n \geq 0} a_n z^n) dz$ and any P reducing to O modulo p,

$$\int_O^P \omega := \int_{\iota(P)} \omega = \sum_{n=0}^{+\infty} \frac{a_n}{n+1} z(P)^{n+1}.$$

Theorem (Coleman)

Under the Chabauty condition $r < g$, if $p > 2g$,

$$\# C(\mathbb{Q}) \leq \# C_{\mathbb{F}_p}(\mathbb{F}_p) + (2g - 2).$$

And its practical execution

And its practical execution

As long as the subset of $C(\mathbb{Q})$ one has found does not satisfy Coleman bound, one cannot say we have determined all $C(\mathbb{Q})$.

And its practical execution

As long as the subset of $C(\mathbb{Q})$ one has found does not satisfy Coleman bound, one cannot say we have determined all $C(\mathbb{Q})$.

The Mordell-Weil sieve

Assume for simplicity $J(\mathbb{Q}) = \mathbb{Z}D_1 \oplus \cdots \oplus \mathbb{Z}D_r$. For every good prime p, the commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \overset{\iota}{\hookrightarrow} & J(\mathbb{Q}) \\ \downarrow & & \downarrow \\ C(\mathbb{F}_p) & \overset{\iota}{\hookrightarrow} & J(\mathbb{F}_p) \end{array}$$

gives, through $W_p = \iota(C(\mathbb{F}_p))$, congruence conditions on the coordinates $(n_1, \cdots, n_r)$ of elements of $\iota(C(\mathbb{Q}))$ modulo N_p the exponent of $J(\mathbb{F}_p)$.

And its practical execution

As long as the subset of $C(\mathbb{Q})$ one has found does not satisfy Coleman bound, one cannot say we have determined all $C(\mathbb{Q})$.

The Mordell-Weil sieve

Assume for simplicity $J(\mathbb{Q}) = \mathbb{Z}D_1 \oplus \cdots \oplus \mathbb{Z}D_r$. For every good prime p, the commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \xhookrightarrow{\iota} & J(\mathbb{Q}) \\ \downarrow & & \downarrow \\ C(\mathbb{F}_p) & \xhookrightarrow{\iota} & J(\mathbb{F}_p) \end{array}$$

gives, through $W_p = \iota(C(\mathbb{F}_p))$, congruence conditions on the coordinates $(n_1, \cdots, n_r)$ of elements of $\iota(C(\mathbb{Q}))$ modulo N_p the exponent of $J(\mathbb{F}_p)$.

Hope for success of Mordell-Weil sieve + Chabauty

Find a finite set of primes S such that $C(\mathbb{Q}) \to \prod_{p \in S} C(\mathbb{F}_p)$ is injective (by Chabauty) and the only coordinates $(n_1, \cdots, n_r)$ satisfying congruences conditions modulo all N_p come from points of $C(\mathbb{Q})$ already known.

Galois representations associated to an elliptic curve

For an elliptic curve E over $\mathbb{Q}$ and a prime number p, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion $E[p]$ defines a *Galois representation*

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Galois representations associated to an elliptic curve

For an elliptic curve E over $\mathbb{Q}$ and a prime number p, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion $E[p]$ defines a *Galois representation*

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Main motivation: Serre's uniformity conjecture

Is there a constant $C > 0$ such that for every prime $p > C$ and every E over $\mathbb{Q}$ without CM, $\rho_{E,p}$ is *surjective* ?

Galois representations associated to an elliptic curve

For an elliptic curve E over $\mathbb{Q}$ and a prime number p, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion $E[p]$ defines a *Galois representation*

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Main motivation: Serre's uniformity conjecture

Is there a constant $C > 0$ such that for every prime $p > C$ and every E over $\mathbb{Q}$ without CM, $\rho_{E,p}$ is *surjective* ?

Splitting of the proof

Three types of maximal proper subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ to consider (each associated to some finite structure stabilised by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$):

Galois representations associated to an elliptic curve

For an elliptic curve E over $\mathbb{Q}$ and a prime number p, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion $E[p]$ defines a *Galois representation*

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Main motivation: Serre's uniformity conjecture

Is there a constant $C > 0$ such that for every prime $p > C$ and every E over $\mathbb{Q}$ without CM, $\rho_{E,p}$ is *surjective* ?

Splitting of the proof

Three types of maximal proper subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ to consider (each associated to some finite structure stabilised by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$):

- *Borel* (cyclic subgroup of order p).

Galois representations associated to an elliptic curve

For an elliptic curve E over $\mathbb{Q}$ and a prime number p, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion $E[p]$ defines a *Galois representation*

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Main motivation: Serre's uniformity conjecture

Is there a constant $C > 0$ such that for every prime $p > C$ and every E over $\mathbb{Q}$ without CM, $\rho_{E,p}$ is *surjective* ?

Splitting of the proof

Three types of maximal proper subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ to consider (each associated to some finite structure stabilised by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$):

- *Borel* (cyclic subgroup of order p).
- *Normaliser of split Cartan* (pair of distinct cyclic subgroups of order p).

Galois representations associated to an elliptic curve

For an elliptic curve E over $\mathbb{Q}$ and a prime number p, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion $E[p]$ defines a *Galois representation*

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Main motivation: Serre's uniformity conjecture

Is there a constant $C > 0$ such that for every prime $p > C$ and every E over $\mathbb{Q}$ without CM, $\rho_{E,p}$ is *surjective* ?

Splitting of the proof

Three types of maximal proper subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ to consider (each associated to some finite structure stabilised by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$):

- *Borel* (cyclic subgroup of order p).
- *Normaliser of split Cartan* (pair of distinct cyclic subgroups of order p).
- *Normaliser of nonsplit Cartan* (semi-linear action with respect to a $\mathbb{F}_{p^2}$-linear structure on $E[p]$).

The viewpoint of modular curves

The viewpoint of modular curves

Modular curves (vague definition)

Modular curves are curves who (except their cusps) parametrise isomorphism classes of elliptic curves E together with a finite structure on E.

The viewpoint of modular curves

Modular curves (vague definition)

Modular curves are curves who (except their cusps) parametrise isomorphism classes of elliptic curves E together with a finite structure on E.

Notations

Three families of modular curves: $X_0(p)$ for Borel, $X_{\mathrm{sp}}^+(p)$ (resp. $X_{\mathrm{nsp}}^+(p)$) for normaliser of split (resp. nonsplit Cartan).
Replacing X by J above will denote their respective jacobians.

The viewpoint of modular curves

Modular curves (vague definition)

Modular curves are curves who (except their cusps) parametrise isomorphism classes of elliptic curves E together with a finite structure on E.

Notations

Three families of modular curves: $X_0(p)$ for Borel, $X_{\mathrm{sp}}^+(p)$ (resp. $X_{\mathrm{nsp}}^+(p)$) for normaliser of split (resp. nonsplit Cartan).
Replacing X by J above will denote their respective jacobians.

Consequence of the algebraic interpretation of modular curves

If $\mathrm{Im}\,\rho_{E,p}$ is in the Borel case, E defines a noncuspidal rational point on $X_0(p)$, and similary for the other cases.

The viewpoint of modular curves

Modular curves (vague definition)

Modular curves are curves who (except their cusps) parametrise isomorphism classes of elliptic curves E together with a finite structure on E.

Notations

Three families of modular curves: $X_0(p)$ for Borel, $X_{\mathrm{sp}}^+(p)$ (resp. $X_{\mathrm{nsp}}^+(p)$) for normaliser of split (resp. nonsplit Cartan).
Replacing X by J above will denote their respective jacobians.

Consequence of the algebraic interpretation of modular curves

If $\mathrm{Im}\, \rho_{E,p}$ is in the Borel case, E defines a noncuspidal rational point on $X_0(p)$, and similary for the other cases.

Restatement of Serre's uniformity conjecture

For any prime $p > C$, the modular curves $X_0(p)$, $X_{\mathrm{sp}}^+(p)$ and $X_{\mathrm{nsp}}^+(p)$ have no noncuspidal non-CM rational points.

Chabauty method in the context of modular curves

Chabauty method in the context of modular curves

Fundamental remark

Chabauty's theorem (and Coleman's method) still hold under the weaker hypothesis

$$\operatorname{rank} A(\mathbb{Q}) < \dim A$$

for some quotient abelian variety A of J, in particular if $A(\mathbb{Q})$ is finite (i.e. A is a *rank zero quotient*).

Chabauty method in the context of modular curves

Fundamental remark

Chabauty's theorem (and Coleman's method) still hold under the weaker hypothesis

$$\operatorname{rank} A(\mathbb{Q}) < \dim A$$

for some quotient abelian variety A of J, in particular if $A(\mathbb{Q})$ is finite (i.e. A is a *rank zero quotient*).

Consequence

It is "enough" to find rank zero quotients of $J_0(p)$, $J_{\mathrm{sp}}^+(p)$ and $J_{\mathrm{nsp}}^+(p)$ to apply theoretically the method.

Chabauty method in the context of modular curves

Fundamental remark

Chabauty's theorem (and Coleman's method) still hold under the weaker hypothesis

$$\operatorname{rank} A(\mathbb{Q}) < \dim A$$

for some quotient abelian variety A of J, in particular if $A(\mathbb{Q})$ is finite (i.e. A is a *rank zero quotient*).

Consequence

It is "enough" to find rank zero quotients of $J_0(p)$, $J^+_{\mathrm{sp}}(p)$ and $J^+_{\mathrm{nsp}}(p)$ to apply theoretically the method.

Mazur's method (roughly)

If $J_0(p)$ has a rank zero quotient, if $\operatorname{Im}\rho_{E,p} \subset$ Borel, the associated point of $X_0(p)$ *never* reduces to a cusp hence $j(E) \in \mathbb{Z}$. The same thing holds for $J^+_{\mathrm{sp}}(p)$ and $J^+_{\mathrm{nsp}}(p)$.

Current knowledge on the three families of modular curves

The $\sim$ sign always denotes an isogeny defined over $\mathbb{Q}$.

Current knowledge on the three families of modular curves

The $\sim$ sign always denotes an isogeny defined over $\mathbb{Q}$. For any odd prime p,

$$J_{\mathrm{sp}}^{+}(p) \sim J_0(p) \oplus J_0(p^2)^{+,\mathrm{new}}, \quad J_{\mathrm{nsp}}^{+}(p) \sim J_0(p^2)^{+,\mathrm{new}} \text{ (Chen)}$$

so only $J_0(p)$ and $J_0(p^2)^{+,\mathrm{new}}$ are to be considered.

Current knowledge on the three families of modular curves

The $\sim$ sign always denotes an isogeny defined over $\mathbb{Q}$. For any odd prime p,

$$J_{\mathrm{sp}}^{+}(p) \sim J_0(p) \oplus J_0(p^2)^{+,\mathrm{new}}, \quad J_{\mathrm{nsp}}^{+}(p) \sim J_0(p^2)^{+,\mathrm{new}} \text{ (Chen)}$$

so only $J_0(p)$ and $J_0(p^2)^{+,\mathrm{new}}$ are to be considered.

Current state of affairs

Current knowledge on the three families of modular curves

The $\sim$ sign always denotes an isogeny defined over $\mathbb{Q}$. For any odd prime p,

$$J_{\mathrm{sp}}^{+}(p) \sim J_0(p) \oplus J_0(p^2)^{+,\mathrm{new}}, \quad J_{\mathrm{nsp}}^{+}(p) \sim J_0(p^2)^{+,\mathrm{new}} \text{ (Chen)}$$

so only $J_0(p)$ and $J_0(p^2)^{+,\mathrm{new}}$ are to be considered.

Current state of affairs

- (Mazur) For any $p \notin \{2, 3, 5, 7, 13\}$, there *is* a rank zero quotient of $J_0(p)$, which allows to apply Mazur's method to both $X_0(p)$ and $X_{\mathrm{sp}}^{+}(p)$.

Current knowledge on the three families of modular curves

The $\sim$ sign always denotes an isogeny defined over $\mathbb{Q}$. For any odd prime p,

$$J_{\mathrm{sp}}^{+}(p) \sim J_0(p) \oplus J_0(p^2)^{+,\mathrm{new}}, \quad J_{\mathrm{nsp}}^{+}(p) \sim J_0(p^2)^{+,\mathrm{new}} \text{ (Chen)}$$

so only $J_0(p)$ and $J_0(p^2)^{+,\mathrm{new}}$ are to be considered.

Current state of affairs

- (Mazur) For any $p \notin \{2, 3, 5, 7, 13\}$, there *is* a rank zero quotient of $J_0(p)$, which allows to apply Mazur's method to both $X_0(p)$ and $X_{\mathrm{sp}}^{+}(p)$.
- (Mazur) For every $p > 37$, there are no noncuspidal non-CM points in $X_0(p)(\mathbb{Q})$.

Current knowledge on the three families of modular curves

The $\sim$ sign always denotes an isogeny defined over $\mathbb{Q}$. For any odd prime p,

$$J_{\mathrm{sp}}^{+}(p) \sim J_0(p) \oplus J_0(p^2)^{+,\mathrm{new}}, \quad J_{\mathrm{nsp}}^{+}(p) \sim J_0(p^2)^{+,\mathrm{new}} \text{ (Chen)}$$

so only $J_0(p)$ and $J_0(p^2)^{+,\mathrm{new}}$ are to be considered.

Current state of affairs

- (Mazur) For any $p \notin \{2,3,5,7,13\}$, there *is* a rank zero quotient of $J_0(p)$, which allows to apply Mazur's method to both $X_0(p)$ and $X_{\mathrm{sp}}^{+}(p)$.
- (Mazur) For every $p > 37$, there are no noncuspidal non-CM points in $X_0(p)(\mathbb{Q})$.
- (Bilu-Parent-Rebolledo) For every $p > 13$, there are no noncuspidal non-CM points in $X_{\mathrm{sp}}^{+}(p)(\mathbb{Q})$.

Current knowledge on the three families of modular curves

The $\sim$ sign always denotes an isogeny defined over $\mathbb{Q}$. For any odd prime p,

$$J_{\mathrm{sp}}^{+}(p) \sim J_0(p) \oplus J_0(p^2)^{+,\mathrm{new}}, \quad J_{\mathrm{nsp}}^{+}(p) \sim J_0(p^2)^{+,\mathrm{new}} \text{ (Chen)}$$

so only $J_0(p)$ and $J_0(p^2)^{+,\mathrm{new}}$ are to be considered.

Current state of affairs

- (Mazur) For any $p \notin \{2,3,5,7,13\}$, there *is* a rank zero quotient of $J_0(p)$, which allows to apply Mazur's method to both $X_0(p)$ and $X_{\mathrm{sp}}^{+}(p)$.
- (Mazur) For every $p > 37$, there are no noncuspidal non-CM points in $X_0(p)(\mathbb{Q})$.
- (Bilu-Parent-Rebolledo) For every $p > 13$, there are no noncuspidal non-CM points in $X_{\mathrm{sp}}^{+}(p)(\mathbb{Q})$.
- For $X_{\mathrm{nsp}}^{+}(p)$, it is likely (see later) that there is never any quotient satisfying Chabauty condition !

Current knowledge on the three families of modular curves

The $\sim$ sign always denotes an isogeny defined over $\mathbb{Q}$. For any odd prime p,

$$J_{\mathrm{sp}}^{+}(p) \sim J_0(p) \oplus J_0(p^2)^{+,\mathrm{new}}, \quad J_{\mathrm{nsp}}^{+}(p) \sim J_0(p^2)^{+,\mathrm{new}} \text{ (Chen)}$$

so only $J_0(p)$ and $J_0(p^2)^{+,\mathrm{new}}$ are to be considered.

Current state of affairs

- (Mazur) For any $p \notin \{2, 3, 5, 7, 13\}$, there *is* a rank zero quotient of $J_0(p)$, which allows to apply Mazur's method to both $X_0(p)$ and $X_{\mathrm{sp}}^{+}(p)$.
- (Mazur) For every $p > 37$, there are no noncuspidal non-CM points in $X_0(p)(\mathbb{Q})$.
- (Bilu-Parent-Rebolledo) For every $p > 13$, there are no noncuspidal non-CM points in $X_{\mathrm{sp}}^{+}(p)(\mathbb{Q})$.
- For $X_{\mathrm{nsp}}^{+}(p)$, it is likely (see later) that there is never any quotient satisfying Chabauty condition !

The two families to study

We will focus now on $X_{\mathrm{nsp}}^{+}(p)$ and $X_0(p)^{+} = X_0(p)/\langle w_p \rangle$ (whose jacobian is isogenous to $J_0(p)^{+}$).

What is the "quadratic Chabauty" method ?

Reinterpretation of Chabauty

What is the "quadratic Chabauty" method ?

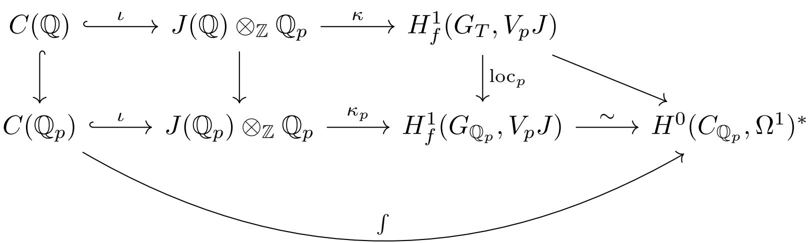
Reinterpretation of Chabauty

Take $V_pJ = T_pJ \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and G_T the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside p.

What is the “quadratic Chabauty” method ?

Reinterpretation of Chabauty

Take $V_pJ = T_pJ \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and G_T the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside p. We have the commutative diagram



where the isomorphism is given by p-adic Hodge theory, $\int$ comes from the p-adic integration pairing and κ, κ_p are Kummer maps.

What is the "quadratic Chabauty" method ?

Reinterpretation of Chabauty

Take $V_pJ = T_pJ \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and G_T the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside p. We have the commutative diagram

$$\begin{array}{ccccccc} C(\mathbb{Q}) & \overset{\iota}{\hookrightarrow} & J(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}_p & \xrightarrow{\kappa} & H^1_f(G_T, V_pJ) & & \\ \downarrow & & \downarrow & & \downarrow \mathrm{loc}_p & \searrow & \\ C(\mathbb{Q}_p) & \overset{\iota}{\hookrightarrow} & J(\mathbb{Q}_p) \otimes_{\mathbb{Z}} \mathbb{Q}_p & \xrightarrow{\kappa_p} & H^1_f(G_{\mathbb{Q}_p}, V_pJ) & \xrightarrow{\sim} & H^0(C_{\mathbb{Q}_p}, \Omega^1)^* \end{array}$$

$$\int : C(\mathbb{Q}_p) \longrightarrow H^0(C_{\mathbb{Q}_p}, \Omega^1)^*$$

where the isomorphism is given by p-adic Hodge theory, $\int$ comes from the p-adic integration pairing and κ, κ_p are Kummer maps.

Kim's idea

Replace V_pJ by a unipotent p-adic Lie group $U \twoheadrightarrow V_pJ$ over $\mathbb{Q}_p$,

Principle of Chabauty-Kim method

Principle of Chabauty-Kim method

Idea

Find U an unipotent algebraic group over $\mathbb{Q}_p$ such that

Principle of Chabauty-Kim method

Idea

Find U an unipotent algebraic group over $\mathbb{Q}_p$ such that

- We have the commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\kappa_U} & \mathrm{Sel}(U) \\ \big\downarrow & & \big\downarrow \mathrm{loc}_p \\ C(\mathbb{Q}_p) & \xrightarrow{\kappa_{U,p}} & H^1_f(G_{\mathbb{Q}_p}, U) \end{array} \qquad (\subset H^1_f(G_T, U))$$

  where κ_U and $\kappa_{U,p}$ are Kummer maps,

Principle of Chabauty-Kim method

Idea

Find U an unipotent algebraic group over $\mathbb{Q}_p$ such that

- We have the commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\kappa_U} & \mathrm{Sel}(U) \\ \downarrow & & \downarrow \mathrm{loc}_p \\ C(\mathbb{Q}_p) & \xrightarrow{\kappa_{U,p}} & H^1_f(G_{\mathbb{Q}_p}, U) \end{array} \qquad (\subset H^1_f(G_T, U))$$

where κ_U and $\kappa_{U,p}$ are Kummer maps, $\mathrm{Sel}(U)$ and $H^1_f(G_{\mathbb{Q}_p}, U)$ have variety structures and loc_p is algebraic.

Principle of Chabauty-Kim method

Idea

Find U an unipotent algebraic group over $\mathbb{Q}_p$ such that

- We have the commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\kappa_U} & \mathrm{Sel}(U) & \qquad (\subset H^1_f(G_T, U)) \\ \big\downarrow & & \big\downarrow \mathrm{loc}_p & \\ C(\mathbb{Q}_p) & \xrightarrow{\kappa_{U,p}} & H^1_f(G_{\mathbb{Q}_p}, U) & \end{array}$$

  where κ_U and $\kappa_{U,p}$ are Kummer maps, $\mathrm{Sel}(U)$ and $H^1_f(G_{\mathbb{Q}_p}, U)$ have variety structures and loc_p is algebraic.
- The map $\kappa_{U,p}$ has locally Zariski-dense image everywhere.

Principle of Chabauty-Kim method

Idea

Find U an unipotent algebraic group over $\mathbb{Q}_p$ such that

- We have the commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\kappa_U} & \mathrm{Sel}(U) \\ \big\downarrow & & \big\downarrow \mathrm{loc}_p \\ C(\mathbb{Q}_p) & \xrightarrow{\kappa_{U,p}} & H^1_f(G_{\mathbb{Q}_p}, U) \end{array} \qquad (\subset H^1_f(G_T, U))$$

  where κ_U and $\kappa_{U,p}$ are Kummer maps, $\mathrm{Sel}(U)$ and $H^1_f(G_{\mathbb{Q}_p}, U)$ have variety structures and loc_p is algebraic.
- The map $\kappa_{U,p}$ has locally Zariski-dense image everywhere.
- The map loc_p is not dominant.

Principle of Chabauty-Kim method

Idea

Find U an unipotent algebraic group over $\mathbb{Q}_p$ such that

- We have the commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\kappa_U} & \mathrm{Sel}(U) \\ \big\downarrow & & \big\downarrow \mathrm{loc}_p \\ C(\mathbb{Q}_p) & \xrightarrow{\kappa_{U,p}} & H^1_f(G_{\mathbb{Q}_p}, U) \end{array} \qquad (\subset H^1_f(G_T, U))$$

  where κ_U and $\kappa_{U,p}$ are Kummer maps, $\mathrm{Sel}(U)$ and $H^1_f(G_{\mathbb{Q}_p}, U)$ have variety structures and loc_p is algebraic.
- The map $\kappa_{U,p}$ has locally Zariski-dense image everywhere.
- The map loc_p is not dominant.

Then, $C(\mathbb{Q}) \hookrightarrow \kappa_{U,p}^{-1}(\mathrm{Im}\,\mathrm{loc}_p)$ which proves it is finite !

Quadratic Chabauty: the main theorem

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\kappa_U} & \mathrm{Sel}(U) \\ \big\downarrow & & \big\downarrow \mathrm{loc}_p \\ C(\mathbb{Q}_p) & \xrightarrow{\kappa_{U,p}} & H^1_f(G_{\mathbb{Q}_p}, U) \end{array}$$

Quadratic Chabauty: the main theorem

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\kappa_U} & \mathrm{Sel}(U) \\ \downarrow & & \downarrow \mathrm{loc}_p \\ C(\mathbb{Q}_p) & \xrightarrow{\kappa_{U,p}} & H^1_f(G_{\mathbb{Q}_p}, U) \end{array}$$

Definition (Néron-Severi group)

Let $\mathrm{NS}(J) := \mathrm{Pic}\, J / \mathrm{Pic}^0\, J$ be the Néron-Severi group of J. It is a finite type $\mathbb{Z}$-module, of rank denoted by $\rho = \rho(J)$.

Quadratic Chabauty: the main theorem

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\kappa_U} & \mathrm{Sel}(U) \\ \big\downarrow & & \big\downarrow \mathrm{loc}_p \\ C(\mathbb{Q}_p) & \xrightarrow{\kappa_{U,p}} & H^1_f(G_{\mathbb{Q}_p}, U) \end{array}$$

Definition (Néron-Severi group)

Let $\mathrm{NS}(J) := \mathrm{Pic}\, J / \mathrm{Pic}^0 J$ be the Néron-Severi group of J. It is a finite type $\mathbb{Z}$-module, of rank denoted by $\rho = \rho(J)$.

Theorem(Balakrishnan, Dogra)

One can find a group U satisfying the first two conditions, and

$$\dim \mathrm{Sel}(U) \leq r = \mathrm{rank}\, J(\mathbb{Q}), \quad \dim H^1_f(G_{\mathbb{Q}_p}, U) \geq g + \rho - 1.$$

Therefore, under the *quadratic Chabauty condition*

$$r < g + \rho - 1,$$

one has proved the finiteness of $C(\mathbb{Q})$!

Applications of the method

Applications of the method

Theorem (Balakrishnan, Dogra, Müller, Tuitman, Vonk)

The set of rational points of $X_{\mathrm{nsp}}^{+}(13)$ (for which $r = g = \rho = 3$) is made up with CM points and $\#X_{\mathrm{nsp}}^{+}(13)(\mathbb{Q}) = 7$.

Applications of the method

Theorem (Balakrishnan, Dogra, Müller, Tuitman, Vonk)

The set of rational points of $X_{\mathrm{nsp}}^{+}(13)$ (for which $r = g = \rho = 3$) is made up with CM points and $\#X_{\mathrm{nsp}}^{+}(13)(\mathbb{Q}) = 7$.

Tools to make effective quadratic Chabauty

Applications of the method

Theorem (Balakrishnan, Dogra, Müller, Tuitman, Vonk)

The set of rational points of $X^+_{\mathrm{nsp}}(13)$ (for which $r = g = \rho = 3$) is made up with CM points and $\#X^+_{\mathrm{nsp}}(13)(\mathbb{Q}) = 7$.

Tools to make effective quadratic Chabauty

- Equation(s) for the curve.

Applications of the method

Theorem (Balakrishnan, Dogra, Müller, Tuitman, Vonk)

The set of rational points of $X^+_{\mathrm{nsp}}(13)$ (for which $r = g = \rho = 3$) is made up with CM points and $\#X^+_{\mathrm{nsp}}(13)(\mathbb{Q}) = 7$.

Tools to make effective quadratic Chabauty

- Equation(s) for the curve.
- Iterated p-adic integrals for 1-forms on the curve to give explicit equations for the rational points.

Applications of the method

Theorem (Balakrishnan, Dogra, Müller, Tuitman, Vonk)

The set of rational points of $X^+_{\mathrm{nsp}}(13)$ (for which $r = g = \rho = 3$) is made up with CM points and $\#X^+_{\mathrm{nsp}}(13)(\mathbb{Q}) = 7$.

Tools to make effective quadratic Chabauty

- Equation(s) for the curve.
- Iterated p-adic integrals for 1-forms on the curve to give explicit equations for the rational points.
- Mordell-Weil sieve to exclude all other possibilities.

Applications of the method

Theorem (Balakrishnan, Dogra, Müller, Tuitman, Vonk)

The set of rational points of $X^+_{\mathrm{nsp}}(13)$ (for which $r = g = \rho = 3$) is made up with CM points and $\# X^+_{\mathrm{nsp}}(13)(\mathbb{Q}) = 7$.

Tools to make effective quadratic Chabauty

- Equation(s) for the curve.
- Iterated p-adic integrals for 1-forms on the curve to give explicit equations for the rational points.
- Mordell-Weil sieve to exclude all other possibilities.
- Special working case : $r = g$, $\rho > 1$.

Applying the method to families of modular curves

Applying the method to families of modular curves

Reasonable working scopes

- Figure out when quadratic Chabauty condition is satisfied.
- (future) Obtain an argument working in families such as Mazur's method.

Applying the method to families of modular curves

Reasonable working scopes

- Figure out when quadratic Chabauty condition is satisfied.
- (future) Obtain an argument working in families such as Mazur's method.

WIP (Dogra, Vonk)

The quadratic Chabauty method also applies for C if

$$\operatorname{rank} A(\mathbb{Q}) < \dim A + \rho(A) - 1$$

for A a quotient abelian variety of J, in particular if $\operatorname{rank} A(\mathbb{Q}) = \dim A$ and $\rho(A) > 1$.

What is special about modular curves

What is special about modular curves

Theory of Eichler-Shimura

- If $f = \sum_{n=1}^{+\infty} a_n q^n$ is a newform of $S_2(\Gamma_0(N))$, $K_f := \mathbb{Q}(\{a_n\})$ is a totally real number field and there is a quotient A_f of $J_0(N)^{\mathrm{new}}$ of dimension $[K_f : \mathbb{Q}]$ with $\mathrm{End}(A_f) \otimes \mathbb{Q} = K_f$.

What is special about modular curves

Theory of Eichler-Shimura

- If $f = \sum_{n=1}^{+\infty} a_n q^n$ is a newform of $S_2(\Gamma_0(N))$, $K_f := \mathbb{Q}(\{a_n\})$ is a totally real number field and there is a quotient A_f of $J_0(N)^{\mathrm{new}}$ of dimension $[K_f : \mathbb{Q}]$ with $\mathrm{End}(A_f) \otimes \mathbb{Q} = K_f$.
- We have the decomposition
$$J_0(N)^{+,\mathrm{new}} \sim \bigoplus_f A_f$$
where f runs through representatives of the orbits of newforms of $S_2(\Gamma_0(N))^+$ by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

What is special about modular curves

Theory of Eichler-Shimura

- If $f = \sum_{n=1}^{+\infty} a_n q^n$ is a newform of $S_2(\Gamma_0(N))$, $K_f := \mathbb{Q}(\{a_n\})$ is a totally real number field and there is a quotient A_f of $J_0(N)^{\mathrm{new}}$ of dimension $[K_f : \mathbb{Q}]$ with $\mathrm{End}(A_f) \otimes \mathbb{Q} = K_f$.
- We have the decomposition
$$J_0(N)^{+,\mathrm{new}} \sim \bigoplus_f A_f$$
where f runs through representatives of the orbits of newforms of $S_2(\Gamma_0(N))^+$ by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

What is special about modular curves

Theory of Eichler-Shimura

- If $f = \sum_{n=1}^{+\infty} a_n q^n$ is a newform of $S_2(\Gamma_0(N))$, $K_f := \mathbb{Q}(\{a_n\})$ is a totally real number field and there is a quotient A_f of $J_0(N)^{\mathrm{new}}$ of dimension $[K_f : \mathbb{Q}]$ with $\mathrm{End}(A_f) \otimes \mathbb{Q} = K_f$.
- We have the decomposition

$$J_0(N)^{+,\mathrm{new}} \sim \bigoplus_f A_f$$

where f runs through representatives of the orbits of newforms of $S_2(\Gamma_0(N))^+$ by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Fundamental remark for modular curves

As $\mathrm{NS}(A_f) \otimes \mathbb{Q} \cong K_f$ here (Pyle), for $J_0(N)^+$, it is enough to find either:

(a) One newform f such that $\mathrm{rank}\, A_f(\mathbb{Q}) = \dim A_f \geq 2$.

(b) Two newforms f such that $\mathrm{rank}\, A_f(\mathbb{Q}) = \dim A_f$.

Our goal: where L-functions appear

Our goal: where L-functions appear

Objective

For $N = p$ or p^2 large enough, prove option (a) or (b).

Our goal: where L-functions appear

Objective

For $N = p$ or p^2 large enough, prove option (a) or (b).

The rank part of BSD conjecture

For any abelian variety A over $\mathbb{Q}$, $\operatorname{rank} A(\mathbb{Q}) = \operatorname{ord}_{s=1} L(A, s)$.

Our goal: where L-functions appear

Objective

For $N = p$ or p^2 large enough, prove option (a) or (b).

The rank part of BSD conjecture

For any abelian variety A over $\mathbb{Q}$, $\operatorname{rank} A(\mathbb{Q}) = \operatorname{ord}_{s=1} L(A, s)$.

Definition

For any modular form f in $S_2(\Gamma_0(N))$, the L-function of f is defined for $\operatorname{Re}(s) > 2$ by

$$L(f, s) = \sum_{n=1}^{+\infty} \frac{a_n(f)}{n^s}.$$

It extends holomorphically to $\mathbb{C}$ and $L(f, 1) = 0$ if $f \in S_2(\Gamma_0(N))^+$.

Our goal: where L-functions appear

Objective

For $N = p$ or p^2 large enough, prove option (a) or (b).

The rank part of BSD conjecture

For any abelian variety A over $\mathbb{Q}$, $\operatorname{rank} A(\mathbb{Q}) = \operatorname{ord}_{s=1} L(A, s)$.

Definition

For any modular form f in $S_2(\Gamma_0(N))$, the L-function of f is defined for $\operatorname{Re}(s) > 2$ by

$$L(f, s) = \sum_{n=1}^{+\infty} \frac{a_n(f)}{n^s}.$$

It extends holomorphically to $\mathbb{C}$ and $L(f, 1) = 0$ if $f \in S_2(\Gamma_0(N))^+$. If f is a newform,

$$L(A_f, s) = \prod_{g \sim f} L(g, s)$$

where g goes through the $[K_f : \mathbb{Q}]$ newforms $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugate to f.

What to prove analytically

$$L(A_f, s) = \prod_{g \sim f} L(g, s)$$

What to prove analytically

$$L(A_f, s) = \prod_{g \sim f} L(g, s)$$

Theorem (Kolyvagin-Logachev)

For f a newform in $S_2(\Gamma_0(N))$, if $\mathrm{ord}_{s=1} L(f,s) = k \in \{0,1\}$ then A_f satisfies the rank part of BSD conjecture, i.e.

$$\mathrm{rank}\, A_f(\mathbb{Q}) = k \cdot \dim A_f.$$

What to prove analytically

$$L(A_f, s) = \prod_{g \sim f} L(g, s)$$

Theorem (Kolyvagin-Logachev)

For f a newform in $S_2(\Gamma_0(N))$, if $\operatorname{ord}_{s=1} L(f,s) = k \in \{0,1\}$ then A_f satisfies the rank part of BSD conjecture, i.e.

$$\operatorname{rank} A_f(\mathbb{Q}) = k \cdot \dim A_f.$$

Restated objective

For any $N = p$ or p^2 large enough, prove:
There are at least two newforms $f \in S_2(\Gamma_0(N))^+$ such that $L'(f,1) \neq 0$.

Nonvanishing of derivatives of modular L-functions

Restated objective

For any $N = p$ or p^2 large enough, prove:
There are at least two newforms $f \in S_2(\Gamma_0(N))^+$ *such that* $L'(f, 1) \neq 0$.

Nonvanishing of derivatives of modular L-functions

Restated objective

For any $N = p$ or p^2 large enough, prove:
There are at least two newforms $f \in S_2(\Gamma_0(N))^+$ such that $L'(f,1) \neq 0$.

Lemma

For any $f \in S_2(\Gamma_0(N))^+$,

$$L'(f,1) = 2\sum_{n=1}^{+\infty} \frac{a_n(f)}{n} E_1\left(\frac{2\pi n}{\sqrt{N}}\right)$$

where $E_1(y) = \int_y^{+\infty} e^{-t}/t dt$ is the exponential integral function.

Nonvanishing of derivatives of modular L-functions

Restated objective

For any $N = p$ or p^2 large enough, prove:
There are at least two newforms $f \in S_2(\Gamma_0(N))^+$ such that $L'(f, 1) \neq 0$.

Lemma

For any $f \in S_2(\Gamma_0(N))^+$,

$$L'(f, 1) = 2 \sum_{n=1}^{+\infty} \frac{a_n(f)}{n} E_1 \left(\frac{2\pi n}{\sqrt{N}} \right)$$

where $E_1(y) = \int_y^{+\infty} e^{-t}/t dt$ is the exponential integral function.

Main idea for computations

To prove that there is one f such that $L'(f, 1) \neq 0$, it is enough to prove that a weighted sum of the $L'(f, 1)$ is nonzero !

Notations for the weighted sums

Notations for the weighted sums

Notations

Notations for the weighted sums

Notations

- For any linear forms A, B on $S_2(\Gamma_0(N))$,

$$\langle A, B \rangle_N = \sum_f \frac{\overline{A(f)}B(f)}{\|f\|^2}$$

where f runs through a Petersson-orthogonal basis of $S_2(\Gamma_0(N))$ with superscripts $+, -, \mathrm{new}$ added for the corresponding subspaces of $S_2(\Gamma_0(N))$.

Notations for the weighted sums

Notations

- For any linear forms A, B on $S_2(\Gamma_0(N))$,

$$\langle A, B\rangle_N = \sum_f \frac{\overline{A(f)}B(f)}{\|f\|^2}$$

  where f runs through a Petersson-orthogonal basis of $S_2(\Gamma_0(N))$ with superscripts $+, -, \mathrm{new}$ added for the corresponding subspaces of $S_2(\Gamma_0(N))$.
- We define $a_m : f \mapsto a_m(f)$, $L : f \to L(f, 1)$, $L' : f \mapsto L'(f, 1)$ and will focus on $\langle a_m, L'\rangle_N^{+,\mathrm{new}}$.

Notations for the weighted sums

Notations

- For any linear forms A, B on $S_2(\Gamma_0(N))$,

$$\langle A, B\rangle_N = \sum_f \frac{\overline{A(f)}B(f)}{\|f\|^2}$$

  where f runs through a Petersson-orthogonal basis of $S_2(\Gamma_0(N))$ with superscripts $+, -, \mathrm{new}$ added for the corresponding subspaces of $S_2(\Gamma_0(N))$.
- We define $a_m : f \mapsto a_m(f)$, $L : f \to L(f,1)$, $L' : f \mapsto L'(f,1)$ and will focus on $\langle a_m, L'\rangle_N^{+,\mathrm{new}}$.

Lemma

For any m prime to p,

$$\langle a_m, L'\rangle_{p^2}^{+,\mathrm{new}} = \langle a_m, L'\rangle_{p^2}^{+} - \frac{1}{p-1}\left(\langle a_m, L'\rangle_p^{+} + \frac{\ln(p)}{2}\langle a_m, L\rangle_p^{-}\right)$$

so it is enough to compute only $\langle a_m, L'\rangle_N^{+}$ and $\langle a_m, L\rangle_p^{-}$.

Our main tool: Petersson trace formula

Proposition (Restricted Petersson trace formula)

For any integers $m, n, N \geq 1$ *:*

$$\frac{\langle a_m, a_n\rangle_N^+}{2\pi\sqrt{mn}} = \delta_{mn} - 2\pi\left(\sum_{N|c}\frac{S(m,n;c)}{c}J_1\left(\frac{4\pi\sqrt{mn}}{c}\right)\right) - 2\pi\left(\sum_{(d,N)=1}\frac{S(m,nN^{-1};d)}{d\sqrt{N}}J_1\left(\frac{4\pi\sqrt{mn}}{d\sqrt{N}}\right)\right)$$

where

Our main tool: Petersson trace formula

Proposition (Restricted Petersson trace formula)

For any integers $m, n, N \geq 1$ *:*

$$\frac{\langle a_m, a_n \rangle_N^+}{2\pi\sqrt{mn}} = \delta_{mn} \quad - \quad 2\pi \left(\sum_{N|c} \frac{S(m,n;c)}{c} J_1\left(\frac{4\pi\sqrt{mn}}{c}\right) \right)$$

$$\quad - \quad 2\pi \left(\sum_{(d,N)=1} \frac{S(m,nN^{-1};d)}{d\sqrt{N}} J_1\left(\frac{4\pi\sqrt{mn}}{d\sqrt{N}}\right) \right)$$

where J_1 *is the Bessel function of first order and first type and*

Our main tool: Petersson trace formula

Proposition (Restricted Petersson trace formula)

For any integers $m, n, N \geq 1$ *:*

$$\frac{\langle a_m, a_n \rangle_N^+}{2\pi\sqrt{mn}} = \delta_{mn} \quad - \quad 2\pi \left(\sum_{N|c} \frac{S(m,n;c)}{c} J_1\left(\frac{4\pi\sqrt{mn}}{c}\right)\right)$$
$$\quad - \quad 2\pi \left(\sum_{(d,N)=1} \frac{S(m,nN^{-1};d)}{d\sqrt{N}} J_1\left(\frac{4\pi\sqrt{mn}}{d\sqrt{N}}\right)\right)$$

where J_1 *is the Bessel function of first order and first type and*

$$S(m,n;c) = \sum_{k \in (\mathbb{Z}/c\mathbb{Z})^*} e^{2i\pi(mk+nk^{-1})/c}$$

is the Kloosterman sum.

Expression of our weighted averages

Using the previous formulas,

Expression of our weighted averages

Using the previous formulas,

$$\frac{\langle a_m, L' \rangle_N^+}{4\pi} = E_1\left(\frac{2\pi m}{\sqrt{N}}\right) - 2\pi\sqrt{m}\left(\sum_{N|c} \frac{\mathcal{S}(c)}{c} + \sum_{(d,p)=1} \frac{\mathcal{T}(d)}{d\sqrt{N}}\right),$$

where

Expression of our weighted averages

Using the previous formulas,

$$\frac{\langle a_m, L'\rangle_N^+}{4\pi} = E_1\left(\frac{2\pi m}{\sqrt{N}}\right) - 2\pi\sqrt{m}\left(\sum_{N|c}\frac{\mathcal{S}(c)}{c} + \sum_{(d,p)=1}\frac{\mathcal{T}(d)}{d\sqrt{N}}\right),$$

where

$$\mathcal{S}(c) = \sum_{n=1}^{+\infty}\frac{S(m,n;c)}{\sqrt{n}}J_1\left(\frac{4\pi\sqrt{mn}}{c}\right)E_1\left(\frac{2\pi n}{\sqrt{N}}\right)$$

and

$$\mathcal{T}(d) = \sum_{n=1}^{+\infty}\frac{S(m,nN^{-1};d)}{\sqrt{n}}J_1\left(\frac{4\pi\sqrt{mn}}{d\sqrt{N}}\right)E_1\left(\frac{2\pi n}{\sqrt{N}}\right),$$

and a similar formula holds for $\langle a_m, L\rangle_N^-$.

Expression of our weighted averages

Using the previous formulas,

$$\frac{\langle a_m, L'\rangle_N^+}{4\pi} = E_1\left(\frac{2\pi m}{\sqrt{N}}\right) - 2\pi\sqrt{m}\left(\sum_{N|c}\frac{\mathcal{S}(c)}{c} + \sum_{(d,p)=1}\frac{\mathcal{T}(d)}{d\sqrt{N}}\right),$$

where

$$\mathcal{S}(c) = \sum_{n=1}^{+\infty}\frac{S(m,n;c)}{\sqrt{n}} J_1\left(\frac{4\pi\sqrt{mn}}{c}\right) E_1\left(\frac{2\pi n}{\sqrt{N}}\right)$$

and

$$\mathcal{T}(d) = \sum_{n=1}^{+\infty}\frac{S(m,nN^{-1};d)}{\sqrt{n}} J_1\left(\frac{4\pi\sqrt{mn}}{d\sqrt{N}}\right) E_1\left(\frac{2\pi n}{\sqrt{N}}\right),$$

and a similar formula holds for $\langle a_m, L\rangle_N^-$.

Remark

For $m \ll \sqrt{N}$, the main term is $E_1(2\pi m/\sqrt{N}) \sim \ln(N)/2$ hence $\langle a_m, L'\rangle_N^+ \sim 2\pi\ln(N)$.

First estimates: Weil bounds

First estimates: Weil bounds

First, one has $|J_1(x)| \le |x|/2$, and

$$E_1(x) = |\ln(x)| - \gamma + O(x) \quad (x \le 1), \quad E_1(x) = O(e^{-x}/x).$$

First estimates: Weil bounds

First, one has $|J_1(x)| \leq |x|/2$, and

$$E_1(x) = |\ln(x)| - \gamma + O(x) \quad (x \leq 1), \quad E_1(x) = O(e^{-x}/x).$$

Proposition (Weil bounds)

For any $m, n, c \geq 1$*,*

$$|S(m,n;c)| \leq (\gcd(m,n,c))^{1/2} \tau(c) \sqrt{c}$$

where τ *is the divisor-counting function.*

First estimates: Weil bounds

First, one has $|J_1(x)| \leq |x|/2$, and

$$E_1(x) = |\ln(x)| - \gamma + O(x) \quad (x \leq 1), \quad E_1(x) = O(e^{-x}/x).$$

Proposition (Weil bounds)

For any $m, n, c \geq 1$,

$$|S(m,n;c)| \leq (\gcd(m,n,c))^{1/2} \tau(c) \sqrt{c}$$

where τ is the divisor-counting function.

Consequence

For $m \ll \sqrt{N}$,

$$\frac{\langle a_m, L' \rangle_N^+}{4\pi} = \frac{\ln(N)}{2} - \ln(m) - (\gamma + \ln(2\pi)) + O\left(\frac{m}{N}\right) + O\left(\frac{m}{\sqrt{N}}\right),$$

the (effective) error terms coming respectively from the $\mathcal{S}(c)$ and $\mathcal{T}(d)$.

How to exploit the estimates

$$\frac{\langle a_m, L' \rangle_N^+}{4\pi} = \frac{\ln(N)}{2} - \ln(m) - (\gamma + \ln(2\pi)) + O\left(\frac{m}{N}\right) + O\left(\frac{m}{\sqrt{N}}\right),$$

How to exploit the estimates

$$\frac{\langle a_m, L'\rangle_N^+}{4\pi} = \frac{\ln(N)}{2} - \ln(m) - (\gamma + \ln(2\pi)) + O\left(\frac{m}{N}\right) + O\left(\frac{m}{\sqrt{N}}\right),$$

Lemma

For $N = p$, it is enough to prove that $\langle a_1, L'\rangle_p^+ \neq 0$ and $\langle a_2, L'\rangle_p^+ / \langle a_1, L'\rangle_p^+ \notin \mathbb{Z}$, and similarly for $N = p^2$.

How to exploit the estimates

$$\frac{\langle a_m, L'\rangle_N^+}{4\pi} = \frac{\ln(N)}{2} - \ln(m) - (\gamma + \ln(2\pi)) + O\left(\frac{m}{N}\right) + O\left(\frac{m}{\sqrt{N}}\right),$$

Lemma

For $N = p$, it is enough to prove that $\langle a_1, L'\rangle_p^+ \neq 0$ and $\langle a_2, L'\rangle_p^+ / \langle a_1, L'\rangle_p^+ \notin \mathbb{Z}$, and similarly for $N = p^2$.

Proof.

When $\langle a_1, L'\rangle_p^+ \neq 0$, the only situation when option (a) is not satisfied is when only one newform f in the basis satisfies $L'(f, 1) \neq 0$, and then

How to exploit the estimates

$$\frac{\langle a_m, L' \rangle_N^+}{4\pi} = \frac{\ln(N)}{2} - \ln(m) - (\gamma + \ln(2\pi)) + O\left(\frac{m}{N}\right) + O\left(\frac{m}{\sqrt{N}}\right),$$

Lemma

For $N = p$, it is enough to prove that $\langle a_1, L' \rangle_p^+ \neq 0$ and $\langle a_2, L' \rangle_p^+ / \langle a_1, L' \rangle_p^+ \notin \mathbb{Z}$, and similarly for $N = p^2$.

Proof.

When $\langle a_1, L' \rangle_p^+ \neq 0$, the only situation when option (a) is not satisfied is when only one newform f in the basis satisfies $L'(f,1) \neq 0$, and then

$$\frac{\langle a_2, L' \rangle_p^+}{\langle a_1, L' \rangle_p^+} = \frac{a_2(f) L'(f,1)}{\|f\|^2} \frac{\|f\|^2}{L'(f,1)} = a_2(f).$$

Now, if $a_2(f) \notin \mathbb{Z}$, $K_f \neq \mathbb{Q}$ so f has nontrivial conjugates g such that $L'(g,1) \neq 0$ as well, contradiction. □

The first range

$$\frac{\langle a_m, L' \rangle_N^+}{4\pi} = \frac{\ln(N)}{2} - \ln(m) - (\gamma + \ln(2\pi)) + O\left(\frac{m}{N}\right) + O\left(\frac{m}{\sqrt{N}}\right),$$

The first range

$$\frac{\langle a_m, L'\rangle_N^+}{4\pi} = \frac{\ln(N)}{2} - \ln(m) - (\gamma + \ln(2\pi)) + O\left(\frac{m}{N}\right) + O\left(\frac{m}{\sqrt{N}}\right),$$

Proposition

After improving the bounds specifically for $m = 1$ *and* $m = 2$*, one finds*

$$\begin{array}{rll|rll}
\langle a_1, L'\rangle_p^+ > 0 & \textit{for} & p \geq 1213 & \langle a_1, L'\rangle_{p^2}^{+,new} > 0 & \textit{for} & p \geq 47 \\
\langle a_2, L'\rangle_p^+ > 0 & \textit{for} & p \geq 5437 & \langle a_2, L'\rangle_{p^2}^{+,new} > 0 & \textit{for} & p \geq 97 \\
\frac{\langle a_2, L'\rangle_p^+}{\langle a_1, L'\rangle_p^+} \in]0,1[& \textit{for} & p \geq 45341 & \frac{\langle a_2, L'\rangle_{p^2}^{+,new}}{\langle a_1, L'\rangle_{p^2}^{+,new}} \in]0,1[& \textit{for} & p \geq 269.
\end{array}$$

The first range

$$\frac{\langle a_m, L' \rangle_N^+}{4\pi} = \frac{\ln(N)}{2} - \ln(m) - (\gamma + \ln(2\pi)) + O\left(\frac{m}{N}\right) + O\left(\frac{m}{\sqrt{N}}\right),$$

Proposition

After improving the bounds specifically for $m = 1$ and $m = 2$, one finds

$$\begin{array}{rll|rll} \langle a_1, L' \rangle_p^+ > 0 & \textit{for} & p \geq 1213 & \langle a_1, L' \rangle_{p^2}^{+,new} > 0 & \textit{for} & p \geq 47 \\ \langle a_2, L' \rangle_p^+ > 0 & \textit{for} & p \geq 5437 & \langle a_2, L' \rangle_{p^2}^{+,new} > 0 & \textit{for} & p \geq 97 \\ \frac{\langle a_2, L' \rangle_p^+}{\langle a_1, L' \rangle_p^+} \in]0,1[& \textit{for} & p \geq 45341 & \frac{\langle a_2, L' \rangle_{p^2}^{+,new}}{\langle a_1, L' \rangle_{p^2}^{+,new}} \in]0,1[& \textit{for} & p \geq 269. \end{array}$$

Remarks to improve this result

The first range

$$\frac{\langle a_m, L' \rangle_N^+}{4\pi} = \frac{\ln(N)}{2} - \ln(m) - (\gamma + \ln(2\pi)) + O\left(\frac{m}{N}\right) + O\left(\frac{m}{\sqrt{N}}\right),$$

Proposition

After improving the bounds specifically for $m = 1$ and $m = 2$, one finds

$$\begin{array}{rll|rll}
\langle a_1, L' \rangle_p^+ > 0 & \textit{for} & p \geq 1213 & \langle a_1, L' \rangle_{p^2}^{+,new} > 0 & \textit{for} & p \geq 47 \\
\langle a_2, L' \rangle_p^+ > 0 & \textit{for} & p \geq 5437 & \langle a_2, L' \rangle_{p^2}^{+,new} > 0 & \textit{for} & p \geq 97 \\
\frac{\langle a_2, L' \rangle_p^+}{\langle a_1, L' \rangle_p^+} \in]0,1[& \textit{for} & p \geq 45341 & \frac{\langle a_2, L' \rangle_{p^2}^{+,new}}{\langle a_1, L' \rangle_{p^2}^{+,new}} \in]0,1[& \textit{for} & p \geq 269.
\end{array}$$

Remarks to improve this result

- Those bounds are still too large to be complemented by computer.

The first range

$$\frac{\langle a_m, L'\rangle_N^+}{4\pi} = \frac{\ln(N)}{2} - \ln(m) - (\gamma + \ln(2\pi)) + O\left(\frac{m}{N}\right) + O\left(\frac{m}{\sqrt{N}}\right),$$

Proposition

After improving the bounds specifically for $m = 1$ and $m = 2$, one finds

$$\begin{array}{rll|rll} \langle a_1, L'\rangle_p^+ > 0 & \textit{for} & p \geq 1213 & \langle a_1, L'\rangle_{p^2}^{+,new} > 0 & \textit{for} & p \geq 47 \\ \langle a_2, L'\rangle_p^+ > 0 & \textit{for} & p \geq 5437 & \langle a_2, L'\rangle_{p^2}^{+,new} > 0 & \textit{for} & p \geq 97 \\ \frac{\langle a_2, L'\rangle_p^+}{\langle a_1, L'\rangle_p^+} \in]0,1[& \textit{for} & p \geq 45341 & \frac{\langle a_2, L'\rangle_{p^2}^{+,new}}{\langle a_1, L'\rangle_{p^2}^{+,new}} \in]0,1[& \textit{for} & p \geq 269. \end{array}$$

Remarks to improve this result

- Those bounds are still too large to be complemented by computer.
- The term $O(m/\sqrt{N})$ coming from the $\mathcal{T}(d)$ needs to be improved.

The first range

$$\frac{\langle a_m, L'\rangle_N^+}{4\pi} = \frac{\ln(N)}{2} - \ln(m) - (\gamma + \ln(2\pi)) + O\left(\frac{m}{N}\right) + O\left(\frac{m}{\sqrt{N}}\right),$$

Proposition

After improving the bounds specifically for $m = 1$ *and* $m = 2$*, one finds*

$$\begin{array}{rll|rll} \langle a_1, L'\rangle_p^+ > 0 & \textit{for} & p \geq 1213 & \langle a_1, L'\rangle_{p^2}^{+,new} > 0 & \textit{for} & p \geq 47 \\ \langle a_2, L'\rangle_p^+ > 0 & \textit{for} & p \geq 5437 & \langle a_2, L'\rangle_{p^2}^{+,new} > 0 & \textit{for} & p \geq 97 \\ \frac{\langle a_2, L'\rangle_p^+}{\langle a_1, L'\rangle_p^+} \in]0,1[& \textit{for} & p \geq 45341 & \frac{\langle a_2, L'\rangle_{p^2}^{+,new}}{\langle a_1, L'\rangle_{p^2}^{+,new}} \in]0,1[& \textit{for} & p \geq 269. \end{array}$$

Remarks to improve this result

- Those bounds are still too large to be complemented by computer.
- The term $O(m/\sqrt{N})$ coming from the $\mathcal{T}(d)$ needs to be improved.
- The Kloosterman sums oscillate a lot.

Pólya-Vinogradov-like inequality for Kloosterman sums

Pólya-Vinogradov-like inequality for Kloosterman sums

Proposition

For every $d > 1$, every k invertible modulo d and every $m, K, K' \in \mathbb{N}$,

$$\left| \sum_{n=K}^{K'} S(m, nk; d) \right| \leq \frac{4d}{\pi^2}(\log(d) + 1.5).$$

Pólya-Vinogradov-like inequality for Kloosterman sums

Proposition

For every $d > 1$, every k invertible modulo d and every $m, K, K' \in \mathbb{N}$,

$$\left| \sum_{n=K}^{K'} S(m, nk; d) \right| \leq \frac{4d}{\pi^2}(\log(d) + 1.5).$$

As $J_1(x) \approx x/2$ for x small, for $d > 1$,

$$\begin{aligned} |\mathcal{T}(d)| &\lessapprox \frac{2\pi\sqrt{m}}{d\sqrt{p}} \sum_{n=1}^{+\infty} S(1, nN^{-1}; d) E_1 \left(\frac{2\pi n}{\sqrt{N}} \right) \\ &\lessapprox \frac{8}{\pi} \frac{\sqrt{m}}{\sqrt{N}} (\log(d) + 1.5) E_1 \left(\frac{2\pi}{\sqrt{N}} \right) \end{aligned}$$

by Abel transform, to be compared to the bound $\tau(d)/\sqrt{d}$ coming from the Weil bounds.

The final result

After optimising on the choice of Weil vs. Polya-Vinogradov, we get:

The final result

After optimising on the choice of Weil vs. Polya-Vinogradov, we get:

Theorem (LF, Siksek)

- We have

$$\frac{\langle a_2, L' \rangle_p^+}{\langle a_1, L' \rangle_p^+} \in]0,1[\quad \text{for} \quad p \geq 8663 \;\Bigg|\; \frac{\langle a_2, L' \rangle_{p^2}^{+,\text{new}}}{\langle a_1, L' \rangle_{p^2}^{+,\text{new}}} \in]0,1[\quad \text{for} \quad p \geq 167,$$

The final result

After optimising on the choice of Weil vs. Polya-Vinogradov, we get:

Theorem (LF, Siksek)

- We have

$$\frac{\langle a_2, L'\rangle_p^+}{\langle a_1, L'\rangle_p^+} \in]0,1[\quad \text{for} \quad p \geq 8663 \;\Big|\; \frac{\langle a_2, L'\rangle_{p^2}^{+,\mathrm{new}}}{\langle a_1, L'\rangle_{p^2}^{+,\mathrm{new}}} \in]0,1[\quad \text{for} \quad p \geq 167,$$

- After *ad hoc* computations for the remaining cases, quadratic Chabauty condition for a quotient is satisfied for *any* $X_0(p)^+$ or $X_{\mathrm{nsp}}^+(p)$ of genus at least two.

The final result

After optimising on the choice of Weil vs. Polya-Vinogradov, we get:

Theorem (LF, Siksek)

- We have

$$\frac{\langle a_2, L' \rangle_p^+}{\langle a_1, L' \rangle_p^+} \in]0,1[\quad \text{for} \quad p \geq 8663 \;\Bigg|\; \frac{\langle a_2, L' \rangle_{p^2}^{+,\text{new}}}{\langle a_1, L' \rangle_{p^2}^{+,\text{new}}} \in]0,1[\quad \text{for} \quad p \geq 167,$$

- After *ad hoc* computations for the remaining cases, quadratic Chabauty condition for a quotient is satisfied for *any* $X_0(p)^+$ or $X_{\text{nsp}}^+(p)$ of genus at least two.

Perspectives

The final result

After optimising on the choice of Weil vs. Polya-Vinogradov, we get:

Theorem (LF, Siksek)

- We have

$$\frac{\langle a_2, L'\rangle_p^+}{\langle a_1, L'\rangle_p^+} \in]0,1[\quad \text{for} \quad p \geq 8663 \;\Bigg|\; \frac{\langle a_2, L'\rangle_{p^2}^{+,\mathrm{new}}}{\langle a_1, L'\rangle_{p^2}^{+,\mathrm{new}}} \in]0,1[\quad \text{for} \quad p \geq 167,$$

- After *ad hoc* computations for the remaining cases, quadratic Chabauty condition for a quotient is satisfied for *any* $X_0(p)^+$ or $X_{\mathrm{nsp}}^+(p)$ of genus at least two.

Perspectives

- Infinite families of jacobians satisfying quadratic Chabauty.

The final result

After optimising on the choice of Weil vs. Polya-Vinogradov, we get:

Theorem (LF, Siksek)

- We have

$$\frac{\langle a_2, L' \rangle_p^+}{\langle a_1, L' \rangle_p^+} \in]0,1[\quad \text{for} \quad p \geq 8663 \;\Big|\; \frac{\langle a_2, L' \rangle_{p^2}^{+,\mathrm{new}}}{\langle a_1, L' \rangle_{p^2}^{+,\mathrm{new}}} \in]0,1[\quad \text{for} \quad p \geq 167,$$

- After *ad hoc* computations for the remaining cases, quadratic Chabauty condition for a quotient is satisfied for *any* $X_0(p)^+$ or $X_{\mathrm{nsp}}^+(p)$ of genus at least two.

Perspectives

- Infinite families of jacobians satisfying quadratic Chabauty.
- Devise a "quadratic Mazur's method".