Rational points on modular curves

(Advancement to Candidacy)

Chris Xu
chx007@ucsd.edu

UC San Diego

April 7th, 2025

Equation solving

Given polynomial $f(x, y) = 0$, find its rational solutions!
That is, given a smooth projective curve $X/\mathbf{Q}$, find $X(\mathbf{Q})$.

Example

Let $f(x, y) := x^2 + y^2 - 1$.
The rational solutions classify Pythagorean triples.

Example

Let $f_n(x, y) := y^2 - x^3 + n^2 x$ for $n \in \mathbf{N}$.
The rational solutions classify right triangles of area n with rational side lengths.

Example

Let $f(x, y) := y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y$. The rational solutions classify elliptic curves with "non-split level 13 structure".

Equation solving

Given polynomial $f(x, y) = 0$, find its rational solutions!
That is, given a smooth projective curve $X/\mathbf{Q}$, find $X(\mathbf{Q})$.

Example

Let $f(x, y) := x^2 + y^2 - 1$.
The rational solutions classify Pythagorean triples.

Example

Let $f_n(x, y) := y^2 - x^3 + n^2 x$ for $n \in \mathbf{N}$.
The rational solutions classify right triangles of area n with rational side lengths.

Example

Let $f(x, y) := y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y$. The rational solutions classify elliptic curves with "non-split level 13 structure".

Equation solving

Given polynomial $f(x,y)=0$, find its rational solutions!
That is, given a smooth projective curve $X/\mathbf{Q}$, find $X(\mathbf{Q})$.

Example

Let $f(x,y) := x^2+y^2-1$.
The rational solutions classify Pythagorean triples.

Example

Let $f_n(x,y) := y^2-x^3+n^2x$ for $n \in \mathbf{N}$.
The rational solutions classify right triangles of area n with rational side lengths.

Example

Let $f(x,y) := y^4+5x^4-6x^2y^2+6x^3+26x^2y+10xy^2-10y^3-32x^2-40xy+24y^2+32x-16y$. The rational solutions classify elliptic curves with "non-split level 13 structure".

Equation solving

Given polynomial $f(x, y) = 0$, find its rational solutions!
That is, given a smooth projective curve $X/\mathbf{Q}$, find $X(\mathbf{Q})$.

Example

Let $f(x, y) := x^2 + y^2 - 1$.
The rational solutions classify Pythagorean triples.

Example

Let $f_n(x, y) := y^2 - x^3 + n^2 x$ for $n \in \mathbf{N}$.
The rational solutions classify right triangles of area n with rational side lengths.

Example

Let $f(x, y) := y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y$. The rational solutions classify elliptic curves with "non-split level 13 structure".

Equation solving

Given polynomial $f(x, y) = 0$, find its rational solutions!
That is, given a smooth projective curve $X/\mathbf{Q}$, find $X(\mathbf{Q})$.

Example

Let $f(x, y) := x^2 + y^2 - 1$.
The rational solutions classify Pythagorean triples.

Example

Let $f_n(x, y) := y^2 - x^3 + n^2 x$ for $n \in \mathbf{N}$.
The rational solutions classify right triangles of area n with rational side lengths.

Example

Let $f(x, y) := y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y$. The rational solutions classify elliptic curves with "non-split level 13 structure".

Equation solving

Given polynomial $f(x, y) = 0$, find its rational solutions!
That is, given a smooth projective curve $X/\mathbf{Q}$, find $X(\mathbf{Q})$.

Example

Let $f(x, y) := x^2 + y^2 - 1$.
The rational solutions classify Pythagorean triples.

Example

Let $f_n(x, y) := y^2 - x^3 + n^2 x$ for $n \in \mathbf{N}$.
The rational solutions classify right triangles of area n with rational side lengths.

Example

Let $f(x, y) := y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y$. The rational solutions classify elliptic curves with "non-split level 13 structure".

Genera

Around the 1920s, it emerged that curves could be put into three classes of increasing complexity: genus 0, genus 1, and genus ≥ 2. My research deals with explicit methods for determining rational points in the genus ≥ 2 case.

Genera

Around the 1920s, it emerged that curves could be put into three classes of increasing complexity: genus 0, genus 1, and genus ≥ 2. My research deals with explicit methods for determining rational points in the genus ≥ 2 case.

Genus 0

In this case, everything is $\mathbf{P}^1$ when viewed over $\mathbf{C}$. If a rational point exists, all other rational points are determined by rational slope chords.

Example

Consider $x^2 + y^2 = 1$.
Take $(1, 0)$. Then all other points are determined by rational slope lines emanating from $(1, 0)$.

Genus 0

In this case, everything is $\mathbf{P}^1$ when viewed over $\mathbf{C}$. If a rational point exists, all other rational points are determined by rational slope chords.

Example

Consider $x^2 + y^2 = 1$.
Take $(1, 0)$. Then all other points are determined by rational slope lines emanating from $(1, 0)$.

Genus 0

In this case, everything is $\mathbf{P}^1$ when viewed over $\mathbf{C}$. If a rational point exists, all other rational points are determined by rational slope chords.

Example

Consider $x^2 + y^2 = 1$.
Take $(1, 0)$. Then all other points are determined by rational slope lines emanating from $(1, 0)$.

Genus 0

In this case, everything is $\mathbf{P}^1$ when viewed over $\mathbf{C}$. If a rational point exists, all other rational points are determined by rational slope chords.

Example

Consider $x^2 + y^2 = 1$.
Take $(1, 0)$. Then all other points are determined by rational slope lines emanating from $(1, 0)$.

Genus 1

Elliptic curves E. There is a group law ("three collinear points sum to zero").

Theorem (Mordell, 1922)

We have $E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus T$ for some r, where T is finite.

The group T has been completely classified (Mazur). There is an algorithm to compute $E(\mathbf{Q})$. But r remains very mysterious.

Example

Consider $y^2 = x^3 - n^2 x$ as n varies over integers. Note that they are all isomorphic to each other over $\mathbf{C}$, but not over $\mathbf{Q}$! (More on this later.) Recent progress on the behavior of r by A. Smith (2017-2022).

Genus 1

Elliptic curves E. There is a group law ("three collinear points sum to zero").

Theorem (Mordell, 1922)

We have $E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus T$ for some r, where T is finite.

The group T has been completely classified (Mazur). There is an algorithm to compute $E(\mathbf{Q})$. But r remains very mysterious.

Example

Consider $y^2 = x^3 - n^2 x$ as n varies over integers. Note that they are all isomorphic to each other over $\mathbf{C}$, but not over $\mathbf{Q}$! (More on this later.) Recent progress on the behavior of r by A. Smith (2017-2022).

Genus 1

Elliptic curves E. There is a group law ("three collinear points sum to zero").

Theorem (Mordell, 1922)

We have $E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus T$ for some r, where T is finite.

The group T has been completely classified (Mazur). There is an algorithm to compute $E(\mathbf{Q})$. But r remains very mysterious.

Example

Consider $y^2 = x^3 - n^2 x$ as n varies over integers. Note that they are all isomorphic to each other over $\mathbf{C}$, but not over $\mathbf{Q}$! (More on this later.) Recent progress on the behavior of r by A. Smith (2017-2022).

Genus 1

Elliptic curves E. There is a group law ("three collinear points sum to zero").

Theorem (Mordell, 1922)

We have $E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus T$ for some r, where T is finite.

The group T has been completely classified (Mazur). There is an algorithm to compute $E(\mathbf{Q})$. But r remains very mysterious.

Example

Consider $y^2 = x^3 - n^2x$ as n varies over integers. Note that they are all isomorphic to each other over $\mathbf{C}$, but not over $\mathbf{Q}$! (More on this later.) Recent progress on the behavior of r by A. Smith (2017-2022).

Genus 1

Elliptic curves E. There is a group law ("three collinear points sum to zero").

Theorem (Mordell, 1922)

We have $E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus T$ for some r, where T is finite.

The group T has been completely classified (Mazur). There is an algorithm to compute $E(\mathbf{Q})$. But r remains very mysterious.

Example

Consider $y^2 = x^3 - n^2x$ as n varies over integers. Note that they are all isomorphic to each other over $\mathbf{C}$, but not over $\mathbf{Q}$! (More on this later.) Recent progress on the behavior of r by A. Smith (2017-2022).

Genus 1

Elliptic curves E. There is a group law ("three collinear points sum to zero").

Theorem (Mordell, 1922)

We have $E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus T$ for some r, where T is finite.

The group T has been completely classified (Mazur). There is an algorithm to compute $E(\mathbf{Q})$. But r remains very mysterious.

Example

Consider $y^2 = x^3 - n^2x$ as n varies over integers. Note that they are all isomorphic to each other over $\mathbf{C}$, but not over $\mathbf{Q}$! (More on this later.) Recent progress on the behavior of r by A. Smith (2017-2022).

Genus 1

Elliptic curves E. There is a group law ("three collinear points sum to zero").

Theorem (Mordell, 1922)

We have $E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus T$ for some r, where T is finite.

The group T has been completely classified (Mazur). There is an algorithm to compute $E(\mathbf{Q})$. But r remains very mysterious.

Example

Consider $y^2 = x^3 - n^2x$ as n varies over integers. Note that they are all isomorphic to each other over $\mathbf{C}$, but not over $\mathbf{Q}$! (More on this later.) Recent progress on the behavior of r by A. Smith (2017-2022).

Genus ≥ 2

Curves "of general type".

Theorem (Faltings, 1983)

Suppose $X/\mathbf{Q}$ has genus at least 2. Then $X(\mathbf{Q})$ is finite.

The most advanced tool we have for *determining* the rational solutions is a family of methods called (depth n) Chabauty, for $n \geq 1$.

Example

Consider $X : y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y = 0$, of genus 3. Determination of $X(\mathbf{Q})$ only happened in 2019 using quadratic Chabauty ($n =$ "$1 + \varepsilon$").

Genus ≥ 2

Curves "of general type".

Theorem (Faltings, 1983)

Suppose $X/\mathbf{Q}$ has genus at least 2. Then $X(\mathbf{Q})$ is finite.

The most advanced tool we have for *determining* the rational solutions is a family of methods called (depth n) Chabauty, for $n \geq 1$.

Example

Consider $X: y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y = 0$, of genus 3. Determination of $X(\mathbf{Q})$ only happened in 2019 using quadratic Chabauty ($n =$ "$1 + \varepsilon$").

Genus ≥ 2

Curves "of general type".

Theorem (Faltings, 1983)

Suppose $X/\mathbf{Q}$ has genus at least 2. Then $X(\mathbf{Q})$ is finite.

The most advanced tool we have for *determining* the rational solutions is a family of methods called (depth n) Chabauty, for $n \geq 1$.

Example

Consider $X : y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y = 0$, of genus 3. Determination of $X(\mathbf{Q})$ only happened in 2019 using quadratic Chabauty ($n =$ "$1 + \varepsilon$").

Genus ≥ 2

Curves "of general type".

Theorem (Faltings, 1983)

Suppose $X/\mathbf{Q}$ has genus at least 2. Then $X(\mathbf{Q})$ is finite.

The most advanced tool we have for *determining* the rational solutions is a family of methods called (depth n) Chabauty, for $n \geq 1$.

Example

Consider $X : y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y = 0$, of genus 3. Determination of $X(\mathbf{Q})$ only happened in 2019 using quadratic Chabauty ($n =$ "$1 + \varepsilon$").

Genus ≥ 2

Curves "of general type".

Theorem (Faltings, 1983)

Suppose $X/\mathbf{Q}$ has genus at least 2. Then $X(\mathbf{Q})$ is finite.

The most advanced tool we have for *determining* the rational solutions is a family of methods called (depth n) Chabauty, for $n \geq 1$.

Example

Consider $X : y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y = 0$, of genus 3. Determination of $X(\mathbf{Q})$ only happened in 2019 using quadratic Chabauty ($n =$ "$1 + \varepsilon$").

Chabauty's original theorem

Choose $b \in X(\mathbf{Q})$ and a prime p. Let J be the Jacobian[1] of X. There is a map $\mathrm{AJ}_b \colon X \to J$ given by $\mathrm{AJ}_b(x) := [x - b]$.

$$\begin{array}{ccc} X(\mathbf{Q}) & \hookrightarrow & X(\mathbf{Q}_p) \\ \downarrow \mathrm{AJ}_b & & \downarrow \mathrm{AJ}_b \\ J(\mathbf{Q}) & \hookrightarrow & J(\mathbf{Q}_p) \end{array}$$

Chabauty's idea: if $J(\mathbf{Q})$ is *not* Zariski dense in $J(\mathbf{Q}_p)$, then $J(\mathbf{Q}) \cap X(\mathbf{Q}_p)$ is a finite set containing $X(\mathbf{Q})$.

Theorem (Chabauty, 1941)

Let $g := \dim(J)$ *and* $r := \mathrm{rk}_{\mathbf{Z}}(J(\mathbf{Q}))$.
Then $X(\mathbf{Q})$ *is finite, provided that* $r < g$ *holds.*

[1] The Jacobian is an abelian variety parametrizing the degree 0 divisors on X. Its dimension is g, the genus of X. An abelian variety is a "higher dimensional elliptic curve". There is a generalization of Mordell-Weil to abelian varieties.

Chabauty's original theorem

Choose $b \in X(\mathbf{Q})$ and a prime p. Let J be the Jacobian[1] of X.
There is a map $\mathrm{AJ}_b \colon X \to J$ given by $\mathrm{AJ}_b(x) := [x - b]$.

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_b"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_b"] \\ J(\mathbf{Q}) \arrow[r, hook] & J(\mathbf{Q}_p) \end{tikzcd}$$

Chabauty's idea: if $J(\mathbf{Q})$ is *not* Zariski dense in $J(\mathbf{Q}_p)$, then $\overline{J(\mathbf{Q})} \cap X(\mathbf{Q}_p)$ is a finite set containing $X(\mathbf{Q})$.

Theorem (Chabauty, 1941)

Let $g := \dim(J)$ and $r := \mathrm{rk}_{\mathbf{Z}}(J(\mathbf{Q}))$.
Then $X(\mathbf{Q})$ is finite, provided that $r < g$ holds.

[1] The Jacobian is an abelian variety parametrizing the degree 0 divisors on X. Its dimension is g, the genus of X. An abelian variety is a "higher dimensional elliptic curve". There is a generalization of Mordell-Weil to abelian varieties.

Chabauty's original theorem

Choose $b \in X(\mathbf{Q})$ and a prime p. Let J be the Jacobian[1] of X. There is a map $\mathrm{AJ}_b \colon X \to J$ given by $\mathrm{AJ}_b(x) := [x - b]$.

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_b"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_b"] \\ J(\mathbf{Q}) \arrow[r, hook] & J(\mathbf{Q}_p) \end{tikzcd}$$

Chabauty's idea: if $J(\mathbf{Q})$ is *not* Zariski dense in $J(\mathbf{Q}_p)$, then $J(\mathbf{Q}) \cap X(\mathbf{Q}_p)$ is a finite set containing $X(\mathbf{Q})$.

Theorem (Chabauty, 1941)

Let $g := \dim(J)$ and $r := \mathrm{rk}_{\mathbf{Z}}(J(\mathbf{Q}))$. Then $X(\mathbf{Q})$ is finite, provided that $r < g$ holds.

[1] The Jacobian is an abelian variety parametrizing the degree 0 divisors on X. Its dimension is g, the genus of X. An abelian variety is a "higher dimensional elliptic curve". There is a generalization of Mordell-Weil to abelian varieties.

Chabauty's original theorem

Choose $b \in X(\mathbf{Q})$ and a prime p. Let J be the Jacobian[1] of X. There is a map $\mathrm{AJ}_b \colon X \to J$ given by $\mathrm{AJ}_b(x) := [x - b]$.

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_b"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_b"] \\ J(\mathbf{Q}) \arrow[r, hook] & J(\mathbf{Q}_p) \end{tikzcd}$$

Chabauty's idea: if $J(\mathbf{Q})$ is *not* Zariski dense in $J(\mathbf{Q}_p)$, then $J(\mathbf{Q}) \cap X(\mathbf{Q}_p)$ is a finite set containing $X(\mathbf{Q})$.

Theorem (Chabauty, 1941)

Let $g := \dim(J)$ and $r := \mathrm{rk}_{\mathbf{Z}}(J(\mathbf{Q}))$. Then $X(\mathbf{Q})$ is finite, provided that $r < g$ holds.

[1] The Jacobian is an abelian variety parametrizing the degree 0 divisors on X. Its dimension is g, the genus of X. An abelian variety is a "higher dimensional elliptic curve". There is a generalization of Mordell-Weil to abelian varieties.

Chabauty's original theorem

Choose $b \in X(\mathbf{Q})$ and a prime p. Let J be the Jacobian[1] of X. There is a map $\mathrm{AJ}_b \colon X \to J$ given by $\mathrm{AJ}_b(x) := [x - b]$.

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_b"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_b"] \\ J(\mathbf{Q}) \arrow[r, hook] & J(\mathbf{Q}_p) \end{tikzcd}$$

Chabauty's idea: if $J(\mathbf{Q})$ is *not* Zariski dense in $J(\mathbf{Q}_p)$, then $\overline{J(\mathbf{Q})} \cap X(\mathbf{Q}_p)$ is a finite set containing $X(\mathbf{Q})$.

Theorem (Chabauty, 1941)

Let $g := \dim(J)$ and $r := \mathrm{rk}_{\mathbf{Z}}(J(\mathbf{Q}))$. Then $X(\mathbf{Q})$ is finite, provided that $r < g$ holds.

[1] The Jacobian is an abelian variety parametrizing the degree 0 divisors on X. Its dimension is g, the genus of X. An abelian variety is a "higher dimensional elliptic curve". There is a generalization of Mordell-Weil to abelian varieties.

Chabauty's original theorem

Choose $b \in X(\mathbf{Q})$ and a prime p. Let J be the Jacobian[1] of X. There is a map $\mathrm{AJ}_b \colon X \to J$ given by $\mathrm{AJ}_b(x) := [x - b]$.

$$\begin{array}{ccc} X(\mathbf{Q}) & \hookrightarrow & X(\mathbf{Q}_p) \\ \downarrow{\scriptstyle \mathrm{AJ}_b} & & \downarrow{\scriptstyle \mathrm{AJ}_b} \\ J(\mathbf{Q}) & \hookrightarrow & J(\mathbf{Q}_p) \end{array}$$

Chabauty's idea: if $J(\mathbf{Q})$ is *not* Zariski dense in $J(\mathbf{Q}_p)$, then $J(\mathbf{Q}) \cap X(\mathbf{Q}_p)$ is a finite set containing $X(\mathbf{Q})$.

Theorem (Chabauty, 1941)

Let $g := \dim(J)$ *and* $r := \mathrm{rk}_{\mathbf{Z}}(J(\mathbf{Q}))$.
Then $X(\mathbf{Q})$ *is finite, provided that* $r < g$ *holds.*

[1] The Jacobian is an abelian variety parametrizing the degree 0 divisors on X. Its dimension is g, the genus of X. An abelian variety is a "higher dimensional elliptic curve". There is a generalization of Mordell-Weil to abelian varieties.

Chabauty's original theorem

Choose $b \in X(\mathbf{Q})$ and a prime p. Let J be the Jacobian[1] of X. There is a map $\mathrm{AJ}_b \colon X \to J$ given by $\mathrm{AJ}_b(x) := [x - b]$.

$$\begin{array}{ccc} X(\mathbf{Q}) & \hookrightarrow & X(\mathbf{Q}_p) \\ \downarrow{\scriptstyle \mathrm{AJ}_b} & & \downarrow{\scriptstyle \mathrm{AJ}_b} \\ J(\mathbf{Q}) & \hookrightarrow & J(\mathbf{Q}_p) \end{array}$$

Chabauty's idea: if $J(\mathbf{Q})$ is *not* Zariski dense in $J(\mathbf{Q}_p)$, then $J(\mathbf{Q}) \cap X(\mathbf{Q}_p)$ is a finite set containing $X(\mathbf{Q})$.

Theorem (Chabauty, 1941)

Let $g := \dim(J)$ and $r := \mathrm{rk}_{\mathbf{Z}}(J(\mathbf{Q}))$.
Then $X(\mathbf{Q})$ is finite, provided that $r < g$ holds.

[1] The Jacobian is an abelian variety parametrizing the degree 0 divisors on X. Its dimension is g, the genus of X. An abelian variety is a "higher dimensional elliptic curve". There is a generalization of Mordell-Weil to abelian varieties.

Coleman's algorithmic interpretation

In the 1980s, Coleman makes Chabauty's ideas into an algorithm by introducing a gadget called a Coleman integral[2].

First, consider the diagram

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_b"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_b"] \arrow[dr, dotted] & \\ J(\mathbf{Q}) \arrow[r, hook] & J(\mathbf{Q}_p) \arrow[r, "\log"] & H^0(X, \Omega^1)^\vee \end{tikzcd}$$

where $\log(D) := \left[\omega \mapsto \int_D \omega\right]$

Next, find a basis of *annihilating differentials*[3] $\omega_1, \ldots, \omega_{g-r}$.

Finally, $X(\mathbf{Q})$ is contained in the finite set given by the locus

$$\int_b^t \omega_1 = \cdots = \int_b^t \omega_{g-r} = 0. \qquad \text{(all are power series in the variable } t.\text{)}$$

[2] A Coleman integral $\int_D \omega$ pairs a divisor $D \in J(\mathbf{Q}_p)$ with a 1-form ω. It behaves like an antiderivative if D is all on a single mod p "residue disk", and otherwise one "extends by Frobenius".

[3] i.e. a 1-form ω such that $\int_D \omega = 0$ for any $D \in J(\mathbf{Q})$

Coleman's algorithmic interpretation

In the 1980s, Coleman makes Chabauty's ideas into an algorithm by introducing a gadget called a Coleman integral[2].
First, consider the diagram

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_b"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_b"] \arrow[dr, dotted] & \\
J(\mathbf{Q}) \arrow[r, hook] & J(\mathbf{Q}_p) \arrow[r, "\log"] & H^0(X, \Omega^1)^\vee
\end{tikzcd}$$

where $\log(D) := \left[\omega \mapsto \int_D \omega\right]$

Next, find a basis of *annihilating differentials*[3] $\omega_1, \ldots, \omega_{g-r}$.
Finally, $X(\mathbf{Q})$ is contained in the finite set given by the locus

$$\int_b^t \omega_1 = \cdots = \int_b^t \omega_{g-r} = 0. \qquad \text{(all are power series in the variable } t.\text{)}$$

[2] A Coleman integral $\int_D \omega$ pairs a divisor $D \in J(\mathbf{Q}_p)$ with a 1-form ω. It behaves like an antiderivative if D is all on a single mod p "residue disk", and otherwise one "extends by Frobenius".

[3] i.e. a 1-form ω such that $\int_D \omega = 0$ for any $D \in J(\mathbf{Q})$

Coleman's algorithmic interpretation

In the 1980s, Coleman makes Chabauty's ideas into an algorithm by introducing a gadget called a Coleman integral[2].
First, consider the diagram

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_b"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_b"] \arrow[dr, dotted] & \\ J(\mathbf{Q}) \arrow[r, hook] & J(\mathbf{Q}_p) \arrow[r, "\log"] & H^0(X, \Omega^1)^\vee \end{tikzcd}$$

where $\log(D) := \left[\omega \mapsto \int_D \omega\right]$

Next, find a basis of *annihilating differentials*[3] $\omega_1, \ldots, \omega_{g-r}$.
Finally, $X(\mathbf{Q})$ is contained in the finite set given by the locus

$$\int_b^t \omega_1 = \cdots = \int_b^t \omega_{g-r} = 0. \qquad \text{(all are power series in the variable } t.)$$

---

[2] A Coleman integral $\int_D \omega$ pairs a divisor $D \in J(\mathbf{Q}_p)$ with a 1-form ω. It behaves like an antiderivative if D is all on a single mod p "residue disk", and otherwise one "extends by Frobenius".

[3] i.e. a 1-form ω such that $\int_D \omega = 0$ for any $D \in J(\mathbf{Q})$.

Coleman's algorithmic interpretation

In the 1980s, Coleman makes Chabauty's ideas into an algorithm by introducing a gadget called a Coleman integral[2].
First, consider the diagram

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_b"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_b"] \arrow[dr, dotted] & \\ J(\mathbf{Q}) \arrow[r, hook] & J(\mathbf{Q}_p) \arrow[r, "\log"] & H^0(X, \Omega^1)^\vee \end{tikzcd}$$

where $\log(D) := \left[\omega \mapsto \int_D \omega\right]$

Next, find a basis of *annihilating differentials*[3] $\omega_1, \ldots, \omega_{g-r}$.
Finally, $X(\mathbf{Q})$ is contained in the finite set given by the locus

$$\int_b^t \omega_1 = \cdots = \int_b^t \omega_{g-r} = 0. \qquad \text{(all are power series in the variable } t.\text{)}$$

[2] A Coleman integral $\int_D \omega$ pairs a divisor $D \in J(\mathbf{Q}_p)$ with a 1-form ω. It behaves like an antiderivative if D is all on a single mod p "residue disk", and otherwise one "extends by Frobenius".

[3] i.e. a 1-form ω such that $\int_D \omega = 0$ for any $D \in J(\mathbf{Q})$.

Kim's nonabelian refinement

What if we do not have $r < g$? In the 2000s, Kim proposes replacing J with a "depth n Selmer variety" $\mathrm{Sel}(\mathrm{U}_n)$ associated to U_n[4].

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[drr, dotted] & & \\ \mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[rr, "\mathrm{D}_{\mathrm{dR}}"] & & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0 \end{tikzcd}$$

Here, $\mathrm{AJ}_{b,n}$ sends x to a "non-abelian" path $[P_{x,b}]$, which is a torsor of $\mathrm{U}_n = P_{x,x}$. The condition $r < g$ gets weaker as n increases.

Conjecture (Kim, 2005)

For any curve $X/\mathbf{Q}$, there is a large enough n such that $\mathrm{Sel}(\mathrm{U}_n)(\mathbf{Q}_p) \cap X(\mathbf{Q}_p) = X(\mathbf{Q})$.

[4] Consider the $\mathbf{Q}_p$-algebraic fundamental group of the Tannakian category of finite étale covers (resp. unipotent connections) on $X_{\mathbf{C}_p}$. Then U_n (resp. $\mathrm{U}_n^{\mathrm{dR}}$) is its maximal n-unipotent quotient.

Kim's nonabelian refinement

What if we do not have $r < g$? In the 2000s, Kim proposes replacing J with a "depth n Selmer variety" $\mathrm{Sel}(\mathrm{U}_n)$ associated to U_n[4].

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[drr, dotted] & & \\
\mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[rr, "\mathrm{D}_{\mathrm{dR}}"] & & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0
\end{tikzcd}$$

Here, $\mathrm{AJ}_{b,n}$ sends x to a "non-abelian" path $[P_{x,b}]$, which is a torsor of $\mathrm{U}_n = P_{x,x}$. The condition $r < g$ gets weaker as n increases.

Conjecture (Kim, 2005)

For any curve $X/\mathbf{Q}$, there is a large enough n such that $\mathrm{Sel}(\mathrm{U}_n)(\mathbf{Q}_p) \cap X(\mathbf{Q}_p) = X(\mathbf{Q})$.

[4] Consider the $\mathbf{Q}_p$-algebraic fundamental group of the Tannakian category of finite étale covers (resp. unipotent connections) on $X_{\mathbf{C}_p}$. Then U_n (resp. $\mathrm{U}_n^{\mathrm{dR}}$) is its maximal n-unipotent quotient.

Kim's nonabelian refinement

What if we do not have $r < g$? In the 2000s, Kim proposes replacing J with a "depth n Selmer variety" $\mathrm{Sel}(\mathrm{U}_n)$ associated to U_n[4].

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[drr, dotted] & & \\
\mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[rr, "\mathbf{D}_{\mathrm{dR}}"] & & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0
\end{tikzcd}$$

Here, $\mathrm{AJ}_{b,n}$ sends x to a "non-abelian" path $[P_{x,b}]$, which is a torsor of $\mathrm{U}_n = P_{x,x}$. The condition $r < g$ gets weaker as n increases.

Conjecture (Kim, 2005)

For any curve $X/\mathbf{Q}$, there is a large enough n such that $\mathrm{Sel}(\mathrm{U}_n)(\mathbf{Q}_p) \cap X(\mathbf{Q}_p) = X(\mathbf{Q})$.

[4] Consider the $\mathbf{Q}_p$-algebraic fundamental group of the Tannakian category of finite étale covers (resp. unipotent connections) on $X_{\mathbf{C}_p}$. Then U_n (resp. $\mathrm{U}_n^{\mathrm{dR}}$) is its maximal n-unipotent quotient.

Kim's nonabelian refinement

What if we do not have $r < g$? In the 2000s, Kim proposes replacing J with a "depth n Selmer variety" $\mathrm{Sel}(\mathrm{U}_n)$ associated to U_n[4].

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[dr, dotted] & \\
\mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[r, "\mathbf{D}_{\mathrm{dR}}"] & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0
\end{tikzcd}$$

Here, $\mathrm{AJ}_{b,n}$ sends x to a "non-abelian" path $[P_{x,b}]$, which is a torsor of $\mathrm{U}_n = P_{x,x}$. The condition $r < g$ gets weaker as n increases.

Conjecture (Kim, 2005)

For any curve $X/\mathbf{Q}$, there is a large enough n such that $\mathrm{Sel}(\mathrm{U}_n)(\mathbf{Q}_p) \cap X(\mathbf{Q}_p) = X(\mathbf{Q})$.

[4] Consider the $\mathbf{Q}_p$-algebraic fundamental group of the Tannakian category of finite étale covers (resp. unipotent connections) on $X_{\mathbf{C}_p}$. Then U_n (resp. $\mathrm{U}_n^{\mathrm{dR}}$) is its maximal n-unipotent quotient.

Kim's nonabelian refinement

What if we do not have $r < g$? In the 2000s, Kim proposes replacing J with a "depth n Selmer variety" $\mathrm{Sel}(\mathrm{U}_n)$ associated to U_n[4].

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[dr, dotted] & \\
\mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[r, "\mathbf{D}_{\mathrm{dR}}"] & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0
\end{tikzcd}$$

Here, $\mathrm{AJ}_{b,n}$ sends x to a "non-abelian" path $[P_{x,b}]$, which is a torsor of $\mathrm{U}_n = P_{x,x}$. The condition $r < g$ gets weaker as n increases.

Conjecture (Kim, 2005)

For any curve $X/\mathbf{Q}$, there is a large enough n such that $\mathrm{Sel}(\mathrm{U}_n)(\mathbf{Q}_p) \cap X(\mathbf{Q}_p) = X(\mathbf{Q})$.

[4] Consider the $\mathbf{Q}_p$-algebraic fundamental group of the Tannakian category of finite étale covers (resp. unipotent connections) on $X_{\mathbf{C}_p}$. Then U_n (resp. $\mathrm{U}_n^{\mathrm{dR}}$) is its maximal n-unipotent quotient.

Kim's nonabelian refinement

What if we do not have $r < g$? In the 2000s, Kim proposes replacing J with a "depth n Selmer variety" $\mathrm{Sel}(\mathrm{U}_n)$ associated to U_n[4].

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[dr, dotted] & \\
\mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[r, "\mathbf{D}_{\mathrm{dR}}"] & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0
\end{tikzcd}$$

Here, $\mathrm{AJ}_{b,n}$ sends x to a "non-abelian" path $[P_{x,b}]$, which is a torsor of $\mathrm{U}_n = P_{x,x}$. The condition $r < g$ gets weaker as n increases.

Conjecture (Kim, 2005)

For any curve $X/\mathbf{Q}$, there is a large enough n such that $\mathrm{Sel}(\mathrm{U}_n)(\mathbf{Q}_p) \cap X(\mathbf{Q}_p) = X(\mathbf{Q})$.

[4] Consider the $\mathbf{Q}_p$-algebraic fundamental group of the Tannakian category of finite étale covers (resp. unipotent connections) on $X_{\mathbf{C}_p}$. Then U_n (resp. $\mathrm{U}_n^{\mathrm{dR}}$) is its maximal n-unipotent quotient.

Algorithmic interpretations of Chabauty-Kim

Consider the diagram:

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[drr, dotted] & & \\ \mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[rr, "\mathbf{D}_{\mathrm{dR}}"] & & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0 \end{tikzcd}$$

Making Chabauty-Kim explicit relies on finding coordinates on the variety $\mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0$. You end up with n-fold Coleman integrals.

- (1985) For $n = 1$, the 1-forms give coordinates on $H^0(X, \Omega^1)^\vee$.
- (2016) The quadratic Chabauty method of Balakrishnan-Dogra gives a coordinate for $n =$ "$1 + \varepsilon$" coming from arithmetic intersection theory.
- (2021) Corwin's motivic Chabauty gives a coordinate for arbitrary n using a "universal cocycle evaluation map".

Algorithmic interpretations of Chabauty-Kim

Consider the diagram:

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[dr, dotted] & \\
\mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[r, "\mathbf{D}_{\mathrm{dR}}"] & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0
\end{tikzcd}$$

Making Chabauty-Kim explicit relies on finding coordinates on the variety $\mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0$. You end up with n-fold Coleman integrals.

- (1985) For $n = 1$, the 1-forms give coordinates on $H^0(X, \Omega^1)^\vee$.
- (2016) The quadratic Chabauty method of Balakrishnan-Dogra gives a coordinate for $n =$ "$1 + \varepsilon$" coming from arithmetic intersection theory.
- (2021) Corwin's motivic Chabauty gives a coordinate for arbitrary n using a "universal cocycle evaluation map".

Algorithmic interpretations of Chabauty-Kim

Consider the diagram:

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[dr, dotted] & \\ \mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[r, "\mathbf{D}_{\mathrm{dR}}"] & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0 \end{tikzcd}$$

Making Chabauty-Kim explicit relies on finding coordinates on the variety $\mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0$. You end up with n-fold Coleman integrals.

- (1985) For $n = 1$, the 1-forms give coordinates on $H^0(X, \Omega^1)^\vee$.
- (2016) The quadratic Chabauty method of Balakrishnan-Dogra gives a coordinate for $n =$ "$1 + \varepsilon$" coming from arithmetic intersection theory.
- (2021) Corwin's motivic Chabauty gives a coordinate for arbitrary n using a "universal cocycle evaluation map".

Algorithmic interpretations of Chabauty-Kim

Consider the diagram:

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[dr, dotted] & \\
\mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[r, "\mathbf{D}_{\mathrm{dR}}"] & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0
\end{tikzcd}$$

Making Chabauty-Kim explicit relies on finding coordinates on the variety $\mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0$. You end up with n-fold Coleman integrals.

- (1985) For $n = 1$, the 1-forms give coordinates on $H^0(X, \Omega^1)^\vee$.
- (2016) The quadratic Chabauty method of Balakrishnan-Dogra gives a coordinate for $n =$ “$1 + \varepsilon$” coming from arithmetic intersection theory.
- (2021) Corwin's motivic Chabauty gives a coordinate for arbitrary n using a “universal cocycle evaluation map”.

Algorithmic interpretations of Chabauty-Kim

Consider the diagram:

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[dr, dotted] & \\ \mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[r, "\mathbf{D}_{\mathrm{dR}}"] & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0 \end{tikzcd}$$

Making Chabauty-Kim explicit relies on finding coordinates on the variety $\mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0$. You end up with n-fold Coleman integrals.

- (1985) For $n = 1$, the 1-forms give coordinates on $H^0(X, \Omega^1)^\vee$.
- (2016) The quadratic Chabauty method of Balakrishnan-Dogra gives a coordinate for $n =$ "$1 + \varepsilon$" coming from arithmetic intersection theory.
- (2021) Corwin's motivic Chabauty gives a coordinate for arbitrary n using a "universal cocycle evaluation map".

Algorithmic interpretations of Chabauty-Kim

Consider the diagram:

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[dr, dotted] & \\ \mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[r, "\mathbf{D}_{\mathrm{dR}}"] & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0 \end{tikzcd}$$

Making Chabauty-Kim explicit relies on finding coordinates on the variety $\mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0$. You end up with n-fold Coleman integrals.

- (1985) For $n = 1$, the 1-forms give coordinates on $H^0(X, \Omega^1)^\vee$.
- (2016) The quadratic Chabauty method of Balakrishnan-Dogra gives a coordinate for $n =$ "$1 + \varepsilon$" coming from arithmetic intersection theory.
- (2021) Corwin's motivic Chabauty gives a coordinate for arbitrary n using a "universal cocycle evaluation map".

Algorithmic interpretations of Chabauty-Kim

Consider the diagram:

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r, hook] \arrow[d, "\mathrm{AJ}_{b,n}"] & X(\mathbf{Q}_p) \arrow[d, "\mathrm{AJ}_{b,n}"] \arrow[dr, dotted] & \\
\mathrm{Sel}(\mathrm{U}_n) \arrow[r, hook] & \mathrm{H}^1_f(\mathrm{Gal}_{\mathbf{Q}_p}, \mathrm{U}_n) \arrow[r, "\mathbf{D}_{\mathrm{dR}}"] & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0
\end{tikzcd}$$

Making Chabauty-Kim explicit relies on finding coordinates on the variety $\mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0$. You end up with n-fold Coleman integrals.

- (1985) For $n = 1$, the 1-forms give coordinates on $H^0(X, \Omega^1)^\vee$.
- (2016) The quadratic Chabauty method of Balakrishnan-Dogra gives a coordinate for $n =$ "$1 + \varepsilon$" coming from arithmetic intersection theory.
- (2021) Corwin's motivic Chabauty gives a coordinate for arbitrary n using a "universal cocycle evaluation map".

Twists

Over $\mathbf{C}$, elliptic curves E are classified by their j-invariant, $j(E) \in \mathbf{C}$.
However, elliptic curves can be isomorphic over $\mathbf{C}$ but not over $\mathbf{Q}$.
This is the phenomenon of twists, caused by the fact that $A_E := \mathrm{Aut}_{\mathbf{C}}(E)$ is nontrivial:

$$A_E = \begin{cases} \mathbf{Z}/6\mathbf{Z} & j(E) = 0 \\ \mathbf{Z}/4\mathbf{Z} & j(E) = 1728 \\ \mathbf{Z}/2\mathbf{Z} & j(E) \notin \{0, 1728\}. \end{cases}$$

Twists

Over $\mathbf{C}$, elliptic curves E are classified by their j-invariant, $j(E) \in \mathbf{C}$. However, elliptic curves can be isomorphic over $\mathbf{C}$ but not over $\mathbf{Q}$. This is the phenomenon of twists, caused by the fact that $A_E := \mathrm{Aut}_{\mathbf{C}}(E)$ is nontrivial:

$$A_E = \begin{cases} \mathbf{Z}/6\mathbf{Z} & j(E) = 0 \\ \mathbf{Z}/4\mathbf{Z} & j(E) = 1728 \\ \mathbf{Z}/2\mathbf{Z} & j(E) \notin \{0, 1728\}. \end{cases}$$

Twists

Over $\mathbf{C}$, elliptic curves E are classified by their j-invariant, $j(E) \in \mathbf{C}$. However, elliptic curves can be isomorphic over $\mathbf{C}$ but not over $\mathbf{Q}$. This is the phenomenon of twists, caused by the fact that $A_E := \mathrm{Aut}_{\mathbf{C}}(E)$ is nontrivial:

$$A_E = \begin{cases} \mathbf{Z}/6\mathbf{Z} & j(E) = 0 \\ \mathbf{Z}/4\mathbf{Z} & j(E) = 1728 \\ \mathbf{Z}/2\mathbf{Z} & j(E) \notin \{0, 1728\}. \end{cases}$$

Twists

Over $\mathbf{C}$, elliptic curves E are classified by their j-invariant, $j(E) \in \mathbf{C}$. However, elliptic curves can be isomorphic over $\mathbf{C}$ but not over $\mathbf{Q}$. This is the phenomenon of twists, caused by the fact that $A_E := \mathrm{Aut}_{\mathbf{C}}(E)$ is nontrivial:

$$A_E = \begin{cases} \mathbf{Z}/6\mathbf{Z} & j(E) = 0 \\ \mathbf{Z}/4\mathbf{Z} & j(E) = 1728 \\ \mathbf{Z}/2\mathbf{Z} & j(E) \notin \{0, 1728\}. \end{cases}$$

Complex multiplication

If we consider the endomorphism ring $\mathrm{End}_{\mathbf{C}}(E)$, we find that it is either $\mathbf{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic field K.

We say that E has CM in the latter case. (For example, E has CM when $j(E) \in \{0, 1728\}$.)

Theorem (Early 1900s)

The maximal abelian extension of K is obtained by first adjoining $j(E)$, and then the coordinates of all the torsion points of E.

Complex multiplication

If we consider the endomorphism ring $\mathrm{End}_{\mathbf{C}}(E)$, we find that it is either $\mathbf{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic field K.
We say that E has CM in the latter case. (For example, E has CM when $j(E) \in \{0, 1728\}$.)

Theorem (Early 1900s)

The maximal abelian extension of K is obtained by first adjoining $j(E)$, and then the coordinates of all the torsion points of E.

Complex multiplication

If we consider the endomorphism ring $\mathrm{End}_{\mathbf{C}}(E)$, we find that it is either $\mathbf{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic field K.
We say that E has CM in the latter case. (For example, E has CM when $j(E) \in \{0, 1728\}$.)

Theorem (Early 1900s)

The maximal abelian extension of K is obtained by first adjoining $j(E)$, and then the coordinates of all the torsion points of E.

Complex multiplication

If we consider the endomorphism ring $\mathrm{End}_{\mathbf{C}}(E)$, we find that it is either $\mathbf{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic field K.
We say that E has CM in the latter case. (For example, E has CM when $j(E) \in \{0, 1728\}$.)

Theorem (Early 1900s)

The maximal abelian extension of K is obtained by first adjoining $j(E)$, and then the coordinates of all the torsion points of E.

Torsion points on elliptic curves

For an elliptic curve E over $\mathbf{C}$, it's a torus. So the group of N-torsion points $E[N](\mathbf{C})$ is just $(\mathbf{Z}/N\mathbf{Z})^2$.

Over $\mathbf{Q}$, there is now an action of $\mathrm{Gal}_{\mathbf{Q}}$. So we get a map $\rho\colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$.

If ρ is non-CM then its image will generally be close to being surjective.

If ρ is CM then its image will be very close to being abelian (cf. previous slide).

Torsion points on elliptic curves

For an elliptic curve E over $\mathbf{C}$, it's a torus. So the group of N-torsion points $E[N](\mathbf{C})$ is just $(\mathbf{Z}/N\mathbf{Z})^2$.
Over $\mathbf{Q}$, there is now an action of $\mathrm{Gal}_{\mathbf{Q}}$. So we get a map $\rho\colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$.
If ρ is non-CM then its image will generally be close to being surjective.
If ρ is CM then its image will be very close to being abelian (cf. previous slide).

Torsion points on elliptic curves

For an elliptic curve E over $\mathbf{C}$, it's a torus. So the group of N-torsion points $E[N](\mathbf{C})$ is just $(\mathbf{Z}/N\mathbf{Z})^2$.
Over $\mathbf{Q}$, there is now an action of $\mathrm{Gal}_{\mathbf{Q}}$. So we get a map $\rho\colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$.
If ρ is non-CM then its image will generally be close to being surjective.
If ρ is CM then its image will be very close to being abelian (cf. previous slide).

Torsion points on elliptic curves

For an elliptic curve E over $\mathbf{C}$, it's a torus. So the group of N-torsion points $E[N](\mathbf{C})$ is just $(\mathbf{Z}/N\mathbf{Z})^2$.
Over $\mathbf{Q}$, there is now an action of $\mathrm{Gal}_{\mathbf{Q}}$. So we get a map $\rho\colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$.
If ρ is non-CM then its image will generally be close to being surjective.
If ρ is CM then its image will be very close to being abelian (cf. previous slide).

Moduli spaces of elliptic curves

Let N be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$.
The modular curve Y_H parametrizes elliptic curves with H-level structure:

$$Y_H(\bar{k}) := \{(j(E), HgA_E) : j(E) \in \bar{k},\ g \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})\}$$
$$Y_H(k) := \{(j(E), HgA_E) : j(E) \in k,\ HgA_E = Hg\rho(\mathrm{Gal}_k)A_E\}.$$

The modular curve X_H is a compactification of Y_H, obtained by adding some finite number of "cusps".

Remark

Given an element of $X_H(k)$, you can always twist it so that the image of Galois lies in H.

Moduli spaces of elliptic curves

Let N be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$. The modular curve Y_H parametrizes elliptic curves with H-level structure:

$$Y_H(\bar{k}) := \{(j(E), HgA_E) : j(E) \in \bar{k},\ g \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})\}$$
$$Y_H(k) := \{(j(E), HgA_E) : j(E) \in k,\ HgA_E = Hg\rho(\mathrm{Gal}_k)A_E\}.$$

The modular curve X_H is a compactification of Y_H, obtained by adding some finite number of "cusps".

Remark

Given an element of $X_H(k)$, you can always twist it so that the image of Galois lies in H.

Moduli spaces of elliptic curves

Let N be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$. The modular curve Y_H parametrizes elliptic curves with H-level structure:

$$Y_H(\bar{k}) := \{(j(E), HgA_E) \colon j(E) \in \bar{k},\ g \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})\}$$
$$Y_H(k) := \{(j(E), HgA_E) \colon j(E) \in k,\ HgA_E = Hg\rho(\mathrm{Gal}_k)A_E\}.$$

The modular curve X_H is a compactification of Y_H, obtained by adding some finite number of "cusps".

Remark

Given an element of $X_H(k)$, you can always twist it so that the image of Galois lies in H.

Moduli spaces of elliptic curves

Let N be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$. The modular curve Y_H parametrizes elliptic curves with H-level structure:

$$Y_H(\bar{k}) := \{(j(E), HgA_E) : j(E) \in \bar{k},\ g \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})\}$$
$$Y_H(k) := \{(j(E), HgA_E) : j(E) \in k,\ HgA_E = Hg\rho(\mathrm{Gal}_k)A_E\}.$$

The modular curve X_H is a compactification of Y_H, obtained by adding some finite number of "cusps".

Remark

Given an element of $X_H(k)$, you can always twist it so that the image of Galois lies in H.

Moduli spaces of elliptic curves

Let N be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$. The modular curve Y_H parametrizes elliptic curves with H-level structure:

$$Y_H(\bar{k}) := \{(j(E), HgA_E) \colon j(E) \in \bar{k},\ g \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})\}$$
$$Y_H(k) := \{(j(E), HgA_E) \colon j(E) \in k,\ HgA_E = Hg\rho(\mathrm{Gal}_k)A_E\}.$$

The modular curve X_H is a compactification of Y_H, obtained by adding some finite number of "cusps".

Remark

Given an element of $X_H(k)$, you can always twist it so that the image of Galois lies in H.

Mazur's Program B

We can vary across all N to get a map[5] $\rho\colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\hat{\mathbf{Z}})$.

Theorem (Serre)

The image of ρ is open in $\mathrm{GL}_2(\hat{\mathbf{Z}})$.

You are led naturally to the following problem: classify all possible images of ρ for non-CM elliptic curves E. This is Mazur's Program B, proposed in the 1970s:

> *Classify the non-CM, non-cuspidal rational points of X_H, for open subgroups[6] $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$.*

In what follows, let us outline our proposed approach to resolve Mazur's Program B once and for all.

[5] Here, $\hat{\mathbf{Z}} := \varprojlim_N \mathbf{Z}/N\mathbf{Z}$, where the transition maps are the usual surjections $\mathbf{Z}/M\mathbf{Z} \twoheadrightarrow \mathbf{Z}/N\mathbf{Z}$ for $N \mid M$.

[6] Any open subgroup H comes from $H' \leq \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ for some integer N.

Mazur's Program B

We can vary across all N to get a map[5] $\rho\colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\hat{\mathbf{Z}})$.

Theorem (Serre)

The image of ρ is open in $\mathrm{GL}_2(\hat{\mathbf{Z}})$.

You are led naturally to the following problem: classify all possible images of ρ for non-CM elliptic curves E. This is Mazur's Program B, proposed in the 1970s:

> *Classify the non-CM, non-cuspidal rational points of X_H, for open subgroups[6] $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$.*

In what follows, let us outline our proposed approach to resolve Mazur's Program B once and for all.

[5] Here, $\hat{\mathbf{Z}} := \varprojlim_N \mathbf{Z}/N\mathbf{Z}$, where the transition maps are the usual surjections $\mathbf{Z}/M\mathbf{Z} \twoheadrightarrow \mathbf{Z}/N\mathbf{Z}$ for $N \mid M$.

[6] Any open subgroup H comes from $H' \leq \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ for some integer N.

Mazur's Program B

We can vary across all N to get a map[5] $\rho\colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\hat{\mathbf{Z}})$.

Theorem (Serre)

The image of ρ is open in $\mathrm{GL}_2(\hat{\mathbf{Z}})$.

You are led naturally to the following problem: classify all possible images of ρ for non-CM elliptic curves E. This is Mazur's Program B, proposed in the 1970s:

> *Classify the non-CM, non-cuspidal rational points of X_H, for open subgroups[6] $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$.*

In what follows, let us outline our proposed approach to resolve Mazur's Program B once and for all.

[5] Here, $\hat{\mathbf{Z}} := \varprojlim_N \mathbf{Z}/N\mathbf{Z}$, where the transition maps are the usual surjections $\mathbf{Z}/M\mathbf{Z} \twoheadrightarrow \mathbf{Z}/N\mathbf{Z}$ for $N \mid M$.

[6] Any open subgroup H comes from $H' \leq \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ for some integer N.

Mazur's Program B

We can vary across all N to get a map[5] $\rho\colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\hat{\mathbf{Z}})$.

Theorem (Serre)

The image of ρ is open in $\mathrm{GL}_2(\hat{\mathbf{Z}})$.

You are led naturally to the following problem: classify all possible images of ρ for non-CM elliptic curves E. This is Mazur's Program B, proposed in the 1970s:

> *Classify the non-CM, non-cuspidal rational points of X_H, for open subgroups[6] $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$.*

In what follows, let us outline our proposed approach to resolve Mazur's Program B once and for all.

[5] Here, $\hat{\mathbf{Z}} := \varprojlim_N \mathbf{Z}/N\mathbf{Z}$, where the transition maps are the usual surjections $\mathbf{Z}/M\mathbf{Z} \twoheadrightarrow \mathbf{Z}/N\mathbf{Z}$ for $N \mid M$.

[6] Any open subgroup H comes from $H' \leq \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ for some integer N.

Mazur's Program B

We can vary across all N to get a map[5] $\rho\colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\hat{\mathbf{Z}})$.

Theorem (Serre)

The image of ρ is open in $\mathrm{GL}_2(\hat{\mathbf{Z}})$.

You are led naturally to the following problem: classify all possible images of ρ for non-CM elliptic curves E. This is Mazur's Program B, proposed in the 1970s:

> *Classify the non-CM, non-cuspidal rational points of X_H, for open subgroups[6] $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$.*

In what follows, let us outline our proposed approach to resolve Mazur's Program B once and for all.

[5] Here, $\hat{\mathbf{Z}} := \varprojlim_N \mathbf{Z}/N\mathbf{Z}$, where the transition maps are the usual surjections $\mathbf{Z}/M\mathbf{Z} \twoheadrightarrow \mathbf{Z}/N\mathbf{Z}$ for $N \mid M$.

[6] Any open subgroup H comes from $H' \leq \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ for some integer N.

Mazur's Program B

We can vary across all N to get a map[5] $\rho\colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\hat{\mathbf{Z}})$.

Theorem (Serre)

The image of ρ is open in $\mathrm{GL}_2(\hat{\mathbf{Z}})$.

You are led naturally to the following problem: classify all possible images of ρ for non-CM elliptic curves E. This is Mazur's Program B, proposed in the 1970s:

> *Classify the non-CM, non-cuspidal rational points of X_H, for open subgroups*[6] $H \le \mathrm{GL}_2(\hat{\mathbf{Z}})$.

In what follows, let us outline our proposed approach to resolve Mazur's Program B once and for all.

[5] Here, $\hat{\mathbf{Z}} := \varprojlim_N \mathbf{Z}/N\mathbf{Z}$, where the transition maps are the usual surjections $\mathbf{Z}/M\mathbf{Z} \twoheadrightarrow \mathbf{Z}/N\mathbf{Z}$ for $N \mid M$.

[6] Any open subgroup H comes from $H' \le \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ for some integer N.

Mazur's Program B: initial reduction

First, it suffices to consider the open subgroups $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ that are maximal with respect to the property "X_H has genus at least 2".

There are infinitely many primes p, so shouldn't there be infinitely many such H?

We have run into our first snag.

Conjecture (Serre's uniformity question)

There is a constant C such that for all primes $p > C$ and all subgroups $H \leq \mathrm{GL}_2(\mathbf{F}_p)$, the set $X_H(\mathbf{Q})$ consists entirely of CM points and cusps.

If Serre uniformity holds, then there are only finitely many open subgroups $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ that are maximal with respect to the property "X_H has genus at least 2, and $X_H(\mathbf{Q})$ consists of CM points and cusps". (More on this in a bit.)

Mazur's Program B: initial reduction

First, it suffices to consider the open subgroups $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ that are maximal with respect to the property "X_H has genus at least 2".

> *There are infinitely many primes p, so shouldn't there be infinitely many such H?*

We have run into our first snag.

Conjecture (Serre's uniformity question)

There is a constant C such that for all primes $p > C$ and all subgroups $H \leq \mathrm{GL}_2(\mathbf{F}_p)$, the set $X_H(\mathbf{Q})$ consists entirely of CM points and cusps.

If Serre uniformity holds, then there are only finitely many open subgroups $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ that are maximal with respect to the property "X_H has genus at least 2, and $X_H(\mathbf{Q})$ consists of CM points and cusps". (More on this in a bit.)

Mazur's Program B: initial reduction

First, it suffices to consider the open subgroups $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ that are maximal with respect to the property "X_H has genus at least 2".

> *There are infinitely many primes p, so shouldn't there be infinitely many such H?*

We have run into our first snag.

Conjecture (Serre's uniformity question)

There is a constant C such that for all primes $p > C$ and all subgroups $H \leq \mathrm{GL}_2(\mathbf{F}_p)$, the set $X_H(\mathbf{Q})$ consists entirely of CM points and cusps.

If Serre uniformity holds, then there are only finitely many open subgroups $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ that are maximal with respect to the property "X_H has genus at least 2, and $X_H(\mathbf{Q})$ consists of CM points and cusps". (More on this in a bit.)

Mazur's Program B: initial reduction

First, it suffices to consider the open subgroups $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ that are maximal with respect to the property "X_H has genus at least 2".

> *There are infinitely many primes p, so shouldn't there be infinitely many such H?*

We have run into our first snag.

Conjecture (Serre's uniformity question)

There is a constant C such that for all primes $p > C$ and all subgroups $H \leq \mathrm{GL}_2(\mathbf{F}_p)$, the set $X_H(\mathbf{Q})$ consists entirely of CM points and cusps.

If Serre uniformity holds, then there are only finitely many open subgroups $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ that are maximal with respect to the property "X_H has genus at least 2, and $X_H(\mathbf{Q})$ consists of CM points and cusps". (More on this in a bit.)

Mazur's Program B: initial reduction

First, it suffices to consider the open subgroups $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ that are maximal with respect to the property "X_H has genus at least 2".

> *There are infinitely many primes p, so shouldn't there be infinitely many such H?*

We have run into our first snag.

Conjecture (Serre's uniformity question)

There is a constant C such that for all primes $p > C$ and all subgroups $H \leq \mathrm{GL}_2(\mathbf{F}_p)$, the set $X_H(\mathbf{Q})$ consists entirely of CM points and cusps.

If Serre uniformity holds, then there are only finitely many open subgroups $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ that are maximal with respect to the property "X_H has genus at least 2, and $X_H(\mathbf{Q})$ consists of CM points and cusps". (More on this in a bit.)

Progress on Serre's uniformity question

If $H \leq \mathrm{GL}_2(\mathbf{F}_p)$ is a maximal subgroup, then one of the following holds. Text in this color describes known necessary conditions for $X_H(\mathbf{Q})$ to contain an "exceptional" point.

1. H contains $\mathrm{SL}_2(\mathbf{F}_p)$. X_H is not even defined over $\mathbf{Q}$.
2. The image of H in $\mathrm{PGL}_2(\mathbf{F}_p)$ is S_4, A_4 or A_5. X_H must have $p \leq 13$ (Serre, 1972).
3. ("Borel") $H = \{\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]\}$. $X_H =: X_0(p)$ must have $p \leq 163$ (Mazur, 1978).
4. ("Normalizer of split Cartan") $H = \{\left[\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right]\} \cup \{\left[\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right]\}$. $X_H =: X_s^+(p)$ must have $p \leq 13$ (Bilu-Parent-Rebolledo, 2013).
5. ("Normalizer of nonsplit Cartan") $H = \{\left[\begin{smallmatrix} x & \varepsilon y \\ y & x \end{smallmatrix}\right]\} \cup \left\{\left[\begin{smallmatrix} x & \varepsilon y \\ -y & -x \end{smallmatrix}\right]\right\}$ where $\varepsilon \in \mathbf{F}_p^\times$ is any non-square (H does not depend on the choice of ε). $X_H =: X_{ns}^+(p)$. Nothing is known!!

Progress on Serre's uniformity question

If $H \leq \mathrm{GL}_2(\mathbf{F}_p)$ is a maximal subgroup, then one of the following holds. Text in this color describes known necessary conditions for $X_H(\mathbf{Q})$ to contain an "exceptional" point.

1. H contains $\mathrm{SL}_2(\mathbf{F}_p)$. X_H is not even defined over $\mathbf{Q}$.
2. The image of H in $\mathrm{PGL}_2(\mathbf{F}_p)$ is S_4, A_4 or A_5. X_H must have $p \leq 13$ (Serre, 1972).
3. ("Borel") $H = \{\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]\}$. $X_H =: X_0(p)$ must have $p \leq 163$ (Mazur, 1978).
4. ("Normalizer of split Cartan") $H = \{\left[\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right]\} \cup \{\left[\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right]\}$. $X_H =: X_s^+(p)$ must have $p \leq 13$ (Bilu-Parent-Rebolledo, 2013).
5. ("Normalizer of nonsplit Cartan") $H = \{\left[\begin{smallmatrix} x & \varepsilon y \\ y & x \end{smallmatrix}\right]\} \cup \left\{\left[\begin{smallmatrix} x & \varepsilon y \\ -y & -x \end{smallmatrix}\right]\right\}$ where $\varepsilon \in \mathbf{F}_p^\times$ is any non-square (H does not depend on the choice of ε). $X_H =: X_{ns}^+(p)$. Nothing is known!!

Progress on Serre's uniformity question

If $H \leq \mathrm{GL}_2(\mathbf{F}_p)$ is a maximal subgroup, then one of the following holds. Text in this color describes known necessary conditions for $X_H(\mathbf{Q})$ to contain an "exceptional" point.

1. H contains $\mathrm{SL}_2(\mathbf{F}_p)$. X_H is not even defined over $\mathbf{Q}$.
2. The image of H in $\mathrm{PGL}_2(\mathbf{F}_p)$ is S_4, A_4 or A_5. X_H must have $p \leq 13$ (Serre, 1972).
3. ("Borel") $H = \{\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]\}$. $X_H =: X_0(p)$ must have $p \leq 163$ (Mazur, 1978).
4. ("Normalizer of split Cartan") $H = \{\left[\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right]\} \cup \{\left[\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right]\}$. $X_H =: X_s^+(p)$ must have $p \leq 13$ (Bilu-Parent-Rebolledo, 2013).
5. ("Normalizer of nonsplit Cartan") $H = \{\left[\begin{smallmatrix} x & \varepsilon y \\ y & x \end{smallmatrix}\right]\} \cup \left\{\left[\begin{smallmatrix} x & \varepsilon y \\ -y & -x \end{smallmatrix}\right]\right\}$ where $\varepsilon \in \mathbf{F}_p^\times$ is any non-square (H does not depend on the choice of ε). $X_H =: X_{ns}^+(p)$. Nothing is known!!

Progress on Serre's uniformity question

If $H \leq \mathrm{GL}_2(\mathbf{F}_p)$ is a maximal subgroup, then one of the following holds. Text in this color describes known necessary conditions for $X_H(\mathbf{Q})$ to contain an "exceptional" point.

1. H contains $\mathrm{SL}_2(\mathbf{F}_p)$. X_H is not even defined over $\mathbf{Q}$.
2. The image of H in $\mathrm{PGL}_2(\mathbf{F}_p)$ is S_4, A_4 or A_5. X_H must have $p \leq 13$ (Serre, 1972).
3. ("Borel") $H = \{\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]\}$. $X_H =: X_0(p)$ must have $p \leq 163$ (Mazur, 1978).
4. ("Normalizer of split Cartan") $H = \{\left[\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right]\} \cup \{\left[\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right]\}$. $X_H =: X_s^+(p)$ must have $p \leq 13$ (Bilu-Parent-Rebolledo, 2013).
5. ("Normalizer of nonsplit Cartan") $H = \{\left[\begin{smallmatrix} x & \varepsilon y \\ y & x \end{smallmatrix}\right]\} \cup \left\{\left[\begin{smallmatrix} x & \varepsilon y \\ -y & -x \end{smallmatrix}\right]\right\}$ where $\varepsilon \in \mathbf{F}_p^\times$ is any non-square (H does not depend on the choice of ε). $X_H =: X_{ns}^+(p)$. Nothing is known!!

Progress on Serre's uniformity question

If $H \leq \mathrm{GL}_2(\mathbf{F}_p)$ is a maximal subgroup, then one of the following holds. Text in this color describes known necessary conditions for $X_H(\mathbf{Q})$ to contain an "exceptional" point.

1. H contains $\mathrm{SL}_2(\mathbf{F}_p)$. X_H is not even defined over $\mathbf{Q}$.
2. The image of H in $\mathrm{PGL}_2(\mathbf{F}_p)$ is S_4, A_4 or A_5. X_H must have $p \leq 13$ (Serre, 1972).
3. ("Borel") $H = \{\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]\}$. $X_H =: X_0(p)$ must have $p \leq 163$ (Mazur, 1978).
4. ("Normalizer of split Cartan") $H = \{\left[\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right]\} \cup \{\left[\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right]\}$. $X_H =: X_s^+(p)$ must have $p \leq 13$ (Bilu-Parent-Rebolledo, 2013).
5. ("Normalizer of nonsplit Cartan") $H = \{\left[\begin{smallmatrix} x & \varepsilon y \\ y & x \end{smallmatrix}\right]\} \cup \left\{\left[\begin{smallmatrix} x & \varepsilon y \\ -y & -x \end{smallmatrix}\right]\right\}$ where $\varepsilon \in \mathbf{F}_p^\times$ is any non-square (H does not depend on the choice of ε). $X_H =: X_{ns}^+(p)$. Nothing is known!!

Progress on Serre's uniformity question

If $H \leq \mathrm{GL}_2(\mathbf{F}_p)$ is a maximal subgroup, then one of the following holds. Text in this color describes known necessary conditions for $X_H(\mathbf{Q})$ to contain an "exceptional" point.

1. H contains $\mathrm{SL}_2(\mathbf{F}_p)$. X_H is not even defined over $\mathbf{Q}$.
2. The image of H in $\mathrm{PGL}_2(\mathbf{F}_p)$ is S_4, A_4 or A_5. X_H must have $p \leq 13$ (Serre, 1972).
3. ("Borel") $H = \{\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]\}$. $X_H =: X_0(p)$ must have $p \leq 163$ (Mazur, 1978).
4. ("Normalizer of split Cartan") $H = \{\left[\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right]\} \cup \{\left[\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right]\}$. $X_H =: X_s^+(p)$ must have $p \leq 13$ (Bilu-Parent-Rebolledo, 2013).
5. ("Normalizer of nonsplit Cartan") $H = \{\left[\begin{smallmatrix} x & \varepsilon y \\ y & x \end{smallmatrix}\right]\} \cup \left\{\left[\begin{smallmatrix} x & \varepsilon y \\ -y & -x \end{smallmatrix}\right]\right\}$ where $\varepsilon \in \mathbf{F}_p^\times$ is any non-square (H does not depend on the choice of ε). $X_H =: X_{ns}^+(p)$. Nothing is known!!

Progress on Serre's uniformity question

If $H \leq \mathrm{GL}_2(\mathbf{F}_p)$ is a maximal subgroup, then one of the following holds. Text in this color describes known necessary conditions for $X_H(\mathbf{Q})$ to contain an "exceptional" point.

1. H contains $\mathrm{SL}_2(\mathbf{F}_p)$. X_H is not even defined over $\mathbf{Q}$.
2. The image of H in $\mathrm{PGL}_2(\mathbf{F}_p)$ is S_4, A_4 or A_5. X_H must have $p \leq 13$ (Serre, 1972).
3. ("Borel") $H = \{\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]\}$. $X_H =: X_0(p)$ must have $p \leq 163$ (Mazur, 1978).
4. ("Normalizer of split Cartan") $H = \{\left[\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right]\} \cup \{\left[\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right]\}$. $X_H =: X_s^+(p)$ must have $p \leq 13$ (Bilu-Parent-Rebolledo, 2013).
5. ("Normalizer of nonsplit Cartan") $H = \{\left[\begin{smallmatrix} x & \varepsilon y \\ y & x \end{smallmatrix}\right]\} \cup \left\{\left[\begin{smallmatrix} x & \varepsilon y \\ -y & -x \end{smallmatrix}\right]\right\}$ where $\varepsilon \in \mathbf{F}_p^\times$ is any non-square (H does not depend on the choice of ε). $X_H =: X_{ns}^+(p)$. Nothing is known!!

Progress on Serre's uniformity question

If $H \leq \mathrm{GL}_2(\mathbf{F}_p)$ is a maximal subgroup, then one of the following holds. Text in this color describes known necessary conditions for $X_H(\mathbf{Q})$ to contain an "exceptional" point.

1. H contains $\mathrm{SL}_2(\mathbf{F}_p)$. X_H is not even defined over $\mathbf{Q}$.
2. The image of H in $\mathrm{PGL}_2(\mathbf{F}_p)$ is S_4, A_4 or A_5. X_H must have $p \leq 13$ (Serre, 1972).
3. ("Borel") $H = \{\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]\}$. $X_H =: X_0(p)$ must have $p \leq 163$ (Mazur, 1978).
4. ("Normalizer of split Cartan") $H = \{\left[\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right]\} \cup \{\left[\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right]\}$. $X_H =: X_s^+(p)$ must have $p \leq 13$ (Bilu-Parent-Rebolledo, 2013).
5. ("Normalizer of nonsplit Cartan") $H = \{\left[\begin{smallmatrix} x & \varepsilon y \\ y & x \end{smallmatrix}\right]\} \cup \left\{\left[\begin{smallmatrix} x & \varepsilon y \\ -y & -x \end{smallmatrix}\right]\right\}$ where $\varepsilon \in \mathbf{F}_p^\times$ is any non-square (H does not depend on the choice of ε). $X_H =: X_{ns}^+(p)$. Nothing is known!!

Serre uniformity in the nonsplit Cartan case: an idea

In the split Cartan case, Bilu-Parent need the following ingredients. Text in this color denotes how you might adapt it to the non-split Cartan case.

- Construct a nontrivial modular unit[7], integral over $\mathbf{Z}[j]$. For $X_{ns}^{+}(p)$, only one $\mathrm{Gal}_{\mathbf{Q}}$-orbit of cusps. Instead you probably have to use CM points. Use Gross-Zagier to construct modular functions f_i supported at Heegner divisors.
- Guarantee that a putative rational point does not intersect the cuspidal divisor. Hope that you need only finitely many f_i such that for any putative rational point, there is some i such that it does not intersect the divisor $D(f_i)$.
- Lower bounds on $|j(E)|$ for E non-CM, coming from bounds on the smallest degree of an isogeny between two isogenous elliptic curves. Non-split case has a somewhat more difficult moduli interpretation cf. Rebolledo-Wuthrich 2017.

[7] poles and zeroes only at cusps

Serre uniformity in the nonsplit Cartan case: an idea

In the split Cartan case, Bilu-Parent need the following ingredients. Text in this color denotes how you might adapt it to the non-split Cartan case.

- Construct a nontrivial modular unit[7], integral over $\mathbf{Z}[j]$. For $X_{ns}^{+}(p)$, only one $\mathrm{Gal}_{\mathbf{Q}}$-orbit of cusps. Instead you probably have to use CM points. Use Gross-Zagier to construct modular functions f_i supported at Heegner divisors.
- Guarantee that a putative rational point does not intersect the cuspidal divisor. Hope that you need only finitely many f_i such that for any putative rational point, there is some i such that it does not intersect the divisor $D(f_i)$.
- Lower bounds on $|j(E)|$ for E non-CM, coming from bounds on the smallest degree of an isogeny between two isogenous elliptic curves. Non-split case has a somewhat more difficult moduli interpretation cf. Rebolledo-Wuthrich 2017.

[7] poles and zeroes only at cusps

Serre uniformity in the nonsplit Cartan case: an idea

In the split Cartan case, Bilu-Parent need the following ingredients. Text in this color denotes how you might adapt it to the non-split Cartan case.

- Construct a nontrivial modular unit[7], integral over $\mathbf{Z}[j]$. For $X_{ns}^{+}(p)$, only one $\mathrm{Gal}_{\mathbf{Q}}$-orbit of cusps. Instead you probably have to use CM points. Use Gross-Zagier to construct modular functions f_i supported at Heegner divisors.
- Guarantee that a putative rational point does not intersect the cuspidal divisor. Hope that you need only finitely many f_i such that for any putative rational point, there is some i such that it does not intersect the divisor $D(f_i)$.
- Lower bounds on $|j(E)|$ for E non-CM, coming from bounds on the smallest degree of an isogeny between two isogenous elliptic curves. Non-split case has a somewhat more difficult moduli interpretation cf. Rebolledo-Wuthrich 2017.

[7] poles and zeroes only at cusps

Serre uniformity in the nonsplit Cartan case: an idea

In the split Cartan case, Bilu-Parent need the following ingredients. Text in this color denotes how you might adapt it to the non-split Cartan case.

- Construct a nontrivial modular unit[7], integral over $\mathbf{Z}[j]$. For $X_{ns}^{+}(p)$, only one $\mathrm{Gal}_{\mathbf{Q}}$-orbit of cusps. Instead you probably have to use CM points. Use Gross-Zagier to construct modular functions f_i supported at Heegner divisors.
- Guarantee that a putative rational point does not intersect the cuspidal divisor. Hope that you need only finitely many f_i such that for any putative rational point, there is some i such that it does not intersect the divisor $D(f_i)$.
- Lower bounds on $|j(E)|$ for E non-CM, coming from bounds on the smallest degree of an isogeny between two isogenous elliptic curves. Non-split case has a somewhat more difficult moduli interpretation cf. Rebolledo-Wuthrich 2017.

[7] poles and zeroes only at cusps

Serre uniformity in the nonsplit Cartan case: an idea

In the split Cartan case, Bilu-Parent need the following ingredients. Text in this color denotes how you might adapt it to the non-split Cartan case.

- Construct a nontrivial modular unit[7], integral over $\mathbf{Z}[j]$. For $X_{ns}^{+}(p)$, only one $\mathrm{Gal}_{\mathbf{Q}}$-orbit of cusps. Instead you probably have to use CM points. Use Gross-Zagier to construct modular functions f_i supported at Heegner divisors.
- Guarantee that a putative rational point does not intersect the cuspidal divisor. Hope that you need only finitely many f_i such that for any putative rational point, there is some i such that it does not intersect the divisor $D(f_i)$.
- Lower bounds on $|j(E)|$ for E non-CM, coming from bounds on the smallest degree of an isogeny between two isogenous elliptic curves. Non-split case has a somewhat more difficult moduli interpretation cf. Rebolledo-Wuthrich 2017.

[7] poles and zeroes only at cusps

Serre uniformity in the nonsplit Cartan case: an idea

In the split Cartan case, Bilu-Parent need the following ingredients. Text in this color denotes how you might adapt it to the non-split Cartan case.

- Construct a nontrivial modular unit[7], integral over $\mathbf{Z}[j]$. For $X_{ns}^{+}(p)$, only one $\mathrm{Gal}_{\mathbf{Q}}$-orbit of cusps. Instead you probably have to use CM points. Use Gross-Zagier to construct modular functions f_i supported at Heegner divisors.
- Guarantee that a putative rational point does not intersect the cuspidal divisor. Hope that you need only finitely many f_i such that for any putative rational point, there is some i such that it does not intersect the divisor $D(f_i)$.
- Lower bounds on $|j(E)|$ for E non-CM, coming from bounds on the smallest degree of an isogeny between two isogenous elliptic curves. Non-split case has a somewhat more difficult moduli interpretation cf. Rebolledo-Wuthrich 2017.

[7] poles and zeroes only at cusps

Serre uniformity in the nonsplit Cartan case: an idea

In the split Cartan case, Bilu-Parent need the following ingredients. Text in this color denotes how you might adapt it to the non-split Cartan case.

- Construct a nontrivial modular unit[7], integral over $\mathbf{Z}[j]$. For $X_{ns}^{+}(p)$, only one $\mathrm{Gal}_{\mathbf{Q}}$-orbit of cusps. Instead you probably have to use CM points. Use Gross-Zagier to construct modular functions f_i supported at Heegner divisors.
- Guarantee that a putative rational point does not intersect the cuspidal divisor. Hope that you need only finitely many f_i such that for any putative rational point, there is some i such that it does not intersect the divisor $D(f_i)$.
- Lower bounds on $|j(E)|$ for E non-CM, coming from bounds on the smallest degree of an isogeny between two isogenous elliptic curves. Non-split case has a somewhat more difficult moduli interpretation cf. Rebolledo-Wuthrich 2017.

[7] poles and zeroes only at cusps

Serre uniformity in the nonsplit Cartan case: an idea

In the split Cartan case, Bilu-Parent need the following ingredients. Text in this color denotes how you might adapt it to the non-split Cartan case.

- Construct a nontrivial modular unit[7], integral over $\mathbf{Z}[j]$. For $X_{ns}^{+}(p)$, only one $\mathrm{Gal}_{\mathbf{Q}}$-orbit of cusps. Instead you probably have to use CM points. Use Gross-Zagier to construct modular functions f_i supported at Heegner divisors.
- Guarantee that a putative rational point does not intersect the cuspidal divisor. Hope that you need only finitely many f_i such that for any putative rational point, there is some i such that it does not intersect the divisor $D(f_i)$.
- Lower bounds on $|j(E)|$ for E non-CM, coming from bounds on the smallest degree of an isogeny between two isogenous elliptic curves. Non-split case has a somewhat more difficult moduli interpretation cf. Rebolledo-Wuthrich 2017.

[7]poles and zeroes only at cusps

Serre uniformity in the nonsplit Cartan case: an idea

In the split Cartan case, Bilu-Parent need the following ingredients. Text in this color denotes how you might adapt it to the non-split Cartan case.

- Construct a nontrivial modular unit[7], integral over $\mathbf{Z}[j]$. For $X_{ns}^{+}(p)$, only one $\mathrm{Gal}_{\mathbf{Q}}$-orbit of cusps. Instead you probably have to use CM points. Use Gross-Zagier to construct modular functions f_i supported at Heegner divisors.
- Guarantee that a putative rational point does not intersect the cuspidal divisor. Hope that you need only finitely many f_i such that for any putative rational point, there is some i such that it does not intersect the divisor $D(f_i)$.
- Lower bounds on $|j(E)|$ for E non-CM, coming from bounds on the smallest degree of an isogeny between two isogenous elliptic curves. Non-split case has a somewhat more difficult moduli interpretation cf. Rebolledo-Wuthrich 2017.

[7] poles and zeroes only at cusps

Maximal subgroups of $g \geq 2$ with exceptional points

Now suppose Serre uniformity holds in the affirmative.

Suppose $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ is maximal of genus ≥ 2 with level $N = p_1^{e_1} \cdots p_m^{e_m}$. Induct on m to classify all possible H, as follows.

1. Enumerate the finitely many H of genus ≤ 1.
2. If $m = 1$, say $N = p^e$, use
$$0 \longrightarrow I(p) \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p) \longrightarrow \mathrm{GL}_2(\mathbf{F}_p) \longrightarrow 0$$
and the fact that $I(p)$ is pro-p to compute the (finitely many) maximal open subgroups of $\mathrm{GL}_2(\mathbf{Z}_p)$ with genus ≥ 2.
3. Suppose $m > 1$. For $1 \leq i \leq m$ let $N^{(i)} := N/p_i^{e_i}$. By assumption on the level N of H, the projections of H onto $\mathrm{GL}_2(\mathbf{Z}/N^{(i)}\mathbf{Z})$ all have genus ≤ 1, and then a "generalized Goursat's lemma" tells you what H can be.

See Zywina's open image papers for an alternate formulation.

Maximal subgroups of $g \geq 2$ with exceptional points

Now suppose Serre uniformity holds in the affirmative.
Suppose $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ is maximal of genus ≥ 2 with level $N = p_1^{e_1} \cdots p_m^{e_m}$. Induct on m to classify all possible H, as follows.

1. Enumerate the finitely many H of genus ≤ 1.
2. If $m = 1$, say $N = p^e$, use
$$0 \longrightarrow I(p) \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p) \longrightarrow \mathrm{GL}_2(\mathbf{F}_p) \longrightarrow 0$$
and the fact that $I(p)$ is pro-p to compute the (finitely many) maximal open subgroups of $\mathrm{GL}_2(\mathbf{Z}_p)$ with genus ≥ 2.
3. Suppose $m > 1$. For $1 \leq i \leq m$ let $N^{(i)} := N/p_i^{e_i}$. By assumption on the level N of H, the projections of H onto $\mathrm{GL}_2(\mathbf{Z}/N^{(i)}\mathbf{Z})$ all have genus ≤ 1, and then a "generalized Goursat's lemma" tells you what H can be.

See Zywina's open image papers for an alternate formulation.

Maximal subgroups of $g \geq 2$ with exceptional points

Now suppose Serre uniformity holds in the affirmative.
Suppose $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ is maximal of genus ≥ 2 with level $N = p_1^{e_1} \cdots p_m^{e_m}$. Induct on m to classify all possible H, as follows.

1. Enumerate the finitely many H of genus ≤ 1.
2. If $m = 1$, say $N = p^e$, use
$$0 \longrightarrow I(p) \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p) \longrightarrow \mathrm{GL}_2(\mathbf{F}_p) \longrightarrow 0$$
and the fact that $I(p)$ is pro-p to compute the (finitely many) maximal open subgroups of $\mathrm{GL}_2(\mathbf{Z}_p)$ with genus ≥ 2.
3. Suppose $m > 1$. For $1 \leq i \leq m$ let $N^{(i)} := N/p_i^{e_i}$. By assumption on the level N of H, the projections of H onto $\mathrm{GL}_2(\mathbf{Z}/N^{(i)}\mathbf{Z})$ all have genus ≤ 1, and then a "generalized Goursat's lemma" tells you what H can be.

See Zywina's open image papers for an alternate formulation.

Maximal subgroups of $g \geq 2$ with exceptional points

Now suppose Serre uniformity holds in the affirmative.
Suppose $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ is maximal of genus ≥ 2 with level $N = p_1^{e_1} \cdots p_m^{e_m}$. Induct on m to classify all possible H, as follows.

1. Enumerate the finitely many H of genus ≤ 1.
2. If $m = 1$, say $N = p^e$, use

$$0 \longrightarrow I(p) \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p) \longrightarrow \mathrm{GL}_2(\mathbf{F}_p) \longrightarrow 0$$

   and the fact that $I(p)$ is pro-p to compute the (finitely many) maximal open subgroups of $\mathrm{GL}_2(\mathbf{Z}_p)$ with genus ≥ 2.
3. Suppose $m > 1$. For $1 \leq i \leq m$ let $N^{(i)} := N/p_i^{e_i}$. By assumption on the level N of H, the projections of H onto $\mathrm{GL}_2(\mathbf{Z}/N^{(i)}\mathbf{Z})$ all have genus ≤ 1, and then a "generalized Goursat's lemma" tells you what H can be.

See Zywina's open image papers for an alternate formulation.

Maximal subgroups of $g \geq 2$ with exceptional points

Now suppose Serre uniformity holds in the affirmative.
Suppose $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ is maximal of genus ≥ 2 with level $N = p_1^{e_1} \cdots p_m^{e_m}$. Induct on m to classify all possible H, as follows.

1. Enumerate the finitely many H of genus ≤ 1.
2. If $m = 1$, say $N = p^e$, use

$$0 \longrightarrow I(p) \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p) \longrightarrow \mathrm{GL}_2(\mathbf{F}_p) \longrightarrow 0$$

   and the fact that $I(p)$ is pro-p to compute the (finitely many) maximal open subgroups of $\mathrm{GL}_2(\mathbf{Z}_p)$ with genus ≥ 2.
3. Suppose $m > 1$. For $1 \leq i \leq m$ let $N^{(i)} := N/p_i^{e_i}$. By assumption on the level N of H, the projections of H onto $\mathrm{GL}_2(\mathbf{Z}/N^{(i)}\mathbf{Z})$ all have genus ≤ 1, and then a "generalized Goursat's lemma" tells you what H can be.

See Zywina's open image papers for an alternate formulation.

Maximal subgroups of $g \geq 2$ with exceptional points

Now suppose Serre uniformity holds in the affirmative.
Suppose $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ is maximal of genus ≥ 2 with level $N = p_1^{e_1} \cdots p_m^{e_m}$. Induct on m to classify all possible H, as follows.

1. Enumerate the finitely many H of genus ≤ 1.
2. If $m = 1$, say $N = p^e$, use

$$0 \longrightarrow I(p) \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p) \longrightarrow \mathrm{GL}_2(\mathbf{F}_p) \longrightarrow 0$$

   and the fact that $I(p)$ is pro-p to compute the (finitely many) maximal open subgroups of $\mathrm{GL}_2(\mathbf{Z}_p)$ with genus ≥ 2.
3. Suppose $m > 1$. For $1 \leq i \leq m$ let $N^{(i)} := N/p_i^{e_i}$. By assumption on the level N of H, the projections of H onto $\mathrm{GL}_2(\mathbf{Z}/N^{(i)}\mathbf{Z})$ all have genus ≤ 1, and then a "generalized Goursat's lemma" tells you what H can be.

See Zywina's open image papers for an alternate formulation.

Maximal subgroups of $g \geq 2$ with exceptional points

Now suppose Serre uniformity holds in the affirmative.
Suppose $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ is maximal of genus ≥ 2 with level $N = p_1^{e_1} \cdots p_m^{e_m}$. Induct on m to classify all possible H, as follows.

1. Enumerate the finitely many H of genus ≤ 1.
2. If $m = 1$, say $N = p^e$, use

$$0 \longrightarrow I(p) \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p) \longrightarrow \mathrm{GL}_2(\mathbf{F}_p) \longrightarrow 0$$

   and the fact that $I(p)$ is pro-p to compute the (finitely many) maximal open subgroups of $\mathrm{GL}_2(\mathbf{Z}_p)$ with genus ≥ 2.
3. Suppose $m > 1$. For $1 \leq i \leq m$ let $N^{(i)} := N/p_i^{e_i}$. By assumption on the level N of H, the projections of H onto $\mathrm{GL}_2(\mathbf{Z}/N^{(i)}\mathbf{Z})$ all have genus ≤ 1, and then a "generalized Goursat's lemma" tells you what H can be.

See Zywina's open image papers for an alternate formulation.

Maximal subgroups of $g \geq 2$ with exceptional points

Now suppose Serre uniformity holds in the affirmative.
Suppose $H \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ is maximal of genus ≥ 2 with level $N = p_1^{e_1} \cdots p_m^{e_m}$. Induct on m to classify all possible H, as follows.

1. Enumerate the finitely many H of genus ≤ 1.
2. If $m = 1$, say $N = p^e$, use

$$0 \longrightarrow I(p) \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p) \longrightarrow \mathrm{GL}_2(\mathbf{F}_p) \longrightarrow 0$$

   and the fact that $I(p)$ is pro-p to compute the (finitely many) maximal open subgroups of $\mathrm{GL}_2(\mathbf{Z}_p)$ with genus ≥ 2.
3. Suppose $m > 1$. For $1 \leq i \leq m$ let $N^{(i)} := N/p_i^{e_i}$. By assumption on the level N of H, the projections of H onto $\mathrm{GL}_2(\mathbf{Z}/N^{(i)}\mathbf{Z})$ all have genus ≤ 1, and then a "generalized Goursat's lemma" tells you what H can be.

See Zywina's open image papers for an alternate formulation.

Motivation

We now have finitely many H for which we need to find $X_H(\mathbf{Q})$.

You could now proceed by computing projective models for each X_H and applying Chabauty.

However, you are left wondering if there is a more natural approach that uses the moduli interpretation of X_H, instead of some potentially nasty commutative algebra.

The answer is yes! But you will have to do some precision analysis instead. This approach is called “equationless” or “model-free” Chabauty.

Motivation

We now have finitely many H for which we need to find $X_H(\mathbf{Q})$. You could now proceed by computing projective models for each X_H and applying Chabauty.

However, you are left wondering if there is a more natural approach that uses the moduli interpretation of X_H, instead of some potentially nasty commutative algebra.

The answer is yes! But you will have to do some precision analysis instead. This approach is called "equationless" or "model-free" Chabauty.

Motivation

We now have finitely many H for which we need to find $X_H(\mathbf{Q})$.
You could now proceed by computing projective models for each X_H and applying Chabauty.
However, you are left wondering if there is a more natural approach that uses the moduli interpretation of X_H, instead of some potentially nasty commutative algebra.
The answer is yes! But you will have to do some precision analysis instead. This approach is called "equationless" or "model-free" Chabauty.

Motivation

We now have finitely many H for which we need to find $X_H(\mathbf{Q})$.
You could now proceed by computing projective models for each X_H and applying Chabauty.
However, you are left wondering if there is a more natural approach that uses the moduli interpretation of X_H, instead of some potentially nasty commutative algebra.
The answer is yes! But you will have to do some precision analysis instead. This approach is called "equationless" or "model-free" Chabauty.

Expressing large Coleman integrals as tiny ones

The difficulty of linear Chabauty boils down to computing Coleman integrals.

If you had a plane curve, you first compute large Coleman integrals into tiny Coleman integrals using a Frobenius lift.

For modular curves, you can use the Hecke correspondence instead. This works because of the Eichler-Shimura relation.

You get the following formula of column vectors:

$$\left[\int_a^b \omega_i\right]_i^T = (p+1-A)^{-1}\left[\sum_{j=1}^{p+1}\left(\int_{b_j}^b \omega_i - \int_{a_j}^a \omega_i\right)\right]_i^T$$

where ω_i is a basis of annihilating differentials, A is the matrix of T_p acting on the ω_i, and $T_p([a]) =: [a_1 + \cdots + a_{p+1}]$ (crucially, note that the a_j all lie in the same disk as a).

Expressing large Coleman integrals as tiny ones

The difficulty of linear Chabauty boils down to computing Coleman integrals.

If you had a plane curve, you first compute large Coleman integrals into tiny Coleman integrals using a Frobenius lift.

For modular curves, you can use the Hecke correspondence instead. This works because of the Eichler-Shimura relation.

You get the following formula of column vectors:

$$\left[\int_a^b \omega_i\right]_i^T = (p+1-A)^{-1}\left[\sum_{j=1}^{p+1}\left(\int_{b_j}^b \omega_i - \int_{a_j}^a \omega_i\right)\right]_i^T$$

where ω_i is a basis of annihilating differentials, A is the matrix of T_p acting on the ω_i, and $T_p([a]) =: [a_1 + \cdots + a_{p+1}]$ (crucially, note that the a_j all lie in the same disk as a).

Expressing large Coleman integrals as tiny ones

The difficulty of linear Chabauty boils down to computing Coleman integrals.
If you had a plane curve, you first compute large Coleman integrals into tiny Coleman integrals using a Frobenius lift.
For modular curves, you can use the Hecke correspondence instead.
This works because of the Eichler-Shimura relation.
You get the following formula of column vectors:

$$\left[\int_a^b \omega_i\right]_i^T = (p+1-A)^{-1}\left[\sum_{j=1}^{p+1}\left(\int_{b_j}^b \omega_i - \int_{a_j}^a \omega_i\right)\right]_i^T$$

where ω_i is a basis of annihilating differentials, A is the matrix of T_p acting on the ω_i, and $T_p([a]) =: [a_1 + \cdots + a_{p+1}]$ (crucially, note that the a_j all lie in the same disk as a).

Expressing large Coleman integrals as tiny ones

The difficulty of linear Chabauty boils down to computing Coleman integrals.

If you had a plane curve, you first compute large Coleman integrals into tiny Coleman integrals using a Frobenius lift.

For modular curves, you can use the Hecke correspondence instead.

This works because of the Eichler-Shimura relation.

You get the following formula of column vectors:

$$\left[\int_a^b \omega_i\right]_i^T = (p+1-A)^{-1}\left[\sum_{j=1}^{p+1}\left(\int_{b_j}^b \omega_i - \int_{a_j}^a \omega_i\right)\right]_i^T$$

where ω_i is a basis of annihilating differentials, A is the matrix of T_p acting on the ω_i, and $T_p([a]) =: [a_1 + \cdots + a_{p+1}]$ (crucially, note that the a_j all lie in the same disk as a).

Expressing large Coleman integrals as tiny ones

The difficulty of linear Chabauty boils down to computing Coleman integrals.

If you had a plane curve, you first compute large Coleman integrals into tiny Coleman integrals using a Frobenius lift.

For modular curves, you can use the Hecke correspondence instead.

This works because of the Eichler-Shimura relation.

You get the following formula of column vectors:

$$\left[\int_a^b \omega_i\right]_i^T = (p+1-A)^{-1}\left[\sum_{j=1}^{p+1}\left(\int_{b_j}^b \omega_i - \int_{a_j}^a \omega_i\right)\right]_i^T$$

where ω_i is a basis of annihilating differentials, A is the matrix of T_p acting on the ω_i, and $T_p([a]) =: [a_1 + \cdots + a_{p+1}]$ (crucially, note that the a_j all lie in the same disk as a).

Computing tiny Coleman integrals

This is easy in the plane curve case: find a uniformizer t on the residue disk, and then compute $\int_a^b \omega = \int_a^b f(t)\,dt$ by formally antidifferentiating each term of $f(t) \in \mathbf{Q}_p[[t]]$.

For modular curves, this is harder: you only have the j-invariant as a coordinate.

You can take a q-expansion of ω and then write it in terms of the uniformizer $j - j_0$ using analytic methods, but then you will have to pin down the coefficients as algebraic numbers.

But this is actually feasible! You can study the ramification of $j\colon X_H \to \mathbf{P}^1$ to figure out the denominators of the coefficients. Then you can use integer programming or Fourier-theoretic techniques to pin down the algebraic integers rigorously. (Rendell-X., 2025)

Remark

My paper requires you are expanding at a CM point, but this is OK because each residue disk has lots of CM points.

Computing tiny Coleman integrals

This is easy in the plane curve case: find a uniformizer t on the residue disk, and then compute $\int_a^b \omega = \int_a^b f(t)\,dt$ by formally antidifferentiating each term of $f(t) \in \mathbf{Q}_p[[t]]$.

For modular curves, this is harder: you only have the j-invariant as a coordinate.

You can take a q-expansion of ω and then write it in terms of the uniformizer $j - j_0$ using analytic methods, but then you will have to pin down the coefficients as algebraic numbers.

But this is actually feasible! You can study the ramification of $j\colon X_H \to \mathbf{P}^1$ to figure out the denominators of the coefficients. Then you can use integer programming or Fourier-theoretic techniques to pin down the algebraic integers rigorously. (Rendell-X., 2025)

Remark

My paper requires you are expanding at a CM point, but this is OK because each residue disk has lots of CM points.

Computing tiny Coleman integrals

This is easy in the plane curve case: find a uniformizer t on the residue disk, and then compute $\int_a^b \omega = \int_a^b f(t)\,dt$ by formally antidifferentiating each term of $f(t) \in \mathbf{Q}_p[[t]]$.

For modular curves, this is harder: you only have the j-invariant as a coordinate.

You can take a q-expansion of ω and then write it in terms of the uniformizer $j - j_0$ using analytic methods, but then you will have to pin down the coefficients as algebraic numbers.

But this is actually feasible! You can study the ramification of $j\colon X_H \to \mathbf{P}^1$ to figure out the denominators of the coefficients. Then you can use integer programming or Fourier-theoretic techniques to pin down the algebraic integers rigorously. (Rendell-X., 2025)

Remark

My paper requires you are expanding at a CM point, but this is OK because each residue disk has lots of CM points.

Computing tiny Coleman integrals

This is easy in the plane curve case: find a uniformizer t on the residue disk, and then compute $\int_a^b \omega = \int_a^b f(t)\,dt$ by formally antidifferentiating each term of $f(t) \in \mathbf{Q}_p[[t]]$.

For modular curves, this is harder: you only have the j-invariant as a coordinate.

You can take a q-expansion of ω and then write it in terms of the uniformizer $j - j_0$ using analytic methods, but then you will have to pin down the coefficients as algebraic numbers.

But this is actually feasible! You can study the ramification of $j\colon X_H \to \mathbf{P}^1$ to figure out the denominators of the coefficients. Then you can use integer programming or Fourier-theoretic techniques to pin down the algebraic integers rigorously. (Rendell-X., 2025)

Remark

My paper requires you are expanding at a CM point, but this is OK because each residue disk has lots of CM points.

Computing tiny Coleman integrals

This is easy in the plane curve case: find a uniformizer t on the residue disk, and then compute $\int_a^b \omega = \int_a^b f(t)\,dt$ by formally antidifferentiating each term of $f(t) \in \mathbf{Q}_p[[t]]$.

For modular curves, this is harder: you only have the j-invariant as a coordinate.

You can take a q-expansion of ω and then write it in terms of the uniformizer $j - j_0$ using analytic methods, but then you will have to pin down the coefficients as algebraic numbers.

But this is actually feasible! You can study the ramification of $j\colon X_H \to \mathbf{P}^1$ to figure out the denominators of the coefficients. Then you can use integer programming or Fourier-theoretic techniques to pin down the algebraic integers rigorously. (Rendell-X., 2025)

Remark

My paper requires you are expanding at a CM point, but this is OK because each residue disk has lots of CM points.

Computing tiny Coleman integrals

This is easy in the plane curve case: find a uniformizer t on the residue disk, and then compute $\int_a^b \omega = \int_a^b f(t)\,dt$ by formally antidifferentiating each term of $f(t) \in \mathbf{Q}_p[[t]]$.

For modular curves, this is harder: you only have the j-invariant as a coordinate.

You can take a q-expansion of ω and then write it in terms of the uniformizer $j - j_0$ using analytic methods, but then you will have to pin down the coefficients as algebraic numbers.

But this is actually feasible! You can study the ramification of $j\colon X_H \to \mathbf{P}^1$ to figure out the denominators of the coefficients. Then you can use integer programming or Fourier-theoretic techniques to pin down the algebraic integers rigorously. (Rendell-X., 2025)

Remark

My paper requires you are expanding at a CM point, but this is OK because each residue disk has lots of CM points.

What is quadratic Chabauty?

Here is how quadratic Chabauty works. Let S be the primes of bad reduction for $X/\mathbf{Q}$. Fix a basepoint $b \in X(\mathbf{Q})$.
For $x \in X(\mathbf{Q})$, we have an identity $h(x) = h_p(x) + \sum_{v \in S} h_v(x)$, where h, h_p and h_v are certain functions

$$h \colon J(\mathbf{Q}) \to \mathbf{Q}_p, \quad h_p \colon X(\mathbf{Q}_p) \to \mathbf{Q}_p, \quad h_v \colon X(\mathbf{Q}_v) \to \mathbf{Q}_p.$$

The function h then p-adically interpolates to a function

$$\tilde{h} \colon J(\mathbf{Q}_p) \to \mathbf{Q}_p.$$

The computation of h_p yields some double Coleman integrals.
On the other hand, h_v lands in a computable finite set $\mathcal{T}$.
So one only needs to find the solutions to the $\#\mathcal{T}$ equations

$$\tilde{h} \circ \mathrm{AJ}_b - h_p - \alpha = 0 \qquad (\alpha \in \mathcal{T})$$

to get a finite set containing $X(\mathbf{Q})$.

What is quadratic Chabauty?

Here is how quadratic Chabauty works. Let S be the primes of bad reduction for $X/\mathbf{Q}$. Fix a basepoint $b \in X(\mathbf{Q})$.

For $x \in X(\mathbf{Q})$, we have an identity $h(x) = h_p(x) + \sum_{v \in S} h_v(x)$, where h, h_p and h_v are certain functions

$$h\colon J(\mathbf{Q}) \to \mathbf{Q}_p, \quad h_p\colon X(\mathbf{Q}_p) \to \mathbf{Q}_p, \quad h_v\colon X(\mathbf{Q}_v) \to \mathbf{Q}_p.$$

The function h then p-adically interpolates to a function

$$\tilde{h}\colon J(\mathbf{Q}_p) \to \mathbf{Q}_p.$$

The computation of h_p yields some double Coleman integrals.
On the other hand, h_v lands in a computable finite set $\mathcal{T}$.
So one only needs to find the solutions to the $\#\mathcal{T}$ equations

$$\tilde{h} \circ \mathrm{AJ}_b - h_p - \alpha = 0 \qquad (\alpha \in \mathcal{T})$$

to get a finite set containing $X(\mathbf{Q})$.

What is quadratic Chabauty?

Here is how quadratic Chabauty works. Let S be the primes of bad reduction for $X/\mathbf{Q}$. Fix a basepoint $b \in X(\mathbf{Q})$.
For $x \in X(\mathbf{Q})$, we have an identity $h(x) = h_p(x) + \sum_{v \in S} h_v(x)$, where h, h_p and h_v are certain functions

$$h\colon J(\mathbf{Q}) \to \mathbf{Q}_p, \quad h_p\colon X(\mathbf{Q}_p) \to \mathbf{Q}_p, \quad h_v\colon X(\mathbf{Q}_v) \to \mathbf{Q}_p.$$

The function h then p-adically interpolates to a function

$$\tilde{h}\colon J(\mathbf{Q}_p) \to \mathbf{Q}_p.$$

The computation of h_p yields some double Coleman integrals.
On the other hand, h_v lands in a computable finite set $\mathcal{T}$.
So one only needs to find the solutions to the $\#\mathcal{T}$ equations

$$\tilde{h} \circ \mathrm{AJ}_b - h_p - \alpha = 0 \qquad (\alpha \in \mathcal{T})$$

to get a finite set containing $X(\mathbf{Q})$.

What is quadratic Chabauty?

Here is how quadratic Chabauty works. Let S be the primes of bad reduction for $X/\mathbf{Q}$. Fix a basepoint $b \in X(\mathbf{Q})$.
For $x \in X(\mathbf{Q})$, we have an identity $h(x) = h_p(x) + \sum_{v\in S} h_v(x)$, where h, h_p and h_v are certain functions

$$h\colon J(\mathbf{Q}) \to \mathbf{Q}_p, \quad h_p\colon X(\mathbf{Q}_p) \to \mathbf{Q}_p, \quad h_v\colon X(\mathbf{Q}_v) \to \mathbf{Q}_p.$$

The function h then p-adically interpolates to a function

$$\tilde{h}\colon J(\mathbf{Q}_p) \to \mathbf{Q}_p.$$

The computation of h_p yields some double Coleman integrals.
On the other hand, h_v lands in a computable finite set $\mathcal{T}$.
So one only needs to find the solutions to the $\#\mathcal{T}$ equations

$$\tilde{h} \circ \mathrm{AJ}_b - h_p - \alpha = 0 \qquad (\alpha \in \mathcal{T})$$

to get a finite set containing $X(\mathbf{Q})$.

What is quadratic Chabauty?

Here is how quadratic Chabauty works. Let S be the primes of bad reduction for $X/\mathbf{Q}$. Fix a basepoint $b \in X(\mathbf{Q})$.
For $x \in X(\mathbf{Q})$, we have an identity $h(x) = h_p(x) + \sum_{v \in S} h_v(x)$, where h, h_p and h_v are certain functions

$$h\colon J(\mathbf{Q}) \to \mathbf{Q}_p, \quad h_p\colon X(\mathbf{Q}_p) \to \mathbf{Q}_p, \quad h_v\colon X(\mathbf{Q}_v) \to \mathbf{Q}_p.$$

The function h then p-adically interpolates to a function

$$\tilde{h}\colon J(\mathbf{Q}_p) \to \mathbf{Q}_p.$$

The computation of h_p yields some double Coleman integrals.
On the other hand, h_v lands in a computable finite set $\mathcal{T}$.
So one only needs to find the solutions to the $\#\mathcal{T}$ equations

$$\tilde{h} \circ \mathrm{AJ}_b - h_p - \alpha = 0 \qquad (\alpha \in \mathcal{T})$$

to get a finite set containing $X(\mathbf{Q})$.

What is quadratic Chabauty?

Here is how quadratic Chabauty works. Let S be the primes of bad reduction for $X/\mathbf{Q}$. Fix a basepoint $b \in X(\mathbf{Q})$.
For $x \in X(\mathbf{Q})$, we have an identity $h(x) = h_p(x) + \sum_{v\in S} h_v(x)$, where h, h_p and h_v are certain functions

$$h\colon J(\mathbf{Q}) \to \mathbf{Q}_p, \quad h_p\colon X(\mathbf{Q}_p) \to \mathbf{Q}_p, \quad h_v\colon X(\mathbf{Q}_v) \to \mathbf{Q}_p.$$

The function h then p-adically interpolates to a function

$$\tilde{h}\colon J(\mathbf{Q}_p) \to \mathbf{Q}_p.$$

The computation of h_p yields some double Coleman integrals.
On the other hand, h_v lands in a computable finite set $\mathcal{T}$.
So one only needs to find the solutions to the $\#\mathcal{T}$ equations

$$\tilde{h} \circ \mathrm{AJ}_b - h_p - \alpha = 0 \qquad (\alpha \in \mathcal{T})$$

to get a finite set containing $X(\mathbf{Q})$.

What is quadratic Chabauty?

Here is how quadratic Chabauty works. Let S be the primes of bad reduction for $X/\mathbf{Q}$. Fix a basepoint $b \in X(\mathbf{Q})$.
For $x \in X(\mathbf{Q})$, we have an identity $h(x) = h_p(x) + \sum_{v \in S} h_v(x)$, where h, h_p and h_v are certain functions

$$h\colon J(\mathbf{Q}) \to \mathbf{Q}_p, \quad h_p\colon X(\mathbf{Q}_p) \to \mathbf{Q}_p, \quad h_v\colon X(\mathbf{Q}_v) \to \mathbf{Q}_p.$$

The function h then p-adically interpolates to a function

$$\tilde{h}\colon J(\mathbf{Q}_p) \to \mathbf{Q}_p.$$

The computation of h_p yields some double Coleman integrals.
On the other hand, h_v lands in a computable finite set $\mathcal{T}$.
So one only needs to find the solutions to the $\#\mathcal{T}$ equations

$$\tilde{h} \circ \mathrm{AJ}_b - h_p - \alpha = 0 \qquad (\alpha \in \mathcal{T})$$

to get a finite set containing $X(\mathbf{Q})$.

Computation of h, the global height pairing

We have the equations

$$\tilde{h} \circ \mathrm{AJ}_b - h_p - \alpha = 0 \qquad (\alpha \in \mathcal{T}).$$

If you have enough rational points, you can compute $\tilde{h} \circ \mathrm{AJ}_b$ simply by "interpolation from h_p".

You may not have enough rational points. But for modular curves, you have an out! The functions h, h_v and h_p come from a certain p-adic height pairing, which can be computed directly via p-adic Gross-Zagier formulae.

The case $X_0^+(N)$ is done in (Hashimoto, 2022). We hope to generalize this to arbitrary modular curves.

Computation of h, the global height pairing

We have the equations

$$\tilde{h} \circ \mathrm{AJ}_b - h_p - \alpha = 0 \qquad (\alpha \in \mathcal{T}).$$

If you have enough rational points, you can compute $\tilde{h} \circ \mathrm{AJ}_b$ simply by "interpolation from h_p".

You may not have enough rational points. But for modular curves, you have an out! The functions h, h_v and h_p come from a certain p-adic height pairing, which can be computed directly via p-adic Gross-Zagier formulae.

The case $X_0^+(N)$ is done in (Hashimoto, 2022). We hope to generalize this to arbitrary modular curves.

Computation of h, the global height pairing

We have the equations

$$\tilde{h} \circ \mathrm{AJ}_b - h_p - \alpha = 0 \qquad (\alpha \in \mathcal{T}).$$

If you have enough rational points, you can compute $\tilde{h} \circ \mathrm{AJ}_b$ simply by "interpolation from h_p".

You may not have enough rational points. But for modular curves, you have an out! The functions h, h_v and h_p come from a certain p-adic height pairing, which can be computed directly via p-adic Gross-Zagier formulae.

The case $X_0^+(N)$ is done in (Hashimoto, 2022). We hope to generalize this to arbitrary modular curves.

Computation of h, the global height pairing

We have the equations

$$\tilde{h} \circ \mathrm{AJ}_b - h_p - \alpha = 0 \qquad (\alpha \in \mathcal{T}).$$

If you have enough rational points, you can compute $\tilde{h} \circ \mathrm{AJ}_b$ simply by "interpolation from h_p".

You may not have enough rational points. But for modular curves, you have an out! The functions h, h_v and h_p come from a certain p-adic height pairing, which can be computed directly via p-adic Gross-Zagier formulae.

The case $X_0^+(N)$ is done in (Hashimoto, 2022). We hope to generalize this to arbitrary modular curves.

Computation of h, the global height pairing

We have the equations

$$\tilde{h} \circ \mathrm{AJ}_b - h_p - \alpha = 0 \qquad (\alpha \in \mathcal{T}).$$

If you have enough rational points, you can compute $\tilde{h} \circ \mathrm{AJ}_b$ simply by "interpolation from h_p".
You may not have enough rational points. But for modular curves, you have an out! The functions h, h_v and h_p come from a certain p-adic height pairing, which can be computed directly via p-adic Gross-Zagier formulae.
The case $X_0^+(N)$ is done in (Hashimoto, 2022). We hope to generalize this to arbitrary modular curves.

Computation of h_v

This requires a semistable model of X at v.

For modular curves, the way to make this equationless is to use (Weinstein, 2016), which gives semistable models of arbitrary level modular curves.[8]

We hope to turn Weinstein's techniques into an algorithm.

[8] So long as $v \neq 2$. Sigh.

Computation of h_v

This requires a semistable model of X at v.
For modular curves, the way to make this equationless is to use (Weinstein, 2016), which gives semistable models of arbitrary level modular curves.[8]
We hope to turn Weinstein's techniques into an algorithm.

[8] So long as $v \neq 2$. Sigh.

Computation of h_v

This requires a semistable model of X at v.
For modular curves, the way to make this equationless is to use (Weinstein, 2016), which gives semistable models of arbitrary level modular curves.[8]
We hope to turn Weinstein's techniques into an algorithm.

[8] So long as $v \neq 2$. Sigh.

Computation of h_p (one aspect of it)

The most salient issue is the conversion of large double Coleman integrals into tiny Coleman integrals.

For modular curves, you cannot use the Hecke correspondence T_p anymore; you have to use an actual function. The map V_p (quotienting an elliptic curve by its canonical subgroup) provides a candidate, provided you pick CM points that are “not too supersingular at p”.

You have a path γ from P to Q which you rewrite as $c_a \circ V_p(\gamma) \circ c_b$, where c_a goes from P to $V_p(P)$ and c_b goes from $V_p(Q)$ to Q.

For Hecke eigenforms ω_1, ω_2, you have $V_p^* \omega_i = \alpha_i \omega_i + df_i$ for $i = 1, 2$.

You can then combine this with the *shuffle relation*

$$\int_\gamma \omega_1\omega_2 = \int_{c_a} \omega_1\omega_2 + \int_{c_b} \omega_1\omega_2 + \int_{V_p(\gamma)} \omega_1\omega_2 + \int_{c_a} \omega_1 \int_{V_p(\gamma)} \omega_2 + \int_{c_a} \omega_1 \int_{c_b} \omega_2 + \int_{V_p(\gamma)} \omega_1 \int_{c_b} \omega_2$$

to get an expression in terms of single integrals and tiny double integrals.

Computation of h_p (one aspect of it)

The most salient issue is the conversion of large double Coleman integrals into tiny Coleman integrals.

For modular curves, you cannot use the Hecke correspondence T_p anymore; you have to use an actual function. The map V_p (quotienting an elliptic curve by its canonical subgroup) provides a candidate, provided you pick CM points that are "not too supersingular at p".

You have a path γ from P to Q which you rewrite as $c_a \circ V_p(\gamma) \circ c_b$, where c_a goes from P to $V_p(P)$ and c_b goes from $V_p(Q)$ to Q.

For Hecke eigenforms ω_1, ω_2, you have $V_p^* \omega_i = \alpha_i \omega_i + df_i$ for $i = 1, 2$.

You can then combine this with the *shuffle relation*

$$\int_\gamma \omega_1\omega_2 = \int_{c_a} \omega_1\omega_2 + \int_{c_b} \omega_1\omega_2 + \int_{V_p(\gamma)} \omega_1\omega_2 + \int_{c_a} \omega_1 \int_{V_p(\gamma)} \omega_2 + \int_{c_a} \omega_1 \int_{c_b} \omega_2 + \int_{V_p(\gamma)} \omega_1 \int_{c_b} \omega_2$$

to get an expression in terms of single integrals and tiny double integrals.

Computation of h_p (one aspect of it)

The most salient issue is the conversion of large double Coleman integrals into tiny Coleman integrals.

For modular curves, you cannot use the Hecke correspondence T_p anymore; you have to use an actual function. The map V_p (quotienting an elliptic curve by its canonical subgroup) provides a candidate, provided you pick CM points that are "not too supersingular at p".

You have a path γ from P to Q which you rewrite as $c_a \circ V_p(\gamma) \circ c_b$, where c_a goes from P to $V_p(P)$ and c_b goes from $V_p(Q)$ to Q.

For Hecke eigenforms ω_1, ω_2, you have $V_p^* \omega_i = \alpha_i \omega_i + df_i$ for $i = 1, 2$.

You can then combine this with the *shuffle relation*

$$\int_\gamma \omega_1\omega_2 = \int_{c_a} \omega_1\omega_2 + \int_{c_b} \omega_1\omega_2 + \int_{V_p(\gamma)} \omega_1\omega_2 + \int_{c_a} \omega_1 \int_{V_p(\gamma)} \omega_2 + \int_{c_a} \omega_1 \int_{c_b} \omega_2 + \int_{V_p(\gamma)} \omega_1 \int_{c_b} \omega_2$$

to get an expression in terms of single integrals and tiny double integrals.

Computation of h_p (one aspect of it)

The most salient issue is the conversion of large double Coleman integrals into tiny Coleman integrals.

For modular curves, you cannot use the Hecke correspondence T_p anymore; you have to use an actual function. The map V_p (quotienting an elliptic curve by its canonical subgroup) provides a candidate, provided you pick CM points that are "not too supersingular at p".

You have a path γ from P to Q which you rewrite as $c_a \circ V_p(\gamma) \circ c_b$, where c_a goes from P to $V_p(P)$ and c_b goes from $V_p(Q)$ to Q.

For Hecke eigenforms ω_1, ω_2, you have $V_p^* \omega_i = \alpha_i \omega_i + df_i$ for $i = 1, 2$. You can then combine this with the *shuffle relation*

$$\int_\gamma \omega_1\omega_2 = \int_{c_a} \omega_1\omega_2 + \int_{c_b} \omega_1\omega_2 + \int_{V_p(\gamma)} \omega_1\omega_2 + \int_{c_a} \omega_1 \int_{V_p(\gamma)} \omega_2 + \int_{c_a} \omega_1 \int_{c_b} \omega_2 + \int_{V_p(\gamma)} \omega_1 \int_{c_b} \omega_2$$

to get an expression in terms of single integrals and tiny double integrals.

Computation of h_p (one aspect of it)

The most salient issue is the conversion of large double Coleman integrals into tiny Coleman integrals.

For modular curves, you cannot use the Hecke correspondence T_p anymore; you have to use an actual function. The map V_p (quotienting an elliptic curve by its canonical subgroup) provides a candidate, provided you pick CM points that are "not too supersingular at p".

You have a path γ from P to Q which you rewrite as $c_a \circ V_p(\gamma) \circ c_b$, where c_a goes from P to $V_p(P)$ and c_b goes from $V_p(Q)$ to Q.

For Hecke eigenforms ω_1, ω_2, you have $V_p^* \omega_i = \alpha_i \omega_i + df_i$ for $i = 1, 2$.

You can then combine this with the *shuffle relation*

$$\int_\gamma \omega_1\omega_2 = \int_{c_a} \omega_1\omega_2 + \int_{c_b} \omega_1\omega_2 + \int_{V_p(\gamma)} \omega_1\omega_2 + \int_{c_a} \omega_1 \int_{V_p(\gamma)} \omega_2 + \int_{c_a} \omega_1 \int_{c_b} \omega_2 + \int_{V_p(\gamma)} \omega_1 \int_{c_b} \omega_2$$

to get an expression in terms of single integrals and tiny double integrals.

Computation of h_p (one aspect of it)

The most salient issue is the conversion of large double Coleman integrals into tiny Coleman integrals.

For modular curves, you cannot use the Hecke correspondence T_p anymore; you have to use an actual function. The map V_p (quotienting an elliptic curve by its canonical subgroup) provides a candidate, provided you pick CM points that are "not too supersingular at p".

You have a path γ from P to Q which you rewrite as $c_a \circ V_p(\gamma) \circ c_b$, where c_a goes from P to $V_p(P)$ and c_b goes from $V_p(Q)$ to Q.

For Hecke eigenforms ω_1, ω_2, you have $V_p^* \omega_i = \alpha_i \omega_i + df_i$ for $i = 1, 2$.

You can then combine this with the *shuffle relation*

$$\int_\gamma \omega_1\omega_2 = \int_{c_a} \omega_1\omega_2 + \int_{c_b} \omega_1\omega_2 + \int_{V_p(\gamma)} \omega_1\omega_2 + \int_{c_a} \omega_1 \int_{V_p(\gamma)} \omega_2 + \int_{c_a} \omega_1 \int_{c_b} \omega_2 + \int_{V_p(\gamma)} \omega_1 \int_{c_b} \omega_2$$

to get an expression in terms of single integrals and tiny double integrals.

Computation of h_p (one aspect of it)

The most salient issue is the conversion of large double Coleman integrals into tiny Coleman integrals.

For modular curves, you cannot use the Hecke correspondence T_p anymore; you have to use an actual function. The map V_p (quotienting an elliptic curve by its canonical subgroup) provides a candidate, provided you pick CM points that are "not too supersingular at p".

You have a path γ from P to Q which you rewrite as $c_a \circ V_p(\gamma) \circ c_b$, where c_a goes from P to $V_p(P)$ and c_b goes from $V_p(Q)$ to Q.

For Hecke eigenforms ω_1, ω_2, you have $V_p^* \omega_i = \alpha_i \omega_i + df_i$ for $i = 1, 2$.

You can then combine this with the *shuffle relation*

$$\int_\gamma \omega_1\omega_2 = \int_{c_a} \omega_1\omega_2 + \int_{c_b} \omega_1\omega_2 + \int_{V_p(\gamma)} \omega_1\omega_2 + \int_{c_a} \omega_1 \int_{V_p(\gamma)} \omega_2 + \int_{c_a} \omega_1 \int_{c_b} \omega_2 + \int_{V_p(\gamma)} \omega_1 \int_{c_b} \omega_2$$

to get an expression in terms of single integrals and tiny double integrals.

Computation of h_p (one aspect of it)

The most salient issue is the conversion of large double Coleman integrals into tiny Coleman integrals.
For modular curves, you cannot use the Hecke correspondence T_p anymore; you have to use an actual function. The map V_p (quotienting an elliptic curve by its canonical subgroup) provides a candidate, provided you pick CM points that are "not too supersingular at p".
You have a path γ from P to Q which you rewrite as $c_a \circ V_p(\gamma) \circ c_b$, where c_a goes from P to $V_p(P)$ and c_b goes from $V_p(Q)$ to Q.
For Hecke eigenforms ω_1, ω_2, you have $V_p^* \omega_i = \alpha_i \omega_i + df_i$ for $i = 1, 2$.
You can then combine this with the *shuffle relation*

$$\int_\gamma \omega_1\omega_2 = \int_{c_a} \omega_1\omega_2 + \int_{c_b} \omega_1\omega_2 + \int_{V_p(\gamma)} \omega_1\omega_2 + \int_{c_a} \omega_1 \int_{V_p(\gamma)} \omega_2 + \int_{c_a} \omega_1 \int_{c_b} \omega_2 + \int_{V_p(\gamma)} \omega_1 \int_{c_b} \omega_2$$

to get an expression in terms of single integrals and tiny double integrals.

Some speculation on motivic Chabauty

Corwin's theory gives a coordinate for arbitrary depth n. He states:

> *"We hope to work with [Jacobians of arbitrary curves] in the future, the only obstacle being the messiness of the representation theory of reductive groups larger than* GL_2*."*

In general, you have to work with GSp_{2g}.

But for a modular curve, all simple factors of its Jacobian are of GL_2-type. For us, it means that you only have to work with $\mathrm{Res}_{K/\mathbf{Q}}\,\mathrm{GL}_2$ for certain number fields K.

We hope to make some progress on this matter.[9]

[9] Unfortunately, there is only so much you can do in a few years...

Some speculation on motivic Chabauty

Corwin's theory gives a coordinate for arbitrary depth n. He states:

> *"We hope to work with [Jacobians of arbitrary curves] in the future, the only obstacle being the messiness of the representation theory of reductive groups larger than* GL_2*."*

In general, you have to work with GSp_{2g}.

But for a modular curve, all simple factors of its Jacobian are of GL_2-type. For us, it means that you only have to work with $\mathrm{Res}_{K/\mathbf{Q}} \mathrm{GL}_2$ for certain number fields K.

We hope to make some progress on this matter.[9]

[9] Unfortunately, there is only so much you can do in a few years.

Some speculation on motivic Chabauty

Corwin's theory gives a coordinate for arbitrary depth n. He states:

> *"We hope to work with [Jacobians of arbitrary curves] in the future, the only obstacle being the messiness of the representation theory of reductive groups larger than* GL_2*."*

In general, you have to work with GSp_{2g}.

But for a modular curve, all simple factors of its Jacobian are of GL_2-type. For us, it means that you only have to work with $\mathrm{Res}_{K/\mathbf{Q}}\,\mathrm{GL}_2$ for certain number fields K.

We hope to make some progress on this matter.[9]

[9] Unfortunately, there is only so much you can do in a few years.

Some speculation on motivic Chabauty

Corwin's theory gives a coordinate for arbitrary depth n. He states:

> *"We hope to work with [Jacobians of arbitrary curves] in the future, the only obstacle being the messiness of the representation theory of reductive groups larger than* GL_2*."*

In general, you have to work with GSp_{2g}.
But for a modular curve, all simple factors of its Jacobian are of GL_2-type. For us, it means that you only have to work with $\mathrm{Res}_{K/\mathbf{Q}}\,\mathrm{GL}_2$ for certain number fields K.
We hope to make some progress on this matter.[9]

[9] Unfortunately, there is only so much you can do in a few years.

Some speculation on motivic Chabauty

Corwin's theory gives a coordinate for arbitrary depth n. He states:

> *"We hope to work with [Jacobians of arbitrary curves] in the future, the only obstacle being the messiness of the representation theory of reductive groups larger than* GL_2*."*

In general, you have to work with GSp_{2g}.
But for a modular curve, all simple factors of its Jacobian are of GL_2-type. For us, it means that you only have to work with $\mathrm{Res}_{K/\mathbf{Q}}\,\mathrm{GL}_2$ for certain number fields K.
We hope to make some progress on this matter.[9]

[9] Unfortunately, there is only so much you can do in a few years...

Thanks for listening!