A brief history of ~~time~~ nonabelian Chabauty

Kiran S. Kedlaya

Department of Mathematics, University of California San Diego
kedlaya@ucsd.edu
These slides can be downloaded from https://kskedlaya.org/slides/.

International Centre for Mathematical Sciences
Edinburgh, Scotland, United Kingdom
November 25, 2024

Supported by (grant DMS-2401536 and prior) and UC San Diego (Warschawski Professorship). Thanks also to the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation.

I acknowledge that my workplace occupies unceded ancestral land of the Kumeyaay Nation.

Contents

Origins

Given an explicit polynomial $P(x, y)$ with rational coefficients, can one fully describe the set

$$\{(x, y) \in \mathbb{Q}^2 \colon Q(x, y) = 0\},$$

particularly in cases where it is guaranteed to be finite?

In modern language: let X be an classical[1] curve of genus g over $\mathbb{Q}$ with some explicit description. When $g > 1$, $X(\mathbb{Q})$ is finite; can one describe it explicitly?

This problem has an extensive history...

[1] Meaning smooth, proper, geometrically irreducible. Also called "nice" by some authors.

Origins

Given an explicit polynomial $P(x, y)$ with rational coefficients, can one fully describe the set

$$\{(x, y) \in \mathbb{Q}^2 \colon Q(x, y) = 0\},$$

particularly in cases where it is guaranteed to be finite?

In modern language: let X be an classical[1] curve of genus g over $\mathbb{Q}$ with some explicit description. When $g > 1$, $X(\mathbb{Q})$ is finite; can one describe it explicitly?

This problem has an extensive history...

[1] Meaning smooth, proper, geometrically irreducible. Also called "nice" by some authors.

Origins

Given an explicit polynomial $P(x, y)$ with rational coefficients, can one fully describe the set

$$\{(x, y) \in \mathbb{Q}^2 \colon Q(x, y) = 0\},$$

particularly in cases where it is guaranteed to be finite?

In modern language: let X be an classical[1] curve of genus g over $\mathbb{Q}$ with some explicit description. When $g > 1$, $X(\mathbb{Q})$ is finite; can one describe it explicitly?

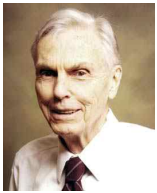
This problem has an extensive history...

[1] Meaning smooth, proper, geometrically irreducible. Also called "nice" by some authors.

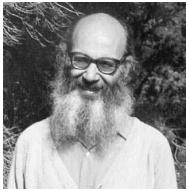
A brief history in photos








Infinite descent

Let X be a classical[2] curve over $\mathbb{Q}$. Fermat's method of **infinite descent** shows that in certain cases,the existence of a $\mathbb{Q}$-rational point on X would imply the existence of a "smaller" $\mathbb{Q}$-rational point on some other curve(s). For instance, for the curve

$$x^4 + y^4 = z^2,$$

this forms a closed loop which shows that there are no $\mathbb{Q}$-rational points other than trivial ones.

For X of genus 1 with a marked point (i.e., an elliptic curve), Mordell adapted Fermat's method to show that $X(\mathbb{Q})$ is a finitely generated abelian group.

For X of genus $g > 1$, the best available analogue is the **Jacobian variety** $J(X)$ in the sense of Weil. Weil adapted Mordell's argument to $J(X)$, and even to a general abelian variety A.

[2] Meaning smooth, proper, geometrically irreducible. Also called "nice" by some authors.

Infinite descent

Let X be a classical[2] curve over $\mathbb{Q}$. Fermat's method of **infinite descent** shows that in certain cases,the existence of a $\mathbb{Q}$-rational point on X would imply the existence of a "smaller" $\mathbb{Q}$-rational point on some other curve(s). For instance, for the curve

$$x^4 + y^4 = z^2,$$

this forms a closed loop which shows that there are no $\mathbb{Q}$-rational points other than trivial ones.

For X of genus 1 with a marked point (i.e., an elliptic curve), Mordell adapted Fermat's method to show that $X(\mathbb{Q})$ is a finitely generated abelian group.

For X of genus $g > 1$, the best available analogue is the **Jacobian variety** $J(X)$ in the sense of Weil. Weil adapted Mordell's argument to $J(X)$, and even to a general abelian variety A.

[2] Meaning smooth, proper, geometrically irreducible. Also called "nice" by some authors.

Infinite descent

Let X be a classical[2] curve over $\mathbb{Q}$. Fermat's method of **infinite descent** shows that in certain cases,the existence of a $\mathbb{Q}$-rational point on X would imply the existence of a "smaller" $\mathbb{Q}$-rational point on some other curve(s). For instance, for the curve

$$x^4 + y^4 = z^2,$$

this forms a closed loop which shows that there are no $\mathbb{Q}$-rational points other than trivial ones.

For X of genus 1 with a marked point (i.e., an elliptic curve), Mordell adapted Fermat's method to show that $X(\mathbb{Q})$ is a finitely generated abelian group.

For X of genus $g > 1$, the best available analogue is the **Jacobian variety** $J(X)$ in the sense of Weil. Weil adapted Mordell's argument to $J(X)$, and even to a general abelian variety A.

[2] Meaning smooth, proper, geometrically irreducible. Also called "nice" by some authors.

Descent and Selmer groups

Weil's approach in the language of Cassels: for $\varphi\colon A \to A$ an isogeny (e.g., multiplication by 2), one has an exact sequence

$$0 \to A(\mathbb{Q})/\varphi(A(\mathbb{Q})) \to \mathrm{Sel}^{\varphi}(A) \to Ш(A)[\varphi] \to 0$$

where $\mathrm{Sel}_{\varphi}(A)$ is a certain "easy" finite Galois cohomology group (the **Selmer group**) and $Ш(A)$ is a fixed but "hard" group (the **Tate–Shafarevich group**).

By composing φ, we can compare sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(\mathbb{Q})/\varphi^{n+1}(A(\mathbb{Q})) & \longrightarrow & \mathrm{Sel}^{\varphi^{n+1}}(A) & \longrightarrow & Ш(A)[\varphi^{n+1}] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(\mathbb{Q})/\varphi^{n}(A(\mathbb{Q})) & \longrightarrow & \mathrm{Sel}^{\varphi^{n}}(A) & \longrightarrow & Ш(A)[\varphi^{n}] & \longrightarrow & 0 \end{array}$$

Descent and Selmer groups

Weil's approach in the language of Cassels: for $\varphi\colon A \to A$ an isogeny (e.g., multiplication by 2), one has an exact sequence

$$0 \to A(\mathbb{Q})/\varphi(A(\mathbb{Q})) \to \mathrm{Sel}^{\varphi}(A) \to Ш(A)[\varphi] \to 0$$

where $\mathrm{Sel}_{\varphi}(A)$ is a certain "easy" finite Galois cohomology group (the **Selmer group**) and $Ш(A)$ is a fixed but "hard" group (the **Tate–Shafarevich group**).

By composing φ, we can compare sequences:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A(\mathbb{Q})/\varphi^{n+1}(A(\mathbb{Q})) & \longrightarrow & \mathrm{Sel}^{\varphi^{n+1}}(A) & \longrightarrow & Ш(A)[\varphi^{n+1}] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A(\mathbb{Q})/\varphi^{n}(A(\mathbb{Q})) & \longrightarrow & \mathrm{Sel}^{\varphi^{n}}(A) & \longrightarrow & Ш(A)[\varphi^{n}] & \longrightarrow & 0
\end{array}$$

Descent and Selmer groups (continued)

By composing φ, we can compare sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(\mathbb{Q})/\varphi^{n+1}(A(\mathbb{Q})) & \longrightarrow & \mathrm{Sel}^{\varphi^{n+1}}(A) & \longrightarrow & Ш(A)[\varphi^{n+1}] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(\mathbb{Q})/\varphi^{n}(A(\mathbb{Q})) & \longrightarrow & \mathrm{Sel}^{\varphi^{n}}(A) & \longrightarrow & Ш(A)[\varphi^{n}] & \longrightarrow & 0 \end{array}$$

The failure of a class in $\mathrm{Sel}^{\varphi^n}(A)$ to lift to $\mathrm{Sel}^{\varphi^{n+1}}(A)$ gives rise to an element of $Ш(A)[\varphi^n]$.

It is conjectured that $Ш(A)$ is finite. If so, one can in principle find all of $Ш(A)[\varphi^\infty]$, give the correct upper bound on $A(\mathbb{Q})/\varphi(A(\mathbb{Q}))$, and find points of $A(\mathbb{Q})$ to match.

In practice this is quite challenging, but it has been carried out in many cases where $\mathrm{Sel}^{\varphi}(A)$ is not too large (e.g., many many elliptic curves). However, when X is a curve of genus $g > 1$, there is still a big gap between computing $J(X)(\mathbb{Q})$ and $X(\mathbb{Q})$.

Descent and Selmer groups (continued)

By composing φ, we can compare sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(\mathbb{Q})/\varphi^{n+1}(A(\mathbb{Q})) & \longrightarrow & \mathrm{Sel}^{\varphi^{n+1}}(A) & \longrightarrow & Ш(A)[\varphi^{n+1}] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(\mathbb{Q})/\varphi^{n}(A(\mathbb{Q})) & \longrightarrow & \mathrm{Sel}^{\varphi^{n}}(A) & \longrightarrow & Ш(A)[\varphi^{n}] & \longrightarrow & 0 \end{array}$$

The failure of a class in $\mathrm{Sel}^{\varphi^n}(A)$ to lift to $\mathrm{Sel}^{\varphi^{n+1}}(A)$ gives rise to an element of $Ш(A)[\varphi^n]$.

It is conjectured that $Ш(A)$ is finite. If so, one can in principle find all of $Ш(A)[\varphi^\infty]$, give the correct upper bound on $A(\mathbb{Q})/\varphi(A(\mathbb{Q}))$, and find points of $A(\mathbb{Q})$ to match.

In practice this is quite challenging, but it has been carried out in many cases where $\mathrm{Sel}^{\varphi}(A)$ is not too large (e.g., many many elliptic curves). However, when X is a curve of genus $g > 1$, there is still a big gap between computing $J(X)(\mathbb{Q})$ and $X(\mathbb{Q})$.

Descent and Selmer groups (continued)

By composing φ, we can compare sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(\mathbb{Q})/\varphi^{n+1}(A(\mathbb{Q})) & \longrightarrow & \mathrm{Sel}^{\varphi^{n+1}}(A) & \longrightarrow & Ш(A)[\varphi^{n+1}] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(\mathbb{Q})/\varphi^{n}(A(\mathbb{Q})) & \longrightarrow & \mathrm{Sel}^{\varphi^{n}}(A) & \longrightarrow & Ш(A)[\varphi^{n}] & \longrightarrow & 0 \end{array}$$

The failure of a class in $\mathrm{Sel}^{\varphi^n}(A)$ to lift to $\mathrm{Sel}^{\varphi^{n+1}}(A)$ gives rise to an element of $Ш(A)[\varphi^n]$.

It is conjectured that $Ш(A)$ is finite. If so, one can in principle find all of $Ш(A)[\varphi^\infty]$, give the correct upper bound on $A(\mathbb{Q})/\varphi(A(\mathbb{Q}))$, and find points of $A(\mathbb{Q})$ to match.

In practice this is quite challenging, but it has been carried out in many cases where $\mathrm{Sel}^{\varphi}(A)$ is not too large (e.g., many many elliptic curves). However, when X is a curve of genus $g > 1$, there is still a big gap between computing $J(X)(\mathbb{Q})$ and $X(\mathbb{Q})$.

Contents

The section conjecture

Inspired by Faltings's proof of the Mordell conjecture, Grothendieck reinterpreted this story in terms of étale fundamental groups. For X a classical[3] curve over $\mathbb{Q}$ and $\overline{x}$ a fixed geometric basepoint, we have an exact sequence

$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x}) \to \pi_1(X, \overline{x}) \to G_{\mathbb{Q}} \to 1.$$

For $x \in X(\mathbb{Q})$, the inclusion $x \to X$ defines (up to conjugation) a section $G_{\mathbb{Q}} \to \pi_1(X, \overline{x})$. The **section conjecture** asserts that conversely every section arises in this way.

Now let U be some characteristic subgroup of $\pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})$. Any section of the previous section (in particular any rational point) also defines a section of

$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})/U \to \pi_1(X, \overline{x})/U \to G_{\mathbb{Q}} \to 1.$$

These may be much easier to classify, but on the other hand there might be too many of them.

[3] Meaning smooth, proper, geometrically irreducible. Also called "nice" by some authors.

The section conjecture

Inspired by Faltings's proof of the Mordell conjecture, Grothendieck reinterpreted this story in terms of étale fundamental groups. For X a classical[3] curve over $\mathbb{Q}$ and $\overline{x}$ a fixed geometric basepoint, we have an exact sequence

$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x}) \to \pi_1(X, \overline{x}) \to G_{\mathbb{Q}} \to 1.$$

For $x \in X(\mathbb{Q})$, the inclusion $x \to X$ defines (up to conjugation) a section $G_{\mathbb{Q}} \to \pi_1(X, \overline{x})$. The **section conjecture** asserts that conversely every section arises in this way.

Now let U be some characteristic subgroup of $\pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})$. Any section of the previous section (in particular any rational point) also defines a section of

$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})/U \to \pi_1(X, \overline{x})/U \to G_{\mathbb{Q}} \to 1.$$

These may be much easier to classify, but on the other hand there might be too many of them.

[3] Meaning smooth, proper, geometrically irreducible. Also called "nice" by some authors.

The abelian case

For example, let U be the kernel of the maximal abelian quotient of $\pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})$. Then the sections of

$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})/U \to \pi_1(X, \overline{x})/U \to G_{\mathbb{Q}} \to 1.$$

are presumptively equal to $J(X)(\mathbb{Q}) \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ (this holds if $Ш(J(X))$ is finite).

Similarly, fix a prime p and let U_p be the kernel of the maximal abelian pro-p quotient of $\pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})$. Then the sections of

$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})/U_p \to \pi_1(X, \overline{x})/U_p \to G_{\mathbb{Q}} \to 1.$$

are presumptively equal to $J(X)(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

For each n, let $U_{p,n}$ be the kernel of the maximal abelian quotient of $\pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})$ killed by p^n. Then the previous sequence is the inverse limit of the sequences

$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})/U_{p,n} \to \pi_1(X, \overline{x})/U_{p,n} \to G_{\mathbb{Q}} \to 1$$

and this mirrors the approximation of $J(X)(\mathbb{Q}) \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}_p$ via $\mathrm{Sel}^{[p^n]}(J(X))$.

The abelian case

For example, let U be the kernel of the maximal abelian quotient of $\pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})$. Then the sections of

$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})/U \to \pi_1(X, \overline{x})/U \to G_{\mathbb{Q}} \to 1.$$

are presumptively equal to $J(X)(\mathbb{Q}) \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ (this holds if $Ш(J(X))$ is finite).

Similarly, fix a prime p and let U_p be the kernel of the maximal abelian pro-p quotient of $\pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})$. Then the sections of

$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})/U_p \to \pi_1(X, \overline{x})/U_p \to G_{\mathbb{Q}} \to 1.$$

are presumptively equal to $J(X)(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

For each n, let $U_{p,n}$ be the kernel of the maximal abelian quotient of $\pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})$ killed by p^n. Then the previous sequence is the inverse limit of the sequences

$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})/U_{p,n} \to \pi_1(X, \overline{x})/U_{p,n} \to G_{\mathbb{Q}} \to 1$$

and this mirrors the approximation of $J(X)(\mathbb{Q}) \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}_p$ via $\mathrm{Sel}^{[p^n]}(J(X))$.

Contents

Chabauty's theorem

As a partial result towards Mordell's conjecture, Chabauty proved that if rank $J(X)(\mathbb{Q}) < g$, then $X(\mathbb{Q})$ is finite.

Sketch of Chabauty's proof: pick any prime p of good reduction. If rank $J(X)(\mathbb{Q}) < g$, then the points of $J(X)(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}_p$ span a p-adic submanifold of $J(X)(\mathbb{Q}_p)$ of positive codimension; the intersection of this submanifold with $X \subset J(X)$ is finite.

Chabauty's theorem

As a partial result towards Mordell's conjecture, Chabauty proved that if $\operatorname{rank} J(X)(\mathbb{Q}) < g$, then $X(\mathbb{Q})$ is finite.

Sketch of Chabauty's proof: pick any prime p of good reduction. If $\operatorname{rank} J(X)(\mathbb{Q}) < g$, then the points of $J(X)(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}_p$ span a p-adic submanifold of $J(X)(\mathbb{Q}_p)$ of positive codimension; the intersection of this submanifold with $X \subset J(X)$ is finite.

Coleman's observation

Coleman observed that Chabauty's method is in a sense **effective**: the intersection points of X with $J(X)(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}_p$ form a computable finite set.

Remembering the "abelian" part of abelian varieties, Coleman reformulated Chabauty's argument in terms of a p-adic path integral on rigid analytic varieties (the **Coleman integral**): if rank $J(X)(\mathbb{Q}) < g$, then there is a positive-dimensional subspace V of $\Gamma(X, \Omega_{X/\mathbb{Q}}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ such that

$$\int_D \omega = 0 \qquad (D \in \mathrm{Div}^0(X), \omega \in V).$$

If we have a single point $B \in X(\mathbb{Q})$ to use as a basepoint, we then have

$$X(\mathbb{Q}) \subseteq \{P \in X(\mathbb{Q}_p) : \int_B^P \omega = 0 \qquad (\omega \in V)\}.$$

Coleman's observation

Coleman observed that Chabauty's method is in a sense **effective**: the intersection points of X with $J(X)(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}_p$ form a computable finite set.

Remembering the "abelian" part of abelian varieties, Coleman reformulated Chabauty's argument in terms of a p-adic path integral on rigid analytic varieties (the **Coleman integral**): if $\operatorname{rank} J(X)(\mathbb{Q}) < g$, then there is a positive-dimensional subspace V of $\Gamma(X, \Omega_{X/\mathbb{Q}}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ such that

$$\int_D \omega = 0 \qquad (D \in \operatorname{Div}^0(X), \omega \in V).$$

If we have a single point $B \in X(\mathbb{Q})$ to use as a basepoint, we then have

$$X(\mathbb{Q}) \subseteq \{P \in X(\mathbb{Q}_p) : \int_B^P \omega = 0 \qquad (\omega \in V)\}.$$

Coleman's observation

Coleman observed that Chabauty's method is in a sense **effective**: the intersection points of X with $J(X)(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}_p$ form a computable finite set.

Remembering the "abelian" part of abelian varieties, Coleman reformulated Chabauty's argument in terms of a p-adic path integral on rigid analytic varieties (the **Coleman integral**): if $\operatorname{rank} J(X)(\mathbb{Q}) < g$, then there is a positive-dimensional subspace V of $\Gamma(X, \Omega_{X/\mathbb{Q}}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ such that

$$\int_D \omega = 0 \qquad (D \in \operatorname{Div}^0(X), \omega \in V).$$

If we have a single point $B \in X(\mathbb{Q})$ to use as a basepoint, we then have

$$X(\mathbb{Q}) \subseteq \{P \in X(\mathbb{Q}_p) : \int_B^P \omega = 0 \qquad (\omega \in V)\}.$$

Contents

Selmer varieties

Kim realized that the Coleman picture could and should be unified with the Grothendieck picture

$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})/U \to \pi_1(X, \overline{x})/U \to G_{\mathbb{Q}} \to 1,$$

so that the former could be generalized to some characteristic subgroups U with **unipotent** quotients (rather than abelian).

In this picture, the analogue of the p-adic Selmer group $\varprojlim_n \mathrm{Sel}^{[p^n]}(J(X)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a certain **Selmer set** consisting of the $\mathbb{Q}_p$-points of a certain algebraic variety (the **Selmer variety**). Note: this definition "cheats" on the Grothendieck picture by identifying a necessary condition on sections to arise from rational points, based on p-adic Hodge theory.

The analogue of the Chabauty set is now defined by the vanishing of certain **iterated** path integrals also defined by Coleman. However, now it only makes sense to integrate between points, not over a degree-0 divisor.

Selmer varieties

Kim realized that the Coleman picture could and should be unified with the Grothendieck picture

$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})/U \to \pi_1(X, \overline{x})/U \to G_{\mathbb{Q}} \to 1,$$

so that the former could be generalized to some characteristic subgroups U with **unipotent** quotients (rather than abelian).

In this picture, the analogue of the p-adic Selmer group $\varprojlim_n \mathrm{Sel}^{[p^n]}(J(X)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a certain **Selmer set** consisting of the $\mathbb{Q}_p$-points of a certain algebraic variety (the **Selmer variety**). Note: this definition "cheats" on the Grothendieck picture by identifying a necessary condition on sections to arise from rational points, based on p-adic Hodge theory.

The analogue of the Chabauty set is now defined by the vanishing of certain **iterated** path integrals also defined by Coleman. However, now it only makes sense to integrate between points, not over a degree-0 divisor.

Selmer varieties

Kim realized that the Coleman picture could and should be unified with the Grothendieck picture

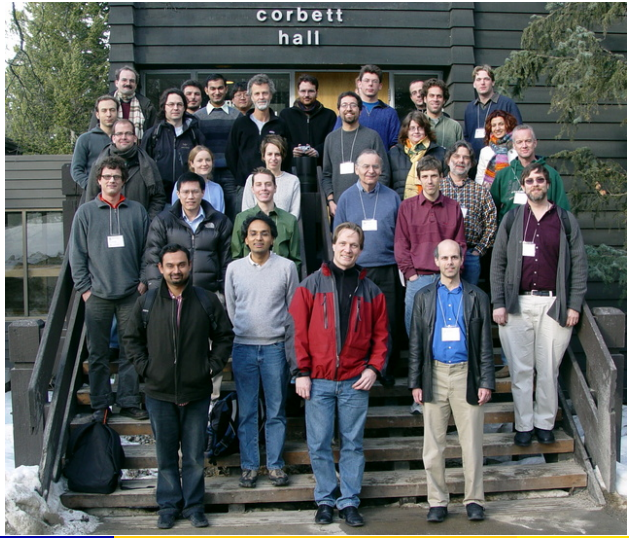
$$1 \to \pi_1(X_{\overline{\mathbb{Q}}}, \overline{x})/U \to \pi_1(X, \overline{x})/U \to G_{\mathbb{Q}} \to 1,$$

so that the former could be generalized to some characteristic subgroups U with **unipotent** quotients (rather than abelian).

In this picture, the analogue of the p-adic Selmer group $\varprojlim_n \mathrm{Sel}^{[p^n]}(J(X)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a certain **Selmer set** consisting of the $\mathbb{Q}_p$-points of a certain algebraic variety (the **Selmer variety**). Note: this definition "cheats" on the Grothendieck picture by identifying a necessary condition on sections to arise from rational points, based on p-adic Hodge theory.

The analogue of the Chabauty set is now defined by the vanishing of certain **iterated** path integrals also defined by Coleman. However, now it only makes sense to integrate between points, not over a degree-0 divisor.

Explicit methods for rational points on curves (Banff, February 2007)



Kim's conjecture

For each n, we can construct the Chabauty–Kim set X_n corresponding to the kernel U_n of the maximal pro-p quotient of nilpotency index $\leq n$. We then have

$$X(\mathbb{Q}) \subseteq \cdots \subseteq X_2 \subseteq X_1 \subseteq X(\mathbb{Q}_p).$$

The finiteness of X_n would follow from a certain analogue of the Chabauty rank condition, which for $n \gg 0$ would follow from a suitable form of the Bloch–Kato conjecture.

Kim conjectures that for $n \gg 0$, not only is X_n finite, but in fact $X_n = X(\mathbb{Q})$. This amounts to a refinement of the section conjecture.

Kim's conjecture

For each n, we can construct the Chabauty–Kim set X_n corresponding to the kernel U_n of the maximal pro-p quotient of nilpotency index $\leq n$. We then have

$$X(\mathbb{Q}) \subseteq \cdots \subseteq X_2 \subseteq X_1 \subseteq X(\mathbb{Q}_p).$$

The finiteness of X_n would follow from a certain analogue of the Chabauty rank condition, which for $n \gg 0$ would follow from a suitable form of the Bloch–Kato conjecture.

Kim conjectures that for $n \gg 0$, not only is X_n finite, but in fact $X_n = X(\mathbb{Q})$. This amounts to a refinement of the section conjecture.

Kim's conjecture

For each n, we can construct the Chabauty–Kim set X_n corresponding to the kernel U_n of the maximal pro-p quotient of nilpotency index $\leq n$. We then have

$$X(\mathbb{Q}) \subseteq \cdots \subseteq X_2 \subseteq X_1 \subseteq X(\mathbb{Q}_p).$$

The finiteness of X_n would follow from a certain analogue of the Chabauty rank condition, which for $n \gg 0$ would follow from a suitable form of the Bloch–Kato conjecture.

Kim conjectures that for $n \gg 0$, not only is X_n finite, but in fact $X_n = X(\mathbb{Q})$. This amounts to a refinement of the section conjecture.

S-units and $\mathbb{P}^1$ minus three points

While we have been assuming until now that X is a proper curve, one can also work with a nonproper hyperbolic curve, e.g., $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. In this context one is interested in S-integral points for some finite set S of primes.

In this context, one can derive new bounds on S-unit equations (Corwin–Dan-Cohen, Betts–Corwin–Leonhardt, Kuhne) and even prove some special cases of Kim's conjecture. For example, if $S = \emptyset$ then eventually $X_n = \emptyset$ (see the upcoming PhD thesis of Baiming Qiao).

S-units and $\mathbb{P}^1$ minus three points

While we have been assuming until now that X is a proper curve, one can also work with a nonproper hyperbolic curve, e.g., $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. In this context one is interested in S-integral points for some finite set S of primes.

In this context, one can derive new bounds on S-unit equations (Corwin–Dan-Cohen, Betts–Corwin–Leonhardt, Kuhne) and even prove some special cases of Kim's conjecture. For example, if $S = \emptyset$ then eventually $X_n = \emptyset$ (see the upcoming PhD thesis of Baiming Qiao).

Computing Chabauty–Kim sets

Building on work with myself and Bradshaw (initiated at the Arizona Winter School in March 2007), Balakrishnan (later Balakrishnan–Tuitman) developed an effective algorithm for computing single and iterated Coleman integrals. This involves separate treatment of **tiny integrals** with endpoints in a single residue disc (which are treated by direct power series manipulation) and **large integrals** with endpoints in distinct residue discs (which are treated using the change of variables property for an analytic Frobenius lift).

This is one key step to computing Chabauty–Kim sets, **but** one also needs some global Galois cohomology to compute Selmer varieties. This seems to be quite challenging!

Computing Chabauty–Kim sets

Building on work with myself and Bradshaw (initiated at the Arizona Winter School in March 2007), Balakrishnan (later Balakrishnan–Tuitman) developed an effective algorithm for computing single and iterated Coleman integrals. This involves separate treatment of **tiny integrals** with endpoints in a single residue disc (which are treated by direct power series manipulation) and **large integrals** with endpoints in distinct residue discs (which are treated using the change of variables property for an analytic Frobenius lift).

This is one key step to computing Chabauty–Kim sets, **but** one also needs some global Galois cohomology to compute Selmer varieties. This seems to be quite challenging!

Quadratic Chabauty (Balakrishnan–Dogra)

Balakrishnan–Dogra were able to make everything more explicit for a certain group between U_1 and U_2, where everything can be described in terms of p-adic height pairings (Coleman–Gross).

The finiteness of the Chabauty–Kim set in this setting is guaranteed by the condition

$$\mathrm{rank}(J(X)(\mathbb{Q})) < g + \rho(J(X))) - 1$$

where $\rho(J(X))$ is the Picard number (rank of Néron–Severi). In the generic case $\rho(J(X)) = 1$ and there is no improvement, but when $\mathrm{NS}(X)$ is large this is extremely useful!

In fact, it would be enough[4] to find a quotient A of $J(X)$ for which

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

as we can adapt the construction to cut $J(X)$ down to A. (Further variations are possible...)

[4] This is not quite the right condition. See Dogra–Le Fourn, "Quadratic Chabauty for modular curves and modular forms of rank one" for a correct treatment.

Quadratic Chabauty (Balakrishnan–Dogra)

Balakrishnan–Dogra were able to make everything more explicit for a certain group between U_1 and U_2, where everything can be described in terms of p-adic height pairings (Coleman–Gross).

The finiteness of the Chabauty–Kim set in this setting is guaranteed by the condition

$$\mathrm{rank}(J(X)(\mathbb{Q})) < g + \rho(J(X))) - 1$$

where $\rho(J(X))$ is the Picard number (rank of Néron–Severi). In the generic case $\rho(J(X)) = 1$ and there is no improvement, but when $\mathrm{NS}(X)$ is large this is extremely useful!

In fact, it would be enough[4] to find a quotient A of $J(X)$ for which

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

as we can adapt the construction to cut $J(X)$ down to A. (Further variations are possible...)

[4] This is not quite the right condition. See Dogra–Le Fourn, "Quadratic Chabauty for modular curves and modular forms of rank one" for a correct treatment.

Quadratic Chabauty (Balakrishnan–Dogra)

Balakrishnan–Dogra were able to make everything more explicit for a certain group between U_1 and U_2, where everything can be described in terms of p-adic height pairings (Coleman–Gross).

The finiteness of the Chabauty–Kim set in this setting is guaranteed by the condition

$$\operatorname{rank}(J(X)(\mathbb{Q})) < g + \rho(J(X))) - 1$$

where $\rho(J(X))$ is the Picard number (rank of Néron–Severi). In the generic case $\rho(J(X)) = 1$ and there is no improvement, but when $\mathrm{NS}(X)$ is large this is extremely useful!

In fact, it would be enough[4] to find a quotient A of $J(X)$ for which

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

as we can adapt the construction to cut $J(X)$ down to A. (Further variations are possible...)

[4] This is not quite the right condition. See Dogra–Le Fourn, "Quadratic Chabauty for modular curves and modular forms of rank one" for a correct treatment.

A target-rich environment: modular curves

Let X be a modular curve of genus g. For every quotient A of $J(X)$, we usually have $\mathrm{rank}(A(\mathbb{Q})) = 0$ or $\mathrm{rank}(A(\mathbb{Q})) = \dim(A)$ according to the sign of the relevant functional equation. Unfortunately, there are certain cases where the latter always occurs, so there is no hope to apply Chabauty–Coleman.

However, in these cases the quadratic Chabauty rank condition is almost always satisfied! For every quotient of A, one has $\mathrm{rank}(\mathrm{NS}(A)) \geq \dim(A)$.

This has been demonstrated spectacularly by Balakrishnan–Dogra–Müller–Tuitman–Vonk, who computed $X(\mathbb{Q})$ for some nonsplit Cartan modular curves in this manner.

A target-rich environment: modular curves

Let X be a modular curve of genus g. For every quotient A of $J(X)$, we usually have $\mathrm{rank}(A(\mathbb{Q})) = 0$ or $\mathrm{rank}(A(\mathbb{Q})) = \dim(A)$ according to the sign of the relevant functional equation. Unfortunately, there are certain cases where the latter always occurs, so there is no hope to apply Chabauty–Coleman.

However, in these cases the quadratic Chabauty rank condition is almost always satisfied! For every quotient of A, one has $\mathrm{rank}(\mathrm{NS}(A)) \geq \dim(A)$.

This has been demonstrated spectacularly by Balakrishnan–Dogra–Müller–Tuitman–Vonk, who computed $X(\mathbb{Q})$ for some nonsplit Cartan modular curves in this manner.

A target-rich environment: modular curves

Let X be a modular curve of genus g. For every quotient A of $J(X)$, we usually have $\mathrm{rank}(A(\mathbb{Q})) = 0$ or $\mathrm{rank}(A(\mathbb{Q})) = \dim(A)$ according to the sign of the relevant functional equation. Unfortunately, there are certain cases where the latter always occurs, so there is no hope to apply Chabauty–Coleman.

However, in these cases the quadratic Chabauty rank condition is almost always satisfied! For every quotient of A, one has $\mathrm{rank}(\mathrm{NS}(A)) \geq \dim(A)$.

This has been demonstrated spectacularly by Balakrishnan–Dogra–Müller–Tuitman–Vonk, who computed $X(\mathbb{Q})$ for some nonsplit Cartan modular curves in this manner.

Contents

What is an "explicit" curve?

At the beginning, I specified that I want to start with an "explicit" curve over $\mathbb{Q}$. What does that mean exactly?

Traditionally this would be interpreted to be mean specifying defining equations in some sense, e.g., the single polynomial defining a singular plane model.

However, for modular curves the more natural "explicit" description is the modular group. Working with a singular plane model creates tremendous computation complexity by comparison.

Is it feasible to describe Chabauty–Kim sets, particularly in the quadratic regime, without having to resort to explicit models?

What is an "explicit" curve?

At the beginning, I specified that I want to start with an "explicit" curve over $\mathbb{Q}$. What does that mean exactly?

Traditionally this would be interpreted to be mean specifying defining equations in some sense, e.g., the single polynomial defining a singular plane model.

However, for modular curves the more natural "explicit" description is the modular group. Working with a singular plane model creates tremendous computation complexity by comparison.

Is it feasible to describe Chabauty–Kim sets, particularly in the quadratic regime, without having to resort to explicit models?

What is an "explicit" curve?

At the beginning, I specified that I want to start with an "explicit" curve over $\mathbb{Q}$. What does that mean exactly?

Traditionally this would be interpreted to be mean specifying defining equations in some sense, e.g., the single polynomial defining a singular plane model.

However, for modular curves the more natural "explicit" description is the modular group. Working with a singular plane model creates tremendous computation complexity by comparison.

Is it feasible to describe Chabauty–Kim sets, particularly in the quadratic regime, without having to resort to explicit models?

What is an "explicit" curve?

At the beginning, I specified that I want to start with an "explicit" curve over $\mathbb{Q}$. What does that mean exactly?

Traditionally this would be interpreted to be mean specifying defining equations in some sense, e.g., the single polynomial defining a singular plane model.

However, for modular curves the more natural "explicit" description is the modular group. Working with a singular plane model creates tremendous computation complexity by comparison.

Is it feasible to describe Chabauty–Kim sets, particularly in the quadratic regime, without having to resort to explicit models?

Avoiding the Frobenius lift

In Balakrishnan–Tuitman, the computation of large Coleman integrals depends on applying a Frobenius lift. For single Coleman integrals on modular curves, we can circumvent this by using the p-th Hecke operator T_p instead.

It is less clear how to handle large iterated Coleman integrals. However, we get a canonical Frobenius lift by splitting up T_p (Eichler–Shimura), and a close reading of Coleman's development of the eigencurve should reveal how to compute pullbacks via this lift.

Avoiding the Frobenius lift

In Balakrishnan–Tuitman, the computation of large Coleman integrals depends on applying a Frobenius lift. For single Coleman integrals on modular curves, we can circumvent this by using the p-th Hecke operator T_p instead.

It is less clear how to handle large iterated Coleman integrals. However, we get a canonical Frobenius lift by splitting up T_p (Eichler–Shimura), and a close reading of Coleman's development of the eigencurve should reveal how to compute pullbacks via this lift.

Model-free tiny integrals

With Chen and Lau, we did some numerical experiments to compute tiny Coleman integrals using **complex** analytic geometry (e.g., on $X_0(37)$). The point is that the local integration involves some manipulation of power series which can be arranged to have $\overline{\mathbb{Q}}$-coefficients (by expanding around CM points), so in principle one can identify these from complex approximations, then project to $\mathbb{Q}_p$.

However, doing this rigorously requires some control on the heights of the rational/algebraic numbers that appear, and we were unable to explain this completely. Xu has recently made some progress on this.

Model-free tiny integrals

With Chen and Lau, we did some numerical experiments to compute tiny Coleman integrals using **complex** analytic geometry (e.g., on $X_0(37)$). The point is that the local integration involves some manipulation of power series which can be arranged to have $\overline{\mathbb{Q}}$-coefficients (by expanding around CM points), so in principle one can identify these from complex approximations, then project to $\mathbb{Q}_p$.

However, doing this rigorously requires some control on the heights of the rational/algebraic numbers that appear, and we were unable to explain this completely. Xu has recently made some progress on this.

Model-free heights

We also need some global input from p-adic heights. By working with CM points, we can hope to access these using some form of p-adic Gross–Zagier (cf. Hashimoto's PhD thesis for the case $X_0(N)^+$).