Triangular Modular Curves (of low genus)

and

Geometric Quadratic Chabauty

Juanita Duque Rosero

Examination Committee: John Voight (advisor), Asher Auel, Pete Clark, and Rosa Orellana.

Outline

- General introduction: Diophantine geometry.

Part 1: triangular modular curves of low genus.

- Basic definitions: triangle groups and triangular modular curves.
- Main theorem and main algorithm for prime level.
- How bad is composite level?

Part 2: geometric quadratic Chabauty.

- Chabauty's theorem and quadratic Chabauty.
- Geometric quadratic Chabauty.
- A comparison theorem and an example.

Welcome to Diophantine Geometry!

Goal. To **describe** rational solutions for systems of polynomial equations

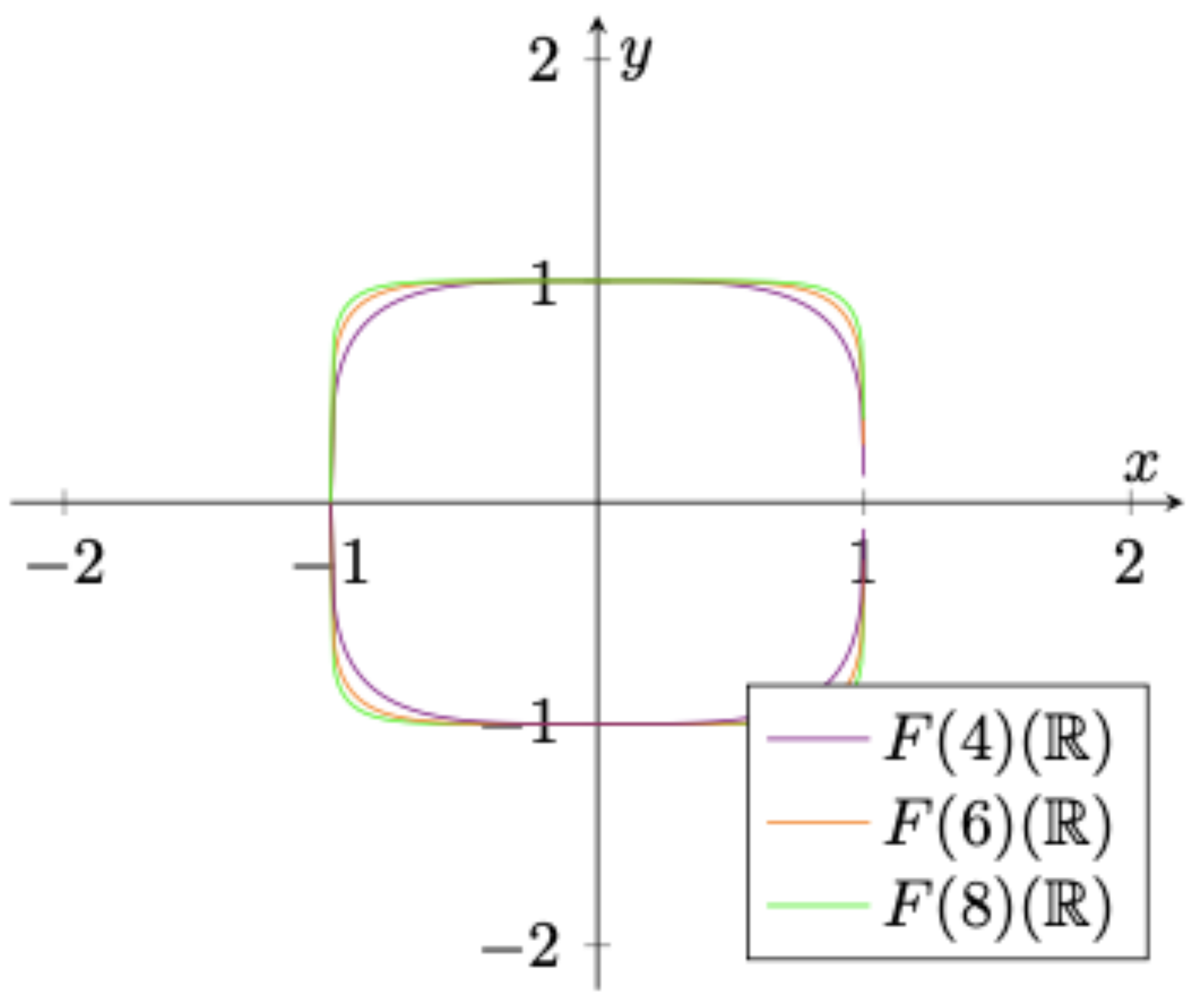
$$X : f_i(x_1, \ldots, x_k) = 0,$$

where $f_i(x_1, \ldots, x_k)$ has rational coefficients.

Examples.

1. Fermat's Last Theorem: for all $n \geq 3$, there are no non-trivial solutions for

$$x^n + y^n - z^n = 0.$$



2. Linear algebra over the rationals.

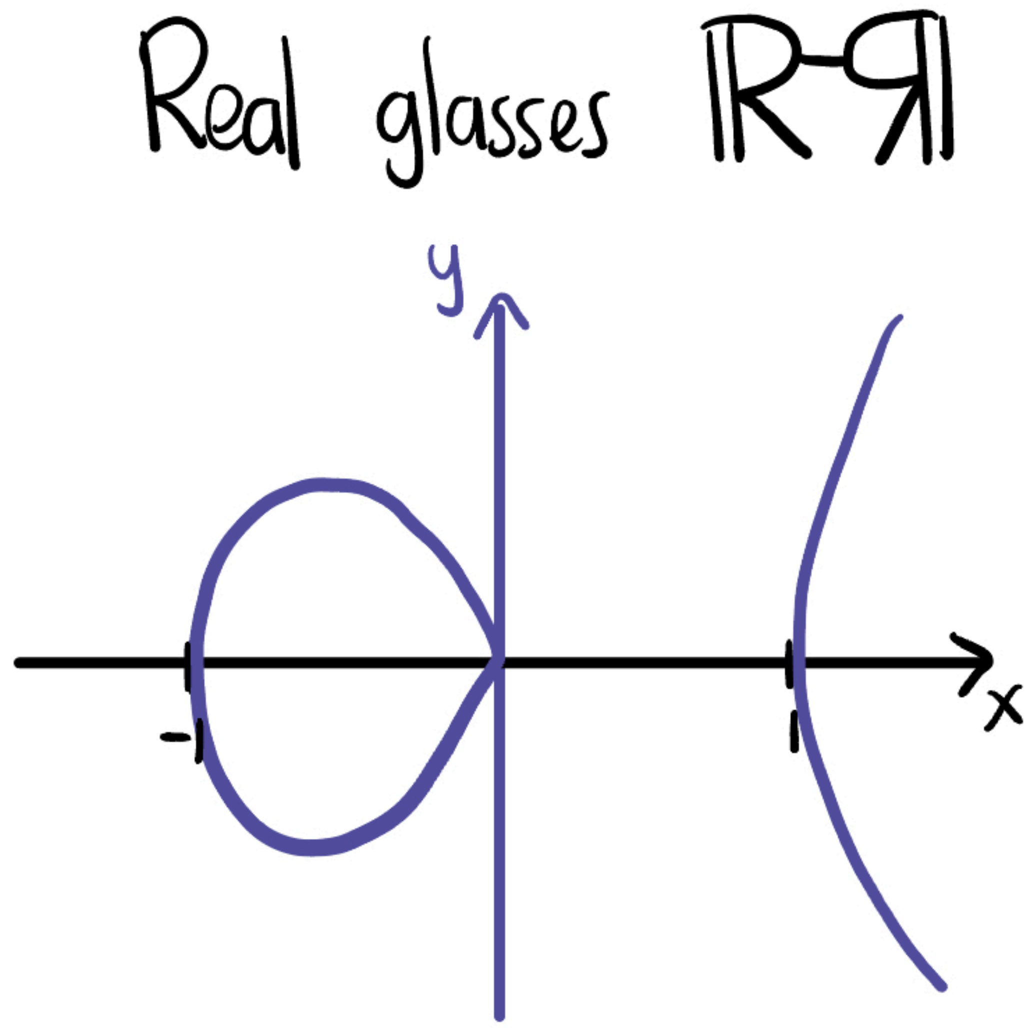
3. $f(x, y) = 0$ gives a **plane curve**.

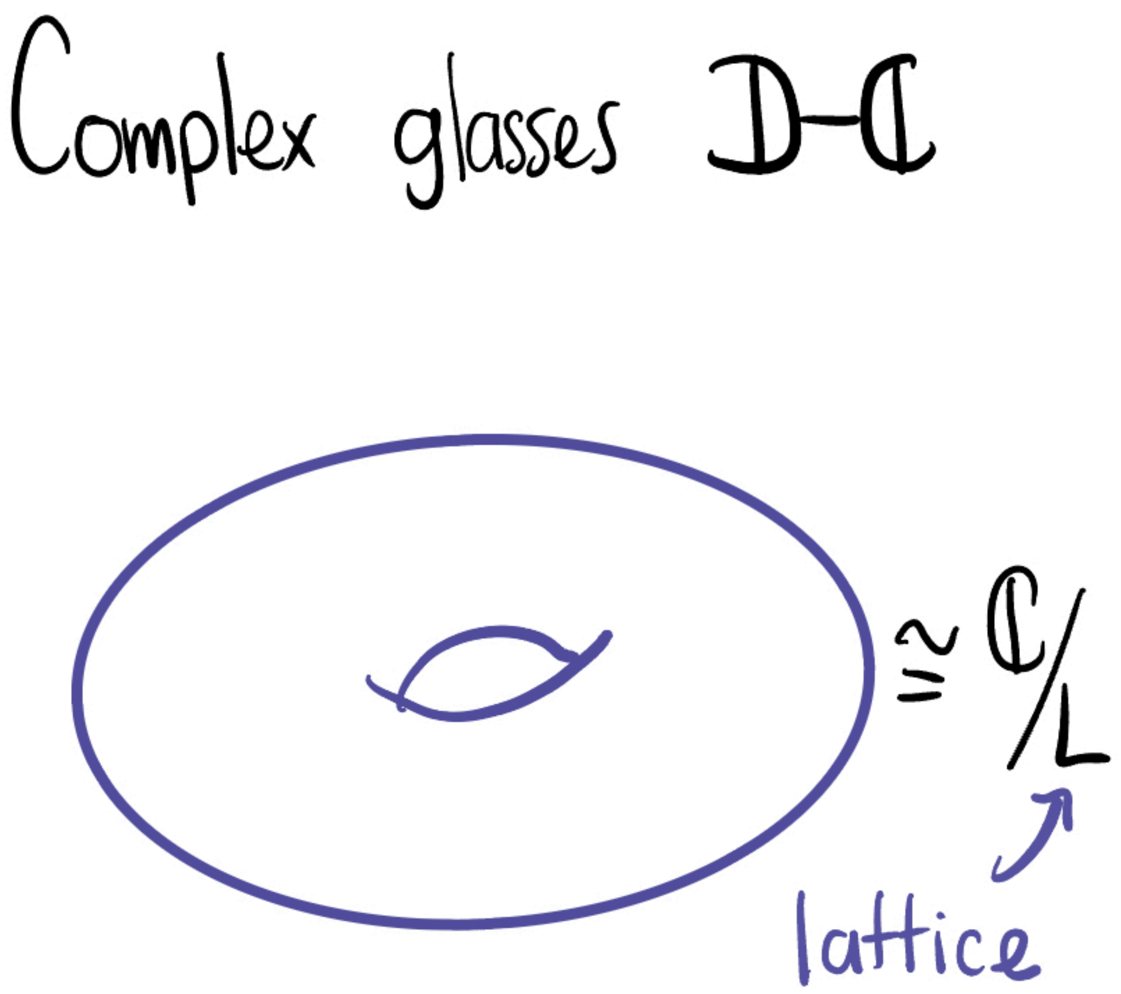
Example: Elliptic Curves

An **elliptic curve** (over $\mathbb{Q}$) consists on solutions of the equation

$$y^2 = f(x),$$

where $f(x)$ is a polynomial of degree 3 defined over $\mathbb{Q}$.





The arithmetic of elliptic curves is rare and amazing! The solutions have the structure of a **finitely generated abelian group** (Mordell's Theorem):

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{Tor}} \times \mathbb{Z}^r .$$

$E(\mathbb{Q})_{\text{Tor}}$

Mazur's Theorem (1978). Let E be an elliptic curve over $\mathbb{Q}$. Then the only possibilities for $E(\mathbb{Q})_{\text{Tor}}$ are:

- $\mathbb{Z}/N\mathbb{Z}$, where $1 \leq N \leq 10$ or $N = 12$; or
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, where $1 \leq N \leq 4$.

Moreover, for each of these possibilities, there are infinitely many curves with that prescribed torsion.

Key idea: we want to understand elliptic curves with torsion group of a certain order.

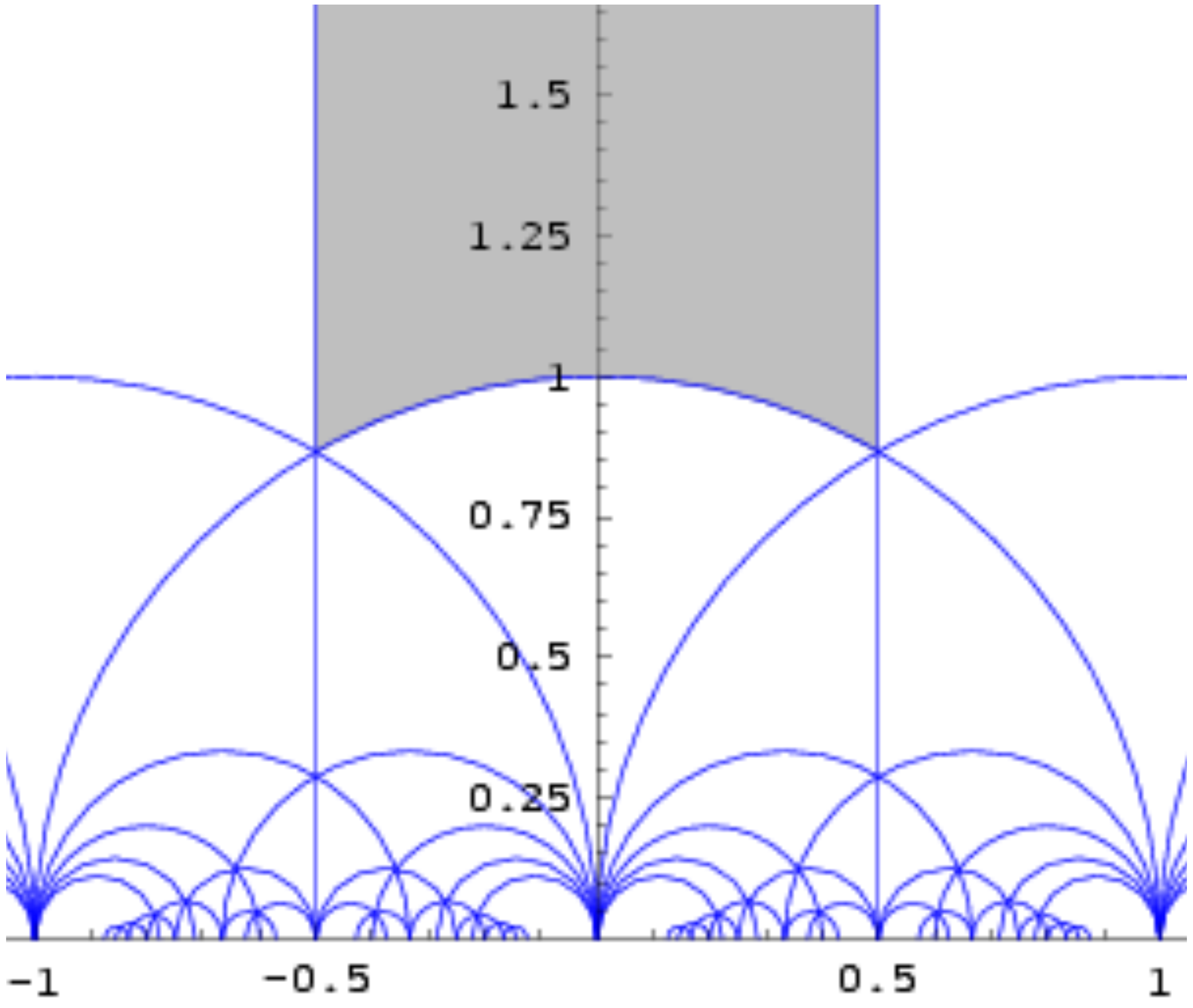
Modular Curves!

Modular Curves

There is an action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathscr{H}$, the upper-half complex plane:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}.$$

By taking the quotient of $\mathscr{H}$ by this action, we obtain a Riemann surface. We call this a **modular curve**.



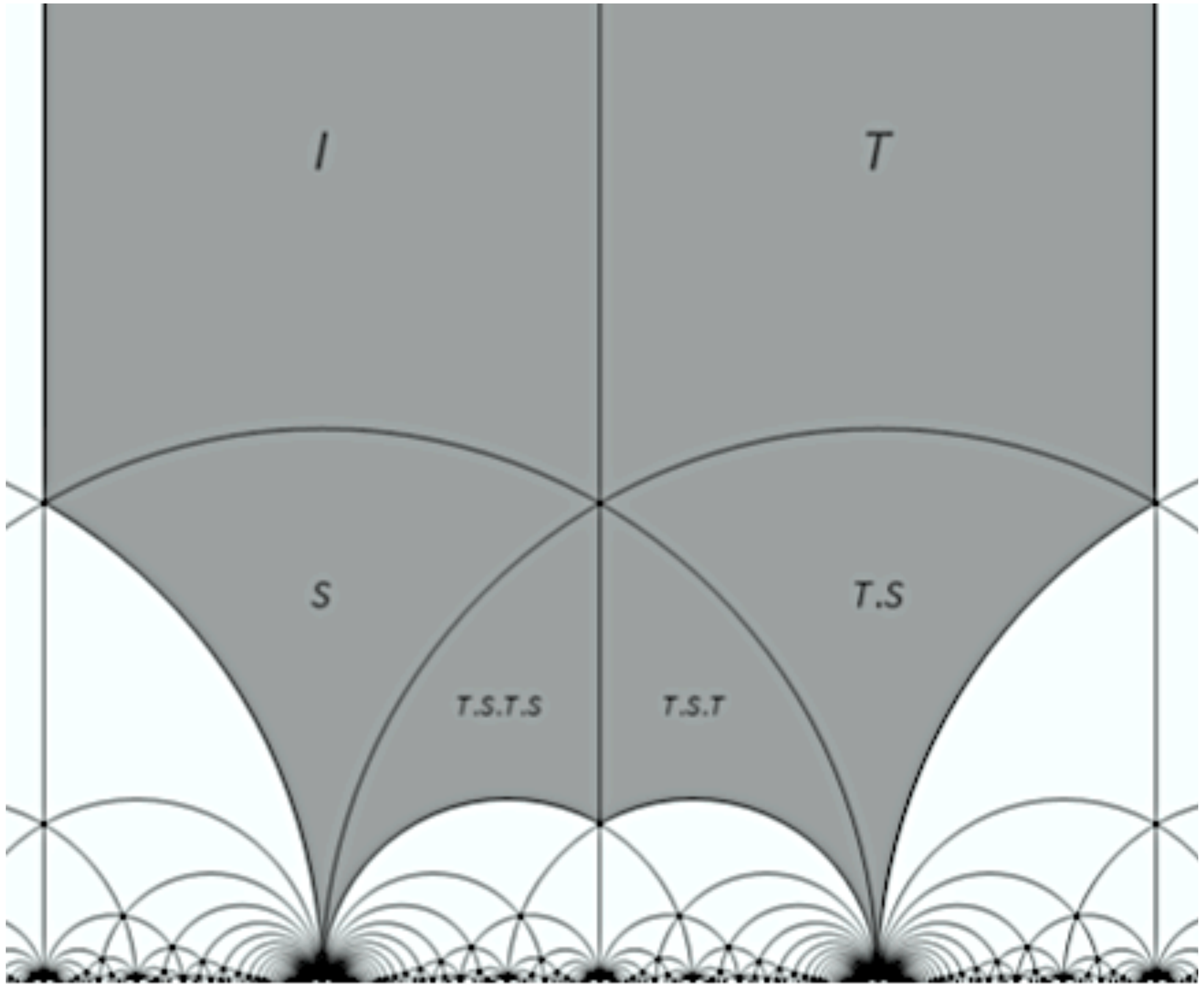
Modular Curves

We can consider quotients by the action of principal congruence subgroups

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a \equiv d \equiv 1 \mod N \text{ and } c \equiv 0 \mod N \right\}$$

and we also obtain modular curves.

Rational points on these curves represent elliptic curves, together with a point of order N.



Fundamental domain of $\Gamma_1(4)$. By Paul Kainberger.

Goal: To Describe Rational Solutions

We call a solution $(x_1, \ldots, x_k) \in \mathbb{Q}^k$ a **rational point** and denote the set of rational points as $X(\mathbb{Q})$.

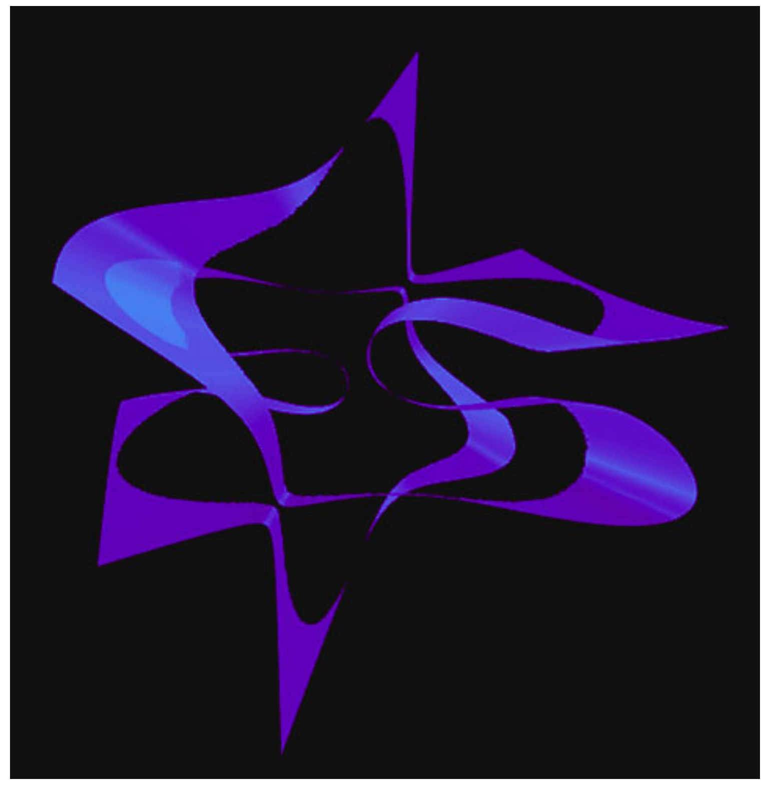
$$y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z - 32x^2z^2 - 40xyz^2 + 24y^2z^2 + 32xz^3 - 16yz^3 = 0$$

$$ay^2 + bx^3 = c^2$$

By Jennifer Balakrishnan and Sachi Hasimoto

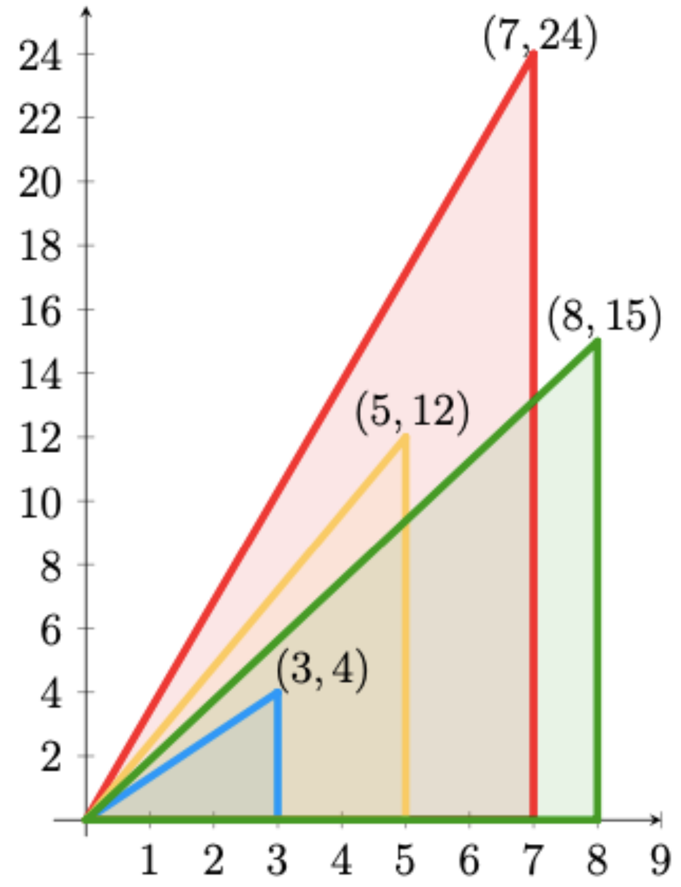
Goal: To Describe Rational Solutions

$y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z - 32x^2z^2 - 40xyz^2 + 24y^2z^2 + 32xz^3 - 16yz^3 = 0$



By Jennifer Balakrishnan
and Sachi Hasimoto

$$a^2 + b^2 = c^2$$



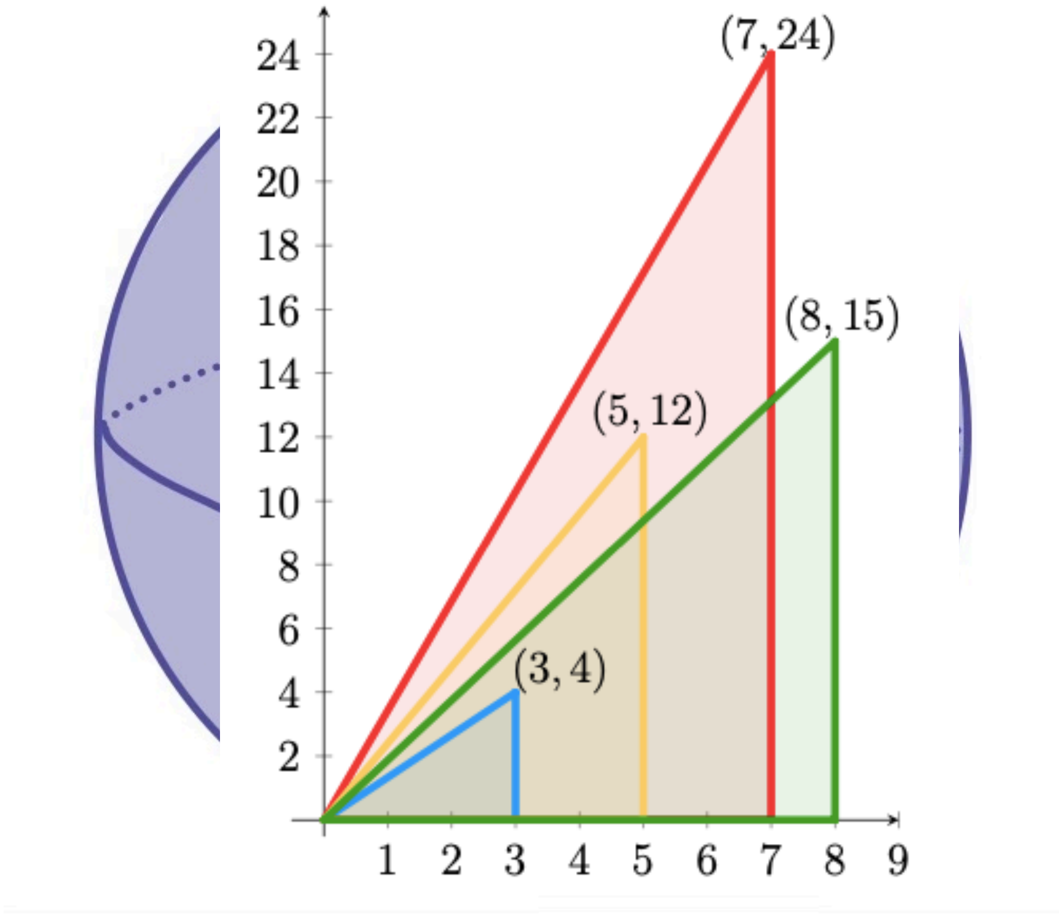
$$y^2 = x^3 - 2$$

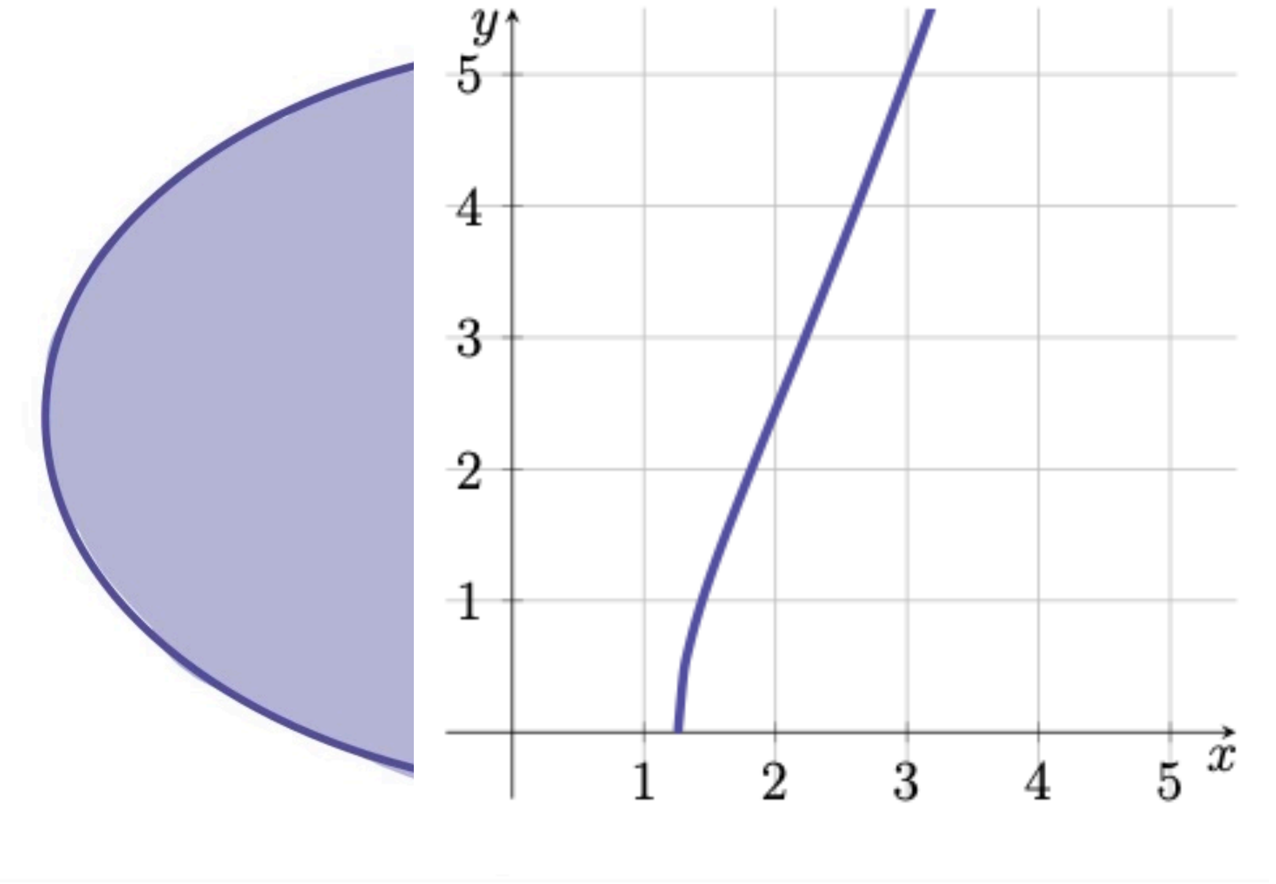
With Meaning!

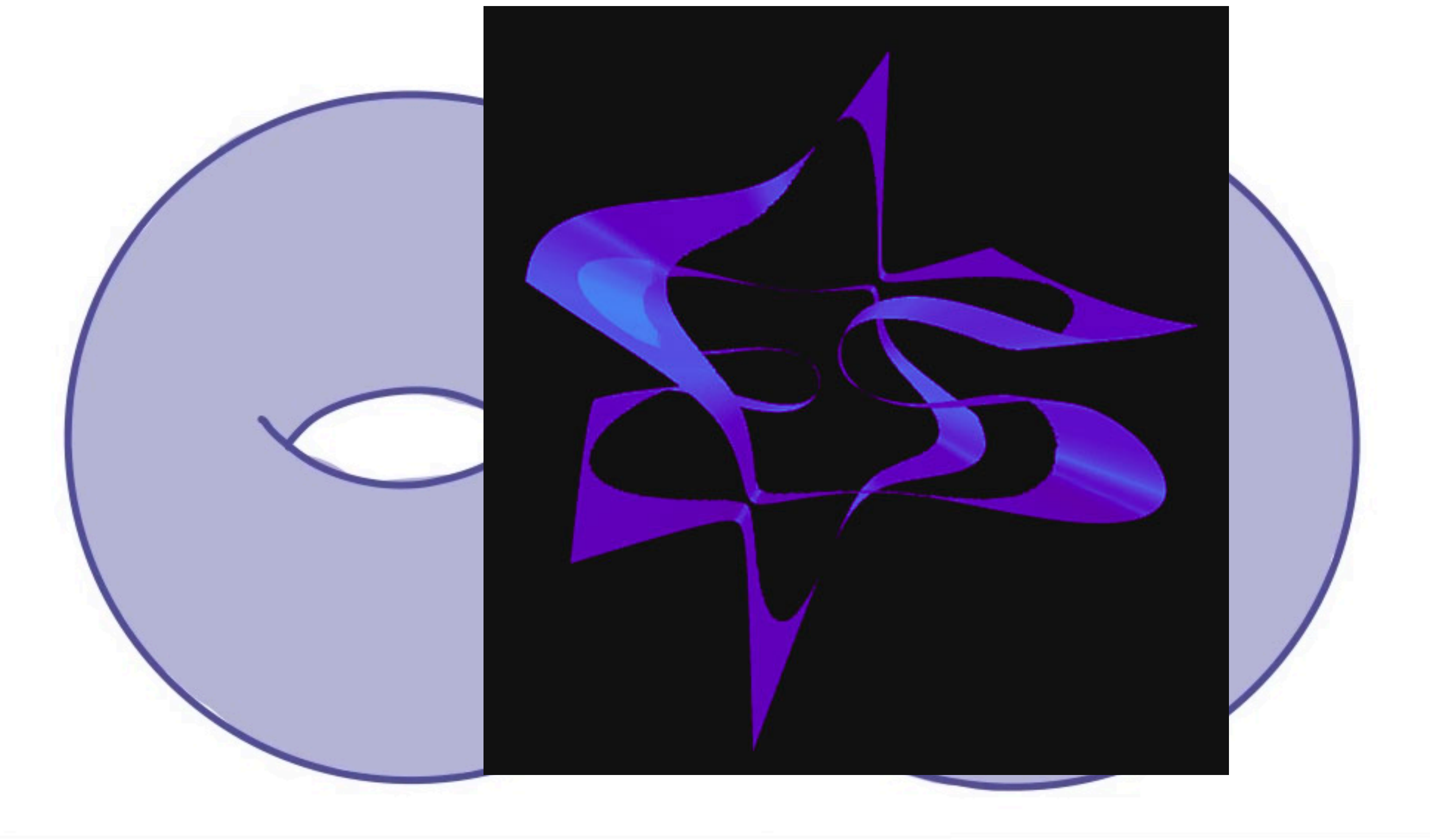
Two Problems…

1. Find meaningful polynomial equations to solve. (Part 1)
2. (Provably) Find all rational points. (Part 2)

How Many Points Can There Be?







Faltings's Theorem (1983). Let C be a nonsingular algebraic curve of genus $g \geq 2$. Then the set of rational points $C(\mathbb{Q})$ is finite.

Part 1: Triangular Modular Curves

Joint work with John Voight

Goal: to find meaningful polynomial equations to solve (by genus).

Goal: to find meaningful polynomial equations to solve (by genus).

Theorem (DR & Voight, 2023). For any $g \in \mathbb{Z}_{\geq 0}$, there are only **finitely many** Borel-type triangular modular curves $X_0(a, b, c; \mathfrak{N})$ and $X_1(a, b, c; \mathfrak{N})$ of genus g with nontrivial admissible level. The number of curves of genus at most 2 are as follows:

Genus	0	1	2
$X_0(a, b, c; \mathfrak{N})$	71	190	153
$X_1(a, b, c; \mathfrak{N})$	28	51	36

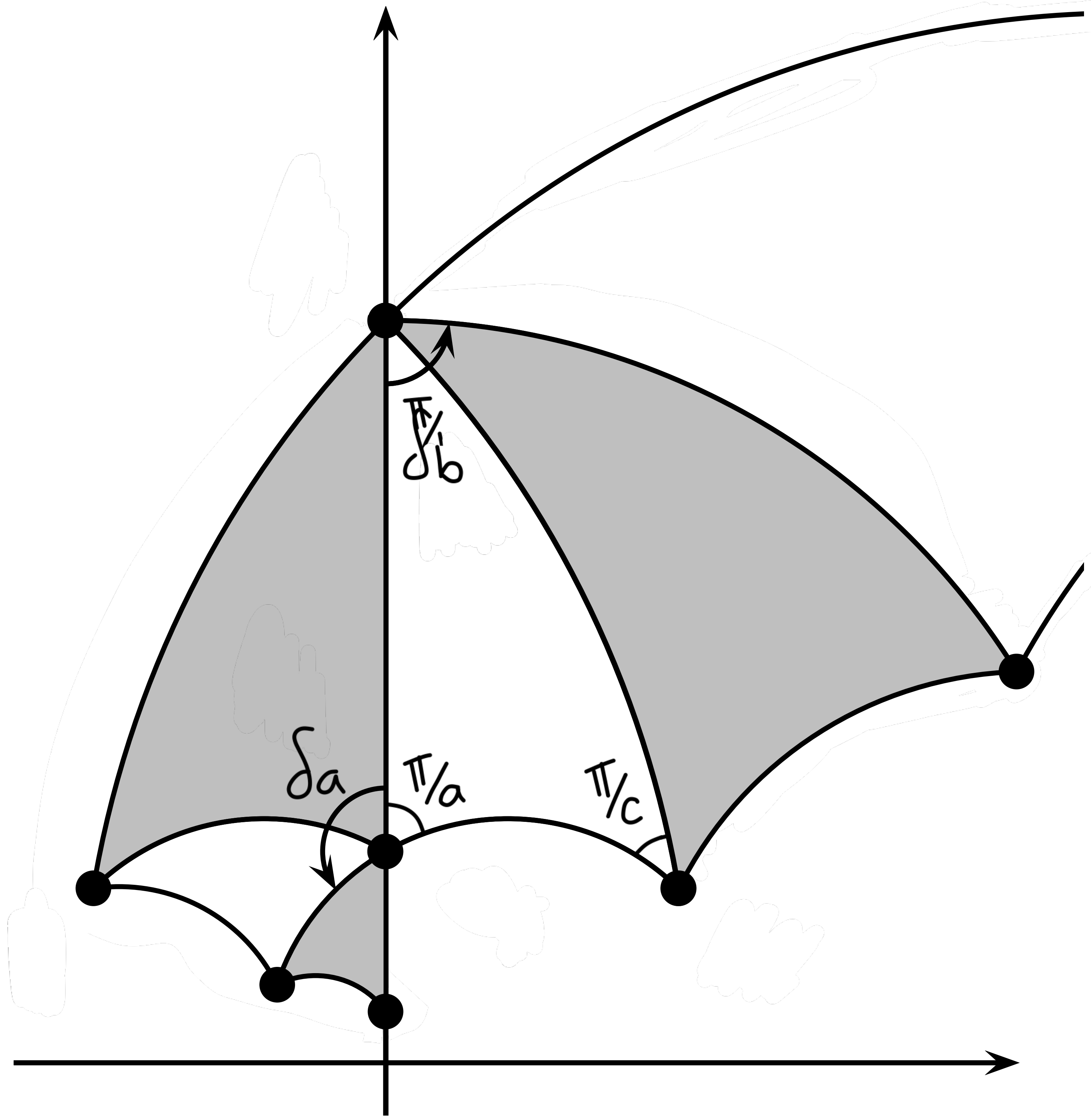
Triangle Groups

- Let $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. The triangle group is a group with presentation:

$$\Delta(a,b,c) := \langle \delta_a, \delta_b, \delta_c \,|\, \delta_a^a = \delta_b^b = \delta_c^c = \delta_a \delta_b \delta_c = 1 \rangle.$$

- We only consider hyperbolic triangles, where

$$\chi(a,b,c) := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 < 0.$$



Triangular Modular Curves (TMC's)

There is an embedding

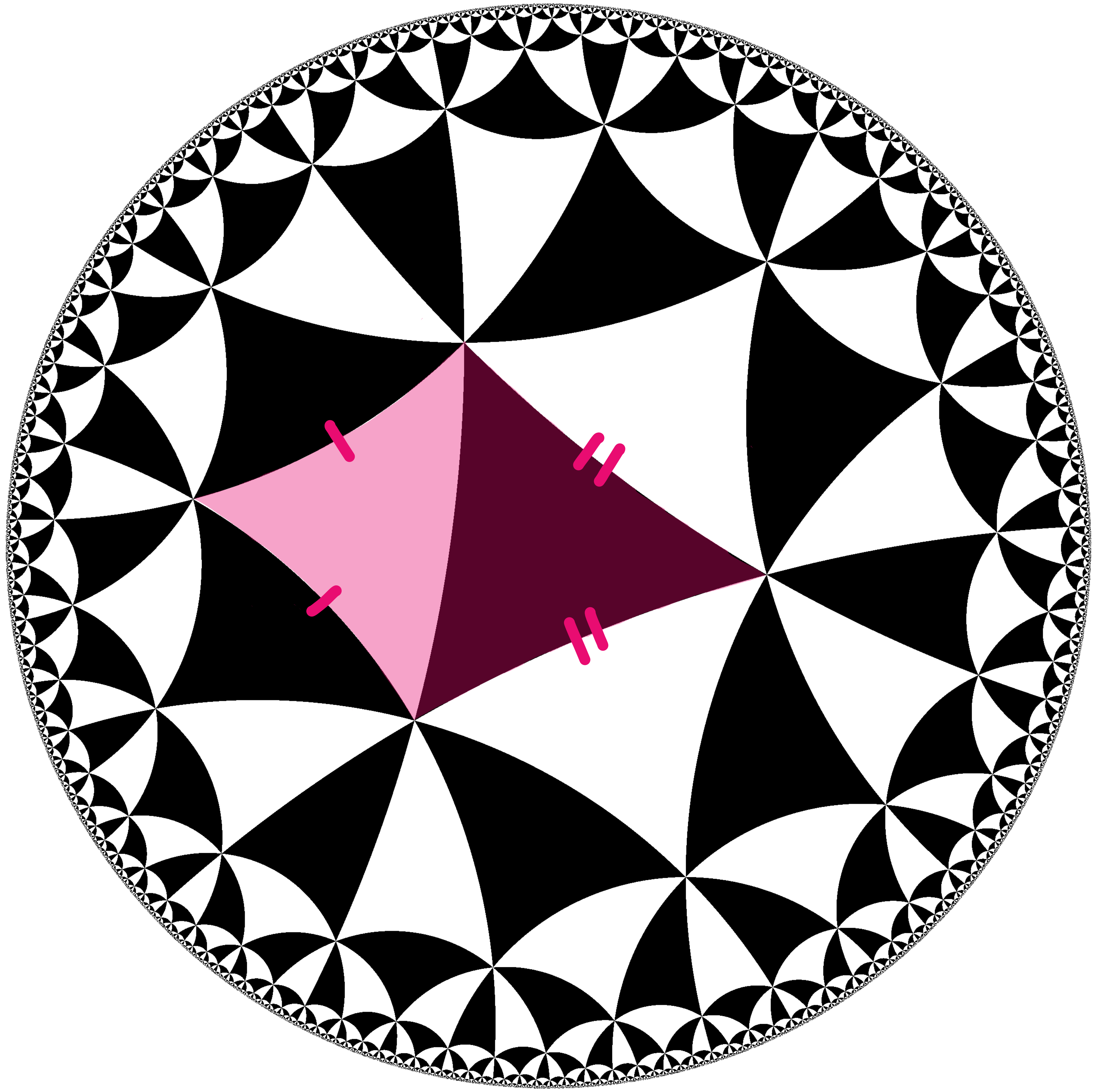
$$\Delta \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$$

that can be explicitly given by square roots, $\sin(\pi/s)$, and $\cos(\pi/s)$ for $s \in \{a, b, c\}$.

Then we can take the quotient

$$X(1) = X(a, b, c; 1) := \Delta \backslash \mathscr{H},$$

and the resulting Riemann surface is a triangular modular curve.



Triangle $\frac{\pi}{4}, \frac{\pi}{4}, \frac{\pi}{4}$ (Wikimedia)

Principal Congruence Subgroups

- Let p be a prime with $p \nmid 2abc$. We consider the number field

$$E = E(a,b,c) := \mathbb{Q}\left(\cos\left(\frac{2\pi}{a}\right),\ \cos\left(\frac{2\pi}{b}\right),\ \cos\left(\frac{2\pi}{c}\right),\right.$$
$$\left.\cos\left(\frac{\pi}{a}\right)\cos\left(\frac{\pi}{b}\right)\cos\left(\frac{\pi}{c}\right)\right).$$

- Let $\mathfrak{p}/p$ **be a prime of** E**.** There is a homomorphism

$$\pi_{\mathfrak{p}} : \Delta \to \mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{p}).$$

- Theorem (Clark & Voight, 2019). The group is PSL_2 or PGL_2 depending on the behavior of $\mathfrak{p}$ in an explicit extension of E.

Principal Congruence Subgroups

$$\pi_{\mathfrak{p}} : \Delta \to \mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{p})$$

The **principal congruence subgroup of level $\mathfrak{p}$** is

$$\Gamma(\mathfrak{p}) := \ker \pi_{\mathfrak{p}} \trianglelefteq \Delta.$$

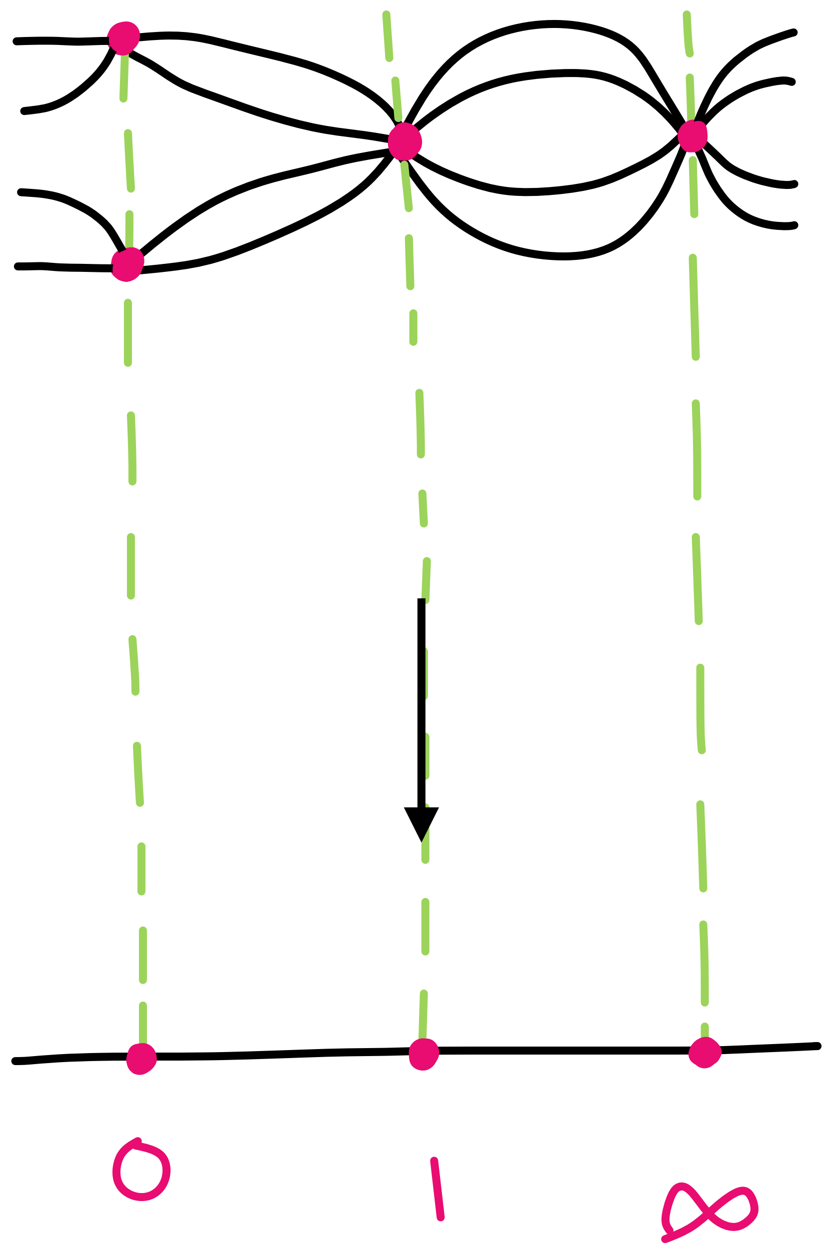
The **triangular modular curve of full level $\mathfrak{p}$** is

$$X(\mathfrak{p}) = X(a,b,c;\mathfrak{p}) := \Gamma(\mathfrak{p}) \backslash \mathscr{H}$$

$X(\mathfrak{p})$

$\downarrow$

$X(1) \simeq \mathbb{P}^1$



Remark. We can extend this definition to primes $\mathfrak{p}$ relatively prime to $\beta(a,b,c) \cdot \mathfrak{d}_{F|E}$.

Isomorphic Curves

Example. Consider the triples $(2,3,c)$ with $c = p^k$, $k \geq 1$ and $p \geq 5$ prime. Then

$$E_k := E(2,3,c) = \mathbb{Q}(\lambda_{2c}) = \mathbb{Q}(\zeta_{2c})^+.$$

The prime p is totally ramified in E so $\mathbb{F}_{\mathfrak{p}_k} \simeq \mathbb{F}_p$ for $\mathfrak{p}_k \mid p$. Thus

$$X(2,3,p^k;\mathfrak{p}_k) \simeq X(2,3,p;\mathfrak{p}_1).$$

$$\begin{array}{c} X(2,3,p^k;\mathfrak{p}_k) \\ \downarrow \\ X(2,3,p;\mathfrak{p}) \\ \downarrow \\ \mathbb{P}^1 \end{array}$$

Isomorphic Curves

$$X(2,3,p^k;\mathfrak{p}_k)$$
$$\downarrow$$
$$X(2,3,p;\mathfrak{p})$$
$$\downarrow$$
$$\mathbb{P}^1$$

A hyperbolic triple (a,b,c) is **admissible** for $\mathfrak{p}$ if the order of $\pi_{\mathfrak{p}}(\delta_s)$ is s for all $s \in \{a,b,c\}$.

Without loss of generality, for the rest of this talk (a,b,c) represents a hyperbolic admissible triple.

Congruence Subgroups

Let $H_0 \leq \mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{p})$ be the image of the upper triangular matrices in $\mathrm{XL}_2(\mathbb{Z}_E/\mathfrak{p})$.

$$\Gamma_0(\mathfrak{p}) = \Gamma_0(a,b,c;\mathfrak{p}) := \pi_{\mathfrak{p}}^{-1}(H_0).$$

We define the TMC with level $\mathfrak{p}$:

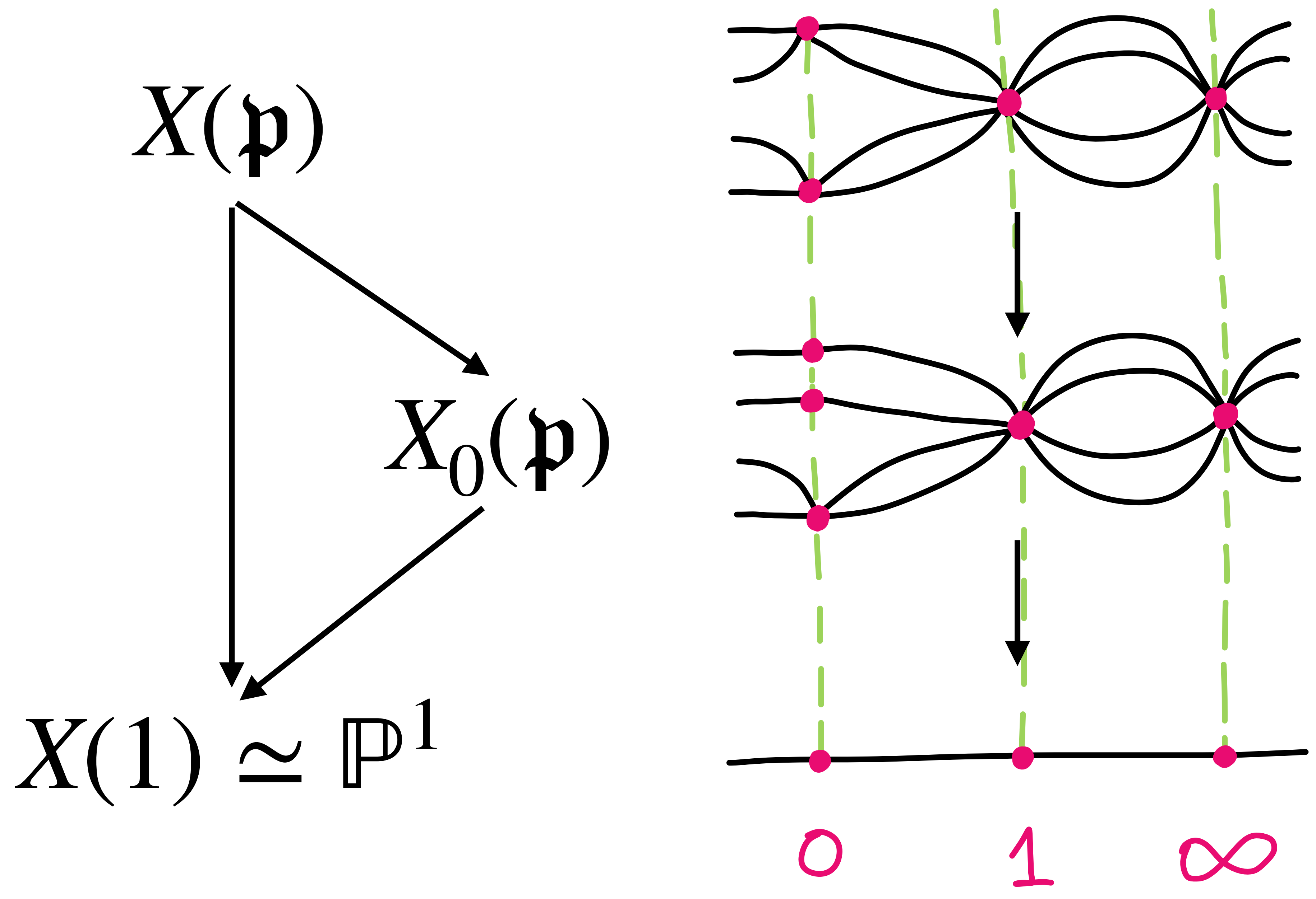
$$X_0(\mathfrak{p}) = X_0(a,b,c;\mathfrak{p}) := \Gamma_0(\mathfrak{p}) \backslash \mathscr{H}.$$

Then we get Belyi maps to $X(1)$

$$X(\mathfrak{p}) \to X_0(\mathfrak{p}) \to X(1).$$

We can also construct $X_1(a,b,c;\mathfrak{p})$ and we get

$$X(\mathfrak{p}) \to X_1(\mathfrak{p}) \to X_0(\mathfrak{p}) \to X(1)$$



Ramification

Lemma (DR & Voight, 2023). Let $G = \mathrm{PXL}_2(\mathbb{F}_q)$ with $q = p^r$ for p prime. (a, b, c) is a hyperbolic admissible triple. Let $\sigma_s \in G$ have order $s \geq 2$ and if $s = 2$ suppose $p = 2$. Then the action of σ_s on G/H_0 has

$$\left\lfloor \frac{q+1}{s} \right\rfloor \text{ orbits of length } s \text{ and } \begin{cases} 0 \text{ fixed points if } s \mid (q+1), \\ 1 \text{ fixed point if } s = p, \\ 2 \text{ fixed points if } s \mid (q-1)\,. \end{cases}$$

In particular s must divide one between $q-1, p,$ or $q+1$ for all $s \in \{a, b, c\}$ and we understand the ramification of the cover

$$X_0(\mathfrak{p}) \to \mathbb{P}^1.$$

TMCs of Bounded Genus

Proposition. Let $g_0 \geq 0$ be the genus of $X_0(a,b,c;\mathfrak{p})$. Recall that $q := \#\mathbb{F}_{\mathfrak{p}}$. Then

$$q \leq \frac{2(g_0+1)}{|\chi(a,b,c)|} + 1$$

In particular the number of TMCs $X_0(a,b,c;\mathfrak{p})$ of genus g_0 is finite.

We obtain an explicit formula for the genus

$$g(X_0(a,b,c;\mathfrak{p})).$$

Main Theorem

Theorem (DR & Voight, 2023). For any $g \in \mathbb{Z}_{\geq 0}$ there are finitely many Borel-type triangular modular curves $X_0(a, b, c; \mathfrak{p})$ of genus g with (admissible) prime level $\mathfrak{p}$. The number of curves $X_0(a, b, c; \mathfrak{p})$ of genus $g \leq 2$ are as follows:

- 76 curves of genus 0;
- 268 curves of genus 1;
- 485 curves of genus 2.

Enumeration Algorithm

Input: $g_0 \in \mathbb{Z}_{\geq 0}$.

Output: A list of $(a, b, c; p)$ such that $X_0(a, b, c; \mathfrak{p})$ has genus bounded by g_0 where $\mathfrak{p}$ is a prime of $E(a, b, c)$ of norm p.

1. Generate a list of possible q values.

2. For each q find all q-admissible hyperbolic triples (a, b, c).

3. Compute the genus g of $X_0(a, b, c; \mathfrak{p})$ by checking divisibility.

4. If $g \leq g_0$ add $(a, b, c; p)$ to the list lowGenus.

Composite Level

Theorem (DR & Voight, 2023). For any $g \in \mathbb{Z}_{\geq 0}$, there are only finitely many Borel-type triangular modular curves $X_0(a, b, c; \mathfrak{N})$ and $X_1(a, b, c; \mathfrak{N})$ of genus g with nontrivial admissible level $\mathfrak{N}$.

Challenges:

1. The map $\mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\} \to \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})$ might not be injective.

2. Describing admissibility is harder.

3. The genus formula is more complicated.

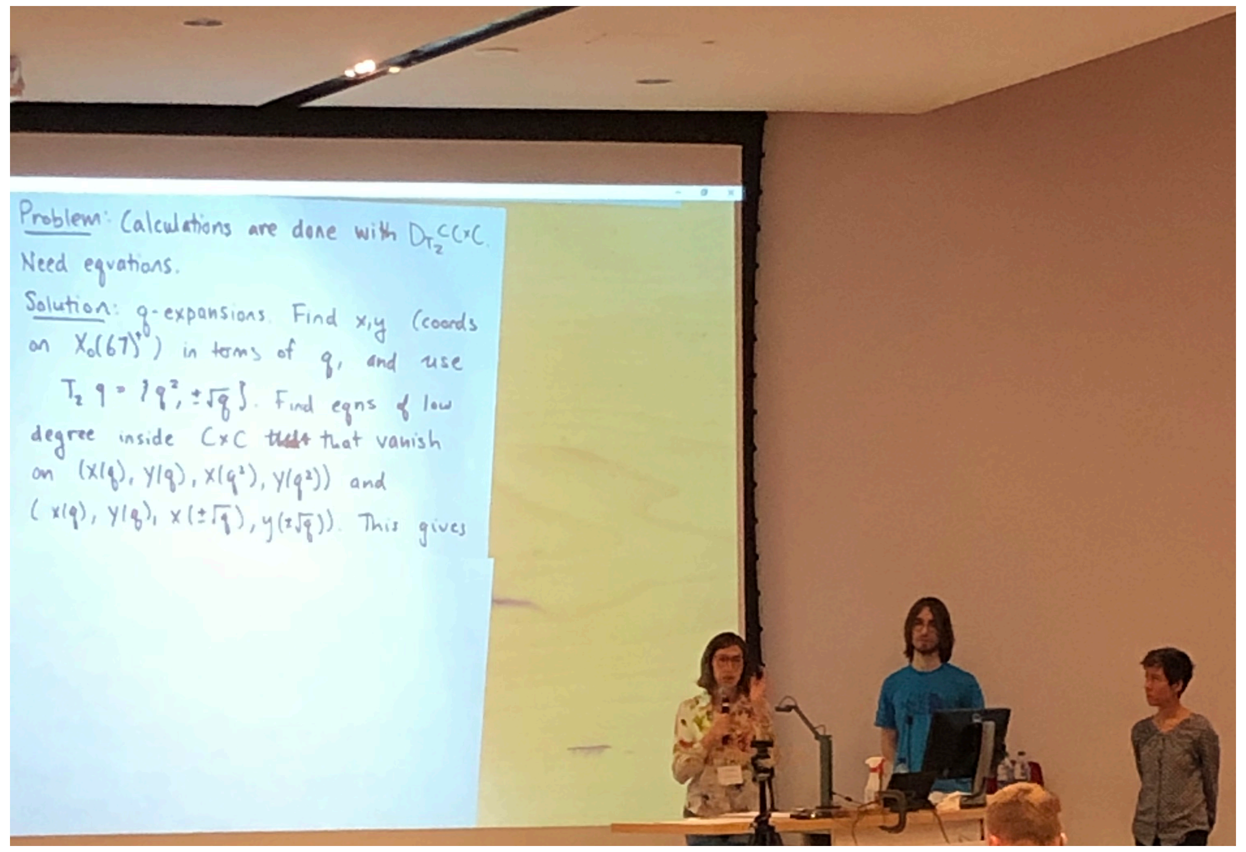
4. The enumeration algorithm takes significantly longer because we are computing matrix groups explicitly.

But This is the Beginning…

- Find models of TMCs of low genus and relate them to the existing database of curves in the LMFDB (at least over $\mathbb{Q}$).

- Describe all rational points (over the field of definition) of TMCs.

- Conjecture. For all $g \geq 0$, there are only finitely many admissible triangular modular curves of genus g.

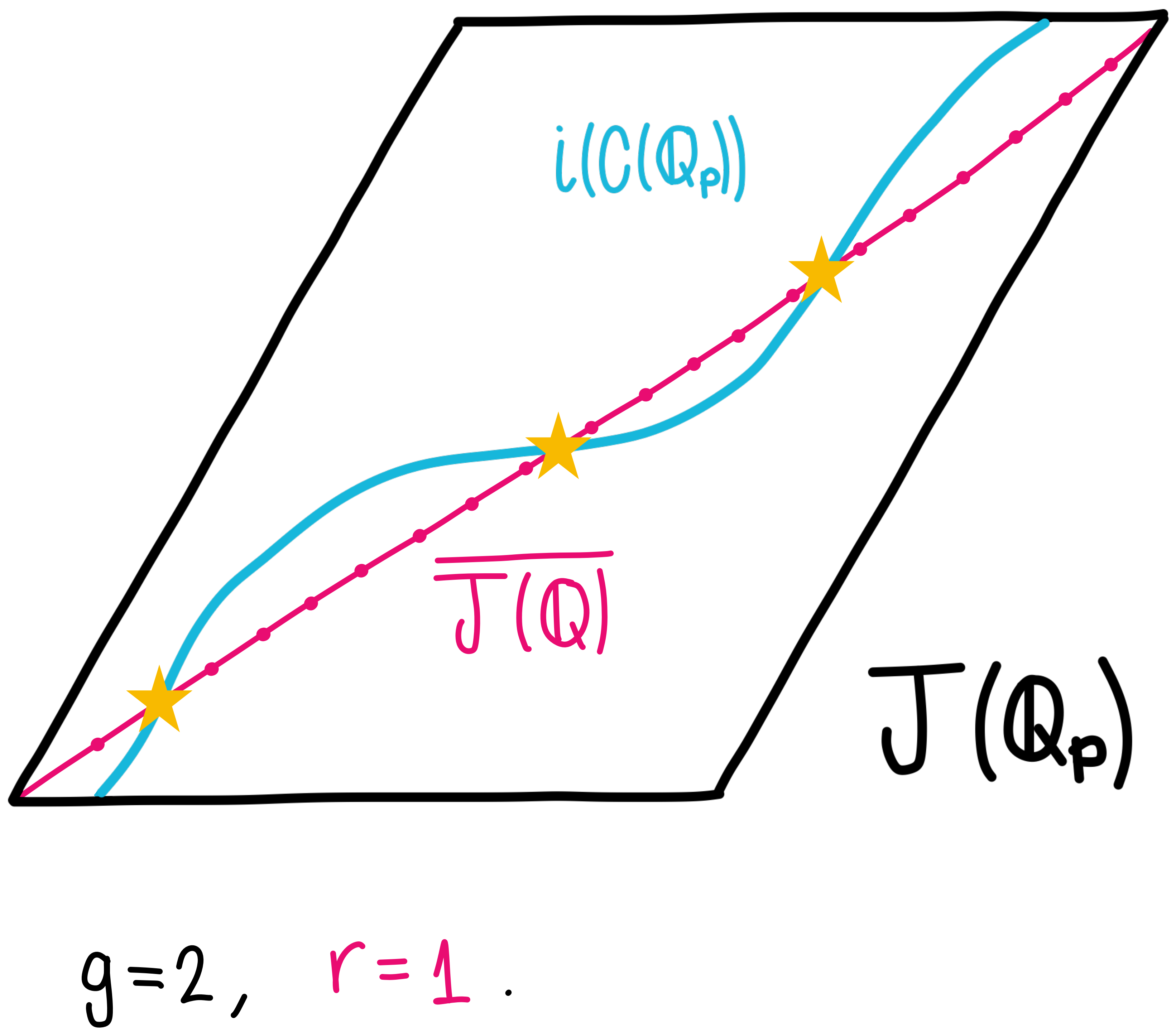


Part 2: Geometric Quadratic Chabauty

Joint work with Sachi Hashimoto and Pim Spelier

Goal: to (provably) find all rational points on a curve.

Chabauty's Theorem



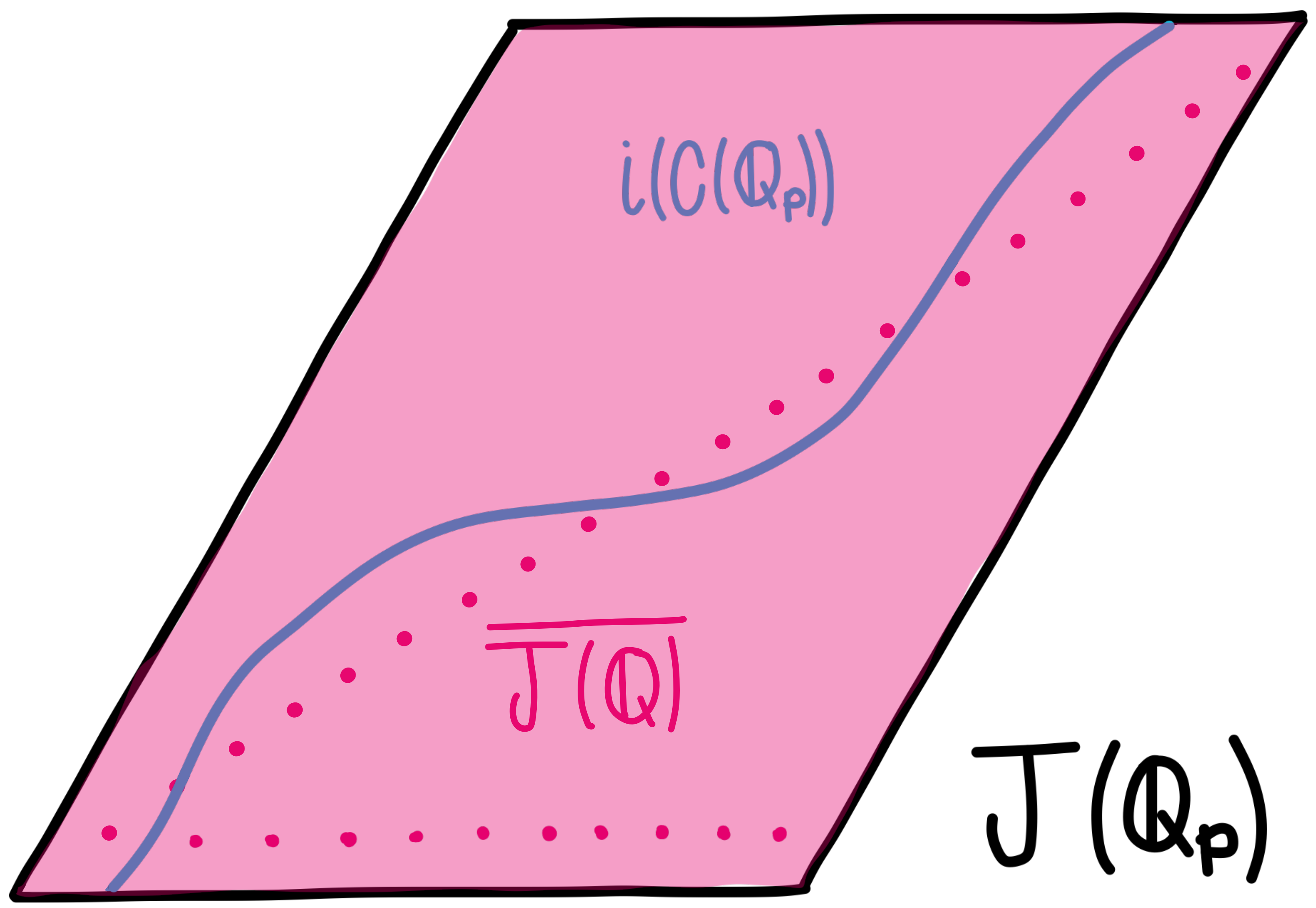
- Let C be a curve (over $\mathbb{Q}$) of genus $g \geq 2$.
- Let J be the Jacobian of C.
- Let r be the Mordell-Weil rank of J.
- Let p be a prime number.

Chabauty's Theorem (1941). If $r < g$, then

$$\iota(C(\mathbb{Q})) \subseteq \iota(C(\mathbb{Q}_p)) \cap \overline{J(\mathbb{Q})} \subseteq J(\mathbb{Q}_p),$$

and this intersection is finite.

Chabauty's Theorem



$g = 2$, $r = 2$.

- Let C be a curve (over $\mathbb{Q}$) of genus $g \geq 2$.
- Let J be the Jacobian of C.
- Let r be the Mordell-Weil rank of J.
- Let p be a prime number.

Chabauty's Theorem (1941). If $r < g$, then

$$\iota(C(\mathbb{Q})) \subseteq \iota(C(\mathbb{Q}_p)) \cap \overline{J(\mathbb{Q})} \subseteq J(\mathbb{Q}_p),$$

and this intersection is finite.

(Cohomological) Quadratic Chabauty

- Chabauty—Kim's Program (2009). To use p-adic methods to determine $C(\mathbb{Q})$.

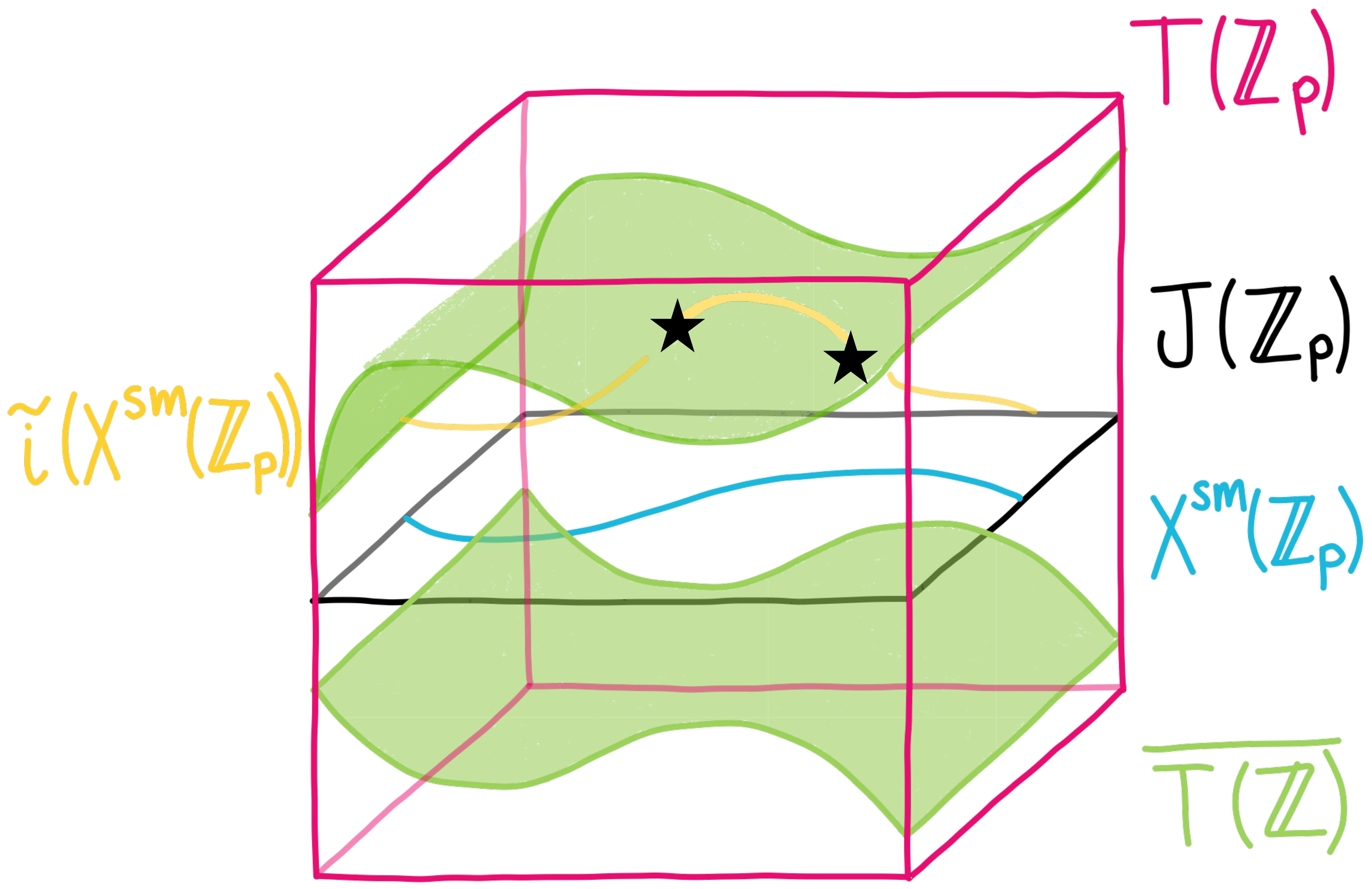
- Balakrishnan & Dogra (2018, 2021). The program is made explicit for $r = g$ and p of good reduction. The method produced a set of $p-$adic points containing the rational points.

- The method is then applied to examples:

  - $X_s(13)$, the cursed curve by Balakrishnan, Dogra, Müller, Tuitman, and Vonk (2019).

  - $X_0(67)^+$ by Balakrishnan, Best, Bianchi, Lawrence, Müller, Triantafillou, and Vonk (2021).

Geometric Quadratic Chabauty



Let C be a nice curve of genus $g \geq 2$, Mordell-Weil rank r, and Néron-Severi rank ρ. Let p be a prime number.

- X^{sm} is the (smooth locus) of a regular model for C. Then $X^{\text{sm}}(\mathbb{Z}) = C(\mathbb{Q})$.
- J_C is the Jacobian of C and $J/\mathbb{Z}$ is its Néron model.
- $b \in C(\mathbb{Q}) = X^{\text{sm}}(\mathbb{Z})$ is a base point.
- $\imath : X^{\text{sm}} \to J$ is the Abel-Jacobi map.

We construct a $\mathbb{G}_m^{\rho-1}$-torsor T over J that trivializes X.

Theorem (Edixhoven & Lido, 2021). If $r < g + \rho - 1$, then the following set is finite:

$$\tilde{\imath}(X^{\text{sm}}(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})} \subseteq T(\mathbb{Z}_p)$$

A Comparison Theorem

Theorem (DR, Hashimoto, and Spelier, 2022). Assume that p is a prime of good reduction for $X_{\mathbb{Q}}$. Assume that $r = g$, $\rho > 1$, and furthermore the $p-$adic closure $\overline{J_{\mathbb{Q}}(\mathbb{Q})}$ is finite index in $J_{\mathbb{Q}}(\mathbb{Q}_p)$. Assume there exists a rational base point $b \in X(\mathbb{Q})$. Let $X(\mathbb{Q}_p)'_2$ be the finite set of $p-$adic points defined under these assumptions in the cohomological quadratic Chabauty method. Then we have the inclusions

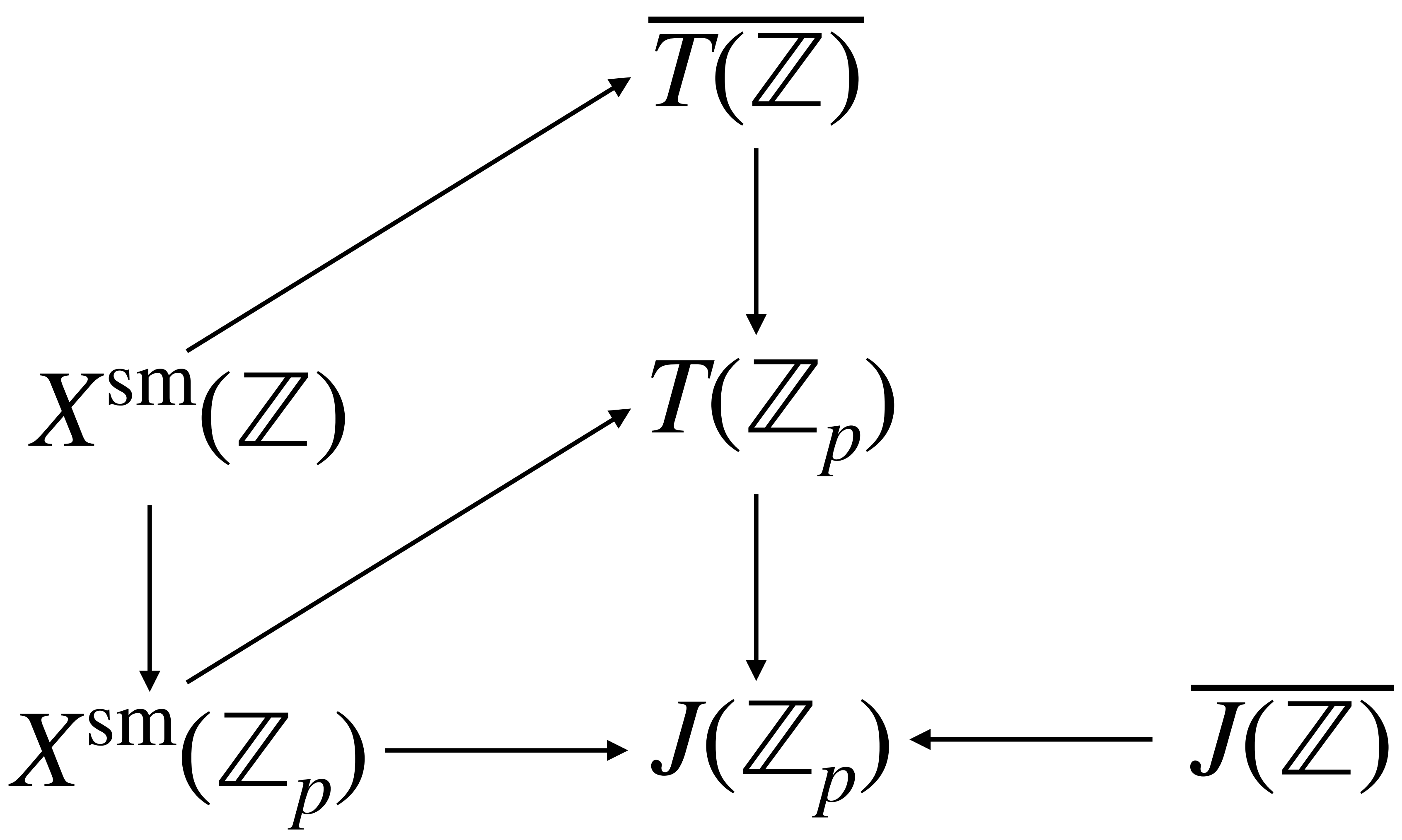
$$X_{\mathbb{Q}}(\mathbb{Q}) \subseteq \tilde{\imath}(X^{\mathrm{sm}}(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})} \subseteq X(\mathbb{Q}_p)'_2 \subseteq X_{\mathbb{Q}}(\mathbb{Q}_p),$$

and we can explicitly characterize $X(\mathbb{Q}_p)'_2 \backslash \tilde{\imath}(X^{\mathrm{sm}}(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})}$.

Example: $X_0(67)^+$

We have $r = g = \rho = 2$.

$$\tilde{\imath}(X^{\mathrm{sm}}(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})} \subseteq T(\mathbb{Z}_p)$$



1. Compute $\tilde{\imath} : X^{\mathrm{sm}} \to T(\mathbb{Z}_p)_{\tilde{\imath}(\bar{P})}$ via a section.
2. Compute $\kappa : \mathbb{Z}_p^r \to T(\mathbb{Z}_p)_{\tilde{\imath}(\bar{P})}$ with image $\overline{T(\mathbb{Z})}_{\tilde{\imath}(\bar{P})}$.
3. A Hensel-like lemma implies that finite precision is enough.

The set of points of $X(\mathbb{Z})$ reducing to $(0, -1)$ are contained in

$$\left\{ \left(0, -1\right), \left(4 \cdot 7 + O(7^2), 6 + O(7^2)\right) \right\}.$$

What is Next?

- Finish the computation for one missing residue disk.
- Find an example in which the difference between the set of points given by cohomological quadratic Chabauty and geometric quadratic Chabauty is made apparent.
- Compute an example of geometric quadratic Chabauty for which $r \neq g$.
- Does one of our algorithms help to compute $p-$adic heights away from p?

Thank You!

- John Voight.
- My committee: John Voight (chair), Asher Auel, Pete Clark, and Rosa Orellana.
- My collaborators Sachi Hashimoto and Pim Spelier.
- Rachel Pries.
- Gracias mamá, papá y toda mi familia.
- The Dartmouth Mathematics department, special thanks to DANTS people.
- All of you for being here and being part of this journey.


STEAM
f(x) = |x|
AVOID NEGATIVITY
STRENGTH IN NUMBERS
UNIVERSIDAD DE LOS ANDES

Summary

- Theorem (DR & Voight, 2023). For any $g \in \mathbb{Z}_{\geq 0}$, there are only finitely many Borel-type triangular modular curves $X_0(a, b, c; \mathfrak{N})$ and $X_1(a, b, c; \mathfrak{N})$ of genus g with nontrivial admissible level $\mathfrak{N}$.

- We present an explicit algorithm to enumerate all such curves of a fixed genus and carry out the enumeration for $g \leq 2$.

- Theorem (DR, Hashimoto, and Spelier, 2023). When the cohomological and the geometric quadratic Chabauty methods apply, the set of p-adic points produced by the cohomological method is contained in the set produced by the geometric method. This difference can be characterized.

- We produced algorithms to make the geometric quadratic Chabauty method explicit for hyperelliptic curves by using p-adic heights.