Triangular modular curves of low genus

Juanita Duque-Rosero

Joint work with John Voight

ANTS XV

August 2022

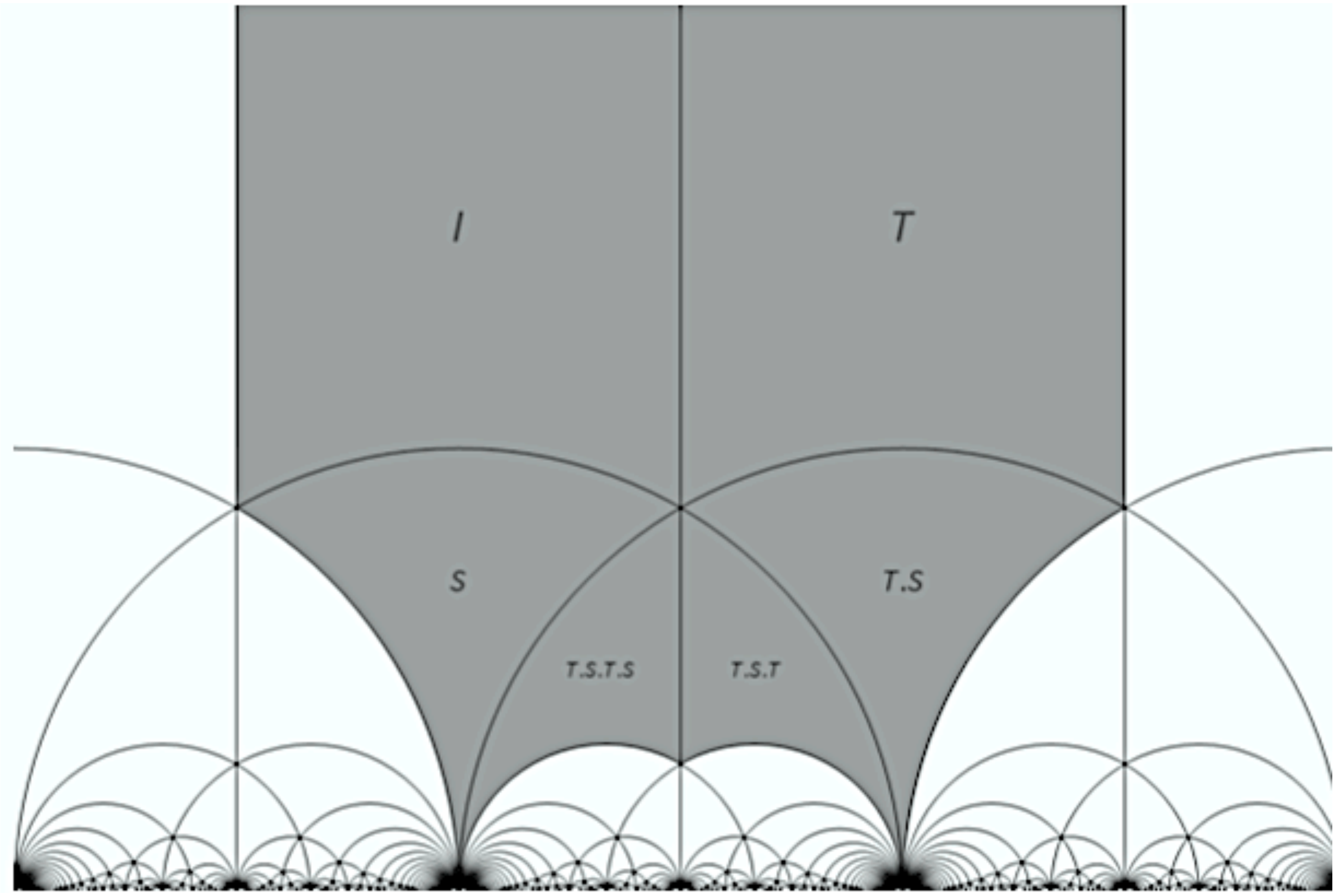
Once upon a time, there were elliptic curves

We consider the Legendre family of elliptic curves

$$E_t : y^2 = x(x-1)(x-t)$$

for a parameter $t \neq 0, 1, \infty$.

- Cyclic covers of $\mathbb{P}^1$ branched at 4 points.
- Parametrization by the modular curve $X(2) = \mathbb{P}^1$.
- We can consider additional level structure. **Example:** specify a cyclic N-isogeny ($X_0(N)$) or an N-torsion point ($X_1(N)$).



Fundamental domain of $\Gamma(2)$. By Paul Kainberger.

Generalizing elliptic curves

We consider the family of curves:

$$X_t : y^m = x^{e_0}(x-1)^{e_1}(x-t)^{e_t}$$

with $t \neq 0, 1, \infty$.

- Cyclic covers of $\mathbb{P}^1$ that are branched at 4 points.
- X_t has a cyclic group of automorphisms of order m defined over $\mathbb{Q}(\zeta_m)$.
- $\mathrm{Prym}(X_t)$ an isogeny factor of $\mathrm{Jac}(\mathrm{X}_\mathrm{t})$.

The family $\mathrm{Prym}(X_t)$ extends to a family of abelian varieties over $\mathbb{P}^1$.

Why triangular modular curves?

- **[Cohen & Wolfart ’90, Archinard ’03].** The extension of the family $\mathrm{Prym}(X_t)$ is parameterized by triangular modular curves.

- **[Darmon ’04].** Darmon’s program: there is a dictionary between finite index subgroups of the triangle group $\Delta(a, b, c)$ and approaches to solve the generalized Fermat equation
$$x^a + y^b + z^c = 0.$$

Main theorem

Theorem [DR & Voight '22]

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 nontrivial prime level $\mathfrak{p}$. The number of curves $X_0(a, b, c; \mathfrak{p})$ of genus $g \leq 2$ are as follows:

- 56 curves of genus 0
- 130 curves of genus 1
- 180 curves of genus 2.

```
> time countBoundedGenus(2);
[ 56, 130, 180 ]
Time: 0.130
```

We have a similar result for $X_1(a, b, c; \mathfrak{p})$

Triangle groups

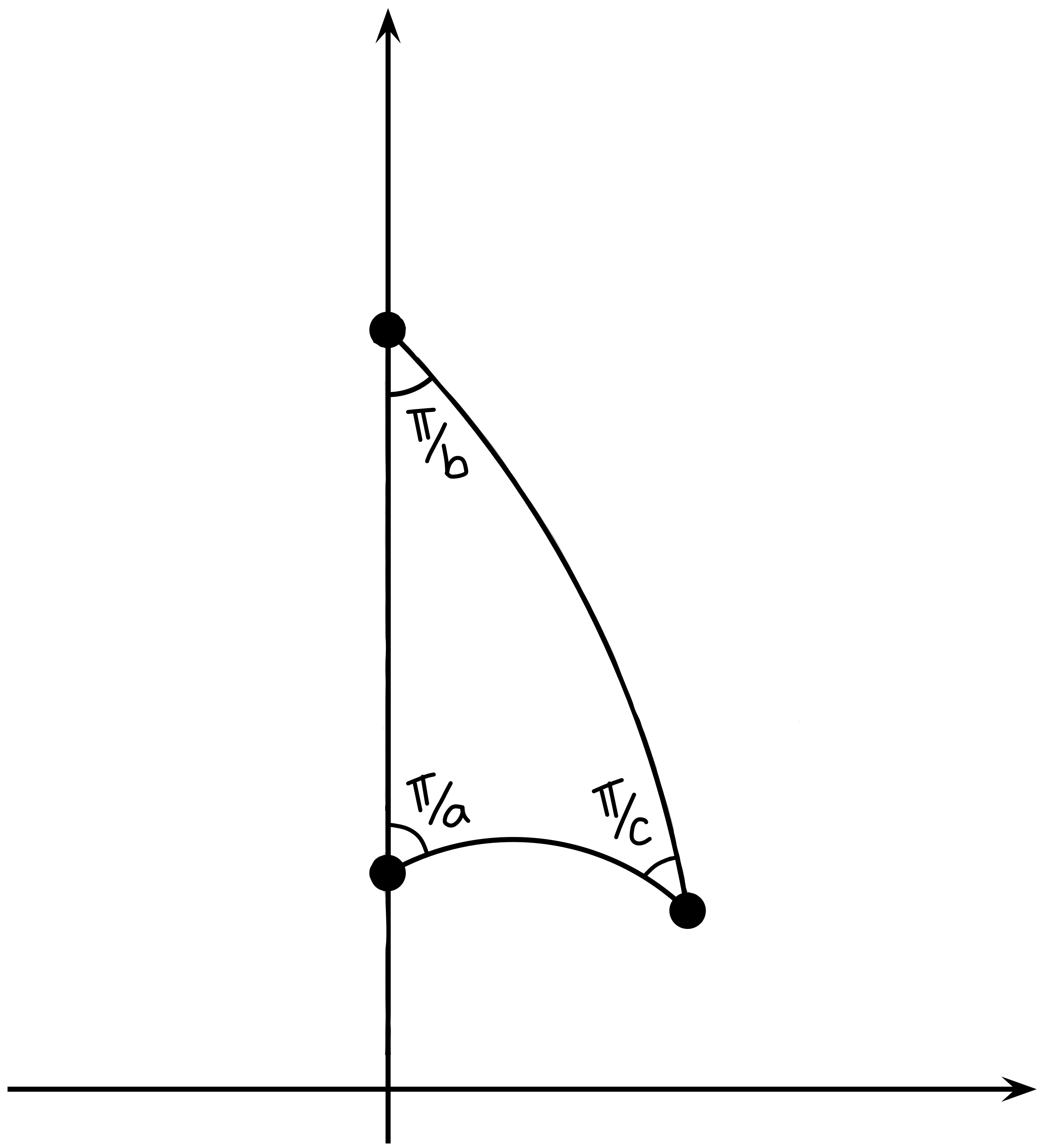
Definition

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

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

We only consider hyperbolic triangles. This is the triple (a, b, c) is hyperbolic:

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



Triangle groups

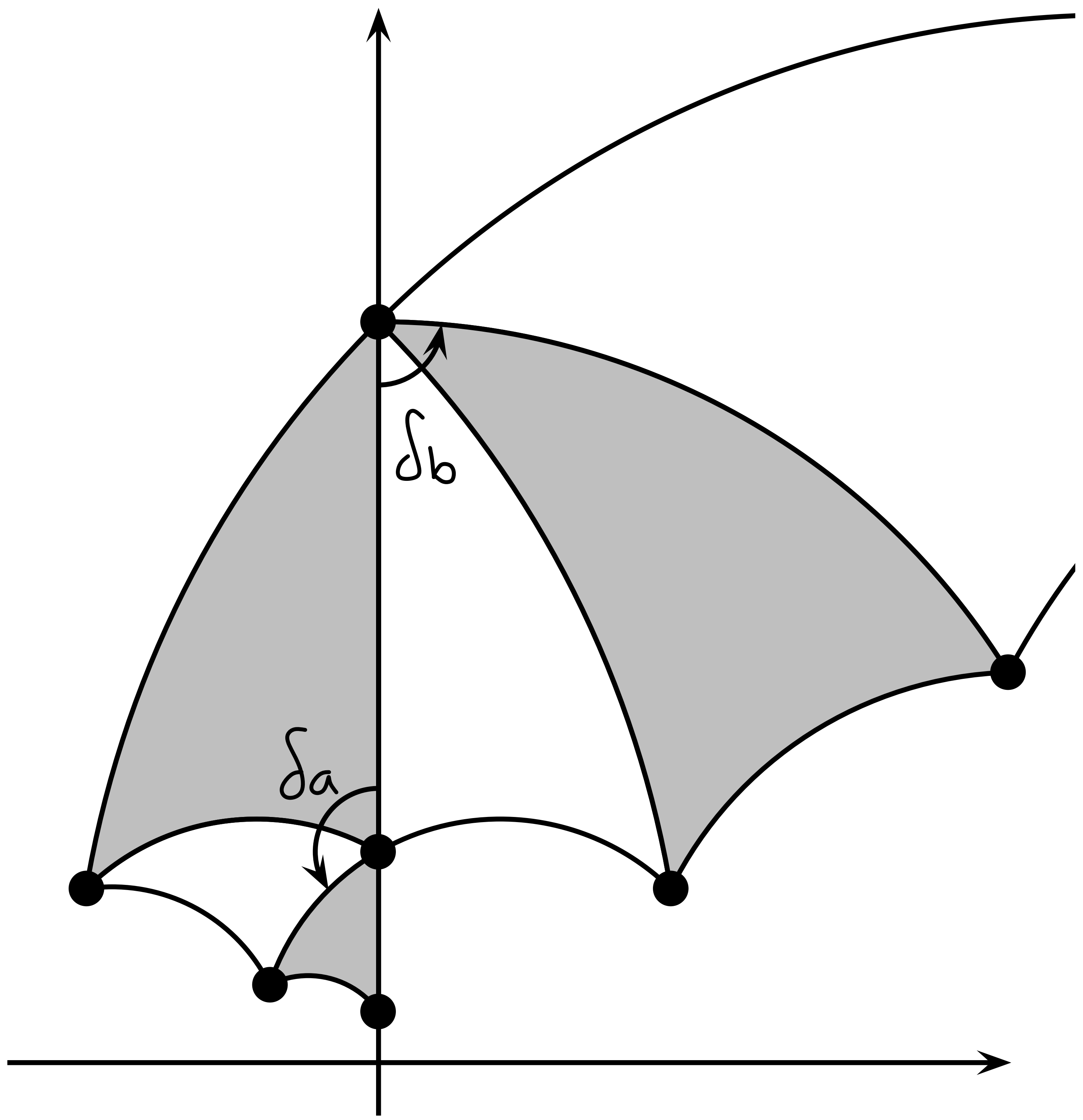
Definition

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. This is the triple (a, b, c) is hyperbolic:

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



Triangular modular curves

Construction

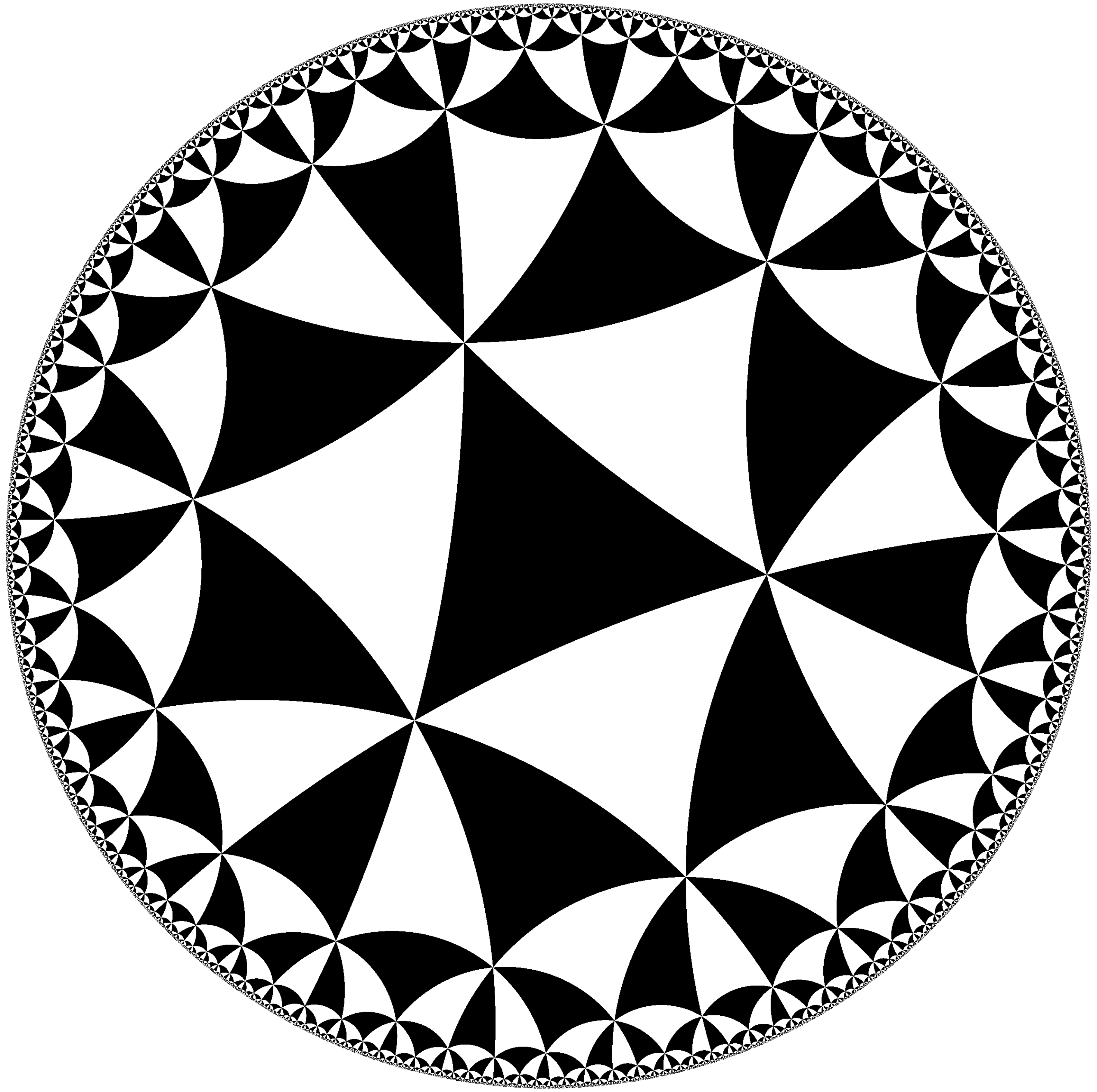
There is an embedding

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

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

A **triangular modular curve TMC** is given by the quotient

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



Triangle $\frac{\pi}{4}, \frac{\pi}{4}, \frac{\pi}{4}$

Triangular modular curves

Construction

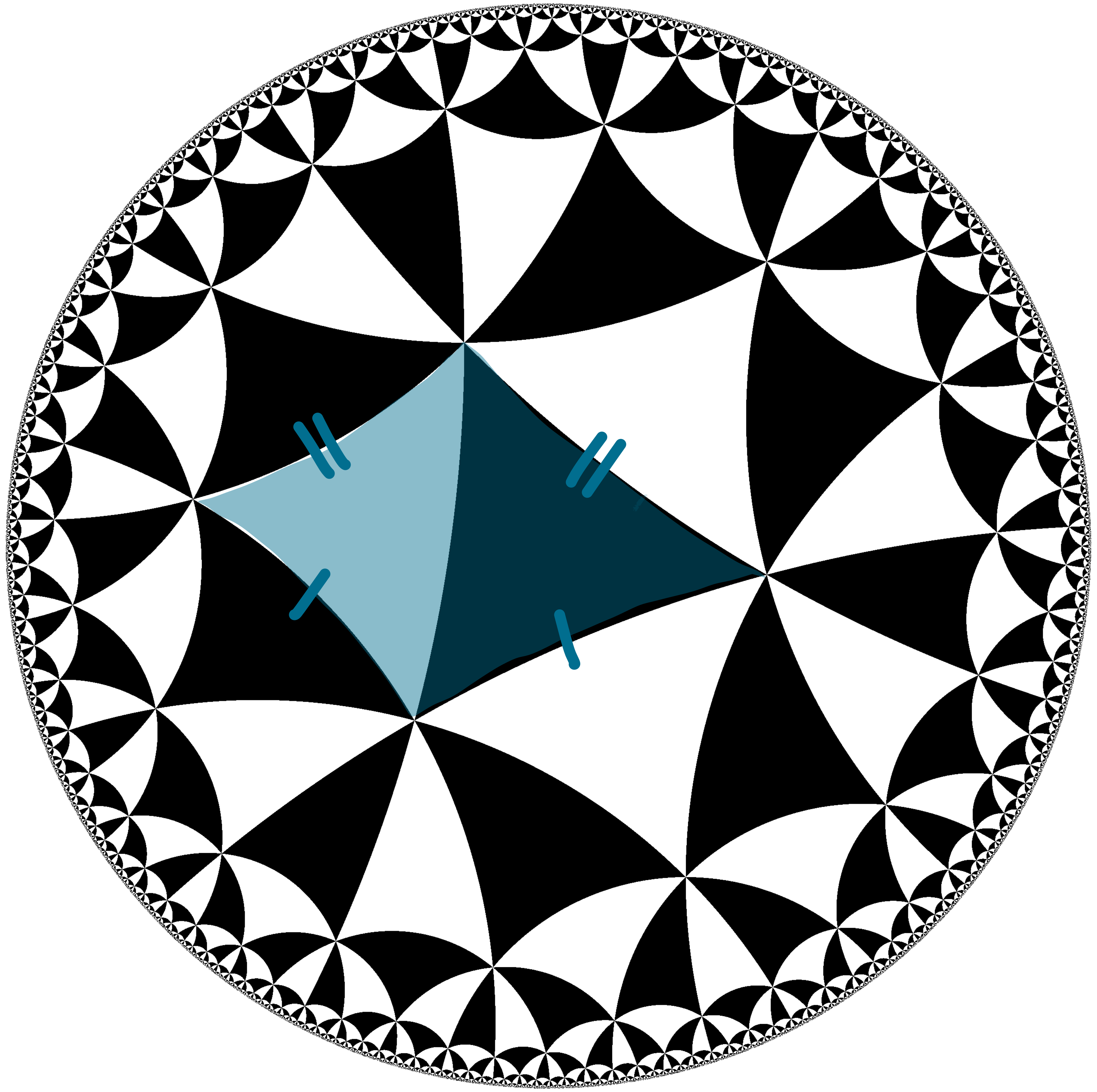
There is an embedding

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

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

A **triangular modular curve TMC** is given by the quotient

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



Triangle $\frac{\pi}{4}, \frac{\pi}{4}, \frac{\pi}{4}$

Level structure

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

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

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

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

We can decide between PSL_2 and PGL_2 from the behavior of $\mathfrak{p}$ in an extension of E.

Level structure

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

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

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

The **TMC of level** $\mathfrak{p}$ is:

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

Note: 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

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

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

For the rest of this talk (a, b, c) represents a hyperbolic admissible triple.

Congruence subgroups

Borel kind

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 $\mathfrak{p}$:

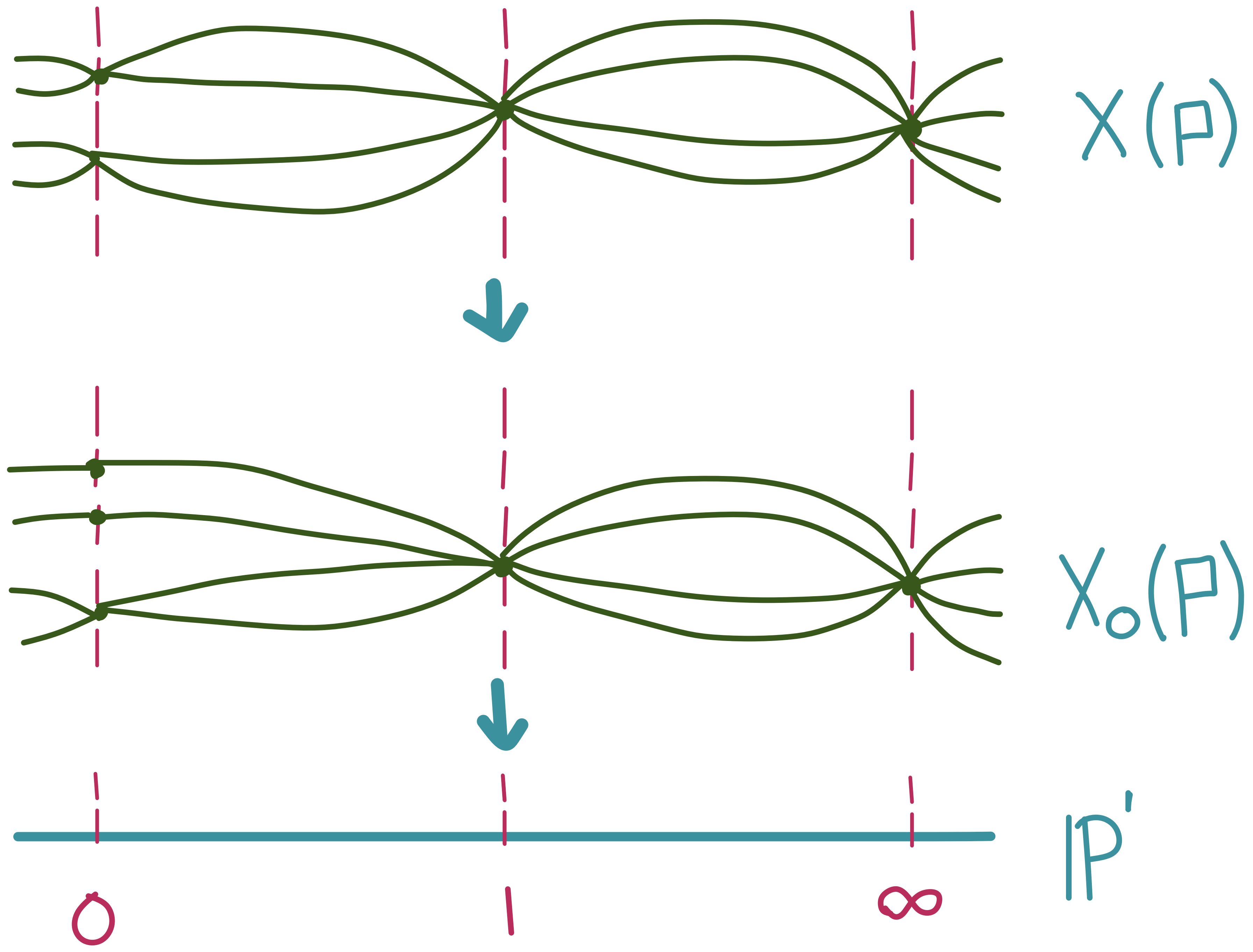
$$X_0(\mathfrak{p}) = X_0(a, b, c; \mathfrak{p}) := \Gamma_0(\mathfrak{p}) \backslash \mathscr{H}.$$

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

The maps to $X(1)$ are Belyi maps!

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. 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:

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

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

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

A bound on the number of TMCs of bounded genus

Theorem [DR & Voight '22]. 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

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

A bound on the number of TMCs of bounded genus

Theorem [DR & Voight '22]. Let $g_0 \geq 0$ be the genus of $X_0(a, b, c; \mathfrak{p})$. Recall that $q := \#\mathbb{F}_{\mathfrak{p}}$. Then

$$q \leq \frac{2(g_0 + 1)}{|-1/42|} + 1.$$

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

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

Enumeration algorithm

Main 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.

Magma implementation

Scan me!

```
> time countBoundedGenus(100);
[ 56, 130, 180, 206, 232, 254, 245, 285, 289, 320, 298, 335, 308, 363, 329, 320,
362, 398, 309, 428, 365, 389, 398, 422, 366, 442, 412, 440, 392, 489, 353, 502, 430,
432, 467, 455, 402, 500, 461, 494, 417, 531, 369, 520, 469, 445, 491, 566, 438, 559,
459, 507, 485, 568, 472, 558, 485, 500, 499, 595, 369, 574, 515, 506, 534, 562, 463,
600, 496, 590, 503, 685, 469, 598, 562, 570, 617, 637, 510, 699, 581, 590, 595, 700,
552, 657, 583, 619, 549, 691, 485, 659, 600, 621, 605, 611, 463, 682, 574, 617, 526
]
Time: 77.310
```

Main theorem

Theorem [DR & Voight '22]

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 nontrivial prime level $\mathfrak{p}$. The number of curves $X_0(a, b, c; \mathfrak{p})$ of genus $g \leq 2$ are as follows:

- 56 curves of genus 0
- 130 curves of genus 1
- 180 curves of genus 2.

Future work

Compute explicit lists for composite level.

Find models using Belyi maps and compute rational points of TMCs of low genus.

Example: the curve $X_0(3,3,4;\mathfrak{p}_7)$ is defined over the number field k with defining polynomial $x^4 - 2x^3 + x^2 - 2x + 1$. We have

$$X_0(3,3,4;\mathfrak{p}_7) \simeq \mathbb{P}^1_k.$$

Conjecture. For all $g \in \mathbb{Z}_{\geq 0}$, there are only finitely many admissible triangular modular curves of genus g of nontrivial level $\mathfrak{N} \neq (1)$ with $\Delta(a,b,c)$ maximal.

Output for $X_0(a, b, c; p)$ of genus 0

a	b	c	p
2	3	7	7
2	3	7	2
2	3	7	13
2	3	7	29
2	3	7	43
2	3	8	7
2	3	8	3
2	3	8	17
2	3	8	5
2	3	9	19
2	3	9	37
2	3	10	11
2	3	10	31
2	3	12	13
2	3	12	5
2	3	13	13
2	3	15	2
2	3	18	19
2	4	5	5
2	4	5	3
2	4	5	11
2	4	5	41
2	4	6	5
2	4	6	7
2	4	6	13
2	4	8	3
2	4	8	17
2	4	12	13
2	5	5	5
2	5	5	11
2	5	10	11
2	6	6	7
2	6	6	13
2	6	7	7
2	8	8	3
3	3	4	7
3	3	4	3
3	3	4	5
3	3	5	2
3	3	6	13
3	3	7	7
3	4	4	5
3	4	4	13
3	6	6	7
4	4	4	3
4	4	5	5
2	3	∞	2
2	3	∞	3
2	3	∞	5
2	4	∞	3
2	5	∞	3
2	∞	∞	3
3	3	∞	3
3	∞	∞	2
3	∞	∞	3
∞	∞	∞	3

Scan me!