Triangular modular curves of low genus
Juanita Duque-Rosero
Joint work with John Voight
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 \( (X_1(N)) \).
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 \( \mathbb{Q}(\zeta_m) \).
- \( \text{Prym}(X_t) \) an isogeny factor of \( \text{Jac}(X_t) \).

The family \( \text{Prym}(X_t) \) 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 $\text{Prym}(X_f)$ 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.

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:

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

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

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

There is an embedding
\[ \Delta \hookrightarrow \text{PSL}_2(\mathbb{R}) \]
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
\[ X(1) = X(a, b, c; 1) := \Delta \backslash \mathcal{H} \]
Triangular modular curves

Construction

There is an embedding

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

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

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

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

We can decide between $\text{PSL}_2$ and $\text{PGL}_2$ from the behavior of $\mathfrak{p}$ in an extension of $E$. 
Level structure

\[ \pi_\mathfrak{p} : \Delta \rightarrow \operatorname{PXL}_2(\mathbb{Z}_E / \mathfrak{p}). \]

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

\[ \Gamma(\mathfrak{p}) := \ker \pi_\mathfrak{p} \leq \Delta. \]

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

\[ X(\mathfrak{p}) = X(a, b, c; \mathfrak{p}) := \Gamma(\mathfrak{p}) \backslash \mathcal{H} \]

**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 $\mathbb{F}_{p_k} \simeq \mathbb{F}_p$ for $p_k | p$. Thus

$$X(2,3,p^k; p_k) \simeq X(2,3,p; p_1).$$
Isomorphic curves

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

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

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

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

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

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

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

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

Lemma. Let $G = \text{PXL}_2(\mathbb{F}_q)$ 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 $\sigma_s$ on $G/H_0$ has:

- orbits of length $s$ 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

\[X_0(p) \to \mathbb{P}^1.\]
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 $q := \# \mathbb{F}_q$. 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

> time countBoundedGenus(100);
[ 56, 130, 180, 206, 232, 254, 245, 285, 289, 320, 298, 335, 308, 363, 329, 320,
  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. [Klug, Musty, Schiavone & Voight, ’14].

Example: the curve $X_0(3,3,4; p_7)$ is defined over the number field $k$ with defining polynomial $x^4 - 2x^3 + x^2 - 2x + 1$. We have

$$X_0(3,3,4; p_7) \simeq \mathbb{P}^1_k.$$

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

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>p</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>7</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>7</td>
<td>29</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>7</td>
<td>43</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>8</td>
<td>17</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>9</td>
<td>19</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>9</td>
<td>37</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>10</td>
<td>31</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>12</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>p</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>15</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>5</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>5</td>
<td>41</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>6</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>17</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>5</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>10</td>
<td>11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>p</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>6</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>6</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>13</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>∞</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>∞</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>∞</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>∞</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>∞</td>
<td>∞</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>∞</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>∞</td>
<td>∞</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>∞</td>
<td>∞</td>
<td>3</td>
</tr>
<tr>
<td>∞</td>
<td>∞</td>
<td>∞</td>
<td>3</td>
</tr>
</tbody>
</table>