ENUMERATING TRIANGULAR MODULAR CURVES OF LOW GENUS

Juanita Duque-Rosero, Dartmouth College
Joint work with John Voight
April 2022, Explicit Modularity

arXiv:2203.08593
**Theorem (DR & Voight, 2022)**

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 level $\mathfrak{N} \neq (1)$. The number of curves $X_0(a, b, c; \mathfrak{N})$ of genus $\leq 2$ are as follows:

- ▶ 71 curves of genus 0,
- ▶ 190 curves of genus 1.
- ▶ 153 curves of genus 2.
We consider the Legendre family of elliptic curves

\[ y^2 = x(x - 1)(x - \lambda) \]

for a parameter \( \lambda \neq 0, 1, \infty \).

- A curve in this family is a cyclic cover of \( \mathbb{P}^1 \) branched at 4 points.
- We can parameterize the family by the modular curve \( X(2) = \mathbb{P}^1 \).
- One can study additional level structure by considering covers of \( X(2) \), specifying extra data such as a cyclic \( N \)-isogeny or an \( N \)-torsion point.

Fundamental domain for \( \Gamma(2) \), by Paul Kainberger.
We consider the family of curves

\[ X_t : y^m = x^{e_0} (x - 1)^{e_1} (t - x)^{e_t}, \]

where \( t \neq 0, 1, \infty \).

- A curve in this family is a cyclic cover of \( \mathbb{P}^1 \) branched at 4 points.
- \( X_t \) has a cyclic group of automorphisms of order \( m \), defined over \( \mathbb{Q}(\zeta_m) \), given by \( \alpha : (x, y) \mapsto (x, \zeta_m y) \).
- We study \( \text{Prym}(X_t) \), an isogeny factor of \( \text{Jac}(X_t) \) where \( \alpha \) acts by a primitive \( m \)-th root of unity.

By work of Cohen & Wolfart (1990), triangular modular curves parameterize the varieties \( \text{Prym}(X_t) \).
For $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$, let $\Delta(a, b, c)$ be the triangle group with presentation

$$\Delta = \Delta(a, b, c) := \langle \delta_a, \delta_b, \delta_c \mid \delta_a^q = \delta_b^b = \delta_c^c = \delta_a \delta_b \delta_c = 1 \rangle.$$
The triple \((a, b, c) \in (\mathbb{Z}_{\geq 2} \cup \{\infty\})^3\) is **hyperbolic** if and only if
\[
\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 < 0.
\]

We now fix a hyperbolic triple \((a, b, c) \in \mathbb{Z}_{\geq 2} \cup \{\infty\} \).
Theorem (Takeuchi, 1977)

There is an embedding

\[ \Delta \hookrightarrow \text{SL}_2(\mathbb{R}) \]

can be given explicitly in terms of the functions \( \sin(\pi/s) \) and \( \cos(\pi/s) \). 
This embedding is unique up to conjugacy in \( \text{SL}_2(\mathbb{R}) \).

The quotient

\[ X(1) := \Delta \backslash \mathcal{H} \]

is a complex Riemannian 1-orbifold of genus zero. We call this quotient a triangular modular curve (TMC).
Let $p$ be a rational prime with $p \nmid 2abc$. We consider the tower of fields

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

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

$$\mathbb{Q}$$

Remark: $2 \cos \left( \frac{2\pi}{s} \right) = \zeta_s + 1/\zeta_s$, where $\zeta_s := \exp(2\pi i/s)$.

There is a homomorphism

$$\phi_p : \Delta \to \text{PSL}_2(\mathbb{Z}_F/\mathfrak{p})$$

We let the subgroup $\Delta(p)$ be the subgroup given by $\ker \phi_p \subseteq \Delta$. 
Theorem (Clark & Voight, 2019)

Let \((a, b, c)\) be a hyperbolic triple with \(a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}\). Let \(\mathfrak{p}\) be a prime of \(E\) with residue field \(\mathbb{F}_p\) and suppose \(\mathfrak{p} \nmid 2abc\). Then there exists a \(G\)-Galois Belyi map \(X(\mathfrak{p}) \to \mathbb{P}^1\) with ramification indices \((a, b, c)\), where

\[
G = \begin{cases} 
PSL_2(\mathbb{F}_p), & \text{if } \mathfrak{p} \text{ splits completely in } F; \\
PGL_2(\mathbb{F}_p), & \text{otherwise}.
\end{cases}
\]

Remark: The genus of \(X(\mathfrak{p})\) is given by

\[
g(X(\mathfrak{p})) = 1 + \frac{\#G}{2} \left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right).
\]

Analogously, we obtain curves \(X(\mathfrak{N}) := \Delta(\mathfrak{N}) \setminus \mathcal{H}\) for every ideal \(\mathfrak{N}\) of \(E\).
Recall the homomorphism

\[ \phi_\mathfrak{N} : \Delta \to \text{PSL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F), \]

and that \( \Delta(\mathfrak{N}) := \ker \phi_\mathfrak{N} \).

Define the subgroups,

\[
H_0 := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \quad H_1 := \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\} \subseteq \text{PSL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F),
\]

\[
\Gamma_0(\mathfrak{N}) := \phi_\mathfrak{N}^{-1}(H_0), \quad \Gamma_1(\mathfrak{N}) := \phi_\mathfrak{N}^{-1}(H_1) \subseteq \Delta.
\]

We define the curves

\[
X_0(\mathfrak{N}) := \Gamma_0(\mathfrak{N})\backslash \mathcal{H}, \quad X_1(\mathfrak{N}) := \Gamma_1(\mathfrak{N})\backslash \mathcal{H}.
\]

Then we have maps

\[
X(\mathfrak{N}) \to X_1(\mathfrak{N}) \to X_0(\mathfrak{N}) \to X(1).
\]
Example

We consider the triple \((a, b, c) = (2, 3, \infty)\). In this case we have that 
\(Q = E = F\) and \(\text{SL}_2(\mathbb{Z}) \cong \Delta(2, 3, \infty)\). By construction, 
\(X(2, 3, \infty; N) = X(N)\).

Example

Let \(p \geq 5\) be a prime. We consider hyperbolic triples of the form \((2, 3, c)\) with 
\(c = p^k\) and \(k \geq 1\). Then 
\(X(2, 3, p^k; p) \cong X(2, 3, p; p)\).

Definition

An ideal \(\mathfrak{m} \subseteq \mathbb{Z}_E\) is **admissible** for \((a, b, c)\) if \(\mathfrak{m}\) is nonzero and the following 
two conditions hold:

1. \(\mathfrak{m}\) is coprime to \(\beta(a, b, c)\), and
2. if \(p \mid \mathfrak{m}\) is a prime lying above \(p \in \mathbb{Z}\), and \(p \mid s\) for \(s \in \{a, b, c\}\), then \(p = s\).
Lemma

Let \( p \) be an odd prime and \( \mathfrak{p} \) be a prime of \( E \) above \( p \). Let \( \mathfrak{p} \) be admissible for \((a, b, c)\) and let \( q = p^r \) be such that \( \mathbb{F}_p = \mathbb{F}_q \). Then the genus of the curve \( X_0(\mathfrak{p}) \) is given by

\[
2g - 2 = -2(q + 1) + k_a(a - 1) + k_b(b - 1) + k_c(c - 1),
\]

where

\[
k_s = \begin{cases} 
\frac{q - 1}{s} & s \mid (q - 1), \\
\frac{q}{s} & s \mid q, \\
\frac{s}{q + 1} & s \mid (q + 1).
\end{cases}
\]
**Corollary**

Let $p$ be an odd prime and $\mathfrak{p}$ be a prime of $E$ above $p$. Let $\mathfrak{p}$ be admissible for $(a, b, c)$ and let $q = p^r$ be such that $\mathbb{F}_p = \mathbb{F}_q$. Then,

$$g(X_0(\mathfrak{p})) \geq \frac{q - 1}{2} \left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right) - 1.$$

If $(a, b, c)$ is a hyperbolic triple, we have

$$1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c} \geq \frac{1}{42}.$$

Then, for a fixed $g_0$,

$$q \leq 82g_0 + 1.$$
Theorem (DR & Voight, 2022)

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 level $\mathfrak{N} \neq (1)$. The number of curves $X_0(a, b, c; \mathfrak{N})$ of genus $\leq 2$ are as follows:

- 71 curves of genus 0,
- 190 curves of genus 1.
- 153 curves of genus 2.
This algorithm returns a list \textit{lowGenus} of all hyperbolic triples \((a, b, c)\), primes \(p\) and Galois groups \(\text{PSL}_2(\mathbb{F}_q)\) or \(\text{PGL}(\mathbb{F}_q)\) such that the genus of \(X_0(a, b, c; p)\) is less than \(g_0\).

1. Loop over the list of possible powers \(q = p^r\), where \(p\) is any rational prime and \(q \leq 84(g_0 + 1) + 1\).

2. For each \(q\), find all hyperbolic triples \((a, b, c)\) for which \(p\) is \((a, b, c)\)-admissible with \(\mathbb{F}_p = \mathbb{F}_q\).

3. For each such triple \((a, b, c)\), compute the genus \(g\) of \(X_0(a, b, c; p)\). If \(g \leq g_0\), add \((a, b, c; p, q)\) to the list \textit{lowGenus}.
Future work

- Address the existence of triangular modular curves (and their genera) without the admissibility hypothesis.
- Find models and compute rational points of TMCs of low genus.
- Study TMCs for all congruence subgroups of triangle groups.

Code is available at GitHub.
### Curves $X_0(a, b, c; p)$ of Genus 0

<table>
<thead>
<tr>
<th>$(a, b, c)$</th>
<th>$p$</th>
<th>$(a, b, c)$</th>
<th>$p$</th>
<th>$(a, b, c)$</th>
<th>$p$</th>
<th>$(a, b, c)$</th>
<th>$p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2, 3, 7)</td>
<td>7</td>
<td>(2, 4, 5)</td>
<td>5</td>
<td>(3, 3, 4)</td>
<td>7</td>
<td>(2, 4, ∞)</td>
<td>5</td>
</tr>
<tr>
<td>(2, 3, 7)</td>
<td>2</td>
<td>(2, 4, 5)</td>
<td>3</td>
<td>(3, 3, 4)</td>
<td>3</td>
<td>(2, 5, ∞)</td>
<td>5</td>
</tr>
<tr>
<td>(2, 3, 7)</td>
<td>13</td>
<td>(2, 4, 5)</td>
<td>11</td>
<td>(3, 3, 4)</td>
<td>5</td>
<td>(2, 5, ∞)</td>
<td>3</td>
</tr>
<tr>
<td>(2, 3, 7)</td>
<td>29</td>
<td>(2, 4, 5)</td>
<td>41</td>
<td>(3, 3, 5)</td>
<td>2</td>
<td>(2, 6, ∞)</td>
<td>7</td>
</tr>
<tr>
<td>(2, 3, 7)</td>
<td>43</td>
<td>(2, 4, 6)</td>
<td>5</td>
<td>(3, 3, 6)</td>
<td>13</td>
<td>(2, 8, ∞)</td>
<td>3</td>
</tr>
<tr>
<td>(2, 3, 8)</td>
<td>7</td>
<td>(2, 4, 6)</td>
<td>7</td>
<td>(3, 3, 7)</td>
<td>7</td>
<td>(2, ∞, ∞)</td>
<td>3</td>
</tr>
<tr>
<td>(2, 3, 8)</td>
<td>3</td>
<td>(2, 4, 6)</td>
<td>13</td>
<td>(3, 4, 4)</td>
<td>5</td>
<td>(2, ∞, ∞)</td>
<td>5</td>
</tr>
<tr>
<td>(2, 3, 8)</td>
<td>17</td>
<td>(2, 4, 8)</td>
<td>3</td>
<td>(3, 4, 4)</td>
<td>13</td>
<td>(3, 3, ∞)</td>
<td>3</td>
</tr>
<tr>
<td>(2, 3, 8)</td>
<td>5</td>
<td>(2, 4, 8)</td>
<td>17</td>
<td>(3, 6, 6)</td>
<td>7</td>
<td>(3, 3, ∞)</td>
<td>7</td>
</tr>
<tr>
<td>(2, 3, 9)</td>
<td>19</td>
<td>(2, 4, 12)</td>
<td>13</td>
<td>(4, 4, 4)</td>
<td>3</td>
<td>(3, 4, ∞)</td>
<td>3</td>
</tr>
<tr>
<td>(2, 3, 9)</td>
<td>37</td>
<td>(2, 5, 5)</td>
<td>5</td>
<td>(4, 4, 5)</td>
<td>5</td>
<td>(3, 7, ∞)</td>
<td>2</td>
</tr>
<tr>
<td>(2, 3, 10)</td>
<td>11</td>
<td>(2, 5, 5)</td>
<td>11</td>
<td>(2, 3, ∞)</td>
<td>2</td>
<td>(3, 15, ∞)</td>
<td>2</td>
</tr>
<tr>
<td>(2, 3, 10)</td>
<td>31</td>
<td>(2, 5, 10)</td>
<td>11</td>
<td>(2, 3, ∞)</td>
<td>3</td>
<td>(3, ∞, ∞)</td>
<td>2</td>
</tr>
<tr>
<td>(2, 3, 12)</td>
<td>13</td>
<td>(2, 6, 6)</td>
<td>7</td>
<td>(2, 3, ∞)</td>
<td>5</td>
<td>(3, ∞, ∞)</td>
<td>3</td>
</tr>
<tr>
<td>(2, 3, 12)</td>
<td>5</td>
<td>(2, 6, 6)</td>
<td>13</td>
<td>(2, 3, ∞)</td>
<td>7</td>
<td>(4, 4, ∞)</td>
<td>5</td>
</tr>
<tr>
<td>(2, 3, 13)</td>
<td>13</td>
<td>(2, 6, 7)</td>
<td>7</td>
<td>(2, 3, ∞)</td>
<td>13</td>
<td>(4, ∞, ∞)</td>
<td>3</td>
</tr>
<tr>
<td>(2, 3, 15)</td>
<td>2</td>
<td>(2, 8, 8)</td>
<td>3</td>
<td>(2, 4, ∞)</td>
<td>3</td>
<td>(∞, ∞, ∞)</td>
<td>3</td>
</tr>
<tr>
<td>(2, 3, 18)</td>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>