TRIANGULAR MODULAR CURVES OF SMALL GENUS

JUANITA DUQUE-ROSERO AND JOHN VOIGHT

Abstract. Triangular modular curves are a generalization of modular curves that arise from quotients of the upper half-plane by congruence subgroups of hyperbolic triangle groups. These curves also arise naturally as Belyi maps with monodromy $\mathrm{PGL}_2(\mathbb{F}_q)$ or $\mathrm{PSL}_2(\mathbb{F}_q)$. We present a computational approach to enumerate triangular modular curves of low genus, and we carry out this enumeration up to genus 2.

1. Introduction

Motivation. The study of modular curves has rewarded mathematicians for perhaps a century. For an integer $N \geq 1$, let $\Gamma_0(N), \Gamma_1(N) \leq \mathrm{SL}_2(\mathbb{Z})$ be the usual congruence subgroups and let $X_0(N), X_1(N)$ be the corresponding quotients of the completed upper half-plane. The genera of $X_0(N)$ and $X_1(N)$ as compact Riemann surfaces can be computed using the Riemann–Hurwitz formula, and it can readily be seen that there are only finitely many of any given genus $g \geq 0$.

The study of modular curves of small genus goes back at least to Fricke [Fri11, p. 357]. At the end of the 20th century, Ogg enumerated and studied elliptic [Ogg73] and hyperelliptic [Ogg74] modular curves; the resulting Diophantine study [Ogg75] informed Mazur's classification of rational isogenies of elliptic curves [Maz78], where the curves of genus 0 are precisely the ones with infinitely many rational points. This explicit study continues today, extended to include all quotients of the upper half-plane by congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$; the list up to genus 24 was computed by Cummins–Pauli [CP03]. Recent papers have studied curves with infinitely many rational points in the context of Mazur's *Program B*—see Rouse–Sutherland–Zureick-Brown [RSZB21] for further references and recent results in this direction.

Given this rich backdrop, it is worthwhile to pursue further generalizations. For example, replacing $\mathrm{SL}_2(\mathbb{Z})$ with its quaternionic cousins, Voight [Voi09] enumerated all Shimura curves of the form $X_0^1(\mathfrak{D}, \mathfrak{M})$ of genus at most 2. In a similar direction, Long–Maclachlan–Reid [LMR06] enumerated all maximal arithmetic Fuchsian groups of genus 0, corresponding to total Atkin–Lehner quotients of Shimura curves.

Setup and main result. In this paper, we consider a different type of generalization: namely, from the point of congruence subgroups of triangle groups as introduced by Clark–Voight [CV19]. We briefly introduce this construction; for more detail, see section 2. Let $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$, and suppose that $1/a + 1/b + 1/c < 1$ (where $1/\infty = 0$). Then there is a triangle in the upper half-plane $\mathcal{H}$ (completed if $\infty \in \{a, b, c\}$) with angles π/a, π/b, and π/c. The reflections in the sides of this triangle generate a discrete subgroup of $\mathrm{PGL}_2(\mathbb{R})$, and the orientation-preserving subgroup (of index 2) defines the triangle group $\Delta = \Delta(a, b, c) \leq \mathrm{PSL}_2(\mathbb{R})$. The triangle group acts properly by isometries on $\mathcal{H}$ and the quotient $X(a, b, c) := \Delta(a, b, c)\backslash\mathcal{H}$ can be given the structure of a compact Riemann surface of genus 0, equipped with a coordinate taking values $0, 1, \infty$ at the vertices labelled a, b, c, respectively. For example, we recover the classical modular group as $\Delta(2, 3, \infty) \simeq \mathrm{PSL}_2(\mathbb{Z})$.

Let $m := \gcd(\{a, b, c\} \smallsetminus \{\infty\})$, with $m = 1$ for $a = b = c = \infty$. Attached to (a, b, c) is an extension

$$E = E(a, b, c) \subseteq F = F(a, b, c) \subseteq \mathbb{Q}(\zeta_{2m})^+ \tag{1.1}$$

of totally real, abelian number fields and a discriminant $\beta = \beta(a, b, c) \in E^\times$ which can be given explicitly (2.6). Let $\mathfrak{N} \subseteq \mathbb{Z}_E$ be a nonzero ideal. We say that $\mathfrak{N}$ is admissible for (a, b, c) if the following conditions hold:

(i) $\mathfrak{N}$ is coprime to $\beta(a, b, c)$, and
(ii) if $\mathfrak{p} \mid \mathfrak{N}$ is a prime lying above $p \in \mathbb{Z}$, and $p \mid s$ for $s \in \{a, b, c\}$, then $p = s$.

For example, if $\mathfrak{N}$ is coprime to $2abc$, then $\mathfrak{N}$ is admissible.

Suppose that $\mathfrak{N}$ is admissible. Then [CV19, Theorem A, Theorem 9.1, Corollary 9.2] there is a normal subgroup $\Gamma(a, b, c; \mathfrak{N}) \trianglelefteq \Delta(a, b, c)$ with quotient

$$G_{\mathfrak{N}} := \mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{N}) \simeq \mathrm{P}\left(\prod_{\mathfrak{p}^e \| \mathfrak{N}} \mathrm{XL}_2(\mathbb{Z}_E/\mathfrak{p}^e)\right) \tag{1.2}$$

where on the right-hand side, XL_2 denotes either SL_2 or GL_2 according as $\mathfrak{p}$ splits or not in $F(a, b, c)$, and the P out front means modulo the subgroup of scalar matrices. We call the subgroup $\Gamma(a, b, c; \mathfrak{N})$ the principal congruence subgroup of level $\mathfrak{N}$ as it arises from a certain kernel modulo $\mathfrak{N}$; it can intuitively be thought of as arising from congruence conditions on matrix entries (but has a rigorous quaternionic interpretation). Writing $X(a, b, c; \mathfrak{N}) := \Gamma(\mathfrak{N})\backslash\mathcal{H}$, the quotient map

$$\varphi\colon X(a, b, c; \mathfrak{N}) \to X(a, b, c) \simeq \mathbb{P}^1_{\mathbb{C}} \tag{1.3}$$

gives rise to a map of smooth projective, complex curves which can be descended to a number field [CV19, Theorem B]. Moreover, the map φ is a Belyi map which is (geometrically, generically) Galois with group $\mathrm{Aut}(\varphi) = G_{\mathfrak{N}}$.

Finally, a triangular modular curve is a quotient $X(a, b, c; \mathfrak{N})/H$ for a subgroup $H \le G_{\mathfrak{N}}$. Of particular interest is the case where H is a Borel-type (upper-triangular) subgroup, giving quotients $X_0(a, b, c; \mathfrak{N})$ and $X_1(a, b, c; \mathfrak{N})$ analogous to the classical modular curves; we again call $\mathfrak{N}$ the level.

Our main result is as follows.

Theorem 1.4. *For any $g \in \mathbb{Z}_{\ge 0}$, 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 $\mathfrak{N} \neq (1)$. The number of curves of genus ≤ 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

Our implementation of the Borel-type computation is available online [DRV22], including the complete list in computer readable format with additional data (e.g. passport representatives). The list for curves $X_0(a, b, c; \mathfrak{p})$ of prime level $\mathfrak{p}$ and $g = 0, 1$ is given in Appendix A.

Discussion. As for classical modular curves, Theorem 1.4 uses the Riemann–Hurwitz theorem. We observe that the ramification at prime level takes a tidy form, and from there we bootstrap to composite level and from there we can conclude finiteness. Then we carry out the explicit enumeration using the existence and classification results of Clark–Voight [CV19], which themselves ultimately rest on work of Macbeath [Mac69] classifying two-generated subgroups of $\mathrm{SL}_2(\mathbb{F}_q)$ in terms of trace triples. The case $a = 2$ causes particular difficulties (see Remark 3.7).

Our theorem has potential applications in arithmetic geometry analogous to classical modular curves. Just as the quotient of the upper half-plane by $\mathrm{PSL}_2(\mathbb{Z})$ is the set of complex points of the moduli space of elliptic curves (parametrized by the affine j-line), Cohen–Wolfart [CW90, §3.3] and Archinard [Arc03] showed that the curves $X(a, b, c)$ naturally parametrize *hypergeometric abelian varieties*, certain Prym varieties of cyclic covers of $\mathbb{P}^1$ (with parameter t) branched over ≤ 4 points. The name comes from the fact that their complex periods are values of ${}_2F_1$-hypergeometric functions for $t \in \mathbb{P}^1(\mathbb{C}) \smallsetminus \{0, 1, \infty\}$. In accordance with Manin's *unity of mathematics* [Cle03], their point counts are defined by finite-field analogues of hypergeometric functions for $t \in \mathbb{P}^1(\mathbb{F}_q) \smallsetminus \{0, 1, \infty\}$; these can be packaged together (in an ℓ-adic Galois representation) to define hypergeometric L-functions attached to a motive for every $t \in \mathbb{P}^1(\mathbb{Q}^{\mathrm{al}}) \smallsetminus \{0, 1, \infty\}$.

More generally, just as classical modular curves parametrize elliptic curves equipped with level structure, triangular modular curves parametrize hypergeometric abelian varieties equipped with level structure: see upcoming work of Kucharczyk–Voight [KV22] for the details, including a natural idelic refinement and a notion of canonical model. In this light, our paper classifies those situations where we might parametrize *infinitely many* such varieties with level structure for $t \in \mathbb{Q}$.

As shown by Takeuchi [Tak77b, Tak77a], only finitely many triples (a, b, c) give rise to arithmetic Fuchsian groups; the remaining triples are *nonarithmetic*. Thus almost all of the corresponding triangular modular curves fall outside the usual scope of the Langlands program. We believe that this is a worthwhile gambit.

As a final possible Diophantine application, we recall work of Darmon [Dar04]: he provides a dictionary between finite index subgroups of the triangle group $\Delta(a, b, c)$ and approaches to solve the generalized Fermat equation $x^a + y^b + z^c = 0$. From this vantage point, the triangular modular curves of low genus "explain" situations where the associated mod $\mathfrak{N}$ Galois representations fail to be surjective.

In future work, we plan to compute equations for these curves (as Belyi maps) using the methods of Klug–Musty–Schiavone–Voight [KMSV14] and then to study their rational points. Even without these equations, we have verified that all but a handful of the genus zero curves necessarily have a ramified rational point (hence are isomorphic to $\mathbb{P}^1$ over any field of definition). It would also be interesting to relax the condition of admissibility (but see Example 2.16) and in particular to pursue cases when $\mathfrak{N}$ is not coprime to β, where the corresponding Galois covers will instead be solvable.

Finally, we peek ahead to more general triangular modular curves, allowing other subgroups $H \leq G_{\mathfrak{N}}$ (prescribing other possible images of the corresponding Galois representations). For the case $\Delta = \mathrm{PSL}_2(\mathbb{Z})$, the story is a long and beautiful one, originating with a conjecture of Rademacher that there are only finitely many genus 0 congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. Thompson [Tho80] proved this for any genus g, but the list of Cummins–Pauli relies upon difficult and delicate p-adic methods of Cox–Parry [CP84] for an explicit bound on the level in terms of the genus. We propose the following conjecture, which predicts a similar result for triangular modular curves.

Conjecture 1.5. *For any $g \in \mathbb{Z}_{\geq 0}$, there are only finitely many (admissible) triangular modular curves $X(a,b,c;\mathfrak{N})/H$ of genus g with $\Delta(a,b,c)$ maximal.*

We restrict to maximal subgroups because the inclusion of triangle groups $\Delta(a,a,c) \trianglelefteq \Delta(2,a,2c)$ allows us to take $H = \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N}_F) \trianglelefteq \mathrm{PGL}_2(\mathbb{Z}_F/\mathfrak{N}_F)$, yielding infinitely many triangular modular curves of genus zero. (We might eliminate this redundancy in another way, but the above conjecture focuses on the essential case.) We consider our main result (Theorem 1.4) as partial progress towards this conjecture—the Borel–type subgroups are the family with the smallest growing index, thus likely to have the smallest genera. It would be interesting to see if the rather delicate p-adic methods of Cox–Parry can be generalized from $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ to groups of the form $\mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{N})$, as this would imply Conjecture 1.5 in an effective way.

Contents. In section 2, we review the construction of triangular modular curves and as a warmup consider the much easier Galois case $X(a,b,c;\mathfrak{N})$. Then in section 3, for the case $X_0(a,b,c;\mathfrak{p})$ with $a,b,c \in \mathbb{Z}$ and prime level $\mathfrak{p}$, we give an explicit formula for the genus and we bound the norm of the level in terms of the genus, proving finiteness; we then provide an algorithm to effectively enumerate them in section 4. To conclude, in section 5 we finish the remaining cases—composite level $\mathfrak{N}$, non-cocompact triples and curves $X_1(a,b,c;\mathfrak{N})$—and we prove Theorem 1.4. Finally, we provide the list in Appendix A.

Acknowledgements. The authors would like to thank Asher Auel for helpful conversations. The authors were supported by a Simons Collaboration grant (550029, to Voight).

2. Triangular modular curves

In this section, we give an overview on the definition of triangular modular curves.

Setup. Beginning again, let $a,b,c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$; to avoid redundancy, we take $a \leq b \leq c$. Let

$$\chi(a,b,c) := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 \tag{2.1}$$

so that $\chi(a,b,c)\pi$ is difference from π of the sum of the angles of a triangle with angles $\pi/a, \pi/b, \pi/c$. If $\chi(a,b,c) \geq 0$, then such a triangle is drawn on the sphere or Euclidean plane, and these are very classical. Otherwise, we say that the triple (a,b,c) is hyperbolic if $\chi(a,b,c) < 0$ as then the triangle lies in the (completed) upper half-plane $\mathcal{H}$. For a hyperbolic triple (a,b,c), we always have

$$\chi(a,b,c) \leq \chi(2,3,7) = -\frac{1}{42} \tag{2.2}$$

bounded away from zero, by a simple maximization argument by cases.

Definition 2.3. Let (a,b,c) be a triple. Then the triangle group $\Delta(a,b,c)$ is the group with presentation

$$\Delta(a,b,c) := \langle \delta_a, \delta_b, \delta_c \mid \delta_a^a = \delta_b^b = \delta_c^c = \delta_a\delta_b\delta_c = 1 \rangle. \tag{2.4}$$

As explained in the introduction, this group arises naturally from the orientation-preserving isometries of the group generated by reflections in the sides of the triangle described above, drawn in the appropriate geometry.

From now on, we suppose that the triple (a, b, c) is hyperbolic. Then there is an associated map $\Delta(a,b,c) \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$, unique up to conjugation when $b < \infty$. The group $\Delta(a,b,c)$ is said to be cocompact the quotient of the upper half-plane by $\Delta(a,b,c)$ is compact, else we say noncocompact. We have $\Delta(a,b,c)$ cocompact if and only if $a,b,c \in \mathbb{Z}_{\geq 2}$; that is to say, $\Delta(a,b,c)$ is noncocompact if and only if one of a,b,c is equal to ∞.

Prime level. We follow the construction of congruence subgroups of triangle groups given by Clark–Voight [CV19]. For $s \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$, let $\zeta_s := \exp(2\pi i/s)$ and let $\lambda_s := \zeta_s + 1/\zeta_s$, with $\zeta_\infty = 1$ and $\lambda_\infty = 2$ by convention. Define the tower of fields

$$\begin{array}{c} F = F(a,b,c) := \mathbb{Q}(\lambda_{2a}, \lambda_{2b}, \lambda_{2c}) \\ \Big| \\ E = E(a,b,c) := \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c, \lambda_{2a}\lambda_{2b}\lambda_{2c}). \end{array} \tag{2.5}$$

The extension $F \supseteq E$ is abelian of exponent at most 2 (since $\lambda_{2s}^2 = \lambda_s + 2$) and has degree at most 4. Let $\mathbb{Z}_F \supseteq \mathbb{Z}_E$ be the corresponding rings of integers.

The reduced discriminant of the $\mathbb{Z}_F$-order $\mathbb{Z}_F\langle\Delta\rangle$ generated over $\mathbb{Z}_F$ by the preimage of Δ in $\mathrm{SL}_2(\mathbb{R}) \subseteq \mathrm{M}_2(\mathbb{R})$ is a principal ideal of $\mathbb{Z}_F$, and it is generated by [CV19, Lemma 5.4]

$$\beta(a,b,c) := \lambda_{2a}^2 + \lambda_{2b}^2 + \lambda_{2c}^2 + \lambda_{2a}\lambda_{2b}\lambda_{2c} - 4 = \lambda_a + \lambda_b + \lambda_c + \lambda_{2a}\lambda_{2b}\lambda_{2c} + 2 \in \mathbb{Z}_E. \tag{2.6}$$

In particular, if $\mathfrak{p} \nmid 2abc$, then $\mathfrak{p} \nmid \beta(a,b,c)$ [CV19, Lemma 5.5]. The quantity β plays an important role in the following theorem, fundamental for our investigations.

Theorem 2.7 ([CV19])**.** *Let $(a,\ b,\ c)$ be a hyperbolic triple. Let $\mathfrak{p}$ be a prime of $\mathbb{Z}_{E(a,b,c)}$ with residue field $\mathbb{F}_\mathfrak{p}$. Let $p \in \mathbb{Z}$ be the prime below $\mathfrak{p}$ and suppose that:*

(i) *$\mathfrak{p} \nmid \beta(a,b,c)$, and*
(ii) *if $p \mid s$ with $s \in \{a,b,c\}$, then $s = p$.*

Then there exists a G-Galois Belyi map $X(a,b,c;\mathfrak{p}) \to \mathbb{P}^1$ with ramification indices (a,b,c), where

$$G = \begin{cases} \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p}), & \text{if } \mathfrak{p} \text{ splits in } F(a,b,c); \\ \mathrm{PGL}_2(\mathbb{F}_\mathfrak{p}), & \text{otherwise.} \end{cases}$$

By "$\mathfrak{p}$ splits in $F(a,b,c)$" we mean that the residue class field of any prime $\mathfrak{p}_F$ above $\mathfrak{p}$ in $F(a,b,c)$ is isomorphic to $\mathbb{F}_\mathfrak{p}$ (i.e., residue class field degree $f = 1$); this allows $\mathfrak{p}$ to be ramified.

Proof. We refer to Clark–Voight [CV19, Theorem A] for the case where $\mathfrak{p} \nmid 2abc$; but examining the argument given [CV19, Remark 5.24, Theorem 9.1], we see that it extends to the above cases. □

Without condition (i) in Theorem 2.7, we are in quite a different situation: the local quaternion order $\mathcal{O}_\mathfrak{p} = \mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{p}_F}$ is not isomorphic to $\mathrm{M}_2(\mathbb{Z}_F)$, so we cannot hope to get simple quotients $\mathrm{PXL}_2(\mathbb{F}_\mathfrak{p})$. Condition (ii) is natural, since if an element of $\mathrm{PXL}_2(\mathbb{F}_\mathfrak{p})$ has order divisible by p, then in fact it has order *equal* to p; so we could not have the conclusion that the ramification indices are equal to (a,b,c).

Admissibility and composite level. Before proceeding, we make a definition to capture the scope of Theorem 2.7.

Definition 2.8. An ideal $\mathfrak{N} \subseteq \mathbb{Z}_E$ is admissible for (a, b, c) if the $\mathfrak{N}$ is nonzero and the following two conditions hold:

(i) $\mathfrak{N}$ is coprime to $\beta(a, b, c)$, and
(ii) if $\mathfrak{p} \mid \mathfrak{N}$ is a prime lying above $p \in \mathbb{Z}$, and $p \mid s$ for $s \in \{a, b, c\}$, then $p = s$.

The branched covers constructed in Theorem 2.7 lift to an arbitrary admissible ideal $\mathfrak{N}$ as follows.

Let $\mathfrak{N} \subseteq \mathbb{Z}_E$ be admissible for (a, b, c). Then [CV19, Proposition 5.23, Remark 5.24, Theorem 9.1] there is a homomorphism

$$\pi = \pi_{\mathfrak{N}} \colon \Delta(a, b, c) \to \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F) \tag{2.9}$$

whose image (under the hypothesis of admissibility) is of the form $\mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{N})$. Let

$$\Gamma(a, b, c; \mathfrak{N}) := \ker \pi_{\mathfrak{N}}; \tag{2.10}$$

we call this the principal congruence subgroup of level $\mathfrak{N}$ (but remind the reader that in general this is a subgroup of a nonarithmetic Fuchsian group). We analogously define

$$X(a, b, c; \mathfrak{N}) := \Delta(a, b, c; \mathfrak{N})\backslash\mathcal{H}. \tag{2.11}$$

Let $H_0 \leq \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N})$ be the image of the upper triangular matrices in $\mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N})$. We also define $H_1 \leq \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N})$ to be the image of the subgroup of upper-triangular matrices with both diagonal entries equal to 1. We then define the subgroups

$$\begin{aligned} \Gamma_0(a, b, c; \mathfrak{N}) &:= \varphi_{\mathfrak{N}}^{-1}(H_0), \\ \Gamma_1(a, b, c; \mathfrak{N}) &:= \varphi_{\mathfrak{N}}^{-1}(H_1). \end{aligned} \tag{2.12}$$

and the corresponding quotients

$$\begin{aligned} X_0(a, b, c; \mathfrak{N}) &:= \Gamma_0(a, b, c; \mathfrak{N})\backslash\mathcal{H} = H_0\backslash X(a, b, c; \mathfrak{N}) \\ X_1(a, b, c; \mathfrak{N}) &:= \Gamma_1(a, b, c; \mathfrak{N})\backslash\mathcal{H} = H_1\backslash X(a, b, c; \mathfrak{N}). \end{aligned} \tag{2.13}$$

Then we have natural quotient maps

$$X(a, b, c; \mathfrak{N}) \to X_1(a, b, c; \mathfrak{N}) \to X_0(a, b, c; \mathfrak{N}) \to X(a, b, c; 1) \simeq \mathbb{P}^1. \tag{2.14}$$

Before ending this section, we note that the notion of admissibility has an important consequence. In general, the same underlying Belyi map can arise for infinitely many triples (a, b, c), owing to the fact that we may not always have $\pi(\delta_s)$ having order s in $G_{\mathfrak{N}}$ (recalling π defined in (2.9)). However, this cannot arise under admissibility.

Lemma 2.15. *If $\mathfrak{N}$ is admissible for (a, b, c), then $\pi(\delta_s)$ has order $s \in G_{\mathfrak{N}}$ for $s = a, b, c$.*

Proof. Since δ_s itself has order s, it is enough to prove this for $\mathfrak{N} = \mathfrak{p}$ prime; and this is proven by Clark–Voight [CV19, Theorem 9.1] (not mentioned in the statement, but proven as a claim in the course of the proof). ☐

Unfortunately, if the hypothesis in Lemma 2.15 is not satisfied, then the orders may drop—as in the following example.

Example 2.16. Consider the triples $(2,3,c)$ with $c = p^k$, where $k \geq 1$ and $p \geq 5$ is prime. Then

$$E_k := E(2,3,c) = F(2,3,c) = \mathbb{Q}(\lambda_{2c}) = \mathbb{Q}(\zeta_{2c})^+ \tag{2.17}$$

and $\beta(2,3,c) = \lambda_c - 1 \in \mathbb{Z}_{E_k}^\times$. The prime p is totally ramified in F, so $\mathbb{F}_{\mathfrak{p}_k} \simeq \mathbb{F}_p$ for $\mathfrak{p}_k \mid p$. Thus $X(2,3,p^k;\mathfrak{p}_k) \simeq X(2,3,p;\mathfrak{p}_1)$.

The upshot of Lemma Lemma 2.15 is that these redundancies do not arise under admissibility; still, we hope in future work to address the existence of triangular modular curves (and their genera) without this hypothesis.

Galois case. To conclude this section, we do a warmup for what follows: we first consider the curves $X(a,b,c;\mathfrak{N})$ corresponding to principal congruence subgroups, with Galois Belyi map $X(a,b,c;\mathfrak{N}) \to X(a,b,c) \simeq \mathbb{P}^1$.

Quite generally, for any G-Galois Belyi map, the ramification indices above each ramification point are equal. By admissibility and Lemma 2.15, a, b, c are also the orders of the ramification points. Thus the Riemann-Hurwitz formula gives

$$2g(X) - 2 = -2(\#G) + \sum_{s=a,b,c} \frac{\#G}{s}(s-1) \tag{2.18}$$

which simplifies to

$$g(X) = 1 - \frac{\#G}{2}\chi(a,b,c). \tag{2.19}$$

From this genus formula and (2.2), we can conclude that, for any fixed genus $g_0 \geq 0$, there are finitely many curves $X(a,b,c;\mathfrak{p})$ of genus $g \leq g_0$. Indeed, for (a,b,c) hyperbolic we have

$$84(g_0 - 1) \geq \#G = \begin{cases} q(q+1)(q-1)/2, & \text{if } G = \mathrm{PSL}_2(\mathbb{F}_q) \text{ and } q \text{ is odd;} \\ q(q+1)(q-1), & \text{otherwise.} \end{cases}$$

Thus, there are no curves $X(a,b,c;\mathfrak{p})$ of genus at most 2. In addition, since $X(a,b,c;\mathfrak{N})$ must cover $X(a,b,c;\mathfrak{p})$ for any prime divisor $\mathfrak{p} \mid \mathfrak{N}$, the same holds for $X(a,b,c;\mathfrak{N})$ with $\mathfrak{N}$ composite.

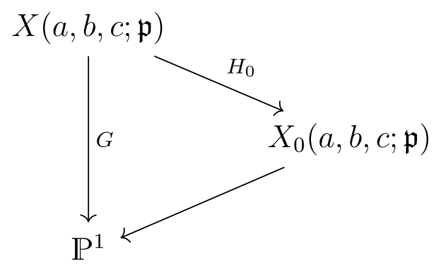
In fact, the smallest genus for a hyperbolic triple with $a,b,c \in \mathbb{Z}_{\geq 2}$ is genus 3 for $(a,b,c) = (2,3,7)$, yielding the famed Klein quartic curve. More generally, see Clark–Voight [CV19, Table 10.5] for examples up to genus 24.

3. Triangular modular curves $X_0(a,b,c;\mathfrak{p})$ of prime level

In this section, we exhibit a formula for the genus of the triangular modular curves $X_0(a,b,c;\mathfrak{p})$ for $\mathfrak{p}$ prime. In particular, we show that there are only finitely many such curves for a fixed genus.

Setup. Let (a,b,c) be a hyperbolic triple and $\mathfrak{p}$ be an admissible prime of E, with residue field degree $\mathbb{F}_\mathfrak{p}$ having $\#\mathbb{F}_\mathfrak{p} = q$. Because E is Galois over $\mathbb{Q}$, all primes $\mathfrak{p}$ have the same ramification and splitting type; it follows that the genus of $X_0(a,b,c;\mathfrak{p})$ only depends on the prime number $p \in \mathbb{Z}$ below $\mathfrak{p}$.

Let G be as in Theorem 2.7. Then the group H_0 consists on the image in G of the upper-triangular matrices of $\mathrm{SL}_2(\mathbb{F}_q)$ or $\mathrm{GL}_2(\mathbb{F}_q)$, depending on G. The cover $X_0(a,b,c;\mathfrak{p}) \to \mathbb{P}^1 = X(a,b,c;1)$ is related to the Galois cover $X(a,b,c;\mathfrak{p}) \to \mathbb{P}^1 = X(a,b,c;1)$ by



We first find the degree of the cover $X_0(a,b,c;\mathfrak{p}) \to \mathbb{P}^1$. If $G = \mathrm{PGL}_2(\mathbb{F}_q)$, then by multiplying by scalar matrices, it is possible to choose representatives of elements of H_0 that have 1 on the first entry of the matrix. Thus, $\#H_0 = q(q-1)$ and

$$[G : H_0] = \frac{q(q+1)(q-1)}{q(q-1)} = q + 1.$$

When q is even, we have an isomorphism $\mathrm{PSL}_2(\mathbb{F}_q) \simeq \mathrm{PGL}_2(\mathbb{F}_q)$. Finally, if $G = \mathrm{PSL}_2(\mathbb{F}_q)$ with q odd, then the upper triangular matrices are defined up to multiplication by -1. Hence

$$[G : H_0] = \frac{\frac{1}{2}q(q+1)(q-1)}{\frac{1}{2}q(q-1)} = q + 1.$$

The set of cosets G/H_0 is therefore naturally in bijection with $\mathbb{P}^1(\mathbb{F}_q)$ via the projection of the first column of the matrix to $\mathbb{P}^1(\mathbb{F}_q)$, and we transport the action via this bijection, which becomes simply matrix multication. The ramification of the cover $X_0(a,b,c;p) \to \mathbb{P}^1$ then depends on the cycle decomposition of the corresponding elements (in G) as an element of $\mathrm{Sym}(\mathbb{P}^1) \simeq S_{q+1}$.

Cycle structure and genus formula. The following lemma describes the cycle structure using only the order of the elements.

Lemma 3.1. *Let $G = \mathrm{PXL}_2(\mathbb{F}_q)$ with $q = p^r$ for a prime number p. Let $\overline{\sigma}_s \in G$ have order $s \geq 2$, and if $s = 2$ suppose $p = 2$. Then the action of $\overline{\sigma}_s$ on $\mathbb{P}^1(\mathbb{F}_q)$ has:*

(i) *two fixed points and $(q-1)/s$ orbits of length s if $s \mid (q-1)$;*
(ii) *one fixed point and q/p orbits of length p if $s = p$ (this is the case when $s \mid q$); and*
(iii) *(no fixed points and) $(q+1)/s$ orbits of length s if $s \mid (q+1)$.*

Proof. We prove this fact by studying in detail each case. Let σ_s be an element of $\mathrm{GL}_2(\mathbb{F}_q)$ whose projection to G is $\overline{\sigma}_s$. If σ_s is diagonalizable, then we say that σ_s is split semisimple, and σ_s is conjugate to say the diagonal matrix $\begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix}$. We must have $u \neq v$ because otherwise $\overline{\sigma}_s$ would be the identity in G, contradicting that $s \geq 2$. The order of $\overline{\sigma}_s$ is s, so s is the minimum integer such that $u^s = v^s$. Thus, the order of s is the order of uv^{-1} in $\mathbb{F}_q^\times$. To find the orbits of the action of $\overline{\sigma}_s$ on $\mathbb{P}^1(\mathbb{F}_q)$, we use that

$$\begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \begin{pmatrix} 1 \\ : \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ : \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \begin{pmatrix} x \\ : \\ 1 \end{pmatrix} = \begin{pmatrix} uv^{-1}x \\ : \\ 1 \end{pmatrix},$$

for any $x \in \mathbb{F}_q$. Hence, the action of $\overline{\sigma}_s$ has two fixed points: $\begin{pmatrix} 1 \\ : \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ : \\ 1 \end{pmatrix}$, and $(q-1)/d$ orbits with s elements.

The element $\overline{\sigma}_s$ is unipotent if and only if it is conjugate to $\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}$ in G for some $u \in \mathbb{F}_q^\times$. This is the case when the characteristic polynomial of σ_s has two equal roots and σ_s is not diagonalizable. This happens if and only if $s = p$. In this case, we have

$$\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}\begin{pmatrix}1\\ : \\ 0\end{pmatrix} = \begin{pmatrix}1\\ : \\ 0\end{pmatrix}, \qquad \begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}\begin{pmatrix}x\\ : \\ 1\end{pmatrix} = \begin{pmatrix}x+1\\ : \\ 1\end{pmatrix},$$

where $x \in \mathbb{F}_q$. There is only one fixed point and there are q/p orbits of size p.

If the characteristic polynomial of σ_s does not split in $\mathbb{F}_q$, we call $\overline{\sigma}_s$ non-split semisimple. The action of $\overline{\sigma}_s$ has no fixed points because this would imply that σ_s has an eigenvector. The splitting field of the characteristic polynomial of σ_s is $\mathbb{F}_{q^2}$. There is $\alpha, \beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that the diagonal matrix $\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}$ is conjugate to σ_s in $\mathbb{F}_{q^2}$ with the relation $\sigma_s = T^{-1}[\alpha, \beta]T$. For all $m \in \mathbb{N}$ such that $\overline{\sigma}_s^m$ fixes $(a : b)^t \in \mathbb{P}^1(\mathbb{F}_q)$, we have that

$$\begin{pmatrix}\alpha^m & 0\\ 0 & \alpha^{-m}\end{pmatrix}\left(T\begin{pmatrix}a\\ : \\ b\end{pmatrix}\right) = \left(T\begin{pmatrix}a\\ : \\ b\end{pmatrix}\right).$$

From the analysis of the split semisimple case, we conclude that every orbit has length s. Thus, the action of σ_s on $\mathbb{P}^1(\mathbb{F}_q)$ has $(q+1)/s$ orbits of length s. □

The previous lemma does not consider the case when $s = 2$ and q is odd. The ambiguity arises since if $s = 2$ then $s \mid (q-1)$ and $s \mid (q+1)$, so $\overline{\sigma}_2$ can be either split or non-split (semisimple). The following lemma partially solves this problem.

Lemma 3.2. *Let $G = \mathrm{PSL}_2(\mathbb{F}_q)$ with q odd, and let $\overline{\sigma}_2 \in G$ be an element of order 2. Then action of $\overline{\sigma}_2$ on $\mathbb{P}^1(\mathbb{F}_q)$ has:*

(i) *two fixed points and $(q-1)/2$ orbits of size 2 if -1 is a square modulo q; and*
(ii) *(no fixed points and) $(q+1)/2$ orbits of size 2, otherwise.*

Proof. Let $\overline{\sigma}_2$ be a matrix of order 2 in $\mathrm{PSL}_2(\mathbb{F}_q)$. Its lift $\sigma_2 \in \mathrm{SL}_2(\mathbb{F}_q)$, has characteristic polynomial $x^2 + 1$, so $\sigma^2 = -1 \in \mathrm{SL}_2(\mathbb{F}_q)$. If $-1 \in \mathbb{F}_q^{\times 2}$, then this characteristic polynomial splits with distinct roots, so we are in the split semisimple case of Lemma 3.1. Otherwise, -1 is not a square and we are in the non-split semisimple case. □

Now we are ready to give a formula for the genus g of $X_0(a, b, c; p)$. For $x \in \mathbb{R}$, we write $\lfloor x \rceil$ for the rounding down of x, so $\lfloor 3/2 \rceil = 1/2$.

Theorem 3.3. *The genus of $X_0(a, b, c; \mathfrak{p})$ is given by*

$$g(X_0(a, b, c; \mathfrak{p})) = -q + \frac{1}{2}\sum_{s \in \{a,b,c\}} \left\lfloor \frac{q}{s} \right\rceil (s-1) + \epsilon(a, b, c; \mathfrak{p}) \tag{3.4}$$

where $q := \mathrm{Nm}(\mathfrak{p})$ and $\epsilon(a, b, c; \mathfrak{p}) \in \{0, 1/2\}$ is uniquely determined by $g(X_0(a, b, c; \mathfrak{p})) \in \mathbb{Z}$. Moreover, we have $\epsilon(a, b, c; \mathfrak{p}) = 0$ unless $a = 2$ and q is odd.

In the latter case ($a = 2$ and q odd), Lemma 3.2 implies that when $G = \mathrm{PSL}_2(\mathbb{F}_q)$, we have $\epsilon(a, b, c; \mathfrak{p}) = 0$ if and only if $q \equiv 1 \pmod 4$ (case (i)).

Proof. Consider elements $\overline{\sigma}_a$, $\overline{\sigma}_b$, $\overline{\sigma}_c \in \mathrm{PXL}_2(\mathbb{F}_q)$ of orders a, b, and c, respectively, such that $\sigma_a\sigma_b\sigma_c = 1$. The Riemann–Hurwitz formula implies

$$2g - 2 = -2(q+1) + \epsilon_a + \epsilon_b + \epsilon_c, \tag{3.5}$$

where ϵ_s is the ramification index at the points that ramify. We can compute ϵ_s from Lemma 3.1 and Lemma 3.2, with $\epsilon_s = k_s(s-1)$, where

$$k_s = \begin{cases} (q-1)/s, & \text{if } s \mid (q-1); \\ q/s, & \text{if } s \mid q; \\ (q+1)/s & \text{if } s \mid (q+1); \end{cases} \tag{3.6}$$

if $s \neq 2$ or ($s = a = 2$ and q is even); whereas if $s = a = 2$ and q is odd, then either $k_2 = (q+1)/2$ or $k_2 = (q-1)/2$ is determined by the fact that $g \in \mathbb{Z}$, since they differ by $1/2$. ☐

Remark 3.7. When the hyperbolic triple is $(2, b, c)$ and $G = \mathrm{PGL}_2(\mathbb{F}_q)$, then σ_2 can be either split or non-split. For example, for $(a, b, c) = (2, 3, 8)$ and $G = \mathrm{PGL}_2(\mathbb{F}_7)$, we have σ_2 split. On the other hand, for $(2, 6, 6)$ and $G = \mathrm{PGL}_2(\mathbb{F}_7)$, we have σ_2 non-split.

Instead of using parity, in the $\mathrm{PGL}_2(\mathbb{F}_q)$ case, we can always explicitly compute elements $\overline{\sigma}_2, \overline{\sigma}_b, \overline{\sigma}_c \in G$, of orders 2, b, and c respectively, such that $\overline{\sigma}_2\overline{\sigma_b\sigma_c} = 1$. We can then decide if $\overline{\sigma}_2$ is split or non-split and use Lemma 3.1 to compute the ramification.

Algorithm. To compute the genus of $X_0(a, b, c; \mathfrak{p})$ explicitly, we describe an algorithm for finding G as in Theorem 2.7. We recall that G is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$ for $q = p^r$, where $\mathbb{F}_q$ is the residue field of $\mathfrak{p}$ on E.

Algorithm 3.8. Let (a, b, c) be a hyperbolic triple and let $\mathfrak{p} \subseteq \mathbb{Z}_{E(a,b,c)}$ be a nonzero prime ideal. This algorithm computes the genus of $X_0(a, b, c; \mathfrak{p})$.

1. Compute the residue field $\mathbb{F}_q$ of $\mathfrak{p}$ and the residue field $\mathbb{F}_{q^r}$ of $\mathfrak{P}_F$, where $\mathfrak{p}_F$ is a prime of $F(a, b, c)$ above $\mathfrak{p}$. If these two fields are equal, then $G = \mathrm{PSL}_2(\mathbb{F}_q)$. Otherwise, we set $G = \mathrm{PGL}_2(\mathbb{F}_q)$.
2. Compute g using Theorem 3.3.

Proof of correctness. Step 1 can be performed by constructing the algebraic number field; it can also be done purely in terms of the prime number p below $\mathfrak{p}$ as in Algorithm 4.1. Correctness follows from the formula in Theorem 3.3. ☐

Bounding the genus. Our goal remains to show that, for fixed genus g_0, there are finitely many curves $X_0(a, b, c; \mathfrak{p})$ of genus $g \leq g_0$. We first characterize the hyperbolic triples (a, b, c) such that the curve $X(a, b, c)$ has Galois group $\mathrm{PXL}_2(\mathbb{F}_q)$, for a given q.

The notion of admissible ideal can be turned around, as follows.

Definition 3.9. Let $q := p^r$ be a power of a prime number p. A hyperbolic triple (a, b, c) is q-admissible if and only if s divides at least one integer in the set $\{q-1,\, p,\, q+1\}$ for all $s \in \{a, b, c\}$, not including ∞.

Lemma 3.10. *For any triangular modular curve $X_0(a, b, c; \mathfrak{p})$ with $q := \operatorname{Nm}\mathfrak{p}$, the triple (a, b, c) is q-admissible.*

Proof. These are the possible orders of elements in $\mathrm{PXL}_2(\mathbb{F}_q)$. ☐

Proposition 3.11. *Let g be the genus of the triangular modular curve $X_0(a, b, c; \mathfrak{p})$. Let $G = \mathrm{PXL}(\mathbb{F}_q)$ be the Galois group of $X(a, b, c; \mathfrak{p})$. Then,*

$$q \leq 84(g+1) + 1.$$

Proof. We study the Belyi map $X_0(a,b,c;\mathfrak{p}) \to \mathbb{P}^1$. Let $\epsilon_a, \epsilon_b, \epsilon_c$ be the ramification degrees of this map. Using Lemma 3.1, we have that for $s \in \{a,b,c\}$,

$$(q-1) - \frac{q-1}{s} = \frac{(s-1)(q-1)}{s} \leq \epsilon_s \leq \frac{(s-1)(q+1)}{s} = (q+1) - \frac{q+1}{s}. \tag{3.12}$$

Because of these bounds and (3.5),

$$\begin{aligned} g(X_0(a,b,c;\mathfrak{p})) &\geq -(q+1) + \frac{(a-1)(q-1)}{2a} + \frac{(b-1)(q-1)}{2b} + \frac{(c-1)(q-1)}{2c} + 1 \\ &= (q-1)\left(-1 + \frac{3}{2} - \frac{1}{2a} - \frac{1}{2b} - \frac{1}{2c}\right) - 1 \\ &= \frac{q-1}{2}\,|\chi(a,b,c)| - 1, \end{aligned} \tag{3.13}$$

where $\chi(a,b,c)$ is as in (2.1). The result then follows from the previous inequality and (2.2). ☐

Corollary 3.14. *For a fixed genus $g_0 \in \mathbb{Z}_{\geq 0}$, there are only finitely many curves $X_0(a,b,c;\mathfrak{p})$ with genus $g \leq g_0$.*

Proof. By Proposition 3.11, we obtain an upper bound on the rational prime p given by $q \leq 84(g_0+1)+1$. Also, for (a,b,c) to be q-admissible, necessarily $s \leq q+1$ or $s = \infty$ for all $s \in \{a,b,c\}$. This leaves only finitely many possibilities. ☐

One can make computations more efficient by considering a bound on q that depends on $\chi(a,b,c)$. For the genus of $X_0(a,b,c;\mathfrak{p})$ to be less than or equal to g_0, it is necessary that

$$q \leq \frac{2g_0}{|\chi(a,b,c)|} + 1. \tag{3.15}$$

This inequality also shows that

$$0 < |\chi(a,b,c)| \leq \frac{2g_0}{q-1}. \tag{3.16}$$

Therefore, we can bound a, b, and c whenever q is fixed.

4. Enumerating curves of low genus

We present the main algorithms that use the theory developed in section 3. As explained in section 2, if $\mathfrak{p}$ is admissible, then G is given by $\mathrm{PXL}_2(\mathbb{F}_q)$. We check for admissibility in the following algorithm.

Algorithm 4.1. Let (a,b,c) be a hyperbolic triple and p be a rational prime. This algorithm returns true if there exists an admissible prime above p in $\mathbb{Z}_{E(a,b,c)}$.

1. If $\mathfrak{p} \nmid 2abc$, then return `true`.
2. If $p = 2$, then check if (a,b,c) is of the form $(mz, m(z+1), mz(z+1))$ for any $m, z \in \mathbb{Z}$. If this is the case, return `false`. Otherwise return `true`.
3. Find $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_q$, where $\mathfrak{p}$ is any prime of E above p.
4. Set $m := \mathrm{lcm}(a,b,c)$. Construct $\mathbb{F}_q(\zeta_{2m})$. Set $z := \zeta_{2m}$.

5. For every $i \in (\mathbb{Z}/2m\mathbb{Z})^\times$, and set $l_{2s} := z^{m/s} + 1/z^{m/s}$ for $s \in \{a, b, c\}$. Compute
$$\beta_i := l_{2a}^2 + l_{2b}^2 + l_{2c}^2 + l_{2a}l_{2b}l_{2c} - 4.$$
If $\beta_i \neq 0$ and whenever $p \mid s$ we have $s = p$, then return `true`. Otherwise, return `false`.

Proof of correctness. In step 3 of Algorithm 4.1, we have that q is independent of the choice of $\mathfrak{p}$ because E is Galois over $\mathbb{Q}$. ☐

Remark 4.2. In step 5 of Algorithm 4.1, we check for every Galois conjugate; however, in every example we computed, either $\beta_i = 0$ for all i or $\beta_i \neq 0$ for all i. It seems as though it should be sufficient in Step 5 to check just one, even though the element $\beta \in \mathbb{Z}_E$ is not itself (typically) invariant under $\mathrm{Gal}(E \,|\, \mathbb{Q})$—but anyway, this is not a time-consuming step.

Now we are ready to present the main algorithm that ties the results of section 3 into an explicit enumeration.

Algorithm 4.3. Returns a list `lowGenus` of all hyperbolic triples $(a, b, c) \in \mathbb{Z}_{\geq 2}^3$, norms of admissible primes $\mathfrak{p}$ of $E(a, b, c)$ and Galois groups $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}(\mathbb{F}_q)$ such that the genus of $X_0(a, b, c; \mathfrak{p})$ is less than g_0.

1. Loop over the list of possible powers $q = p^r$, where p is any rational prime and $q \leq 84(g_0 + 1) + 1$, as in Proposition 3.11.
2. For each q, find all q-admissible hyperbolic triples (a, b, c) as in Definition 3.9.
3. For each q-admissible triple (a, b, c), check if $\chi(a, b, c)$ satisfies (3.16) and if $\mathfrak{p}$ is split for (a, b, c) using Algorithm 4.1. If yes, compute the genus g of $X_0(a, b, c; \mathfrak{p})$ using Algorithm 3.8. If $g \leq g_0$, add $(a, b, c; p, q)$ to the list `lowGenus`.

Proof of correctness. Every projective q-admissible triple gives rise to one such curve. The correctness of the rest of the algorithm follows from the work done in section 3. ☐

5. Remaining cases

In this section, we build upon the ideas developed in section 3 and section 4 to complete the list of all triangular modular curves of low genus.

Composite level. Let (a, b, c) be a hyperbolic triple with $a, b, c \in \mathbb{Z}_{\geq 2}$ and let $\mathfrak{N} \subseteq \mathbb{Z}_E$ be an admissible ideal. We abbreviate $X_0(a, b, c; \mathfrak{N})$ by $X_0(\mathfrak{N})$.

Lemma 5.1. *Let $\overline{\sigma}_s \in \mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{N})$ be an element of order $s \geq 2$. Then the following statements hold.*

(a) *Suppose that $\mathfrak{N} = \mathfrak{p}^e$, where $\mathfrak{p}$ is a prime ideal above a rational prime p such that $\gcd(s, p) = 1$. Let $\mathfrak{p}_F$ be a prime of F above $\mathfrak{p}$. Then the action of $\overline{\sigma}_s$ on $\mathbb{P}^1(\mathbb{Z}_E/\mathfrak{p})$ has the same number of fixed points as the number of points in $\mathbb{P}^1(\mathbb{Z}_E/\mathfrak{p})$ fixed by $\overline{\sigma}_s$.*

(b) *Assume that $\mathfrak{N} = \mathfrak{p}^e$, where $\mathfrak{p}$ is a prime ideal above a rational prime p such that $s = p$. Then the action of $\overline{\sigma}_s$ on $\mathbb{P}^1(\mathbb{Z}_E/\mathfrak{p})$ has p^{e-1} fixed points and the rest of the orbits have length s.*

(c) *If $\mathfrak{N}$ is a product of different primes, then the number of fixed points of the action of $\overline{\sigma}_s$ on $\mathbb{P}^1(\mathbb{Z}_E/\mathfrak{N})$ equals the product of the number of points in $\mathbb{P}^1(\mathbb{Z}_F/\mathfrak{p}^{e_i})$ fixed by $\overline{\sigma}_s$ for every $\mathfrak{p}^{e_i} \parallel \mathfrak{N}$. The rest of the orbits have length s.*

Proof. Let $\sigma_s \in \mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{N})$ be a matrix such that its image in $\mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{N})$ has order s. Let $\mathfrak{N} = \mathfrak{p}^e$ with $(p) = \mathfrak{p} \cap \mathbb{Z}$ and $\gcd(s,p) = 1$. Because $\gcd(s,p) = 1$, we have that σ_s is semisimple, just like in the proof of Lemma 3.1. Then, we can use Hensel's lemma to lift the roots for the characteristic polynomial of this element, meaning that we can use again Lemma 3.1.

We assume $\mathfrak{N} = \mathfrak{p}^e$ with $(p) = \mathfrak{p} \cap \mathbb{Z}$ and $s = p$. Thus, $\overline{\sigma_p}$ is unipotent, i.e. $\overline{\sigma_s}$ is conjugate to an upper diagonal matrix with ones in the diagonal. The fixed points of $\overline{\sigma_s}$ are the elements $(a : b)^t$ such that $p \mid b$.

Now, we let $\mathfrak{N} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be a product of primes coprime to $s\mathbb{Z}_E$. The Chinese Reminder Theorem implies that

$$\mathbb{P}^1(\mathbb{Z}_E/\mathfrak{N}) \cong \prod_{i=1}^{r} \mathbb{P}^1(\mathbb{Z}_E/\mathfrak{p}_i^{e_i}). \tag{5.2}$$

Thus, the orbits of $\overline{\sigma}_s$ in $\mathbb{P}^1(\mathbb{Z}_E/\mathfrak{N})$ have length the least common multiple of the orbits of $\overline{\sigma}_s$ in $\mathbb{P}^1(\mathbb{Z}_E/\mathfrak{p}^{e_i})$ for every $i = 1, \dots, r$. Because of the prime case, the orbits of $\overline{\sigma}_s$ in $\mathbb{P}^1(\mathbb{Z}_E/\mathfrak{p}^{e_i})$ have length either 1 or s, so we get the desired result. □

Theorem 5.3. *Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_E$ such that $N\mathbb{Z} = \mathfrak{N} \cap \mathbb{Z}$ and $\gcd(s,N) = 1$, or $s = p$ and p is the highest power of p that divides N. Let $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be the prime factorization of $\mathfrak{N}$. Let $q_i := \#\mathbb{F}_{\mathfrak{p}_i}$ be the residue field degree of $\mathfrak{p}_i$. Then the genus of $X_0(\mathfrak{N})$ is given by*

$$g(X_0(\mathfrak{N})) = 1 - \prod_{i=1}^{r}(q_i^{e_i} + q_i^{e_i-1}) + \frac{1}{2} \sum_{s \in \{a,b,c\}} k_s(s-1), \tag{5.4}$$

where

$$k_s = \left(\prod_{i=1}^{r}(q_i^{e_i} + q_i^{e_i-1}) - \prod_{i=1}^{r} f_{q_i,s} \right)/s, \tag{5.5}$$

where $f_{q,s}$ is the number of fixed points of the action of an element of degree s on $\mathbb{P}^1(\mathbb{F}_{q_i})$. This quantity can be computed from Lemma 3.1.

Proof. By (5.2), we have that the degree of the cover $X_0(\mathfrak{N}) \to X(1)$ is

$$\prod_{i=1}^{r} \#\mathbb{P}^1(\mathbb{Z}_E/\mathfrak{p}_i^{e_i}) = \prod_{i=1}^{r} \left(q_i^{e_i} + q_i^{e_i-1}\right). \tag{5.6}$$

The Riemann-Hurwitz formula and Lemma 5.1 complete the proof. □

Remark 5.7. This theorem allows us to compute the genus of the curves $X_1(\mathfrak{N})$ by using Algorithm 3.8 for each prime factor of $\mathfrak{N}$.

Proposition 5.8. *Let $g_0 \in \mathbb{Z}_{\geq 0}$. There are finitely many curves $X_0(a,b,c;\mathfrak{N})$ of genus $g \leq g_0$ where (a,b,c) is a hyperbolic triple and $\mathfrak{N}$ is an ideal of $E(a,b,c)$.*

Proof. For every prime divisor $\mathfrak{p}$ of $\mathfrak{N}$, there is a cover $X_0(\mathfrak{N}) \to X_0(\mathfrak{p})$. Hence the only curves $X_0(\mathfrak{N})$ that have genus g bounded by g_0 are curves such that $X_0(\mathfrak{p})$ also has genus also bounded by g_0 for every prime divisor of $\mathfrak{N}$. By Corollary 3.14, the list of curves $X_0(\mathfrak{p})$ of genus bounded by g_0 is finite. This also implies that the list of possible primes is finite too. In addition, the proof of Proposition 3.11 gives a bound on the degree of the cover, which bounds the possible powers of primes. □

Non-cocompact triangle groups. We still need to consider the case of one of the elements a, b, c being ∞. For that, we need the following lemma.

Lemma 5.9. *Let $\mathfrak{p}$ be a prime ideal of $E(a,b,c)$ for a hyperbolic triple (a,b,c). Let p be the rational prime below $\mathfrak{p}$. There is a bijection between curves $X_0(a,b,c;\mathfrak{p})$ and curves $X_0(a^\#, b^\#, c^\#; \mathfrak{p})$, where $s^\# = s$ if $s \neq \infty$ and $s^\# = p$ otherwise.*

Proof. If $s = \infty$, then the homomorphism given in (2.9) maps the element δ_∞ to an element of $\mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N}_F)$ of order p. □

Lemma 5.10. *A prime ideal $\mathfrak{p}$ is coprime to the discriminant $\beta(a,b,c)$ if and only if it is coprime to $\beta(a^\#, b^\#, c^\#)$.*

Proof. We have that $\lambda_\infty = 2$ and $\lambda_{2p} = \zeta_{2p} + \zeta_{2p}^{-1}$, where ζ_{2p} is a $2p$-th root of unity. Because ζ_{2p} is a $2p$-th root of unity, then we have that $\zeta_{2p} \equiv 1 \pmod{\mathfrak{P}}$, showing that $\lambda_\infty \equiv \lambda_{2p} \pmod{\mathfrak{P}}$. Because β as in (2.6) can be given by products of these elements minus 4, we get the desired result. □

The genus of $X_1(a,b,c)$. Once we have the list of all triangular modular curves $X_0(a,b,c;\mathfrak{p})$ of low genus, we describe how to find the list of all curves $X_1(a,b,c;\mathfrak{p}) = X(a,b,c;\mathfrak{p})/H_1$ of low genus with H_1 as in section 2.

We use the covers $X_1(a,b,c;\mathfrak{p}) \to X_0(a,b,c;\mathfrak{p}) \to X(a,b,c;1)$ to compute the genus of $X_1(a,b,c;\mathfrak{p})$.

Lemma 5.11. *Let $G = \mathrm{PXL}_2(\mathbb{F}_q)$. The quotient G/H_1 can be described as follows.*

(i) *If $G = \mathrm{PSL}_2(\mathbb{F}_q)$, then $G/H_1 \cong (\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\langle \pm 1\rangle$. This isomorphism can be made explicit by mapping $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q$ to the class of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where b and d are any elements of $\mathbb{F}_q$ such that $ad - bc = 1$.*

(ii) *If $G = \mathrm{PGL}_2(\mathbb{F}_q)$, then $G/H_1 \cong (\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\langle \pm 1\rangle \times \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$. This isomorphism can be made explicit by choosing a non-square $\mu \in \mathbb{F}_q$ and mapping the element $((a,b),u) \in (\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\}) \times \mathbb{F}_q$ to the class of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where b and c are elements of $\mathbb{F}_q$ such that $ad - bc = 1$ if u is a square and $ad - bc = \mu$ otherwise.*

Proof. Let $G = \mathrm{PSL}_2(\mathbb{F}_q)$ with q odd. We consider the sequence

$$1 \to H_1 \to H_0 \to \mathbb{F}_q^{\times 2} \to 1,$$

where a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_0$ is mapped to ad^{-1}. Thus, $\# H_1 = q$ and $[G : H_1] = \frac{q^2-1}{2}$. The coset representatives of G/H_1 can be parameterized by $(a,c) \in (\mathbb{F}_q \times \mathbb{F}_q)/\langle \pm 1\rangle$. Indeed, two elements in $\mathrm{PSL}_2(\mathbb{F}_q)$ are in the same coset of G/H_1 if and only if there is $x \in \mathbb{F}_q$ such that

$$\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \pm \begin{pmatrix} a & ax + b \\ c & cx + d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix},$$

which is the case if and only if $(a,c) = \pm(a',c')$. Thus, that the homomorphism is an injection and, by counting cardinalities, an isomorphism.

Now we let $G = \mathrm{PGL}_2(\mathbb{F}_q)$. We also have a sequence

$$1 \to H_1 \to H_0 \to \mathbb{F}_q^\times \to 1,$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_0$ is sent to ad^{-1}. This implies that $\#H_1 = q$ and $[G : H_1] = q^2 - 1$. The quotient G/H_1 is isomorphic to $(\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\{\pm 1\} \times \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$. To present this isomorphism, we fix a non-square $\mu \in \mathbb{F}_q$. For any $\pm(a,c) \in (\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\langle \pm 1\rangle$, and any $u \in \{1, \mu\} \cong \mathbb{F}_q/\mathbb{F}_q^\times$, we choose values of $b, d \in \mathbb{F}_q$ such that $ad - bc = u$ and we map $\pm(a,c)$ to the class of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{PGL}_2(\mathbb{F}_q)$. Indeed, if we make two different choices $b, d \in \mathbb{F}_q$ and $b', d' \in \mathbb{F}_q$, if $a \neq 0$, then

$$\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b' \\ c & d' \end{pmatrix} \begin{pmatrix} 1 & a^{-1}(b-b') \\ 0 & 1 \end{pmatrix}.$$

If $a = 0$, then $c \neq 0$ and $0 \neq u = bc = b'd$. Thus, $b = b'$. Also,

$$\pm \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & b \\ c & d' \end{pmatrix} \begin{pmatrix} 1 & c^{-1}(d-d') \\ 0 & 1 \end{pmatrix}.$$

Thus, the map $(\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\{\pm 1\} \times \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2} \to G/H_1$ is well defined homomorphism. In addition, multiplication by elements in H_1 does not change the square class of the determinant or the first column of the matrix, so the homomorphism described above is injective. By counting cardinalities, we conclude that this is an isomorphism. □

Lemma 5.12. *Let $\overline{\sigma}_s \in G = \mathrm{PXL}_2(\mathbb{F}_q)$ and assume that the order of $\overline{\sigma}_s$ is s. Let σ_s be any element of $\mathrm{GL}_2(\mathbb{F}_q)$ that maps to $\overline{\sigma}_s$ in the quotient to G. The structure of the action of $\overline{\sigma}_s$ on G/H_1 is:*

(i) *if σ_s is semisimple, then there are (no fixed points and) $\frac{q^2-1}{s}$ orbits of length s,*
(ii) *if σ_s is unipotent, then:*
  (a) *if $G = \mathrm{PSL}_2(\mathbb{F}_q)$ and q is odd, there are $(p-1)/2$ fixed points and $(q^2/p-1)/2$ orbits of length p,*
  (b) *otherwise, there are $p-1$ fixed points and $q^2/p-1$ orbits of length p.*

Proof. We use the description of the quotient G/H_1 given in Lemma 5.11.

If σ_s is split semisimple, then it is conjugate to a diagonal matrix $[u, v]$. Because the order of $\overline{\sigma}_s$ is s, we have that s is the smallest positive integer such that $u^s = v^s$, so uv^{-1} has order s. We also have that

$$\begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ua & ub \\ vc & vd \end{pmatrix}.$$

Thus, an element of G/H_1 is a fixed point if the first column is fixed, up to sign. So the element is a fixed point if $(u,v) = \pm(1,1)$, contradicting that $s \geq 2$. Thus, there are no fixed points. By the same degree argument, we see that every orbit has length s.

If σ_s is non-split semisimple, then σ_s is split in a quadratic extension of $\mathbb{F}_q$. We assume that $\sigma_s = T^{-1}[\alpha, \beta]T$ in this extension. This is the split case again, so there are no fixed points. Also, if σ_s^r fixes an element, then we have

$$\pm \begin{pmatrix} \alpha^r & 0 \\ 0 & \beta^r \end{pmatrix} T \begin{pmatrix} a & b \\ c & d \end{pmatrix} = T \begin{pmatrix} a & b' \\ c & d' \end{pmatrix}.$$

Because multiplication by T leaves the first columns of the matrices equal and multiplies the determinants by the same factor, we are back to the split semisimple case and the orbits of the action of $\overline{\sigma}_s$ have size s.

If σ_s is unipotent, then σ_s can be chosen (by multiplying by scalar matrices) to be conjugate to an upper diagonal matrix with ones in the diagonal. Then,

$$\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+uc & b+ud \\ c & d \end{pmatrix},$$

so this is a fixed point if and only if $uc = 0$, which is the case if and only if $c = 0$. We note that if $c \neq 0$, then the orbit of the element has length p. In $G = \mathrm{PSL}_2(\mathbb{F}_q)$, there are $(p-1)/2$ representatives for which $c = 0$, i.e. fixed points. Similarly, if $G = \mathrm{PGL}_2(\mathbb{F}_q)$, then there are $p-1$ fixed points. □

Corollary 5.13. *Let $(a,b,c) \in \mathbb{Z}^3_{\geq 2}$ be a q-admissible hyperbolic triple. Let $\mathfrak{p}$ be a prime ideal of $E(a,b,c)$ above a rational prime p. The genus of $X_1(a,b,c;\mathfrak{p})$ is given by*

$$g(X_1(a,b,c;\mathfrak{p})) = -[G : H_1] + \frac{1}{2}\sum_{s\in\{a,b,c\}} k_s(s-1) + 1,$$

where

$$k_s = \begin{cases} (q^2/p - 1)/2 & s = p \text{ and } G = \mathrm{PSL}_2(\mathbb{F}_q), \\ q^2/p - 1 & s = p \text{ and } G = \mathrm{PGL}_2(\mathbb{F}_q), \\ (q^2-1)/s & \text{otherwise.} \end{cases}$$

Lemma 5.14. *Let $s \in \{a,b,c\}$ and let $\overline{\sigma}_s \in \mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{N})$ be an element of order s. The following statements hold.*

(a) *Assume that $\mathfrak{N} = \mathfrak{p}^e$, where $e > 1$ and $\mathfrak{p}$ is a prime ideal. Then the action of $\overline{\sigma}_s$ on $\mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{N})/H_1$ has no fixed points and the rest of the orbits have length s.*

(b) *If $\mathfrak{N}$ is a product of different primes, then the number of fixed points of the action of $\overline{\sigma}_s$ on $\mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{N})/H_1$ equals the product of the number of points in $\mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{p}^{e_i})/H_1$ fixed by $\overline{\sigma}_s$ for every $\mathfrak{p}^{e_i} \parallel \mathfrak{N}$. The rest of the orbits have length s.*

Proof. If $\mathfrak{N} = \mathfrak{p}^e$ with $e > 1$ and $\gcd(p,s) = 1$, then the action of $\overline{\sigma}_s$ has no fixed points in $\mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{p})$ by Lemma 5.14. This implies that there are no fixed points in $\mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{p}^e)$.

Now, if $\mathfrak{N} = \mathfrak{p}^e$ with $e > 1$ and $s = p$, then we claim that there is no element of order p in $\Gamma_1(\mathfrak{p}^e)$. This element would have to have an eigenvalue a $2p$-th root of unity ζ_{2p} or its inverse. Because the element would be unipotent, 1 would also be an eigenvalue modulo $\mathfrak{p}^e$. This implies that $\zeta_{2p} = 1 \pmod{\mathfrak{p}}^e$, which is a contradiction. Thus, all the orbits of the action of $\overline{\sigma}_s$ has length p.

Because of the previous two cases, we only have fixed points if $s = p$ and $\mathfrak{p}$ is a prime above p. Because the length of the orbits is the least common multiple of the length of the orbits for all primes dividing $\mathfrak{N}$, we finish the proof. □

Now we are ready to give a genus formula for $X_1(\mathfrak{N})$. To do so, we define an extension of the usual Euler totient function to ideals: if $\mathfrak{N} \subseteq \mathbb{Z}_E$ is a nonzero ideal, we define $\phi(\mathfrak{N}) := \#(\mathbb{Z}_E/\mathfrak{N})^\times$.

Theorem 5.15. *Let $\mathfrak{N} = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ be an ideal of E, admissible for (a,b,c). If $\mathfrak{N}$ is not a product of prime ideals above p with $e_1 = \cdots = e_r = 1$ when $p \in \{a,b,c\}$, then the genus of $X_1(\mathfrak{N})$ is given by*

$$g(X_1(a,b,c;\mathfrak{N})) = \left(\frac{\phi(\mathfrak{N})}{2}\cdot\prod_{i=1}^{r}(q_i^{e_i} + q_i^{e_i-1})\right)\frac{|\chi(a,b,c)|}{2} + 1. \tag{5.16}$$

Otherwise,

$$g(X_1(a,b,c;\mathfrak{N})) = \left(\frac{\phi(\mathfrak{N})}{2} \cdot \prod_{i=1}^{r}(q_i^{e_i} + q_i^{e_i-1})\right) \frac{|\chi(a,b,c)|}{2} + 1 - \sum_{s\in\{a,b,c\}} \epsilon_s, \tag{5.17}$$

where, if $f_{q_i,s}$ is the number of fixed points as in Lemma 5.12, we have

$$\epsilon_s := \begin{cases} 0 & s \neq p \\ \left(\prod_i f_{q_i,s}\right)/2p & \text{otherwise.} \end{cases} \tag{5.18}$$

Proof. We use the Riemann-Hurwitz formula for the cover $X_1(\mathfrak{N}) \to \mathbb{P}^1$. By Lemma 5.11, the degree of this cover equals the degree of the sub–cover $X_0(\mathfrak{N}) \to \mathbb{P}^1$ times half of $\phi(\mathfrak{N})$. The ramification follows from Lemma 5.12 and Lemma 5.14. ☐

Algorithm 5.19. Returns a list `lowGenusX1` of all hyperbolic triples (a,b,c), admissible primes p and Galois groups $\mathrm{PXL}_2(\mathbb{F}_q)$ such that the genus of $X_1(a,b,c;p)$ is less than g_0.

1. Loop over all hyperbolic triples (a,b,c) from the list `lowGenus` of genus $g \le g_0$ from Algorithm 4.3.
2. Compute the genus g of $X_1(a,b,c;p)$ using Corollary 5.13. If $g \le g_0$, add $(a,b,c;p,q)$ to the list `lowGenusX1`.

Proof of theorem. We conclude the paper by proving our main result.

Proof of Theorem 1.4. By Proposition 5.8, there are only finitely many curves $X_0(a,b,c;\mathfrak{p})$ with prime level $\mathfrak{p}$ and genus $g \le g_0$. Since every curve $X_1(a,b,c;\mathfrak{N})$ covers $X_0(a,b,c;\mathfrak{N})$, the same is true for $X_1(a,b,c;\mathfrak{N})$.

For the computation, we run Algorithm 4.3 with $g_0 = 2$, adding noncocompact cases according to Lemma 5.9. To finish, we run Algorithm 5.19 on the prime level curves, leaving only the composite cases which can be computed using Theorem 5.15. ☐

Appendix A. Tables

We present tables of all hyperbolic triples (a, b, c) and norms of primes $\mathfrak{p}$ such that the curve $X_0(a, b, c; \mathfrak{p})$ has genus 0 or 1. The complete list is available online [DRV22].

To record the information about the group $G = \mathrm{PXL}_2(\mathbb{F}_q)$, we write 1 in the PXL field if $G = \mathrm{PSL}_2(\mathbb{F}_q)$ and -1 if $G = \mathrm{PGL}_2(\mathbb{F}_q)$. We also record the information about the field $E(a, b, c)$.

Nugent–Voight [NV17] define an invariant, the arithmetic dimension $\mathrm{adim}(a, b, c)$, to be the dimension of a quaternionic Shimura variety attached to $\Delta(a, b, c)$ (the number of split real places of a certain quaternion algebra). In particular, the triangle group $\Delta(a, b, c)$ is arithmetic if and only if $\mathrm{adim}(a, b, c) = 1$.

One subtlety is that there can be an isomorphism between the cover coming from a nonarithmetic group and the cover coming from an arithmetic group. This can only happen when the arithmetic group is of noncompact type, with

$$(a, b, c) = (2, 3, \infty), (2, 4, \infty), (2, 6, \infty), (2, \infty, \infty), (3, 3, \infty), (3, \infty, \infty), \\ (4, 4, \infty), (6, 6, \infty), (\infty, \infty, \infty)$$

by Takeuchi [Tak77a]. All of these arise from finite-index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$, so they are related to classical modular curves, and are defined over $\mathbb{Q}$. The ramification of the curve $X_0(a, b, c; \mathfrak{p})$ for $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ replaces any occurrence of ∞ by p; this allows one to readily identify when this extra isomorphism applies.

Genus 0, cocompact case.

(a,b,c)	p	q	PXL	adim	$E(a,b,c)$
$(2,3,7)$	7	7	1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,7)$	2	8	1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,7)$	13	13	1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,7)$	29	29	1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,7)$	43	43	1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,8)$	7	7	-1	1	$\mathbb{Q}(\sqrt{8})$
$(2,3,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{8})$
$(2,3,8)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$
$(2,3,8)$	5	25	-1	1	$\mathbb{Q}(\sqrt{8})$
$(2,3,9)$	19	19	1	1	$\mathbb{Q}(\lambda_9)$
$(2,3,9)$	37	37	1	1	$\mathbb{Q}(\lambda_9)$
$(2,3,10)$	11	11	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,3,10)$	31	31	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,3,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$
$(2,3,12)$	5	25	1	1	$\mathbb{Q}(\sqrt{12})$
$(2,3,13)$	13	13	1	2	$\mathbb{Q}(\lambda_{13})$
$(2,3,15)$	2	16	1	2	$\mathbb{Q}(\lambda_{15})$
$(2,3,18)$	19	19	-1	1	$\mathbb{Q}(\lambda_9)$
$(2,4,5)$	5	5	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,4,5)$	3	9	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,4,5)$	11	11	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,4,5)$	41	41	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,4,6)$	5	5	-1	1	$\mathbb{Q}$
$(2,4,6)$	7	7	-1	1	$\mathbb{Q}$
$(2,4,6)$	13	13	-1	1	$\mathbb{Q}$
$(2,4,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{8})$
$(2,4,8)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$
$(2,4,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$
$(2,5,5)$	5	5	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,5,5)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,5,10)$	11	11	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,6,6)$	7	7	-1	1	$\mathbb{Q}$
$(2,6,6)$	13	13	1	1	$\mathbb{Q}$
$(2,6,7)$	7	7	-1	2	$\mathbb{Q}(\lambda_7)$
$(2,8,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{8})$
$(3,3,4)$	7	7	1	1	$\mathbb{Q}(\sqrt{8})$
$(3,3,4)$	3	9	1	1	$\mathbb{Q}(\sqrt{8})$
$(3,3,4)$	5	25	1	1	$\mathbb{Q}(\sqrt{8})$
$(3,3,5)$	2	4	1	1	$\mathbb{Q}(\sqrt{5})$
$(3,3,6)$	13	13	1	1	$\mathbb{Q}(\sqrt{12})$
$(3,3,7)$	7	7	1	1	$\mathbb{Q}(\lambda_7)$
$(3,4,4)$	5	5	-1	1	$\mathbb{Q}$
$(3,4,4)$	13	13	-1	1	$\mathbb{Q}$
$(3,6,6)$	7	7	-1	1	$\mathbb{Q}$
$(4,4,4)$	3	9	1	1	$\mathbb{Q}(\sqrt{8})$
$(4,4,5)$	5	5	-1	1	$\mathbb{Q}(\sqrt{5})$

Genus 0, noncocompact case.

(a,b,c)	p	q	PXL	adim	$E(a,b,c)$
$(2,3,\infty)$	2	2	1	1	$\mathbb{Q}$
$(2,3,\infty)$	3	3	1	1	$\mathbb{Q}$
$(2,3,\infty)$	5	5	1	1	$\mathbb{Q}$
$(2,3,\infty)$	7	7	1	1	$\mathbb{Q}$
$(2,3,\infty)$	13	13	1	1	$\mathbb{Q}$
$(2,4,\infty)$	3	3	-1	1	$\mathbb{Q}$
$(2,4,\infty)$	5	5	-1	1	$\mathbb{Q}$
$(2,5,\infty)$	5	5	1	2	$\mathbb{Q}(\sqrt{5})$
$(2,5,\infty)$	3	9	1	2	$\mathbb{Q}(\sqrt{5})$
$(2,6,\infty)$	7	7	-1	1	$\mathbb{Q}$
$(2,8,\infty)$	3	9	-1	2	$\mathbb{Q}(\sqrt{8})$
$(2,\infty,\infty)$	3	3	1	1	$\mathbb{Q}$
$(2,\infty,\infty)$	5	5	1	1	$\mathbb{Q}$
$(3,3,\infty)$	3	3	1	1	$\mathbb{Q}$
$(3,3,\infty)$	7	7	1	1	$\mathbb{Q}$
$(3,4,\infty)$	3	9	1	2	$\mathbb{Q}(\sqrt{8})$
$(3,7,\infty)$	2	8	-1	3	$\mathbb{Q}(\lambda_7)$
$(3,15,\infty)$	2	16	-1	4	$\mathbb{Q}(\lambda_{15})$
$(3,\infty,\infty)$	2	2	-1	1	$\mathbb{Q}$
$(3,\infty,\infty)$	3	3	1	1	$\mathbb{Q}$
$(4,4,\infty)$	5	5	-1	1	$\mathbb{Q}$
$(4,\infty,\infty)$	3	9	1	2	$\mathbb{Q}$
(∞,∞,∞)	3	3	1	1	$\mathbb{Q}$

Genus 1, cocompact case. This long table is split into three tables (over the next three pages).

(a,b,c)	p	q	PXL	adim	E
$(2,3,7)$	3	27	1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,7)$	41	41	1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,7)$	71	71	1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,7)$	97	97	1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,7)$	113	113	1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,7)$	127	127	1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,8)$	23	23	-1	1	$\mathbb{Q}(\sqrt{8})$
$(2,3,8)$	31	31	1	1	$\mathbb{Q}(\sqrt{8})$
$(2,3,8)$	41	41	-1	1	$\mathbb{Q}(\sqrt{8})$
$(2,3,8)$	73	73	-1	1	$\mathbb{Q}(\sqrt{8})$
$(2,3,8)$	97	97	1	1	$\mathbb{Q}(\sqrt{8})$
$(2,3,9)$	2	8	1	1	$\mathbb{Q}(\lambda_9)$
$(2,3,9)$	17	17	1	1	$\mathbb{Q}(\lambda_9)$
$(2,3,9)$	73	73	1	1	$\mathbb{Q}(\lambda_9)$
$(2,3,10)$	3	9	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,3,10)$	19	19	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,3,10)$	41	41	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,3,10)$	61	61	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,3,11)$	11	11	1	1	$\mathbb{Q}(\lambda_5)$
$(2,3,11)$	23	23	1	1	$\mathbb{Q}(\lambda_5)$
$(2,3,12)$	11	11	-1	1	$\mathbb{Q}(\sqrt{12})$
$(2,3,12)$	37	37	-1	1	$\mathbb{Q}(\sqrt{12})$
$(2,3,12)$	7	49	1	1	$\mathbb{Q}(\sqrt{12})$
$(2,3,13)$	5	25	1	2	$\mathbb{Q}(\lambda_{13})$
$(2,3,13)$	3	27	1	2	$\mathbb{Q}(\lambda_{13})$
$(2,3,14)$	13	13	-1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,14)$	29	29	1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,14)$	43	43	-1	1	$\mathbb{Q}(\lambda_7)$
$(2,3,15)$	31	31	1	2	$\mathbb{Q}(\lambda_{15})$
$(2,3,16)$	17	17	-1	1	$\mathbb{Q}(\lambda_{16})$
$(2,3,17)$	2	16	1	2	$\mathbb{Q}(\lambda_{17})$
$(2,3,17)$	17	17	1	2	$\mathbb{Q}(\lambda_{17})$
$(2,3,18)$	37	37	1	1	$\mathbb{Q}(\lambda_9)$
$(2,3,19)$	19	19	1	3	$\mathbb{Q}(\lambda_{19})$
$(2,3,20)$	19	19	-1	2	$\mathbb{Q}(\lambda_{20})$
$(2,3,22)$	23	23	-1	2	$\mathbb{Q}(\lambda_5)$
$(2,3,24)$	5	25	-1	1	$\mathbb{Q}(\sqrt{2},\sqrt{3})$
$(2,3,26)$	3	27	-1	2	$\mathbb{Q}(\lambda_{13})$
$(2,3,30)$	31	31	-1	1	$\mathbb{Q}(\lambda_{15})$
$(2,4,5)$	19	19	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,4,5)$	29	29	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,4,5)$	31	31	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,4,5)$	7	49	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,4,5)$	61	61	-1	1	$\mathbb{Q}(\sqrt{5})$

⋮

(a,b,c)	p	q	PXL	adim	E
$(2,4,6)$	11	11	-1	1	$\mathbb{Q}$
$(2,4,6)$	17	17	-1	1	$\mathbb{Q}$
$(2,4,6)$	19	19	-1	1	$\mathbb{Q}$
$(2,4,6)$	29	29	-1	1	$\mathbb{Q}$
$(2,4,6)$	31	31	-1	1	$\mathbb{Q}$
$(2,4,6)$	37	37	-1	1	$\mathbb{Q}$
$(2,4,7)$	7	7	1	1	$\mathbb{Q}(\lambda_7)$
$(2,4,7)$	13	13	-1	1	$\mathbb{Q}(\lambda_7)$
$(2,4,7)$	29	29	-1	1	$\mathbb{Q}(\lambda_7)$
$(2,4,8)$	7	7	-1	1	$\mathbb{Q}(\sqrt{8})$
$(2,4,8)$	5	25	-1	1	$\mathbb{Q}(\sqrt{8})$
$(2,4,9)$	17	17	1	2	$\mathbb{Q}(\lambda_9)$
$(2,4,9)$	19	19	-1	2	$\mathbb{Q}(\lambda_9)$
$(2,4,10)$	3	9	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,4,10)$	11	11	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,4,11)$	11	11	-1	2	$\mathbb{Q}(\lambda_5)$
$(2,4,12)$	5	25	1	1	$\mathbb{Q}(\sqrt{12})$
$(2,4,13)$	13	13	-1	3	$\mathbb{Q}(\lambda_{13})$
$(2,4,14)$	13	13	-1	2	$\mathbb{Q}(\lambda_7)$
$(2,4,16)$	17	17	-1	2	$\mathbb{Q}(\lambda_{16})$
$(2,4,17)$	17	17	1	4	$\mathbb{Q}(\lambda_{17})$
$(2,5,5)$	3	9	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,5,5)$	31	31	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,5,5)$	41	41	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,5,6)$	5	5	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,5,6)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$
$(2,5,6)$	19	19	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,5,6)$	31	31	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,5,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{2},\sqrt{5})$
$(2,5,11)$	11	11	1	4	$\mathbb{Q}(\sqrt{5},\lambda_{11})$
$(2,5,12)$	11	11	-1	2	$\mathbb{Q}(\sqrt{3},\sqrt{5})$
$(2,5,15)$	2	16	1	2	$\mathbb{Q}(\lambda_{15})$
$(2,6,6)$	5	5	-1	1	$\mathbb{Q}$
$(2,6,6)$	19	19	-1	1	$\mathbb{Q}$
$(2,6,7)$	13	13	1	2	$\mathbb{Q}(\lambda_7)$
$(2,6,8)$	7	7	-1	1	$\mathbb{Q}(\sqrt{8})$
$(2,6,9)$	19	19	-1	2	$\mathbb{Q}(\lambda_9)$
$(2,6,10)$	11	11	-1	2	$\mathbb{Q}(\sqrt{5})$
$(2,6,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$
$(2,6,13)$	13	13	1	4	$\mathbb{Q}(\lambda_{13})$
$(2,7,7)$	7	7	1	1	$\mathbb{Q}(\lambda_7)$
$(2,7,8)$	7	7	-1	2	$\mathbb{Q}(\sqrt{2},\lambda_7)$
$(2,7,9)$	2	8	1	3	$\mathbb{Q}(\lambda_7,\lambda_9)$
$(2,8,8)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$
$(2,8,10)$	3	9	-1	3	$\mathbb{Q}(\sqrt{2},\sqrt{5})$
$(2,10,10)$	11	11	-1	1	$\mathbb{Q}(\sqrt{5})$
$(2,10,11)$	11	11	-1	6	$\mathbb{Q}(\sqrt{5},\lambda_{11})$
$(2,12,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$

$\vdots$

(a,b,c)	p	q	PXL	adim	E
$(3,3,4)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$
$(3,3,4)$	31	31	1	1	$\mathbb{Q}(\sqrt{8})$
$(3,3,5)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$
$(3,3,5)$	19	19	1	1	$\mathbb{Q}(\sqrt{5})$
$(3,3,5)$	31	31	1	1	$\mathbb{Q}(\sqrt{5})$
$(3,3,6)$	5	25	1	1	$\mathbb{Q}(\sqrt{12})$
$(3,3,7)$	2	8	1	1	$\mathbb{Q}(\lambda_7)$
$(3,3,7)$	13	13	1	1	$\mathbb{Q}(\lambda_7)$
$(3,3,9)$	19	19	1	1	$\mathbb{Q}(\lambda_9)$
$(3,3,13)$	13	13	1	2	$\mathbb{Q}(\lambda_{13})$
$(3,3,15)$	2	16	1	1	$\mathbb{Q}(\lambda_{15})$
$(3,4,4)$	3	3	1	1	$\mathbb{Q}$
$(3,4,4)$	7	7	1	1	$\mathbb{Q}$
$(3,4,4)$	17	17	1	1	$\mathbb{Q}$
$(3,4,5)$	3	9	1	2	$\mathbb{Q}(\sqrt{5},\sqrt{8})$
$(3,4,6)$	5	5	-1	1	$\mathbb{Q}(\sqrt{24})$
$(3,4,7)$	7	7	1	2	$\mathbb{Q}(\sqrt{2},\lambda_7)$
$(3,4,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{3})$
$(3,5,5)$	2	4	1	1	$\mathbb{Q}(\sqrt{5})$
$(3,5,5)$	5	5	1	1	$\mathbb{Q}(\sqrt{5})$
$(3,5,5)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$
$(3,6,6)$	13	13	1	1	$\mathbb{Q}$
$(3,6,8)$	7	7	-1	3	4.4.18432.1
$(3,7,7)$	7	7	1	2	$\mathbb{Q}(\lambda_7)$
$(3,7,7)$	2	8	1	2	$\mathbb{Q}(\lambda_7)$
$(3,8,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{8})$
$(4,4,4)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$
$(4,4,5)$	3	9	1	1	$\mathbb{Q}(\sqrt{5})$
$(4,4,6)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$
$(4,5,6)$	5	5	-1	2	$\mathbb{Q}(\sqrt{5},\sqrt{24})$
$(4,6,6)$	7	7	-1	1	$\mathbb{Q}(\sqrt{8})$
$(4,8,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{2})$
$(5,5,5)$	5	5	1	1	$\mathbb{Q}(\sqrt{5})$
$(5,5,5)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$
$(6,6,7)$	7	7	-1	2	$\mathbb{Q}(\lambda_7)$
$(7,7,7)$	2	8	1	1	$\mathbb{Q}(\lambda_7)$

Genus 1, noncocompact case.

(a,b,c)	p	q	PXL	adim	E
$(2,3,\infty)$	11	11	1	1	$\mathbb{Q}$
$(2,3,\infty)$	17	17	1	1	$\mathbb{Q}$
$(2,3,\infty)$	19	19	1	1	$\mathbb{Q}$
$(2,4,\infty)$	7	7	1	1	$\mathbb{Q}$
$(2,4,\infty)$	11	11	-1	1	$\mathbb{Q}$
$(2,4,\infty)$	13	13	-1	1	$\mathbb{Q}$
$(2,4,\infty)$	17	17	1	1	$\mathbb{Q}$
$(2,5,\infty)$	11	11	1	2	$\mathbb{Q}(\sqrt{5})$
$(2,6,\infty)$	5	5	-1	1	$\mathbb{Q}$
$(2,6,\infty)$	13	13	1	1	$\mathbb{Q}$
$(2,7,\infty)$	7	7	1	3	$\mathbb{Q}(\lambda_7)$
$(2,7,\infty)$	3	27	1	3	$\mathbb{Q}(\lambda_7)$
$(2,8,\infty)$	7	7	-1	2	$\mathbb{Q}(\sqrt{8})$
$(2,10,\infty)$	3	9	-1	2	$\mathbb{Q}(\sqrt{5})$
$(2,10,\infty)$	11	11	-1	2	$\mathbb{Q}(\sqrt{5})$
$(2,13,\infty)$	3	27	1	6	$\mathbb{Q}(\lambda_{13})$
$(2,26,\infty)$	3	27	-1	6	$\mathbb{Q}(\lambda_{13})$
$(2,\infty,\infty)$	7	7	1	1	$\mathbb{Q}$
$(3,3,\infty)$	5	5	1	1	$\mathbb{Q}$
$(3,3,\infty)$	13	13	1	1	$\mathbb{Q}$
$(3,4,\infty)$	7	7	1	2	$\mathbb{Q}$
$(3,5,\infty)$	5	5	1	2	$\mathbb{Q}(\sqrt{5})$
$(3,5,\infty)$	3	9	1	2	$\mathbb{Q}(\sqrt{5})$
$(3,7,\infty)$	7	7	1	3	$\mathbb{Q}(\lambda_7)$
$(3,9,\infty)$	2	8	-1	3	$\mathbb{Q}(\lambda_9)$
$(3,17,\infty)$	2	16	-1	8	$\mathbb{Q}(\lambda_{17})$
$(3,\infty,\infty)$	5	5	1	1	$\mathbb{Q}$
$(3,\infty,\infty)$	7	7	1	2	$\mathbb{Q}$
$(4,4,\infty)$	3	3	-1	1	$\mathbb{Q}$
$(4,5,\infty)$	3	9	1	4	$\mathbb{Q}(\sqrt{5},\sqrt{8})$
$(4,6,\infty)$	5	5	-1	2	$\mathbb{Q}(\sqrt{24})$
$(5,5,\infty)$	2	4	-1	2	$\mathbb{Q}(\sqrt{5})$
$(5,5,\infty)$	5	5	1	2	$\mathbb{Q}(\sqrt{5})$
$(5,15,\infty)$	2	16	-1	4	$\mathbb{Q}(\lambda_{15})$
$(5,\infty,\infty)$	5	5	1	2	$\mathbb{Q}(\sqrt{5})$
$(5,\infty,\infty)$	3	9	1	2	$\mathbb{Q}(\sqrt{5})$
$(6,6,\infty)$	7	7	-1	1	$\mathbb{Q}$
$(7,9,\infty)$	2	8	-1	9	$\mathbb{Q}(\lambda_7,\lambda_9)$
$(8,8,\infty)$	3	9	-1	2	$\mathbb{Q}(\sqrt{8})$
(∞,∞,∞)	5	5	1	1	$\mathbb{Q}$

References

[Arc03] Natália Archinard. Hypergeometric abelian varieties. *Canad. J. Math.*, 55(5):897–932, 2003.

[Cle03] C. Herbert Clemens. *A scrapbook of complex curve theory*, volume 55 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 2003.

[CP84] David A. Cox and Walter R. Parry. Genera of congruence subgroups in $\mathbf{Q}$-quaternion algebras. *J. Reine Angew. Math.*, 351:66–112, 1984.

[CP03] C. J. Cummins and S. Pauli. Congruence subgroups of $\mathrm{PSL}(2,\mathbb{Z})$ of genus less than or equal to 24. *Experiment. Math.*, 12(2):243–255, 2003.

[CV19] Pete L. Clark and John Voight. Algebraic curves uniformized by congruence subgroups of triangle groups. *Trans. Amer. Math. Soc.*, 371(1):33–82, 2019.

[CW90] Paula Cohen and Jürgen Wolfart. Modular embeddings for some nonarithmetic Fuchsian groups. *Acta Arith.*, 56(2):93–110, 1990.

[Dar04] Henri Darmon. A fourteenth lecture on Fermat's last theorem. In *Number theory*, volume 36 of *CRM Proc. Lecture Notes*, pages 103–115. Amer. Math. Soc., Providence, RI, 2004.

[Dic58] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory*. Dover Publications, Inc., New York, 1958. With an introduction by W. Magnus.

[DRV22] J. Duque-Rosero and J. Voight. Enumerating triangular modular curves of low genus. https://github.com/juanitaduquer/triangularModularCurves.git, 2022.

[Fri11] Robert Fricke. *Die elliptischen Funktionen und ihre Anwendungen. Zweiter Teil. Die algebraischen Ausführungen*. Springer, Heidelberg, 2011.

[Hup67] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967.

[KMSV14] Michael Klug, Michael Musty, Sam Schiavone, and John Voight. Numerical calculation of three-point branched covers of the projective line. *LMS J. Comput. Math.*, 17(1):379–430, 2014.

[KV22] Robert Kucharczyk and John Voight. Hypergeometric functions and shimura varieties. unpublished, 2022.

[LMR06] D. D. Long, C. Maclachlan, and A. W. Reid. Arithmetic Fuchsian groups of genus zero. *Pure Appl. Math. Q.*, 2(2, Special Issue: In honor of John H. Coates. Part 2):569–599, 2006.

[Mac69] A. M. Macbeath. Generators of the linear fractional groups. In *Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967)*, pages 14–32. Amer. Math. Soc., Providence, R.I., 1969.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[NV17] Steve Nugent and John Voight. On the arithmetic dimension of triangle groups. *Math. Comp.*, 86(306):1979–2004, 2017.

[Ogg73] A. P. Ogg. Rational points on certain elliptic modular curves. In *Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 221–231, 1973.

[Ogg74] Andrew P. Ogg. Hyperelliptic modular curves. *Bull. Soc. Math. France*, 102:449–462, 1974.

[Ogg75] A. P. Ogg. Diophantine equations and modular forms. *Bull. Amer. Math. Soc.*, 81:14–27, 1975.

[RSZB21] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. ℓ-adic images of galois for elliptic curves over $\mathbb{Q}$, 2021.

[SV14] J. Sijsling and J. Voight. On computing Belyi maps. In *Numéro consacré au trimestre "Méthodes arithmétiques et applications", automne 2013*, volume 2014/1 of *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 73–131. Presses Univ. Franche-Comté, Besançon, 2014.

[Tak77a] Kisao Takeuchi. Arithmetic triangle groups. *J. Math. Soc. Japan*, 29(1):91–106, 1977.

[Tak77b] Kisao Takeuchi. Commensurability classes of arithmetic triangle groups. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 24(1):201–212, 1977.

[Tho80] J. G. Thompson. A finiteness theorem for subgroups of $\mathrm{PSL}(2, \mathbf{R})$ which are commensurable with $\mathrm{PSL}(2, \mathbf{Z})$. In *The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)*, volume 37 of *Proc. Sympos. Pure Math.*, pages 533–555. Amer. Math. Soc., Providence, R.I., 1980.

[Voi09] John Voight. Shimura curves of genus at most two. *Math. Comp.*, 78(266):1155–1172, 2009.

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA
Email address: juanita.duque.rosero.gr@dartmouth.edu

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA
Email address: jvoight@gmail.com