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 a source of Belyi maps with monodromy $\mathrm{PGL}_2(\mathbb{F}_q)$ or $\mathrm{PSL}_2(\mathbb{F}_q)$. We present a computational approach to enumerate Borel-type triangular modular curves of low genus, and we carry out this enumeration for prime level and small genus.

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 [9, p. 357]. At the end of the twentieth century, Ogg enumerated and studied elliptic [17] and hyperelliptic [18] modular curves; the resulting Diophantine study [19] informed Mazur's classification of rational isogenies of elliptic curves [15], 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 [7]. Recent papers have studied curves with infinitely many rational points in the context of Mazur's *Program B*—see Rouse–Sutherland–Zureick-Brown [20] for further references and recent results in this direction.

Given this rich backdrop, it is worthwhile to pursue generalizations. For example, replacing $\mathrm{SL}_2(\mathbb{Z})$ with its quaternionic cousins, Voight [25] 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 [12] enumerated all maximal arithmetic Fuchsian groups of genus 0 over $\mathbb{Q}$, corresponding to quotients of Shimura curves by the full group of Atkin–Lehner involutions.

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 [3]. 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, unique up to isometry. 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 $\Delta = \Delta(a, b, c) \leq \mathrm{PSL}_2(\mathbb{R})$, with presentation

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

(omitting the relation δ_s^s when $s = \infty$). 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, isomorphic to $\mathbb{P}^1$ with a unique coordinate t taking values $0, 1, \infty$ at the vertices labelled a, b, c, respectively. For example, we recover the classical modular group as $\Delta(2,3,\infty) \simeq \mathrm{PSL}_2(\mathbb{Z})$, with coordinate $t = j/1728$.

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. The field F is the subfield of $\mathbb{R}$ generated by $\operatorname{Tr}\Delta$, and similarly E, called the **invariant trace field**, is the subfield generated by $\operatorname{Tr}\Delta^{(2)}$ where $\Delta^{(2)} \leq \Delta$ is the subgroup generated by squares. Let $\mathbb{Z}_E \subset E$ be the ring of integers and similarly $\mathbb{Z}_F \subset F$.

Let $\mathfrak{N} \subseteq \mathbb{Z}_E$ be a nonzero ideal. Then there is a natural reduction homomorphism $\varpi_{\mathfrak{N}}$ with domain Δ, intuitively thought of as reducing matrix entries modulo $\mathfrak{N}$ but with a rigorous quaternionic interpretation (see below). The kernel $\Gamma(a,b,c;\mathfrak{N}) := \ker \varpi_{\mathfrak{N}}$ is called the **principal congruence subgroup of level $\mathfrak{N}$**. A subgroup $\Gamma \leq \Delta(a,b,c)$ is said to be **congruence** if $\Gamma \geq \Gamma(a,b,c;\mathfrak{N})$ for some $\mathfrak{N}$; the **level** of a congruence subgroup is the minimal such $\mathfrak{N}$. Given a congruence subgroup $\Gamma \leq \Delta(a,b,c)$, we call the quotient $X(a,b,c;\Gamma) := \Gamma\backslash\mathcal{H}$ a **triangular modular curve**, since they generalize the classical modular curves. The quotient map

$$\varphi_{\mathfrak{N}} \colon X(a,b,c;\Gamma) \to X(a,b,c) \simeq \mathbb{P}^1_{\mathbb{C}} \tag{1.2}$$

(generalizing the j-invariant) is a Belyi map, unramified away from $\{0,1,\infty\}$ (by our normalization). Accordingly, the curve $X(a,b,c;\mathfrak{N})$ descends to a number field [3, Theorem B].

In light of the motivation above, we focus now on a nice class of congruence subgroups. The E-subalgebra $A := E\langle\Delta^{(2)}\rangle \leq \mathrm{M}_2(\mathbb{R})$ generated by (any lift of) the image of $\Delta^{(2)} \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$ is a quaternion algebra, and $\Lambda := \mathbb{Z}_E\langle\Delta\rangle$ is a $\mathbb{Z}_E$-order in A. Then there is a commutative square

$$\begin{tikzcd} \Delta^{(2)} \arrow[r, hook] \arrow[d, hook] & \Lambda^1/\{\pm 1\} \arrow[d, hook] \\ \Delta \arrow[r, hook] & N_{A^\times}(\Lambda)/E^\times \end{tikzcd} \tag{1.3}$$

where $\Lambda^1 := \{\gamma \in \Lambda : \operatorname{nrd}(\gamma) = 1\}$ are the elements of reduced norm 1.

Suppose $\mathfrak{N} \subseteq \mathbb{Z}_E$ is coprime to $\operatorname{discrd}(\Lambda)$ and $\mathfrak{d}_{F|E}$, the relative discriminant of F over E; for example, this holds if $\mathfrak{N}$ is coprime to $2abc$. Then the reduction $\Lambda \to \Lambda/\mathfrak{N}\Lambda \simeq \mathrm{M}_2(\mathbb{Z}_E/\mathfrak{N})$ gives a well-defined group homomorphism

$$\pi_{\mathfrak{N}} \colon \Delta \to \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N}). \tag{1.4}$$

Combined with (1.3), we obtain a commutative diagram (Proposition 3.6)

$$\begin{tikzcd} \Delta^{(2)} \arrow[r] \arrow[d, hook] & \mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\} \arrow[d] \\ \Delta \arrow[r, "\pi_{\mathfrak{N}}"] & \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N}) \end{tikzcd} \tag{1.5}$$

Let $G_{\mathfrak{N}} := \pi_{\mathfrak{N}}(\Delta)$ be the image. Let $s^\sharp$ be the order of $\pi_{\mathfrak{N}}(\delta_s)$ for $s = a, b, c$; then $a^\sharp, b^\sharp, c^\sharp$ are the ramification degrees in $\varphi_{\mathfrak{N}}$ above $0, 1, \infty$, and the homomorphism $\pi_{\mathfrak{N}}$ factors through $\Delta(a^\sharp, b^\sharp, c^\sharp)$. To avoid redundancy, we say that $\mathfrak{N}$ is admissible for (a, b, c) if $s^\sharp = s$ for all $s = a, b, c$—so in particular, $s \neq \infty$.

Without loss of generality (but see Proposition 3.13), we now suppose that $\mathfrak{N}$ is admissible for (a, b, c). Then the main result of Clark–Voight [3, Theorem A] (see Theorem 3.12) describes the group $G_{\mathfrak{N}}$. For example, when $\mathfrak{N} = \mathfrak{p}$ is *prime*, then

$$G_{\mathfrak{N}} \simeq \mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{p}) \tag{1.6}$$

where $\mathrm{PXL}_2 = \mathrm{PSL}_2$ if $\mathfrak{p}$ (necessarily unramified in F) splits completely in F, and otherwise $\mathrm{PXL}_2 = \mathrm{PGL}_2$.

With this in mind, in this paper we focus on the case where $\mathfrak{N} = \mathfrak{p}$ is prime. This case is already a quite interesting first step, and still relevant for our motivation (see the next section). Moreover, the case of composite level $\mathfrak{N}$ builds on the prime level case and at the same time introduces several new challenges that are not present in prime level. We plan to pursue the general case in future work.

Returning now to our original motivation, the usual upper-triangular (Borel-type) subgroups

$$H_{1,\mathfrak{p}} \leq H_{0,\mathfrak{p}} := \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \leq \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{p}) \tag{1.7}$$

naturally include into $G_{\mathfrak{p}}$ via (1.6). We define the Borel-type congruence subgroups of Δ

$$\begin{aligned} \Gamma_0(a, b, c; \mathfrak{p}) &:= \pi_{\mathfrak{p}}^{-1}(H_{0,\mathfrak{p}}) \\ \Gamma_1(a, b, c; \mathfrak{p}) &:= \pi_{\mathfrak{p}}^{-1}(H_{1,\mathfrak{p}}) \end{aligned} \tag{1.8}$$

We write $X_0(a, b, c; \mathfrak{p})$ and $X_1(a, b, c; \mathfrak{p})$ for the corresponding quotients. For $(a, b, c) = (2, 3, \infty)$, we recover the classical modular curves $X_0(p)$ and $X_1(p)$.

Our main result is as follows.

Theorem 1.9. *For any $g \in \mathbb{Z}_{\geq 0}$, there are only finitely many Borel-type triangular modular curves of genus g with admissible prime level $\mathfrak{N} = \mathfrak{p}$. The number of curves of genus at most 2 are as follows:*

	genus		
	0	1	2
$X_0(a, b, c; \mathfrak{p})$	69	248	453
$X_1(a, b, c; \mathfrak{p})$	6	9	11

Our proof of Theorem 1.9 includes a complete enumeration, computed using an implementation in Magma [2] available online [26] (including the list in computer readable format with additional data). For the list with $g = 0, 1$ and prime level, see Appendix A.

Discussion. As for classical modular curves, Theorem 1.9 uses the Riemann–Hurwitz theorem. We observe that the ramification at prime level takes a tidy form. We carry out the explicit enumeration using the existence and classification results of Clark–Voight [3], which themselves ultimately rest on work of Macbeath [13] classifying two-generated subgroups of $\mathrm{SL}_2(\mathbb{F}_q)$ in terms of trace triples. The case $a = 2$ causes particular difficulties (see Example 4.2).

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 [5, §3.3] and Archinard [1] showed that the curves $X(a,b,c)$ over $\mathbb{C}$ naturally parametrize *hypergeometric abelian varieties*, certain Prym varieties of cyclic covers of $\mathbb{P}^1$ branched over ≤ 4 points. The name comes from the fact that their complex periods are values of ${}_2F_1$-hypergeometric functions for the parameter $t \in \mathbb{P}^1(\mathbb{C}) \smallsetminus \{0,1,\infty\}$. In accordance with Manin's "unity of mathematics" [4], 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 [11] 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 (nontrivial Borel-type) level structure for $t \in \mathbb{Q}$.

As shown by Takeuchi [22, 23], 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 are *thin* subgroups of the adelic points of a quaternionic group, so fall outside the usual scope of the Langlands program.

As a final possible Diophantine application, we recall work of Darmon [8]: 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 $\mathfrak{p}$ Galois representations are reducible.

In future work, we plan to compute equations for these curves (as Belyi maps) using the methods of Klug–Musty–Schiavone–Voight [10] 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 pursue cases when $\mathfrak{p}$ ramifies in A, where the corresponding Galois covers will instead be solvable.

To conclude, we peek ahead to more general triangular modular curves, allowing other subgroups $\Gamma \leq \Gamma(a,b,c;\mathfrak{N})$ (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 [24] proved this for any genus g, but the list of Cummins–Pauli relies upon difficult and delicate p-adic methods of Cox–Parry [6] 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 1.10. *For all $g \in \mathbb{Z}_{\geq 0}$, there are only finitely many admissible triangular modular curves of genus g.*

We consider our main result (Theorem 1.9) 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 1.10 in an effective way.

Contents. In section 2, we set up triangular modular curves and as a warmup consider the much easier Galois case $X(a,b,c;\mathfrak{p})$. In section 3, we extend the work of Clark–Voight to understand the arithmetic requirements to construct triangular modular curves. Then in section 4, for the case $X_0(a,b,c;\mathfrak{p})$ with $a,b,c \in \mathbb{Z}$, 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 5. In section 6, we provide analogous results for curves $X_1(a,b,c;\mathfrak{N})$, and finally we prove Theorem 1.9. We conclude by providing the list in Appendix A.

Acknowledgements. The authors would like to thank Asher Auel and Robert Kucharczyk for helpful conversations and the anonymous referees for their constructive feedback. The authors were supported by a Simons Collaboration grant (550029, to Voight).

2. Setup and definitions

In this section, we give some basic setup and notation, define congruence subgroups, and consider the enumeration problem in the Galois case; for further reference, see Clark–Voight [3].

Triangle groups. Beginning again, let $a,b,c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. Let

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

so that $\chi(a,b,c)\pi$ measures 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 $\chi(a,b,c) < 0$ and we say that the triple (a,b,c) is hyperbolic, 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.

As in the introduction, let $\Delta(a,b,c)$ be the subgroup of orientation-preserving isometries of the group generated by reflections in the sides of the triangle described above, drawn in the appropriate geometry. Then we have a presentation

$$\Delta(a,b,c) := \langle \delta_a, \delta_b, \delta_c \,|\, \delta_a^a = \delta_b^b = \delta_c^c = \delta_a\delta_b\delta_c = 1 \rangle. \tag{2.3}$$

where δ_s corresponds to a counterclockwise rotation at the vertex with angle $2\pi/s$. By cyclic permutation and inversion [3, Remark 2.2], we can reorganize the generators and suppose without loss of generality that

$$a \leq b \leq c. \tag{2.4}$$

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. We will often suppress the dependence on the triple from notation, writing for example $\Delta = \Delta(a,b,c)$.

The group Δ is said to be cocompact if the quotient of the upper half-plane by Δ is compact, else we say Δ is noncocompact. We have Δ noncocompact if and only if at least one of a, b, c is equal to ∞.

Let $\Delta^{(2)}$ denote the subgroup of Δ generated by the set of squares $\{\delta^2 : \delta \in \Delta\}$. Then $\Delta^{(2)} \trianglelefteq \Delta$ is a normal subgroup, in fact [3, (5.9)] the quotient $\Delta/\Delta^{(2)}$ is represented by the elements δ_s with $s \in \{a, b, c\}$ such that either $s = \infty$ or $s \in \mathbb{Z}_{\geq 2}$ is even, hence

$$\Delta/\Delta^{(2)} \simeq \begin{cases} \{0\}, & \text{if at least two of } a, b, c \text{ are odd integers;} \\ \mathbb{Z}/2\mathbb{Z}, & \text{if exactly one of } a, b, c \text{ is an odd integer;} \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if all of } a, b, c \text{ are even integers or } \infty. \end{cases} \tag{2.5}$$

Lemma 2.6. *The group $\Delta^{(2)}$ is generated by the set*

$$\{\delta_s^{-1}\delta_t^2\delta_s : s, t \in \{a, b, c\}\} \cup \{\delta_s\delta_t\delta_s^{-1}\delta_t^{-1} : s, t \in \{a, b, c\}\}. \tag{2.7}$$

Proof. Follows from Takeuchi [22, Lemma 3, Proposition 5]: the generating set presented there is smaller (depending on cases), whereas we collect these and symmetrize to make a uniform statement. □

Quaternions. For $s \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$, let $\zeta_s := \exp(2\pi i/s)$ and let $\lambda_s := \zeta_s + 1/\zeta_s = 2\cos(2\pi/s)$, with $\zeta_\infty = 1$ and $\lambda_\infty = 2$ by convention. Define the tower of fields

$$\begin{tikzcd} F = F(a, b, c) := \mathbb{Q}(\lambda_{2a}, \lambda_{2b}, \lambda_{2c}) \arrow[d, dash] \\ E = E(a, b, c) := \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c, \lambda_{2a}\lambda_{2b}\lambda_{2c}). \end{tikzcd} \tag{2.8}$$

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, and let $\mathfrak{d}_{F|E}$ be the relative discriminant of $F \,|\, E$. The field F is the trace field of the image of Δ in $\mathrm{PSL}_2(\mathbb{R})$, and E the trace field for $\Delta^{(2)}$, also called the invariant trace field (see Maclachlan–Reid [14, Section 5.5]).

As above, we have a map $\Delta \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$; the F-subalgebra $B := F\langle\Delta\rangle \leq \mathrm{M}_2(\mathbb{R})$ generated by any lift of the image (well-defined, since $-1 \in F$) is a quaternion algebra, similarly $\mathcal{O} := \mathbb{Z}_F\langle\Delta\rangle$ is a $\mathbb{Z}_F$-order in B [21, Propositions 2–3]. The reduced discriminant of $\mathcal{O}$ is a principal ideal of $\mathbb{Z}_F$ generated by [3, Lemma 5.4]

$$\beta(a, b, c) := \lambda_{2a}^2 + \lambda_{2b}^2 + \lambda_{2c}^2 + \lambda_{2a}\lambda_{2b}\lambda_{2c} - 4 = \lambda_a + \lambda_b + \lambda_c + \lambda_{2a}\lambda_{2b}\lambda_{2c} + 2 \in \mathbb{Z}_E. \tag{2.9}$$

The same construction applies to $\Delta^{(2)}$, yielding a quaternion E-algebra A and a $\mathbb{Z}_E$-order Λ. Let $\mathcal{O}^1 := \{\gamma \in \mathcal{O} : \mathrm{nrd}(\gamma) = 1\}$ be the elements of reduced norm 1 in $\mathcal{O}$, and define Λ^1 similarly. Then we have a commutative square of group homomorphisms

$$\begin{tikzcd} \Delta^{(2)} \arrow[r, hook] \arrow[d, hook] & \Lambda^1/\{\pm 1\} \arrow[d, hook] \\ \Delta \arrow[r, hook] & \mathcal{O}^1/\{\pm 1\} \end{tikzcd} \tag{2.10}$$

In fact, the bottom map descends to the *normalizer* $N_A(\Lambda)$ of Λ in A, as follows.

Lemma 2.11. *The composition of the maps*

$$\Delta \hookrightarrow \frac{\mathcal{O}^1}{\{\pm 1\}} \hookrightarrow \frac{N_{B^\times}(\mathcal{O})}{F^\times}$$

factors via the map

$$\begin{aligned} \Delta &\hookrightarrow \frac{N_{A^\times}(\Lambda)}{E^\times} \\ \delta_s &\mapsto \begin{cases} \delta_s^2 + 1 = \lambda_{2s}\delta_s, & \text{if } s \neq 2; \\ (\delta_c^2+1)(\delta_b^2+1) = \lambda_{2b}\lambda_{2c}\delta_a, & \text{if } s = a = 2; \end{cases} \end{aligned} \tag{2.12}$$

followed by the natural inclusion $N_{A^\times}(\Lambda)/E^\times \hookrightarrow N_{B^\times}(\mathcal{O})/F^\times$*.*

Proof. See Clark–Voight [3, Proposition 5.13]. (The description fails to be uniform when $a = 2$ because $\lambda_4 = 0$; since $a \leq b \leq c$ we must have $b > 2$, else (a, b, c) is not hyperbolic. The map is nevertheless uniquely determined, since $\delta_a\delta_b\delta_c = 1$.) □

Congruence subgroups: general definition. We now define congruence subgroups. Let $\mathfrak{N} \subseteq \mathbb{Z}_E$ be a nonzero ideal. Then reducing elements modulo $\mathfrak{N}$, as in (2.10) we obtain a commutative diagram

$$\begin{tikzcd} 1 \arrow[r] & \Gamma^{(2)}(\mathfrak{N}) \arrow[r] \arrow[d, hook] & \Delta^{(2)} \arrow[r] \arrow[d, hook] & (\Lambda/\mathfrak{N}\Lambda)^1/\{\pm 1\} \arrow[d, hook] \\ 1 \arrow[r] & \Gamma(\mathfrak{N}) \arrow[r] & \Delta \arrow[r, "\varpi_{\mathfrak{N}}"] & (\mathcal{O}/\mathfrak{N}\mathcal{O})^1/\{\pm 1\} \end{tikzcd} \tag{2.13}$$

but now with kernels in the rows: in particular, we have a group homomorphism

$$\varpi_{\mathfrak{N}} \colon \Delta \to (\mathcal{O}/\mathfrak{N}\mathcal{O})/\{\pm 1\} \tag{2.14}$$

with kernel

$$\Gamma(\mathfrak{N}) := \ker \pi_{\mathfrak{N}} = \{\delta \in \Delta : \delta \equiv \pm 1 \pmod{\mathfrak{N}\mathcal{O}}\} \trianglelefteq \Delta \tag{2.15}$$

called the principal congruence subgroup of level $\mathfrak{N}$. As in the introduction, we define congruence subgroups of Δ to be those that contain a principal congruence subgroup, and a triangular modular curve to be a quotient of the (completed) upper half-plane by a congruence subgroup of a triangle group, for example

$$X(\mathfrak{N}) = X(a, b, c; \mathfrak{N}) := \Gamma(\mathfrak{N})\backslash\mathcal{H} \tag{2.16}$$

are called the principal triangular modular curves.

Remark 2.17. One could work more generally with ideals of $\mathbb{Z}_F$ instead, arriving at the same definition of congruence subgroups but with a different notion of level. In light of what follows, especially the robust failure of $\varpi_{\mathfrak{N}}$ to be surjective, we prefer to work with levels in $\mathbb{Z}_E$.

Since Δ normalizes $\Delta^{(2)}$ and therefore Λ and $\mathfrak{N}\Lambda$, there is descent to the normalizer as in Lemma 2.11. However, the precise description of $\Gamma(\mathfrak{N})$ depends on the ramification behavior of the primes dividing $\mathfrak{N}$ in the extension $F \mid E$ and in the algebras A and B (and this already introduces some subtleties when $\mathfrak{N}$ is composite). We pursue this in the next section.

Galois case. Before proceeding, as a warmup we consider the curves $X(a,b,c;\mathfrak{p})$ corresponding to principal congruence subgroups, where $X(a,b,c;\mathfrak{p}) \to X(a,b,c) \simeq \mathbb{P}^1$ is a generically Galois Belyi map.

Quite generally, for any generically Galois Belyi map with group G, the ramification indices above each ramification point are equal. Without loss of generality, we may suppose that 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 hyperbolic G-Galois Belyi maps with genus g_0.

We are of course interested in the special case where

$$G = \Gamma(\mathfrak{p})\backslash\Delta \simeq \mathrm{PXL}_2(\mathbb{F}_\mathfrak{p})$$

where $\mathbb{F}_\mathfrak{p} := \mathbb{Z}_E/\mathfrak{p}$ is the residue field and $\mathrm{PXL}_2(\mathbb{F}_\mathfrak{p})$ denotes either $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ or $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{p})$. (The major task in the next section is to precisely investigate this arithmetically.) Plugging $G = \mathrm{PXL}_2(\mathbb{F}_q)$ into the above:

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

Thus, there are no curves $X(a,b,c;\mathfrak{p})$ of genus at most 1. For genus 2, we can use the inequality to see that q must be less than 6, so $\#G \leq 60$ and, if $g(X(a,b,c;\mathfrak{p})) = 2$, then

$$-\frac{1}{\chi(a,b,c)} \leq 30.$$

This inequality implies that $a \leq b \leq c \leq 7$ and, by checking the genera of these possibilities with (2.19), we conclude that there are no curves $X(a,b,c;\mathfrak{p})$ of genus 2.

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 [3, Table 10.5] for examples up to genus 24.

3. Triangular modular curves

In this section, we study triangular modular curves generalizing the classical modular curves; the main results are Proposition 3.6, where we define the relevant matrix representation of Δ, and Theorem 3.12, describing its image building on work of Clark–Voight [3]. Throughout, we retain our notation from the previous section.

Congruence subgroups: matrix case. We return to (2.13), and identify matrix groups. Recalling (2.9), we first suppose that $\beta = \operatorname{discrd} \mathcal{O}$ is coprime to $\mathfrak{N}$, so all primes $\mathfrak{p} \mid \mathfrak{N}$ are unramified in B but more strongly we have $(\mathcal{O}/\mathfrak{N}\mathcal{O})^1/\{\pm 1\} \simeq \mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F)/\{\pm 1\}$.

For the order Λ, we recall Lemma 2.6: given a,b,c, we can compute its $\mathbb{Z}_E$-module span in A and therefore a $\mathbb{Z}_E$-pseudobasis for Λ, hence its reduced discriminant. Since $\Lambda\mathbb{Z}_F \subseteq \mathcal{O}$, we have $\beta \mid \operatorname{discrd}(\Lambda)$ [3, Corollary 5.17].

So we make the stronger assumption that $\mathfrak{N}$ is coprime to $\operatorname{discrd}(\Lambda)$. Then from (2.10) we get

$$\begin{tikzcd}
\Delta^{(2)} \arrow[r] \arrow[d, hook] & (\Lambda/\mathfrak{N}\Lambda)^1/\{\pm 1\} \arrow[r, "\sim"] \arrow[d, hook] & \mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\} \\
\Delta \arrow[r, "\pi_{\mathfrak{N}}"] & (\mathcal{O}/\mathfrak{N}\mathcal{O})^1/\{\pm 1\} \arrow[r, "\sim"] & \mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F)/\{\pm 1\}
\end{tikzcd} \tag{3.1}$$

To descend the bottom map to the normalizer as in Lemma 2.11, we restrict our scope taking $\mathfrak{N} = \mathfrak{p}$ prime and work just a little bit more.

Let

$$\mathbb{Z}_{E,(\mathfrak{p})} := \{\alpha \in E : \operatorname{ord}_{\mathfrak{p}}(\alpha) \geq 0\} \subseteq E \tag{3.2}$$

be the localization of $\mathbb{Z}_E$ at the ideal $\mathfrak{p}$ (all elements coprime to $\mathfrak{p}$ become units).

Lemma 3.3. *Suppose that $\mathfrak{p} \nmid \mathfrak{d}_{F|E}$. Then for $s = a, b, c$, we can write*

$$\lambda_s + 2 = \upsilon_s \theta_s^2 \in E^\times \tag{3.4}$$

with:

- *$\upsilon_s \in \mathbb{Z}_{E,(\mathfrak{p})}^\times$, well-defined up to multiplication by an element of $\mathbb{Z}_{E,(\mathfrak{p})}^{\times 2}$, i.e., up to the square of an element of $\mathbb{Z}_{E,(\mathfrak{p})}^\times$, and*
- *$\theta_s \in E^\times$, well-defined up to $\mathbb{Z}_{E,(\mathfrak{p})}^\times$.*

If $\mathfrak{p}$ is coprime to $2abc$, then we may take $\theta_s = 1$ and $\upsilon_s = \lambda_s + 2$.

Moreover, the prime $\mathfrak{p}$ (necessarily unramified in F) splits completely in F if and only if the Kronecker symbols $(\upsilon_s \,|\, \mathfrak{p}) = 1$ are trivial for all $s = a, b, c$.

Proof. First, a bit of generality: for $\alpha \in E^\times$ with even valuation at all primes $\mathfrak{p} \mid \mathfrak{N}$, by weak approximation in E we can write

$$\alpha = \upsilon\theta^2 \in E^\times \tag{3.5}$$

with υ, θ as in the statement of the lemma.

Now to apply this, we observe that $F = E(\lambda_{2a}, \lambda_{2b}, \lambda_{2c})$ and recall that $\lambda_{2s}^2 = \lambda_s + 2$. By hypothesis, we have $\mathfrak{p} \nmid \mathfrak{d}_{F|E}$; in particular the elements $\lambda_s + 2$ must have even (nonnegative) valuation at $\mathfrak{p}$. Thus (3.5) applies, giving (3.4). The final statement follows from the usual splitting criterion in quadratic fields. □

We obtain the following result.

Proposition 3.6. *Suppose that $\mathfrak{p} \nmid \operatorname{discrd}(\Lambda)\mathfrak{d}_{F|E}$. Then there is a commutative diagram*

$$\begin{tikzcd}
\Delta^{(2)} \arrow[r] \arrow[d, hook] & \mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{p})/\{\pm 1\} \arrow[d] \\
\Delta \arrow[r, "\pi_{\mathfrak{N}}"] & \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{p})
\end{tikzcd} \tag{3.7}$$

and the map $\pi_{\mathfrak{N}} \colon \Delta \to \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})$ factors through $\varpi_{\mathfrak{N}}$.

We let $G_{\mathfrak{p}} := \pi_{\mathfrak{p}}(\Delta) \leq \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{p})$ be the image of $\pi_{\mathfrak{p}}$.

Proof. Combine (3.1) with Lemma 3.3. □

Remark 3.8. A similar argument works when $\mathfrak{N}$ is composite; however the right-hand vertical map $\mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\} \to \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})$ may no longer be injective when $\mathfrak{N}$ is composite. This leads to certain ambiguities about the definition which we will return to in future work.

Admissibility, projectivity, and image. It can and does happen that two different triangular modular curves are isomorphic (as curves and as covers of $\mathbb{P}^1$). The issue is simply that in the homomorphism $\pi_{\mathfrak{N}}$ from $\Delta(a,b,c)$ to a matrix group, the generators δ_s need not have order s in the image (for $s = a,b,c$). In other words, the reduction homomorphism factors through a triangle group with a smaller triple. This happens for example when $s = \infty$, as the order of $\pi_{\mathfrak{N}}(\delta_s)$ is always finite! To illustrate this phenomena, we present the following example.

Example 3.9. Consider the triples $(2,3,c)$ with $c = p^k$, where $k \geq 1$ and $p \geq 5$ is prime. Then

$$E_k := E(2,3,c) = F(2,3,c) = \mathbb{Q}(\lambda_{2c}) = \mathbb{Q}(\zeta_{2c})^+ \tag{3.10}$$

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

To avoid this redundancy, we make the following definition.

Definition 3.11. Given a triple (a,b,c), an ideal $\mathfrak{p} \subseteq \mathbb{Z}_{E(a,b,c)}$ is admissible for (a,b,c) if

- $\mathfrak{p} \nmid \mathrm{discrd}(\Lambda)\mathfrak{d}_{F|E}$, and
- the order of $\pi_{\mathfrak{p}}(\delta_s)$ is equal to s for all $s = a,b,c$.

Theorem 3.12 (Clark–Voight). *We have $\pi_{\mathfrak{p}}(G_{\mathfrak{p}}^{(2)}) = \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{p})$ and*

$$\pi_{\mathfrak{p}}(G_{\mathfrak{p}}) = \mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{p})$$

where PXL_2 denotes PSL_2 or PGL_2 according as $\mathfrak{p}$ splits in $F \supseteq E$ or not.

Proof. We refer to Clark–Voight [3, Theorem A] for the case where $\mathfrak{p} \nmid 2abc$; but examining the argument given [3, Remark 5.24, proof of Theorem 9.1] in light of the above, we see that it extends when $\mathfrak{p} \nmid \mathrm{discrd}(\Lambda)\beta\mathfrak{d}_{F|E}$. □

Hyperbolic triples reducing to non-hyperbolic triples. In considering admissible triples, we may lose the hypothesis that (a,b,c) is hyperbolic; however, this situation is easy to characterize. We note that in most cases, these groups do not contain $\mathrm{PSL}_2(\mathbb{F}_q)$, so they are not considered in this paper.

Proposition 3.13. *Let $(a,b,c) \in (\mathbb{Z}_{\geq 0} \cup \{\infty\})^3$ be a triple and let $\mathfrak{p} \subset \mathbb{Z}_E$ be a nonzero prime ideal. Suppose further that $(a^\sharp, b^\sharp, c^\sharp)$ is a projective triple, but not hyperbolic. Then $(a,b,c;p,q)$ is one of the elements listed in the following table. In the table, p lies below $\mathfrak{p}$*

and q is the residue field degree of $\mathfrak{p}$.

(3.14)

(a, b, c)	*conditions*	p	q	**PXL**	$E(a^\sharp, b^\sharp, c^\sharp)$
$(2^{k_a}, 2^{k_b}, 3 \cdot 2^{k_c})$, $(3 \cdot 2^{k_c}, \infty, \infty)$, $(2^{k_a}, 3 \cdot 2^{k_c}, \infty)$	$1 \le k_a < k_b$	2	2	1	$\mathbb{Q}$
$(3^{k_a}, 3^{k_b}, 3^{k_c})$, $(3^{k_a}, \infty, \infty)$, $(3^{k_a}, 3^{k_b}, \infty)$, (∞, ∞, ∞)	$1 \le k_a \le k_b < k_c$	3	3	1	$\mathbb{Q}$
$(2 \cdot 3^{k_a}, 3^{k_b}, 3^{k_c})$, $(2 \cdot 3^{k_a}, 3^{k_b}, \infty)$, $(2 \cdot 3^{k_a}, \infty, \infty)$	$1 \le k_b \le k_c$, $k_a k_b k_c \neq 1$	3	3	1	$\mathbb{Q}$
$(2 \cdot 3^{k_a}, 3^{k_b}, 4 \cdot 3^{k_c})$, $(2 \cdot 3^{k_a}, 4 \cdot 3^{k_b}, \infty)$	$1 \le k_b$, $k_a k_b k_c \neq 1$	3	3	-1	$\mathbb{Q}$
$(2^{k_a}, 3 \cdot 2^{k_b}, 5 \cdot 2^{k_c})$, $(3 \cdot 2^{k_b}, 5 \cdot 2^{k_c}, \infty)$	$1 \le k_a$, $k_a k_b k_c \neq 1$	2	4	1	$\mathbb{Q}(\sqrt{5})$
$(2 \cdot 5^{k_a}, 3 \cdot 5^{k_b}, 5^{k_c})$, $(2 \cdot 5^{k_a}, 3 \cdot 5^{k_b}, \infty)$	$1 \le k_c$, $k_a k_b k_c \neq 1$	5	5	1	$\mathbb{Q}(\sqrt{5})$

Furthermore, the curves $X(a, b, c; \mathfrak{p})$ with $(a, b, c; \mathfrak{p})$ as above all have genus 0.

Proof. We first focus on the prime ideal case and make a case by case study. The only triples $(a, b, c) \in (\mathbb{Z}_{\geq 0} \cup \{\infty\})^3$ that are not hyperbolic are

$$(2, 2, n) \text{ for } n > 1,\ (2, 3, 3),\ (2, 3, 4),\ (2, 3, 5),\ (2, 3, 6),\ (2, 4, 4),\ \text{ or } (3, 3, 3).$$

Assume first that $(a^\sharp, b^\sharp, c^\sharp) = (2, 2, c)$ for $c > 1$. The image of $\pi_\mathfrak{p} : \Delta(2, 2, c) \to \mathrm{PGL}_2(\mathbb{F}_q)$ must be dihedral. The only dihedral group that is isomorphic to $\mathrm{PXL}_2(\mathbb{F}_q)$ for any q is $D_6 \simeq \mathrm{PSL}_2(\mathbb{F}_2)$. Thus, we only have the triple $(a^\sharp, b^\sharp, c^\sharp) = (2, 2, 3)$ and prime $\mathfrak{p}_2$.

The group $\Delta(2, 3, 6)$ is solvable since it fits in the exact sequence:

$$1 \to \mathbb{Z}^2 \to \Delta(2, 3, 6) \to \mathbb{Z}/6\mathbb{Z} \to 1.$$

The only solvable groups of the form $\mathrm{PXL}_2(\mathbb{F}_q)$ are $S_4 \simeq \mathrm{PGL}_2(\mathbb{F}_3)$ and $A_4 \simeq \mathrm{PSL}_2(\mathbb{F}_3)$. The triple $(2, 3, 6)$ is not admissible for $q = 2$ or $q = 3$, so $(2, 3, 6)$ is not projective and admissible for any prime ideal $\mathfrak{p}$. With the same analysis, we can rule out $(2, 4, 4)$. We also have that the group $\Delta(3, 3, 3)$ is solvable. Hence, the image of $\pi_\mathfrak{p} : \Delta(3, 3, 3) \to \mathrm{PXL}_2(\mathbb{F}_q)$ must be solvable. The only solvable groups of this form are $A_4 \simeq \mathrm{PSL}_2(\mathbb{F}_3)$ and $S_4 \simeq \mathrm{PGL}_2(\mathbb{F}_3)$. Thus, the only option is that $\mathfrak{p}$ is a prime above 3 with residue field $\mathbb{F}_3$.

The last triples to consider are $(2, 3, 3)$, $(2, 3, 4)$ and $(2, 3, 5)$. These triples are all *exceptional*. Tthe only projective linear groups that can arise from exceptional triples [3, Remark 8.4] are the following:

$$\mathrm{PSL}_2(\mathbb{F}_3), \mathrm{PGL}_2(\mathbb{F}_3), \mathrm{PGL}_2(\mathbb{F}_4), \mathrm{PSL}_2(\mathbb{F}_5).$$

We now use this fact to finish the analysis. When $(a^\sharp, b^\sharp, c^\sharp) = (2, 3, 3)$, the admissible prime ideals $\mathfrak{p}$ have residue field degree $3, 4$ and 5. The field $E(2, 3, 3)$ is the rational field, so $\mathbb{Z}_E/\mathfrak{p}_2 \simeq \mathbb{F}_2$. In addition, the ideal $2\mathbb{Z}_E$ is totally ramified in any field $E(2 \cdot 2^{k_a}, 3 \cdot 2^{k_b}, 3 \cdot 2^{k_c})$, so $q \neq 4$. The only options then are $q = 3$ and $q = 5$. A quick Magma [2] calculation shows that elements with these orders cannot generate $\mathrm{PSL}_2(\mathbb{F}_5)$.

Similarly, when $(a^\sharp, b^\sharp, c^\sharp) = (2, 3, 4)$, the only possibilities for q which make the triple projective and admissible for $\mathfrak{p}$ are $q = 3$ or $q = 5$. However, the field $E(2, 3, 4)$ is the rational field and 5 is inert in F, so we would have $G_{5\mathbb{Z}_E} \simeq \mathrm{PGL}_2(\mathbb{F}_5)$, which is not on the list of possible groups. The same happens for $(a^\sharp, b^\sharp, c^\sharp) = (2, 3, 5)$; the options of q for an admissible prime $\mathfrak{p}$ are $q = 2, 3, 4, 5$. The ideal $2\mathbb{Z}_E$ is inert in $E(2, 3, 5)$, an extension of $\mathbb{Q}$ of degree 2, thus $q = 2$ is not possible. The ideal $3\mathbb{Z}_E$ is also inert in $E(2, 3, 5)$, so an isomorphism with $\mathrm{PXL}_2(\mathbb{F}_3)$ is not possible. The only options for q are $q = 4$ and $q = 5$.

For all of the possible triples $(a^\sharp, b^\sharp, c^\sharp)$ and primes $\mathfrak{p}$ described above, we certify that such map is possible by exhibiting passports for each curve. Finally, we use Equation (2.19) to compute the genus of each of these curves, finding that they all have genus 0. □

Borel-type subgroups. As in the introduction, let

$$\left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z}_E/\mathfrak{p} \text{ and } ad \in (\mathbb{Z}_E/\mathfrak{p})^\times\right\} \leq \mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{p}) \tag{3.15}$$

be the upper-triangular matrices in $\mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{p})$, and let $H_{0,\mathfrak{p}}$ be its image in the projection to $\mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{p})$. Similarly, let

$$\left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}_E/\mathfrak{p}\right\} \leq \mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{p}) \tag{3.16}$$

be the upper unipotent subgroup and $H_{1,\mathfrak{p}}$ again its image in $\mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{p})$.

We then define the subgroups

$$\begin{aligned} \Gamma_0(a, b, c; \mathfrak{p}) &:= \varphi_{\mathfrak{p}}^{-1}(H_{0,\mathfrak{p}}), \\ \Gamma_1(a, b, c; \mathfrak{p}) &:= \varphi_{\mathfrak{p}}^{-1}(H_{1,\mathfrak{p}}). \end{aligned} \tag{3.17}$$

and the corresponding quotients

$$\begin{aligned} X_0(a, b, c; \mathfrak{p}) &:= \Gamma_0(a, b, c; \mathfrak{p})\backslash\mathcal{H} = H_{0,\mathfrak{p}}\backslash X'(a, b, c; \mathfrak{p}) \\ X_1(a, b, c; \mathfrak{p}) &:= \Gamma_1(a, b, c; \mathfrak{p})\backslash\mathcal{H} = H_{1,\mathfrak{p}}\backslash X(a, b, c; \mathfrak{p}). \end{aligned} \tag{3.18}$$

Then we have natural quotient maps

$$X(a, b, c; \mathfrak{N}) \to X_1(a, b, c; \mathfrak{N}) \to X_0(a, b, c; \mathfrak{N}) \to X(a, b, c; 1) \simeq \mathbb{P}^1. \tag{3.19}$$

4. 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. Using this formula we show that there are only finitely many such curves with bounded genus.

Setup. Let (a, b, c) be a hyperbolic triple and $\mathfrak{p}$ be an admissible prime of $E = E(a, b, c)$ with residue field $\mathbb{F}_{\mathfrak{p}}$. Let $q := \#\mathbb{F}_{\mathfrak{p}}$, so $\mathbb{F}_{\mathfrak{p}} \simeq \mathbb{F}_q$. 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 $\mathfrak{p}$ (and the inertial degree of $\mathfrak{p}$ over p).

Let $G := G_{\mathfrak{p}}$ be as in Theorem 3.12. Then the group $H_0 = H_{0,\mathfrak{p}}$ consists of 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. By construction, the curves $X_0(a, b, c; \mathfrak{p})$ and $X(a, b, c; \mathfrak{p})$ fit in the following diagram.

$$\begin{tikzcd}
X(a,b,c;\mathfrak{p}) \arrow[dd, "G"'] \arrow[dr, "H_0"] & \\
& X_0(a,b,c;\mathfrak{p}) \arrow[dl] \\
\mathbb{P}^1 &
\end{tikzcd}$$

We first compute the index $[G : H_0]$, which corresponds to the degree of the cover $X_0(a,b,c;\mathfrak{p}) \to \mathbb{P}^1$. If $G = \mathrm{PGL}_2(\mathbb{F}_q)$, up to multiplication by a scalar matrix, 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 $[G : H_0] = q+1$. When q is even, we have an isomorphism $\mathrm{PSL}_2(\mathbb{F}_q) \simeq \mathrm{PGL}_2(\mathbb{F}_q)$, so the index $[G : H_0]$ is the same as above. Finally, if $G = \mathrm{PSL}_2(\mathbb{F}_q)$ with q odd, then representatives can be chosen to have 1 on the first entry of the matrix as above. Also, the upper triangular matrices are defined up to multiplication by -1. Hence $\#H_0 = \frac{1}{2}q(q-1)$ and $[G : H_0] = q+1$.

Via the projection of the first column of the matrix to $\mathbb{P}^1(\mathbb{F}_q)$, the set of cosets G/H_0 is naturally in bijection with $\mathbb{P}^1(\mathbb{F}_q)$. With this bijection, the action of $\pi_{\mathfrak{p}}(\Delta)$ on G/H_0 becomes simply matrix multiplication. 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. Recall we write PXL_2 for either PSL_2 or PGL_2.

Lemma 4.1. *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 note that each class in G is represented by matrices that are diagonalizable over $\mathbb{F}_q$, diagonalizable only over $\mathbb{F}_{q^2}$, or not diagonalizable. We prove the Lemma 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 $\overline{\sigma}_s$ 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 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 $(q-1)/s$ 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 over $\mathbb{F}_q^2$. This happens if and only if $s = p$. In this case, we have

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

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 $\mathbb{F}_{q^2}$. Let $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be the roots of this polynomial. Then σ_s is conjugate with the diagonal matrix $[\alpha_1, \alpha_2]$ with $\sigma_s = T^{-1}[\alpha_1, \alpha_2]T$ for some invertible matrix T. For all $m \in \mathbb{N}$ such that $\overline{\sigma}_s^m$ fixes $(x : y)^t \in \mathbb{P}^1(\mathbb{F}_q)$, we have that

$$\begin{pmatrix}\alpha_1^m & 0\\ 0 & \alpha_2^m\end{pmatrix}\left(T\begin{pmatrix}x\\ :\\ y\end{pmatrix}\right) = \left(T\begin{pmatrix}x\\ :\\ y\end{pmatrix}\right).$$

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).

Example 4.2. 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.

The following lemma partially solves this problem.

Lemma 4.3. *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 the 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 $\mathrm{PSL}_2(\mathbb{F}_q)$. Pick a lift $\sigma_2 \in \mathrm{SL}_2(\mathbb{F}_q)$ of $\overline{\sigma}_2$. Because σ_2^4 is the identity, its characteristic polynomial must be a quadratic polynomial dividing $x^4 - 1$. In addition, the constant of this polynomial must be 1 since this is the determinant of σ_2. The only possibility for such a polynomial is $x^2 + 1$. 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 4.1. 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 $\lfloor 3/2 \rceil = 1$.

Theorem 4.4. *Let (a, b, c) be a hyperbolic admissible triple and $\mathfrak{p}$ be a prime of E above a rational prime p. Then the genus of $X_0(a, b, c; \mathfrak{p})$ is given by*

$$g(X_0(a, b, c; \mathfrak{p})) = -q + \frac{1}{2}\sum_{s \in \{a,b,c\}} \left\lfloor \frac{q}{s} \right\rceil (s-1) + \epsilon(a, b, c; \mathfrak{p}) \tag{4.5}$$

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 4.3 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 $\sigma_a\sigma_b\sigma_c = 1$. We recall that the map $X_0(a,b,c;\mathfrak{p}) \to X(1)$ has degree $q+1$ since $[G : H_0] = q+1$. The Riemann–Hurwitz formula implies

$$2g-2 = -2(q+1) + \epsilon_a + \epsilon_b + \epsilon_c, \tag{4.6}$$

where ϵ_s is the ramification index at the points that ramify. We can compute ϵ_s from Lemma 4.1 and Lemma 4.3, with $\epsilon_s = k_s(s-1)$, where

$$k_s = \begin{cases} (q-1)/s, & \text{if } s \mid (q-1); \\ q/s, & \text{if } s \mid q; \\ (q+1)/s & \text{if } s \mid (q+1); \end{cases} \tag{4.7}$$

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. □

Remark 4.8. Instead of using parity, in the $\mathrm{PGL}_2(\mathbb{F}_q)$ and q odd 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 $\overline{\sigma}_2\overline{\sigma}_b\overline{\sigma}_c = 1$. We can then decide if $\overline{\sigma}_2$ is split or non-split and use Lemma 4.1 to compute the ramification.

Algorithm. We present an implementation of Theorem 4.4.

Algorithm 4.9. 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 $X_0(a,b,c;\mathfrak{p})$ and the Galois group $G_{\mathfrak{p}}$ of the cover $X(a,b,c;\mathfrak{p}) \to \mathbb{P}^1$.

1. Compute the residue field of $\mathfrak{p}$ and set $q := \#\mathbb{F}_{\mathfrak{p}}$.
2. Compute the residue field $\mathbb{Z}_F/\mathfrak{p}_F$, where $\mathfrak{p}_F$ is a prime of $F(a,b,c)$ above $\mathfrak{p}$. If $\mathbb{F}_q \simeq \mathbb{Z}_F/\mathfrak{p}_F$, then $G = \mathrm{PSL}_2(\mathbb{F}_q)$. Otherwise set $G = \mathrm{PGL}_2(\mathbb{F}_q)$.
3. Compute g using Theorem 4.4.

Proof of correctness. Correctness follows from the formula in Theorem 4.4. Steps 1 and 2 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 5.1. □

Bounding the genus. Our goal remains to show that, for fixed genus g_0, there are finitely many admissible 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.

In the prime case, the notion of admissible ideal can be turned around, as follows.

Definition 4.10. Let $q := p^r$ be a power of a prime number p. A hyperbolic triple (a,b,c) is q-admissible 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 4.11. *For any triangular modular curve $X_0(a,b,c;\mathfrak{p})$ with $q := \mathrm{Nm}\,\mathfrak{p}$ and $\mathfrak{p}$ admissible for (a,b,c), the triple (a,b,c) is q-admissible.*

Proof. As shown in the proof of Lemma 4.1, the order of every element in $\mathrm{PXL}_2(\mathbb{F}_q)$ needs to divide one of $\{q-1, p, q+1\}$. □

Proposition 4.12. *Let g be the genus of the triangular modular curve $X_0(a,b,c;\mathfrak{p})$ and set $q := \mathbb{Z}_E/\mathfrak{p}$. Then,*

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

Proof. Let $s^\sharp$ be the order of $\pi_{\mathfrak{p}}(\delta_s)$. The cases where $(a^\sharp, b^\sharp, c^\sharp)$ is not hyperbolic are handled in Proposition 3.13: we get $g = 0$, and the inequality holds. So we may suppose without loss of generality that $s^\sharp = s$ for $s = \{a, b, c\}$, and still that (a, b, c) is hyperbolic.

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 4.1, we have that for $s \in \{a, b, c\}$,

$$(q-1) - \frac{q-1}{s} = \frac{(s-1)(q-1)}{s} \leq \epsilon_s \leq \frac{(s-1)(q+1)}{s} = (q+1) - \frac{q+1}{s}. \tag{4.13}$$

Because of these bounds and (4.6),

$$\begin{aligned} g(X_0(a,b,c;\mathfrak{p})) &\geq -(q+1) + \frac{(a-1)(q-1)}{2a} + \frac{(b-1)(q-1)}{2b} + \frac{(c-1)(q-1)}{2c} + 1 \\ &= (q-1)\left(-1 + \frac{3}{2} - \frac{1}{2a} - \frac{1}{2b} - \frac{1}{2c}\right) - 1 \qquad (4.14)\\ &= \frac{q-1}{2}\,|\chi(a,b,c)| - 1, \end{aligned}$$

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

Corollary 4.15. *For a fixed genus $g_0 \in \mathbb{Z}_{\geq 0}$, there are only finitely many hyperbolic triples (a, b, c) and admissible primes $\mathfrak{p}$ such that the curves $X_0(a, b, c; \mathfrak{p})$ have genus $g \leq g_0$.*

Proof. By Proposition 4.12, 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 $s \leq q + 1$ for all $s \in \{a, b, c\}$. This leaves only finitely many possibilities. □

Remark 4.16. To make computations more efficient, we can consider 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

$$q \leq \frac{2(g_0+1)}{|\chi(a,b,c)|} + 1. \tag{4.17}$$

This inequality also shows that

$$0 < |\chi(a,b,c)| \leq \frac{2(g_0+1)}{q-1}. \tag{4.18}$$

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

5. Enumerating curves of low genus

We present the main algorithms that use the theory developed in section 4. The goal of this section is to effectively enumerate the curves $X_0(a, b, c; \mathfrak{p})$ of bounded genus. The number of curves is finite from Corollary 4.15. As explained in section 2, if $\mathfrak{p}$ is admissible, then G is given by $\mathrm{PXL}_2(\mathbb{F}_q)$. The first condition (coprimality) in admissibility can be expensive to check, so we first check the easier necessary (but not sufficient) condition that $\mathfrak{p} \nmid \beta(a, b, c)$.

Algorithm 5.1. Let (a, b, c) be a hyperbolic triple and p be a prime number. This algorithm returns `true` if there exists a prime $\mathfrak{p} \subseteq \mathbb{Z}_{E(a,b,c)}$ above p such that $\mathfrak{p} \nmid \beta(a, b, c)$.

```
1. If $p \nmid 2abc$, then return true.
2. Find $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_q$, where $\mathfrak{p}$ is any prime of $E$ above $p$.
```

3. Set $m := \operatorname{lcm}(a,b,c)$. Construct $\mathbb{F}_q(\zeta_{2m})$. Set $z := \zeta_{2m}$.
4. For every $i \in (\mathbb{Z}/2m\mathbb{Z})^\times$, and set $l_{2s} := z^{im/s} + 1/z^{im/s}$ 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. Let $\mathfrak{p}$ be a prime of $\mathbb{Z}_{E(a,b,c)}$ above p. If $p \nmid 2abc$ then $\mathfrak{p} \nmid \beta(a,b,c)$ [3, Lemma 5.5]. When $\mathfrak{p} \mid abc$, checking that $\mathfrak{p}$ does not divide $\beta(a,b,c)$ is more involved. We do this in steps 2 to 4 by computing β in the residue field of $\mathfrak{p}$. This computation is independent of the prime $\mathfrak{p}$ chosen above p because E is Galois over $\mathbb{Q}$. □

Now we are ready to present the main algorithm that ties the results of section 4 into an explicit enumeration.

Algorithm 5.2. Returns a list `lowGenus` of all hyperbolic triples $(a,b,c) \in \mathbb{Z}^3_{\geq 2}$ and norms of prime ideals $\mathfrak{p}$ of $E(a,b,c)$ that are admissible such that the genus of $X_0(a,b,c;\mathfrak{p})$ is at most g_0.

1. Loop over the list of possible powers $q = p^r$, where p is a prime number and $q \leq 84(g_0+1)+1$.
2. For each q from step 1, find all q-admissible hyperbolic triples (a,b,c) (as in Definition 4.10).
3. For each q-admissible triple (a,b,c) from step 2, check if $\chi(a,b,c)$ satisfies (4.18) and if $\mathfrak{p}$ does not divide $\beta(a,b,c)$ using Algorithm 5.1. If yes, compute the candidate genus g of $X_0(a,b,c;\mathfrak{p})$ using Algorithm 4.9.
4. If $g \leq g_0$, check that $\mathfrak{p} \nmid \operatorname{discrd}(\Lambda)\mathfrak{d}_{F|E}$. If yes, add $(a,b,c;q)$ to the list `lowGenus`.

Proof of correctness. For step 1, see Proposition 4.12. Every hyperbolic q-admissible triple gives rise to one such curve. The correctness of the rest of the algorithm follows from the work done in section 4. □

We list the CPU time (in seconds) for our implementation to compute the list of curves $X_0(a,b,c;\mathfrak{p})$ of genus up to bounds 0, 1, and 2 on a standard laptop:

Genus bound	0	1	2
Time (s)	1.7	9.7	1110.3

6. Triangular modular curves $X_1(a,b,c;\mathfrak{p})$

In this section, we use section 4 to give analogous results for triangular modular curves $X_1(a,b,c;\mathfrak{p})$, completing the proof of our main result.

We recall that $X_1(a,b,c;\mathfrak{p})$ is defined in (3.18) as the quotient of $\mathcal{H}$ by $\Gamma_1(a,b,c;\mathfrak{p})$.

Corollary 6.1. *For any integer $g_0 \geq 0$, there are finitely many triangular modular curves $X_1(a,b,c;\mathfrak{p})$ with $\mathfrak{p}$ admissible.*

Proof. For every triple $(a,b,c) \in (\mathbb{Z}_{\geq 2} \cup \{\infty\})^3$ and prime ideal $\mathfrak{p}$ of $E(a,b,c)$, there is a cover $X_1(a,b,c;\mathfrak{p}) \to X_0(a,b,c;\mathfrak{p})$. All curves $X_1(a,b,c;\mathfrak{p})$ of genus bounded above by g_0 cover curves $X_0(a,b,c;\mathfrak{p})$ of genus bounded above by g_0. Because of Corollary 4.15, there are finitely many admissible triples (a,b,c) and prime ideals $\mathfrak{p}$ that give rise to curves $X_0(a,b,c;\mathfrak{p})$ of genus bounded above by g_0. □

We now focus on explicitly enumerating all curves of bounded genus. The goal first is to prove group-theoretic results that describe the degree and ramification of the cover $X_1(\mathfrak{p}) \to X(1)$. We describe the structure of the quotient $\mathrm{PXL}_2(\mathbb{F}_q)$ modulo $H_{1,\mathfrak{p}}$ and then describe the action of $\pi_{\mathfrak{p}}(\delta_s)$ on this quotient. The main difference with section 4 is that the quotient $G/H_{0,\mathfrak{p}}$ does not depend on G being isomorphic to $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$, whereas the structure of $G/H_{1,\mathfrak{p}}$ depends on the choice of G. Let $H_1 := H_{1,\mathfrak{p}}$.

Lemma 6.2. *Let $G = \mathrm{PXL}_2(\mathbb{F}_q)$, where $\mathbb{F}_q := \mathbb{Z}_E/\mathfrak{p}$. The quotient G/H_1 can be described as follows.*

(i) *If $G = \mathrm{PSL}_2(\mathbb{F}_q)$, then $G/H_1 \simeq (\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\langle \pm 1\rangle$: explicitly, the class of $(x,z) \in \mathbb{F}_q \times \mathbb{F}_q$ maps to the coset of $\begin{pmatrix} x & y \\ z & w\end{pmatrix}$, where $y, w \in \mathbb{F}_q$ satisfy $xw - yz = 1$.*

(ii) *If $G = \mathrm{PGL}_2(\mathbb{F}_q)$, then $G/H_1 \simeq (\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\langle \pm 1\rangle \times \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$: explicitly, for $\mu \in \mathbb{F}_q^\times \smallsetminus \mathbb{F}_q^{\times 2}$ the class of $((x,y),u) \in (\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\}) \times \mathbb{F}_q^\times$ maps to the coset of $\begin{pmatrix} x & y \\ z & w\end{pmatrix}$, where $z, w \in \mathbb{F}_q$ satisfy $xw - yz = 1$ if u is a square and $xw - yz = \mu$ otherwise.*

Proof. Let $G = \mathrm{PSL}_2(\mathbb{F}_q)$ with q odd. Because $\#H_1 = \#\mathbb{F}_q$, we have that $[G : H_1] = (q^2-1)/2$. The coset representatives of G/H_1 can be parameterized by $(x,z) \in (\mathbb{F}_q \times \mathbb{F}_q)/\langle \pm 1\rangle$. 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 $\alpha \in \mathbb{F}_q$ such that

$$\pm\begin{pmatrix} x & y \\ z & w\end{pmatrix}\begin{pmatrix} 1 & \alpha \\ 0 & 1\end{pmatrix} = \pm\begin{pmatrix} x & x\alpha + y \\ z & z\alpha + w\end{pmatrix} = \begin{pmatrix} x' & y' \\ z' & w'\end{pmatrix},$$

which is the case if and only if $(x,z) = \pm(x',z')$. Thus, the map $(\mathbb{F}_q \times \mathbb{F}_q)/\langle \pm 1\rangle \to G/H_1$ defined by the parametrization is a well-defined, injective homomorphism. By a cardinality comparison it follows that it is an isomorphism.

Now we let $G = \mathrm{PGL}_2(\mathbb{F}_q)$, so $[G : H_1] = q^2 - 1$. We claim that 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 $\mu \in \mathbb{F}_q^\times \smallsetminus \mathbb{F}_q^{\times 2}$. For any $\pm(x,z) \in (\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\langle \pm 1\rangle$, and any $u \in \{1, \mu\} \simeq \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$, we choose values of $y, w \in \mathbb{F}_q$ such that $xw - yz = u$ and map $\pm(x,z)$ to the class of the matrix $\begin{pmatrix} x & y \\ z & w\end{pmatrix}$ in $\mathrm{PGL}_2(\mathbb{F}_q)$. Given two different choices $y, w \in \mathbb{F}_q$ and $y', w' \in \mathbb{F}_q$, if $x \neq 0$, then

$$\pm\begin{pmatrix} x & y \\ z & w\end{pmatrix} = \begin{pmatrix} x & y' \\ z & w'\end{pmatrix}\begin{pmatrix} 1 & x^{-1}(y-y') \\ 0 & 1\end{pmatrix}.$$

If $x = 0$, then $z \neq 0$ and $0 \neq u = yz = y'z$. Thus, $y = y'$. Also,

$$\pm\begin{pmatrix} 0 & y \\ z & w\end{pmatrix} = \begin{pmatrix} 0 & y \\ z & w'\end{pmatrix}\begin{pmatrix} 1 & z^{-1}(w-w') \\ 0 & 1\end{pmatrix}.$$

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 a 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. Since the cardinalities of the domain and range are equal, we conclude that this is an isomorphism. □

We proceed to describe the ramification of the cover $X_1(a,b,c;\mathfrak{p}) \to \mathbb{P}^1$. This lemma is similar to Lemma 4.1. The main difference is that in certain cases there are more fixed points than strictly necessary.

Lemma 6.3. *Let $\overline{\sigma}_s \in G = \mathrm{PXL}_2(\mathbb{F}_q)$ and assume that the order of $\overline{\sigma}_s$ is s. The structure of the action of $\overline{\sigma}_s$ on G/H_1 is as follows:*

(i) *if σ_s is semisimple, then there are (no fixed points and) $\frac{[G:H_1]}{s}$ 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 $(q-1)/2$ fixed points and $(q^2-q)/(2p)$ orbits of length p,*
  (b) *otherwise, there are $q-1$ fixed points and $(q^2-q)/p$ orbits of length p.*

Proof. We use the description of the quotient G/H_1 given in Lemma 6.2. Let σ_s be any element of $\mathrm{GL}_2(\mathbb{F}_q)$ that maps to $\overline{\sigma}_s$ in the quotient to G.

If σ_s is split semisimple, then it is conjugate over $\mathbb{F}_q$ to a diagonal matrix with entries u, v. Because the order of $\overline{\sigma}_s$ is s, then s is the order of uv^{-1}. We pick a class in the quotient G/H_1 represented by a matrix M. If the class of M is fixed by the action of $\overline{\sigma}_s$, then the first column of M is, up to multiplication by ± 1, fixed by multiplication by the diagonal matrix. This implies that $(u,v) = \pm(1,1)$, contradicting that $s \geq 2$. Thus, there are no fixed points of the action of $\overline{\sigma}_s$ on G/H_1. A similar argument shows that orbits of elements that are not fixed cannot have length less than s. Thus, every element belongs to an orbit of 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 $\sigma_s = T^{-1}[\alpha_1, \alpha_2]T$ in this extension. If σ_s^r fixes an element for $r \geq 1$, then we have

$$\pm \begin{pmatrix} \alpha_1^r & 0 \\ 0 & \alpha_2^r \end{pmatrix} T \begin{pmatrix} x & y \\ z & w \end{pmatrix} = T \begin{pmatrix} x & y' \\ z & w' \end{pmatrix}.$$

Multiplication by T does not change the equality in G/H_1. Thus, we are back to the split semisimple case and the orbits of the action of $\overline{\sigma}_s$ all 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,

$$\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x+uz & y+uw \\ z & w \end{pmatrix},$$

so the class of this matrix in G/H_1 is fixed by multiplication by σ_s if and only if $uz = 0$. Since $s \geq 2$, then z must be 0. We note that if $z \neq 0$, then the orbit of the element has length p. In $G = \mathrm{PSL}_2(\mathbb{F}_q)$ there are $(q-1)/2$ representatives for which $z = 0$, i.e. fixed points. Similarly, if $G = \mathrm{PGL}_2(\mathbb{F}_q)$, then there are $q-1$ fixed points. □

Corollary 6.4. *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. Then the genus of $X_1(a,b,c;\mathfrak{p})$ is given by*

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

where

$$k_s = \begin{cases} (q^2-q)/(2p), & \textit{if } s = p \textit{ and } G = \mathrm{PSL}_2(\mathbb{F}_q); \\ (q^2-q)/p, & \textit{if } s = p \textit{ and } G = \mathrm{PGL}_2(\mathbb{F}_q); \\ (q^2-1)/s, & \textit{if } s \neq p \textit{ and } G = \mathrm{PGL}_2(\mathbb{F}_q); \textit{and} \\ (q^2-1)/(2s), & \textit{if } s \neq p \textit{ and } q \textit{ is odd and } G = \mathrm{PSL}_2(\mathbb{F}_q). \end{cases}$$

Proof. This formula is given by using the Riemann-Hurwitz formula on $X_1(\mathfrak{p}) \to \mathbb{P}^1$ and Lemma 6.3. □

Now we are ready to present an algorithm that enumerates all curves $X_1(a,b,c;\mathfrak{p})$.

Algorithm 6.5. Returns a list `lowGenusX1` of all hyperbolic triples (a,b,c) and admissible ideals $\mathfrak{p}$ such that the genus of $X_1(a,b,c;\mathfrak{p})$ is $g \leq g_0$.

1. Loop over all hyperbolic triples (a,b,c) and prime ideals $\mathfrak{p}$ such that $X_0(a,b,c;\mathfrak{p})$ has genus bounded above by g_0. This list can be obtained from Algorithm 5.2.
2. For each triple (a,b,c) and ideal $\mathfrak{p}$ of the previous step, compute the genus g of $X_1(a,b,c;\mathfrak{p})$ with Corollary 6.4. If $g \leq g_0$, then add $(a,b,c;\mathfrak{p})$ to the list `lowGenusX1`.

Proof of correctness. For all triples (a,b,c) and prime ideals $\mathfrak{p}$ there are maps $X_1(a,b,c;\mathfrak{p}) \to X_0(a,b,c;\mathfrak{p})$. Thus, the only curves $X_1(a,b,c;\mathfrak{p})$ that can have genus $g \leq g_0$ must be covering curves $X_0(a,b,c;\mathfrak{p})$ of genus bounded above by g_0. □

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

Proof of Theorem 1.9. By Corollary 4.15, there are only finitely many curves $X_0(a,b,c;\mathfrak{p})$ with nontrivial admissible prime level $\mathfrak{p}$ and genus $g \leq g_0$. Since every curve $X_1(a,b,c;\mathfrak{p})$ covers $X_0(a,b,c;\mathfrak{p})$, the same is true for $X_1(a,b,c;\mathfrak{p})$ (see Corollary 6.1).

For the computation, we run Algorithm 5.2 with $g_0 = 2$, adding extra cases according to Proposition 3.13. To finish, we run Algorithm 6.5. The implementation of this computation can be found in our Magma code [26]. □

Appendix A. Tables

We present tables of all hyperbolic triples (a, b, c) and admissible primes $\mathfrak{p}$ such that the curve $X_0(a, b, c; \mathfrak{p})$ has genus 0 or 1. The list with additional data is available online [26].

To record $\mathfrak{p}$, we list the prime number p below $\mathfrak{p}$. We describe the group $G = \mathrm{PXL}_2(\mathbb{F}_q)$ by presenting q and writing 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 $E(a, b, c)$ and the number of different prime ideals of E above p.

Nugent–Voight [16] define an invariant, the arithmetic dimension $\operatorname{adim}(a, b, c)$, to be the dimension of a quaternionic Shimura variety attached to $\Delta(a, b, c)$ given by the number of split real places of $E(a, b, c)$ of the quaternion algebra $A = E\langle\Delta^{(2)}\rangle$. In particular, the triangle group $\Delta(a, b, c)$ is arithmetic if and only if $\operatorname{adim}(a, b, c) = 1$.

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 [23]. 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. We record this by adding (1) to the arithmetic dimension entry on the table.

For the arithmetic triangle groups $\Delta(a, b, c)$ such that $\Delta \simeq \Lambda^1$, the corresponding list of curves is contained in [25, Tables 4.1–4.7]. We confirmed that the intersection is in agreement.

Finally, for noncocompact triples see Proposition 3.13.

Genus 0, $X_0(a,b,c;\mathfrak{p})$**.**

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

Genus 1, $X_0(a,b,c;\mathfrak{p})$. This long table is split into three tables (over the next three pages).

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

$\vdots$

(a,b,c)	p	q	**PXL**	**adim**	E	# of $\mathfrak{p}$
$(2,4,5)$	19	19	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,4,5)$	29	29	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,4,5)$	31	31	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,4,5)$	7	49	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(2,4,5)$	61	61	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,4,6)$	11	11	-1	1	$\mathbb{Q}$	1
$(2,4,6)$	17	17	-1	1	$\mathbb{Q}$	1
$(2,4,6)$	19	19	-1	1	$\mathbb{Q}$	1
$(2,4,6)$	29	29	-1	1	$\mathbb{Q}$	1
$(2,4,6)$	31	31	-1	1	$\mathbb{Q}$	1
$(2,4,6)$	37	37	-1	1	$\mathbb{Q}$	1
$(2,4,7)$	7	7	1	1	$\mathbb{Q}(\lambda_7)$	1
$(2,4,7)$	13	13	-1	1	$\mathbb{Q}(\lambda_7)$	3
$(2,4,7)$	29	29	-1	1	$\mathbb{Q}(\lambda_7)$	3
$(2,4,8)$	7	7	-1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2,4,8)$	5	25	-1	1	$\mathbb{Q}(\sqrt{8})$	1
$(2,4,9)$	17	17	1	2	$\mathbb{Q}(\lambda_9)$	3
$(2,4,9)$	19	19	-1	2	$\mathbb{Q}(\lambda_9)$	3
$(2,4,10)$	3	9	-1	1	$\mathbb{Q}(\sqrt{5})$	1
$(2,4,10)$	11	11	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,4,11)$	11	11	-1	2 (1)	$\mathbb{Q}(\lambda_5)$	1
$(2,4,12)$	5	25	1	1	$\mathbb{Q}(\sqrt{12})$	1
$(2,4,13)$	13	13	-1	3 (1)	$\mathbb{Q}(\lambda_{13})$	1
$(2,4,14)$	13	13	-1	2	$\mathbb{Q}(\lambda_7)$	3
$(2,4,16)$	17	17	-1	2	$\mathbb{Q}(\lambda_{16})$	4
$(2,4,17)$	17	17	1	4 (1)	$\mathbb{Q}(\lambda_{17})$	1
$(2,5,5)$	3	9	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(2,5,5)$	31	31	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,5,5)$	41	41	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,5,6)$	5	5	-1	1	$\mathbb{Q}(\sqrt{5})$	1
$(2,5,6)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,5,6)$	19	19	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,5,6)$	31	31	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,5,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{2},\sqrt{5})$	2
$(2,5,11)$	11	11	1	4 (2)	$\mathbb{Q}(\sqrt{5},\lambda_{11})$	2
$(2,5,12)$	11	11	-1	2	$\mathbb{Q}(\sqrt{3},\sqrt{5})$	4
$(2,5,15)$	2	16	1	2	$\mathbb{Q}(\lambda_{15})$	1
$(2,6,6)$	5	5	-1	1	$\mathbb{Q}$	1
$(2,6,6)$	19	19	-1	1	$\mathbb{Q}$	1
$(2,6,7)$	13	13	1	2	$\mathbb{Q}(\lambda_7)$	3
$(2,6,8)$	7	7	-1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2,6,9)$	19	19	-1	2	$\mathbb{Q}(\lambda_9)$	3

$\vdots$

$(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c})$	$\boldsymbol{p}$	$\boldsymbol{q}$	**PXL**	**adim**	$\boldsymbol{E}$	# of $\mathfrak{p}$
$(2,6,10)$	11	11	-1	2	$\mathbb{Q}(\sqrt{5})$	2
$(2,6,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$	2
$(2,6,13)$	13	13	1	4 (1)	$\mathbb{Q}(\lambda_{13})$	1
$(2,7,7)$	7	7	1	1	$\mathbb{Q}(\lambda_7)$	1
$(2,7,8)$	7	7	-1	2	$\mathbb{Q}(\sqrt{2},\lambda_7)$	2
$(2,7,9)$	2	8	1	3	$\mathbb{Q}(\lambda_7,\lambda_9)$	3
$(2,8,8)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2,8,10)$	3	9	-1	3	$\mathbb{Q}(\sqrt{2},\sqrt{5})$	2
$(2,10,10)$	11	11	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,10,11)$	11	11	-1	6 (2)	$\mathbb{Q}(\sqrt{5},\lambda_{11})$	2
$(2,12,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$	2
$(3,3,4)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$	2
$(3,3,4)$	31	31	1	1	$\mathbb{Q}(\sqrt{8})$	2
$(3,3,5)$	3	9	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(3,3,5)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(3,3,5)$	19	19	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(3,3,5)$	31	31	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(3,3,6)$	5	25	1	1	$\mathbb{Q}(\sqrt{12})$	1
$(3,3,7)$	2	8	1	1	$\mathbb{Q}(\lambda_7)$	1
$(3,3,7)$	13	13	1	1	$\mathbb{Q}(\lambda_7)$	3
$(3,3,9)$	19	19	1	1	$\mathbb{Q}(\lambda_9)$	3
$(3,3,15)$	2	16	1	1	$\mathbb{Q}(\lambda_{15})$	1
$(3,4,4)$	7	7	1	1	$\mathbb{Q}$	1
$(3,4,4)$	17	17	1	1	$\mathbb{Q}$	1
$(3,4,5)$	3	9	1	2	$\mathbb{Q}(\sqrt{5},\sqrt{8})$	2
$(3,4,6)$	5	5	-1	1	$\mathbb{Q}(\sqrt{24})$	2
$(3,4,7)$	7	7	1	2	$\mathbb{Q}(\sqrt{2},\lambda_7)$	2
$(3,4,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{3})$	2
$(3,5,5)$	2	4	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(3,5,5)$	5	5	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(3,5,5)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(3,6,6)$	13	13	1	1	$\mathbb{Q}$	1
$(3,6,8)$	7	7	-1	3	4.4.18432.1	4
$(3,7,7)$	7	7	1	2 (1)	$\mathbb{Q}(\lambda_7)$	1
$(3,7,7)$	2	8	1	2 (1)	$\mathbb{Q}(\lambda_7)$	1
$(4,4,4)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$	2
$(4,4,5)$	3	9	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(4,4,6)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$	2
$(4,5,6)$	5	5	-1	2	$\mathbb{Q}(\sqrt{5},\sqrt{24})$	2
$(4,6,6)$	7	7	-1	1	$\mathbb{Q}(\sqrt{8})$	2
$(4,8,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{2})$	1
$(5,5,5)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(7,7,7)$	2	8	1	1	$\mathbb{Q}(\lambda_7)$	1

References

[1] Natália Archinard, *Hypergeometric abelian varieties.* Canad. J. Math. **55** (2003), no. 5, 897–932. ↑4.

[2] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), vol. 3–4, 235–265. ↑3, 12.

[3] Pete L. Clark and John Voight, *Algebraic curves uniformized by congruence subgroups of triangle groups.* Trans. Amer. Math. Soc. **371** (2019), no. 1, 33–82. ↑1, 2, 3, 5, 6, 7, 8, 10, 11, 17.

[4] C. Herbert Clemens, *A scrapbook of complex curve theory*, 2nd. ed. Graduate Studies in Mathematics, vol. 55. Amer. Math. Soc., Providence, RI, 2003. ↑4.

[5] Paula Cohen and Jürgen Wolfart, *Modular embeddings for some nonarithmetic Fuchsian groups.* Acta Arith. **56** (1990), no. 2, 93–110. ↑4.

[6] David A. Cox and Walter R. Parry, *Genera of congruence subgroups in $\mathbb{Q}$-quaternion algebras.* J. Reine Angew. Math. **351** (1984), 66–112. ↑4.

[7] Chris J. Cummins and Sebastian Pauli, *Congruence subgroups of* $\mathrm{PSL}(2,\mathbb{Z})$ *of genus less than or equal to 24.* Experiment. Math. **12** (2003), no. 2, 243–255. ↑1.

[8] Henri Darmon, *A fourteenth lecture on Fermat's last theorem.* Number theory, 103–115, CRM Proc. Lecture Notes, vol. 36, Amer. Math. Soc., Providence, RI, 2004. ↑4.

[9] Robert Fricke, *Die elliptischen Funktionen und ihre Anwendungen. Zweiter Teil. Die algebraischen Ausführungen. (German)* Reprint of the 1922 original. Springer, Heidelberg, 2011. ↑1.

[10] 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** (2014), no. 1, 379–430. ↑4.

[11] Robert Kucharczyk and John Voight, *Hypergeometric functions and Shimura varieties*, unpublished, 2022. ↑4.

[12] Darren D. Long, Colin Maclachlan, and Alan W. Reid, *Arithmetic Fuchsian groups of genus zero.* Pure Appl. Math. Q. **2** (2006), no. 2, 569–599. ↑1.

[13] Alexander M. Macbeath, *Generators of the linear fractional groups.* 1969 Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967), 14-32. Amer. Math. Soc., Providence, RI. ↑3.

[14] Colin Maclachlan and Alan W. Reid, *The arithmetic of hyperbolic 3-manifolds.* Graduate Texts in Mathematics, 219. Springer-Verlag, New York, 2003. xiv+463 pp. ISBN: 0-387-98386-4 (Reviewer: Kerry N. Jones). ↑6.

[15] Barry Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld).* Invent. Math. **44** (1978), no. 2, 129–162. ↑1.

[16] Steve Nugent and John Voight, *On the arithmetic dimension of triangle groups.* Math. Comp. **86** (2017), no. 306, 1979–2004. ↑21.

[17] Andrew P. Ogg, *Rational points on certain elliptic modular curves.* Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972), 221–231. Amer. Math. Soc., Providence, RI, 1973. ↑1.

[18] Andrew P. Ogg, *Hyperelliptic modular curves.* Bull. Soc. Math. France **102** (1974), 449–462. ↑1.

[19] Andrew P. Ogg, *Diophantine equations and modular forms.* Bull. Amer. Math. Soc. **81** (1975), 14–27. ↑1.

[20] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$*, 2021, `arXiv:2106.11141`. ↑1.

[21] Kisao Takeuchi, *On some discrete subgroups of* $\mathrm{SL}_2(\mathbb{R})$, J. Fac. Sci. Univ. Tokyo Sect. I **16** (1969), 97–100. ↑6.

[22] Kisao Takeuchi, *Commensurability classes of arithmetic triangle groups.* J. Fac. Sci. Univ. Tokyo Sect. IA Math. **24** (1977), no. 1, 201–212. ↑4, 6.

[23] Kisao Takeuchi, *Arithmetic triangle groups.* J. Math. Soc. Japan **29** (1977), no. 1, 91–106. ↑4, 21.

[24] John G. Thompson, *A finiteness theorem for subgroups of* $\mathrm{PSL}(2,\mathbf{R})$ *which are commensurable with* $\mathrm{PSL}(2,\mathbf{Z})$. The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), 533–555, Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., Providence, R.I., 1980. ↑4.

[25] John Voight, *Shimura curves of genus at most two.* Math. Comp. **78** (2009), no. 266, 1155–1172. ↑1, 21.

[26] Juanita Duque-Rosero and John Voight, *Enumerating triangular modular curves of low genus*, `https://github.com/juanitaduquer/triangularModularCurves.git`, 2022. ↑3, 20, 21.

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