ACTA ARITHMETICA
175.2 (2016)

Congruence covers of triangular modular curves and their Galois groups

by

Luiz Kazuo Takei (Sainte-Anne-de-Bellevue)

0. Introduction. The classical modular group $\mathrm{SL}_2(\mathbb{Z})$ has been extensively studied, especially because of its connection with elliptic curves and Fermat's Last Theorem (cf. [DS05] for a detailed account of that connection). In this article we study a family of Fuchsian groups of which $\mathrm{SL}_2(\mathbb{Z})$ is a particular member, namely the (hyperbolic) triangle groups (denoted $\Gamma_{a,b,c}$). Our motivation is twofold:

- according to Belyĭ's Theorem (cf. [Bel79]), every algebraic curve defined over a number field is uniformized, when viewed as a Riemann surface, by a triangle group;
- more recently, Darmon (cf. [Dar04]) speculated that triangle groups may provide a powerful approach to understand the generalized Fermat equations.

To study the connection between $\mathrm{SL}_2(\mathbb{Z})$ and elliptic curves, one can start with the definition of congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ such as $\Gamma(N)$ and $\Gamma_0(N)$ and their corresponding modular curves $X(N) = \Gamma(N)\backslash\mathcal{H}^*$ and $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$, where $\mathcal{H}^*$ is the union of the Poincaré upper half-plane and the cusps of $\mathrm{SL}_2(\mathbb{Z})$ (cf. [DS05, Chapters 1 and 2]). One is then led to consider maps such as

$$X(N) \to X(1) \cong \mathbb{P}^1,$$

which is a Galois cover. Some natural questions then quickly arise:

(1) What is the Galois group of that cover?
(2) What is the genus of $X(N)$?
(3) What is the genus of $X_0(N)$?

2010 *Mathematics Subject Classification*: Primary 11G18; Secondary 11F06.
Key words and phrases: triangle groups, Galois groups, genus, congruence subgroups, triangular modular curves.
Received 2 March 2015; revised 24 May 2016.
Published online 15 September 2016.

DOI: 10.4064/aa8097-6-2016

Section 1 essentially shows that the notions and questions from the previous paragraph still make sense when $\mathrm{SL}_2(\mathbb{Z})$ is replaced by a triangle group $\Gamma_{a,\infty,\infty}$. In particular, it shows that $\Gamma_{a,\infty,\infty} \subseteq \mathrm{SL}_2(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers of the totally real field $\mathbb{Q}(\zeta_{2a} + \zeta_{2a}^{-1})$. It is then possible to define congruence subgroups $\Gamma_{a,\infty,\infty}(\mathfrak{p})$ and $\Gamma^{(0)}_{a,\infty,\infty}(\mathfrak{p})$ for a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ and their corresponding modular curves $X_{a,\infty,\infty}(\mathfrak{p})$ and $X^{(0)}_{a,\infty,\infty}(\mathfrak{p})$.

The questions above have all been answered in the case of the classical modular group $\mathrm{SL}_2(\mathbb{Z})$ (cf. [DS05, Chapter 3]). When the more general triangle groups are considered, those questions become more challenging and have only been answered in some cases. For instance, Lang–Lim–Tan [LLT00] answered questions (1) and (2) for triangle groups of type $\Gamma_{2,b,\infty}$. The present article follows, for the most part, the approach of Lang–Lim–Tan to answer the above questions for triangle groups of type $\Gamma_{a,\infty,\infty}$. More precisely, questions (1)–(3) are answered respectively by the results below.

Theorem 2.11. *Let $a \geq 3$ be an odd integer and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ lying above $p\mathbb{Z}$ where $p \geq 2$. Moreover, let G denote the Galois group of*

$$\varphi : X_{a,\infty,\infty}(\mathfrak{p}) \to X_{a,\infty,\infty}(1) \cong \mathbb{P}^1.$$

(i) *If $p = 2$, then $G \cong D_{2a}$.*
(ii) *If $p = 3$ and $(2 + \zeta_{2a} + \zeta_{2a}^{-1})^2 - 2 \in \mathfrak{p}$, then $G \cong \mathrm{PSL}_2(\mathbb{F}_5)$.*
(iii) *Otherwise, $G \cong \mathrm{PSL}_2(\mathcal{O}/\mathfrak{p})$.*

Remark. Clark–Voight have done an extensive study of triangle groups. In particular, they indepently proved a result which overlaps with the theorem above (cf. [CV, Theorem 9.1]).

Proposition 3.1. *Suppose a is an odd number and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$ lying above $p\mathbb{Z}$. Suppose also that $p \nmid a$. Then the genus of $X_{a,\infty,\infty}(\mathfrak{p})$ is*

$$1 + \frac{|G|}{2}\left(1 - \frac{2}{p} - \frac{1}{a}\right),$$

where G denotes the Galois group of φ.

Theorem 4.5. *Let $p \neq q$ be prime numbers strictly greater than 2 and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ above $p\mathbb{Z}$. Assume that the Galois group of φ is isomorphic to $\mathrm{PSL}_2(\mathcal{O}/\mathfrak{p})$ (always true when $p \geq 5$ by Theorem 2.11). Then the genus of the curve $X^{(0)}_{q,\infty,\infty}(\mathfrak{p})$ is given by*

$$g = \frac{q-1}{2} \cdot \frac{p^f - \delta}{q} - p^{f-1},$$

where

- *f is the smallest positive integer such that $p^f \equiv \pm 1 \pmod{q}$, and*
- *$\delta \in \{\pm 1\}$ is such that $p^f \equiv \delta \pmod{q}$.*

Finally, we use the formulas above to compute the genera of $X^{(0)}_{q,\infty,\infty}(\mathfrak{p})$ and $X_{q,\infty,\infty}(\mathfrak{p})$ for the first few prime numbers p, q and summarize the results in Section 5.

1. Basic definitions and notation.

Let $a \le b \le c$ be three elements of $\mathbb{Z}_{\ge 2} \cup \{\infty\}$ such that $1/a + 1/b + 1/c < 1$. This condition allows the construction of a hyperbolic triangle with angles π/a, π/b and π/c.

Definition 1.1. A (*hyperbolic*) *triangle group* of type (a, b, c) (or an (a, b, c)-*triangle group*) is a subgroup of $\mathrm{SL}_2(\mathbb{R})$ whose image in $\mathrm{PSL}_2(\mathbb{R})$ is generated by r_1r_2, r_2r_3 and r_3r_1, where r_1, r_2, r_3 are the reflections across the sides of a hyperbolic triangle in the Poincaré upper half-plane with angles $\pi/a, \pi/b, \pi/c$.

Theorem 10.6.4 in [Bea83] says that an (a, b, c)-triangle group is a Fuchsian group of the first kind (cf. [Shi94, Chapter 1] for the basic definitions and results related to those Fuchsian groups). Moreover, for (a, b, c) fixed, [Tak77, Proposition 1] says that an (a, b, c)-triangle group is essentially unique in the sense that it is independent of the particular hyperbolic triangle used in its construction.

In this article, we will restrict our attention to the (a, ∞, ∞)-triangle groups. Furthermore, $\Gamma_{a,\infty,\infty}$ will denote a specific realization of an (a, ∞, ∞)-triangle group: namely, it is the triangle group constructed from the hyperbolic triangle having as sides an arc of the unit circle and the vertical half-lines $x = 0$ and $x = 1$. By the definition of $\Gamma_{a,\infty,\infty}$, it follows that a fundamental domain (for the natural action of $\Gamma_{a,\infty,\infty}$ on the Poincaré upper half-plane $\mathcal{H}$) is given by two copies of that triangle as shown in Figure 1: the original one and its reflection about one of its sides (for instance, the side $x = 1$).

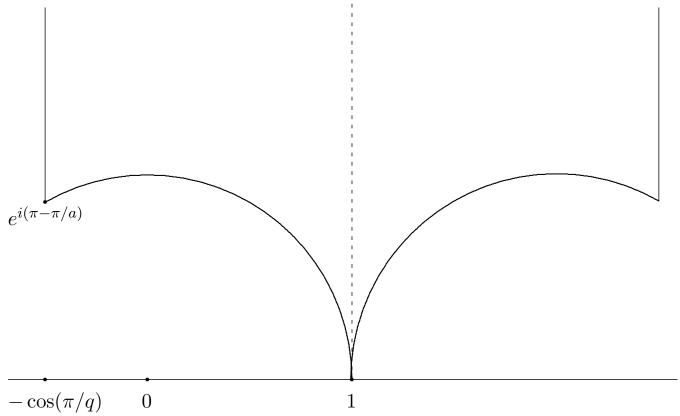

Fig. 1. A fundamental region for $\Gamma_{a,\infty,\infty}$

The two propositions below are now an easy consequence of the previous discussion.

Proposition 1.2. *As a Riemann surface,*

$$\overline{\varGamma_{a,\infty,\infty}}\backslash\mathcal{H}^* \cong \mathbb{P}^1,$$

where $\mathcal{H}^* = \mathcal{H} \cup \{$*cusps of* $\varGamma_{a,\infty,\infty}\}$.

Proposition 1.3. *The group* $\varGamma_{a,\infty,\infty}$ *has* (*up to* $\varGamma_{a,\infty,\infty}$*-equivalence*)

(i) *one elliptic point:* $z_0 = e^{i(\pi-\pi/a)}$;
(ii) *two cusps:* 1 *and* ∞.

From the construction of $\varGamma_{a,\infty,\infty}$ explained above, it follows that $\varGamma_{a,\infty,\infty}$ is the subgroup of $\mathrm{SL}_2(\mathbb{R})$ generated by

$$\gamma_1 = \begin{pmatrix} -2\cos(\pi/a) & -1 \\ 1 & 0 \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}, \quad \gamma_3 = \begin{pmatrix} 1 & 2+2\cos(\pi/a) \\ 0 & 1 \end{pmatrix}.$$

Note that $\varGamma_{a,\infty,\infty}$ is a subgroup of $\mathrm{SL}_2(\mathcal{O})$, where $\mathcal{O} = \mathbb{Z}[\zeta_{2a}+\zeta_{2a}^{-1}]$ is the ring of integers of the maximal real subfield of $\mathbb{Q}(\zeta_{2a})$ and $\zeta_n = \exp(2\pi i/n)$.

Definition 1.4. Given a prime ideal $\mathfrak{p}$ of $\mathcal{O}$, the *congruence subgroups* of $\varGamma_{a,\infty,\infty}$ with level $\mathfrak{p}$ are defined to be

$$\varGamma_{a,\infty,\infty}(\mathfrak{p}) = \left\{ M \in \varGamma_{a,\infty,\infty} \;\middle|\; M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{p}} \right\},$$

$$\varGamma^{(0)}_{a,\infty,\infty}(\mathfrak{p}) = \left\{ M \in \varGamma_{a,\infty,\infty} \;\middle|\; M \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{\mathfrak{p}} \right\}.$$

Remark 1. The classical modular group $\mathrm{SL}_2(\mathbb{Z})$ is also a triangle group (in fact, it is the triangle group $\varGamma_{2,3,\infty}$), and its congruence subgroups as defined above are simply the well known congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. For more details, see [Tak12, Section 2].

Remark 2. Unlike $\mathrm{SL}_2(\mathbb{Z})$, the group $\varGamma_{a,\infty,\infty}$ is not necessarily arithmetic. In fact, $\varGamma_{a,\infty,\infty}$ is arithmetic if and only if $a \in \{2,3\}$ (cf. [Tak77, Theorem 3]).

In analogy with the classical case, the *triangular modular curves* associated to those groups are defined as follows:

$$\begin{aligned} X_{a,\infty,\infty} &:= \varGamma_{a,\infty,\infty}\backslash\mathcal{H}^*, \\ X_{a,\infty,\infty}(\mathfrak{p}) &:= \varGamma_{a,\infty,\infty}(\mathfrak{p})\backslash\mathcal{H}^*, \\ X^{(0)}_{a,\infty,\infty}(\mathfrak{p}) &:= \varGamma^{(0)}_{a,\infty,\infty}(\mathfrak{p})\backslash\mathcal{H}^*. \end{aligned} \tag{1}$$

As mentioned in the introduction, one of the goals of this article is the computation of the Galois group of the cover

$$\varphi : X_{a,\infty,\infty}(\mathfrak{p}) \to X_{a,\infty,\infty}.$$

Throughout this article, the following notation will be used:

$$\lambda_a = \zeta_{2a} + \zeta_{2a}^{-1} \quad \text{and} \quad \mu_a = 2 + \lambda_a,$$

so that

$$\gamma_1 = \begin{pmatrix} -\lambda_a & -1 \\ 1 & 0 \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}, \quad \gamma_3 = \begin{pmatrix} 1 & \mu_a \\ 0 & 1 \end{pmatrix}.$$

Moreover,

$$\rho : \Gamma_{a,\infty,\infty} \to \mathrm{SL}_2\left(\frac{\mathbb{Z}[\lambda_a]}{\mathfrak{p}}\right) \tag{2}$$

denotes the map which sends each matrix to the matrix with reduced entries. Since $\Gamma_{a,\infty,\infty}(\mathfrak{p}) = \ker(\rho)$, it follows that the group $\Gamma_{a,\infty,\infty}(\mathfrak{p})$ is normal in $\Gamma_{a,\infty,\infty}$. Finally, whenever $\Gamma \subseteq \mathrm{SL}_2(\mathbb{R})$, the symbol $\overline{\Gamma} \subseteq \mathrm{PSL}_2(\mathbb{R})$ will denote the image group of Γ in $\mathrm{PSL}_2(\mathbb{R})$.

2. Galois group of φ

2.1. Special linear groups over finite fields. In this section we will use the facts below.

FACT 2.1. *A presentation for* $\mathrm{SL}_2(\mathbb{F}_5)$ *is given by*

$$\mathrm{SL}_2(\mathbb{F}_5) = \langle x, y \mid x^5 = y^3 = (xy)^4 = 1,\ (xy)^2x = x(xy)^2,\ (xy)^2y = y(xy)^2\rangle$$

(cf. [Suz82, Chapter 2, Section 6, Example 4]).

FACT 2.2. *The center* $Z(\mathrm{SL}_2(F))$ *of* $\mathrm{SL}_2(F)$ (*where F is any field*) *is equal to* $\{\pm I\}$ (cf. [Suz82, Chapter 1, Corollary 2 of Result 9.8]).

We state a theorem due to Dickson [Suz82, Chapter 3, Theorem 6.17].

THEOREM 2.3. *Let F be an algebraically closed field of characteristic $p \geq 2$, and G be a finite subgroup of $\mathrm{SL}_2(F)$ such that $|G|$ is divisible by p and that G admits at least two Sylow p-subgroups of order p^r. Then G is isomorphic to one of the following groups:*

(i) *$p = 2$ and G is dihedral of order $2n$ where n is odd,*
(ii) *$p = 3$ and $G \cong \mathrm{SL}_2(\mathbb{F}_5)$,*
(iii) *$\mathrm{SL}_2(K)$,*
(iv) *the subgroup generated by $\mathrm{SL}_2(K)$ and $d_\pi = \left(\begin{smallmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{smallmatrix}\right)$,*

where K is a field of p^r elements and π is an element such that $K(\pi)$ is a field of p^{2r} elements and π^2 is a generator of $K^\times$.

This allows us to prove the following:

Corollary 2.4. *Let $p \geq 3$ be a prime number and $E = \mathbb{F}_p(z)$ be the field with p^m elements, where $z \neq 0$. Let G be the subgroup of* $\mathrm{SL}_2(E)$ *generated by*

$$\begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \quad \textit{and} \quad \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}.$$

Then:

(i) $G \cong \mathrm{SL}_2(\mathbb{F}_5)$ *if* $p = 3$ *and* $z^2 = 2$*;*
(ii) $G \cong \mathrm{SL}_2(E)$ *otherwise.*

Proof. Let

$$v = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \quad \text{and} \quad u_z = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}.$$

It is clear that u_z has order p. The same is true for v since its Jordan canonical form is $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. We shall prove that v and u_z belong to two distinct Sylow p-subgroups of G.

Claim. *Let $U = \{u_a \mid a \in \mathbb{F}_q\} \subseteq \mathrm{SL}_2(E)$ where $q = p^m$ and $u_a = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$. Then $U \cap G$ is a p-Sylow of G. More generally, $U \cap G$ is the only p-Sylow of G that contains u_z.*

Let P be a p-Sylow of $\mathrm{SL}_2(E)$ containing u_z. We will prove $P = U$. The claim would then follow by one of the Sylow theorems (namely the one which says that any p-subgroup is contained in a p-Sylow). In fact, by one of the Sylow theorems, $P = \alpha U \alpha^{-1}$ for some $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{F}_q)$ (because U is a p-Sylow of $\mathrm{SL}_2(\mathbb{F}_q)$). So, there exists $z' \in \mathbb{F}_q \setminus \{0\}$ such that

$$u_z = \alpha u_{z'} \alpha^{-1} = \begin{pmatrix} 1 - acz' & a^2 z \\ -c^2 z & 1 + acz \end{pmatrix}.$$

Hence, $c = 0$. Thus, $P = U$.

Therefore, v and u_z belong to two distinct p-Sylows of G. So, we can use Theorem 2.3.

Since we are assuming $p > 2$, there are only three possibilities for G: $\mathrm{SL}_2(\mathbb{F}_5)$ (by Theorem 2.3, this can only happen when $p = 3$), $\mathrm{SL}_2(\mathbb{F}_{p^r})$ or $\langle \mathrm{SL}_2(\mathbb{F}_{p^r}), d_\pi \rangle$, where p^r is the order of a p-Sylow of G.

Claim. $G \ncong \langle \mathrm{SL}_2(\mathbb{F}_{p^r}), d_\pi \rangle$.

Let $H = \langle \mathrm{SL}_2(\mathbb{F}_{p^r}), d_\pi \rangle$. If $G \cong H$, then their respective abelianizations are also isomorphic: $G^{\mathrm{ab}} \cong H^{\mathrm{ab}}$. As $G = \langle v, u_z \rangle$ and $\mathrm{ord}(v) = \mathrm{ord}(u_z) = p$, every element of G^{ab} has order dividing p. We claim that $\overline{d_\pi}$ (the image of d_π in H^{ab}) does not have order dividing p.

In fact, $\operatorname{ord}(d_\pi) = \operatorname{ord}(\pi)$. We know that $\operatorname{ord}(\pi^2) = p^r - 1$. On the other hand,

$$\operatorname{ord}(\pi) = \begin{cases} \operatorname{ord}(\pi^2) & \text{if } \operatorname{ord}(\pi) \text{ is odd,} \\ 2\operatorname{ord}(\pi^2) & \text{if } \operatorname{ord}(\pi) \text{ is even.} \end{cases}$$

So, $\operatorname{ord}(\pi) = p^r - 1$ or $2(p^r - 1)$.

Since $\operatorname{ord}(\overline{d_\pi}) \mid \operatorname{ord}(d_\pi)$ and $p \nmid 2(p^r - 1)$, we have $\operatorname{ord}(\overline{d_\pi}) \nmid p$.

It remains to show that if $p = 3$, then $G \cong \mathrm{SL}_2(\mathbb{F}_5)$ if and only if $z^2 = 2$.

Claim. *If $p = 3$ and $G \cong \mathrm{SL}_2(\mathbb{F}_5)$, then $z^2 = 2$.*

By Fact 2.2, we have $Z(G) = \{\pm I\}$, and thus $|Z(G)| = 2$. So, by [Suz82, Chapter 1, Corollary of Theorem 9.9], $\frac{G}{Z(G)}$ is a simple group of order 60. Therefore, by [Suz82, Chapter 3, Section 3, Exercise 9], we have $\frac{G}{Z(G)} \cong A_5$.

Let $\overline{v}$ and $\overline{u_z^{-1}}$ be the images of v and u_z^{-1} respectively in A_5. Since v and u_z^{-1} are clearly not in $Z(G)$ and their order is 3, we deduce that $\operatorname{ord}(\overline{v}) = \operatorname{ord}(\overline{u_z^{-1}}) = 3$. So, $\overline{v} = (abc)$ and $\overline{u_z^{-1}} = (def)$. Obviously we need to have $\{a, b, c, d, e, f\} = \{1, 2, 3, 4, 5\}$. Without loss of generality, $\overline{v} = (123)$ and $\overline{u_z^{-1}} = (145)$. Consequently, $\overline{v}\overline{u_z^{-1}} = (12345)$. So, $(vu_z^{-1})^5 = \pm I$. Thus, $\operatorname{ord}(vu_z^{-1}) = 5$ or 10. Hence, looking at the Jordan canonical form of vu_z^{-1}, we get

$$z + 2 = \operatorname{tr}(vu_z^{-1}) = \pm(x + x^{-1})$$

for some primitive fifth root of unity x over $\mathbb{F}_3$.

Since $x^4 + x^3 + x^2 + x + 1 = 0$,

$$(z+2)^2 = \mp(z+2) + 1, \quad \text{i.e.,} \quad z^2 = z + 1 \text{ or } z^2 = 2.$$

If $z^2 = z + 1$, then $G = \langle v, u_z \rangle$ has 720 elements. Hence, $z^2 = 2$.

Claim. *If $p = 3$ and $z^2 = 2$, then $G \cong \mathrm{SL}_2(\mathbb{F}_5)$.*

Let $h = (vu_z)^2 = \left(\begin{smallmatrix} 2 & 2+2z \\ z+1 & 2+2z \end{smallmatrix}\right)$. Since $v = h^{-1}u_z h$, it follows that $G = \langle h, u_z \rangle$. Moreover, $h^5 = u_z^3 = (hu_z)^4 = 1$ and $(hu_z)^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Therefore, Fact 2.1 implies that G is a homomorphic image of $\mathrm{SL}_2(\mathbb{F}_5)$. Using the computer algebra system Sage [S$^+$12], we have verified that $|G| = 120$, and thus $G \cong \mathrm{SL}_2(\mathbb{F}_5)$. ■

2.2. A bit of algebraic number theory

Lemma 2.5. *Let $a > 2$ be an integer and p a prime number such that $p \nmid a$. If $\mathfrak{p}$ is a prime in $\mathbb{Q}(\zeta_a + \zeta_a^{-1})$ above p, then the inertia degree of $\mathfrak{p}$ over p (i.e., the degree of $\mathbb{F}_\mathfrak{p}$ over $\mathbb{F}_p$) is the smallest positive integer f such that $p^f \equiv \pm 1 \pmod{a}$.*

Proof. Let $\sigma_p \in \operatorname{Gal}(\mathbb{Q}(\zeta_a)/\mathbb{Q})$ be the Frobenius automorphism of $\mathbb{Q}(\zeta_a)$ associated to a prime above p. Then $\sigma_p(\zeta_a) = \zeta_a^p$ (cf. [Was82, proof of

Theorem 2.13]). Note that $\sigma_p|_{\mathbb{Q}(\zeta_a+\zeta_a^{-1})}$ (also denoted σ_p) is the Frobenius automorphism of $\mathbb{Q}(\zeta_a + \zeta_a^{-1})$ associated to $\mathfrak{p}$. Hence, the order of $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_a + \zeta_a^{-1})/\mathbb{Q})$ is the inertia degree of $\mathfrak{p}$ over p. Therefore, the inertia degree of $\mathfrak{p}$ over p is the smallest positive integer f such that

$$\sigma_p^f(\zeta_a + \zeta_a^{-1}) = \zeta_a + \zeta_a^{-1} \ \Leftrightarrow\ \zeta_a^{p^f} + \zeta_a^{-p^f} = \zeta_a + \zeta_a^{-1} \ \Leftrightarrow\ p^f \equiv \pm 1 \pmod a,$$

where the last equivalence follows from the fact that $\{\zeta_a^r + \zeta_a^{-r} \mid 1 \le r \le (a-1)/2,\ (r,a) = 1\}$ is the set of all the $\varphi(a)/2$ roots of the minimal polynomial of $\zeta_a + \zeta_a^{-1}$. ■

Proposition 2.6. *Let $a > 2$ be an integer and p a prime number. If $\mathfrak{p}$ is a prime in $\mathbb{Q}(\zeta_a + \zeta_a^{-1})$ above p, then the inertia degree of $\mathfrak{p}$ over p is the smallest positive integer f such that $p^f \equiv \pm 1 \pmod{a'}$, where $a' = a/p^\nu$ and p^ν is the greatest power of p dividing a.*

Proof. Let $f_m(x) \in \mathbb{Z}[x]$ be the minimal polynomial of $\zeta_m + \zeta_m^{-1}$. By [Neu99, Proposition 8.3], the inertia degree of $\mathfrak{p}$ over p is given by the degree of the irreducible factors of $f_a(x) \pmod p$. Note that

$$f_a(x) = \prod_{i,j} \big(x - (\zeta_{a'}^i \zeta_{p^\nu}^j + (\zeta_{a'}^i \zeta_{p^\nu}^j)^{-1})\big),$$

where j varies over $\{j \mid 0 \le j \le (p^\nu - 1),\ (p,j) = 1\}$ and i varies over $\{i \mid 0 \le i \le a'/2, (a', i) = 1\}$. Since $x^{p^\nu} - 1 = (x-1)^{p^\nu} \pmod p$, it follows that $\zeta_{p^\nu} \equiv 1 \pmod{\hat{\mathfrak{p}}}$, where $\hat{\mathfrak{p}}$ is a prime in $\mathbb{Q}(\zeta_a)$ above $\mathfrak{p}$. Therefore

$$f_a(x) \equiv \prod_i \big(x - (\zeta_{a'}^i + (\zeta_{a'}^i)^{-1})\big)^{\varphi(p^\nu)} \equiv f_{a'}(x)^{\varphi(p^\nu)} \pmod{\mathfrak{p}},$$

and thus

$$f_a(x) \equiv f_{a'}(x)^{\varphi(p^\nu)} \pmod p.$$

The result is now a consequence of the previous lemma. ■

2.3. Computing $[\overline{\Gamma_{a,\infty,\infty}} : \overline{\Gamma_{a,\infty,\infty}(\mathfrak{p})}]$. Let ρ be the map defined in (2). We define

$$\overline{\rho} : \overline{\Gamma_{a,\infty,\infty}} \to \mathrm{PSL}_2(E), \qquad \overline{g} \mapsto \overline{\rho(g)},$$

where $E = \mathbb{Z}[\lambda_a]/\mathfrak{p}$ and $^-$ denotes the image in PSL_2. This map is well defined because $\rho(-g) = -\rho(g)$.

Therefore, we have a commutative diagram

$$\begin{tikzcd}
\Gamma_{a,\infty,\infty} \arrow[r, "\rho"] \arrow[d] & \mathrm{SL}_2(E) \arrow[d] \\
\overline{\Gamma_{a,\infty,\infty}} \arrow[r, "\overline{\rho}"] & \mathrm{PSL}_2(E)
\end{tikzcd}$$

Lemma 2.7. $\ker(\overline{\rho}) = \overline{\varGamma_{a,\infty,\infty}(\mathfrak{p})}$.

Proof. Since $\ker(\rho) = \varGamma_{a,\infty,\infty}(\mathfrak{p})$, it is clear that $\overline{\varGamma_{a,\infty,\infty}(\mathfrak{p})} \subseteq \ker(\overline{\rho})$.

Now, take $\overline{g} \in \ker(\overline{\rho})$, i.e., $\rho(g) = \pm I$ (I is the identity matrix). Since $\rho(-g) = -\rho(g)$, we get $\pm g \in \ker(\rho) = \varGamma_{a,\infty,\infty}(\mathfrak{p})$. So, $g \in \pm\varGamma_{a,\infty,\infty}(\mathfrak{p})$. Hence, $\overline{g} \in \overline{\varGamma_{a,\infty,\infty}(\mathfrak{p})}$. ∎

This shows that $\overline{\varGamma_{a,\infty,\infty}}/\overline{\varGamma_{a,\infty,\infty}(\mathfrak{p})} \cong \operatorname{img}(\overline{\rho})$.

Lemma 2.8. *If $a \geq 3$ is an odd integer, then*

(i) $\mathrm{N}_{\mathbb{Q}(\zeta_{2a})/\mathbb{Q}}(1+\zeta_{2a})$ *divides* a,
(ii) $\mathrm{N}_{\mathbb{Q}(\zeta_{2a})/\mathbb{Q}}(\mu_a)$ *divides* a^2, *and*
(iii) *all prime factors of* $\mathrm{N}_{\mathbb{Q}(\zeta_{2a})/\mathbb{Q}}(\zeta_{2a}^n - \zeta_{2a}^{-n})$ *are divisors of* a, *for any* $n \in \mathbb{Z}$ *such that* $a \nmid n$.

Moreover, if a is an odd prime, then items (i) *and* (ii) *are equalities.*

Proof. Note that $\mu_a = (1+\zeta_{2a})(1+\zeta_{2a}^{-1})$. Since a is odd, $-\zeta_{2a}$ is a primitive ath root of unity. So, the minimal polynomial of ζ_{2a} is $\phi_a(-x)$, where ϕ_a is the ath cyclotomic polynomial. So, the minimal polynomial of $1+\zeta_{2a}$ is $h(x) = \phi_a(-(x-1)) = \phi_a(-x+1)$. Since $\phi_a(x) \mid (x^{a-1} + x^{a-2} + \cdots + x + 1)$ in $\mathbb{Z}[x]$,

$$h(x) \mid \big((-x+1)^{a-1} + \cdots + (-x+1) + 1 = x^{a-1} + \cdots + a\big),$$

and thus the constant term of h divides a in $\mathbb{Z}$. So, $\mathrm{N}_{\mathbb{Q}(\zeta_{2a})/\mathbb{Q}}(1+\zeta_{2a})$ divides a. Similarly, $\mathrm{N}_{\mathbb{Q}(\zeta_{2a})/\mathbb{Q}}(1+\zeta_{2a}^{-1})$ divides a. Hence, $\mathrm{N}_{\mathbb{Q}(\zeta_{2a})/\mathbb{Q}}(\mu_a) = \mathrm{N}_{\mathbb{Q}(\zeta_{2a})/\mathbb{Q}}(1+\zeta_{2a}) \cdot \mathrm{N}_{\mathbb{Q}(\zeta_{2a})/\mathbb{Q}}(1+\zeta_{2a}^{-1})$ divides a^2.

When a is prime,

$$h(x) = (-x+1)^{a-1} + \cdots + (-x+1) + 1 = x^{a-1} + \cdots + a$$

and the lemma follows.

For the last item, note that

$$\zeta_{2a}^n - \zeta_{2a}^{-n} = \zeta_{2a}^{-n}(\zeta_{2a}^{2n} - 1) = \zeta_{2a}^{-n}(\zeta_a^n - 1).$$

Since ζ_{2a}^n is a unit, its norm is ± 1, and thus it suffices to check the prime divisors of $\mathrm{N}_{\mathbb{Q}(\zeta_{2a})/\mathbb{Q}}(\zeta_a^n - 1)$. Note that $a \nmid n$ implies that $\zeta_a^n - 1 \neq 0$. The argument is now similar to the one used to prove the first item. ∎

Lemma 2.9. *If $\mathfrak{p}$ is a prime ideal lying above $2\mathbb{Z}$ and a is odd, then* $\operatorname{img}(\overline{\rho}) \cong D_{2a}$.

Proof. Note that $\operatorname{img}(\overline{\rho}) = \overline{\operatorname{img}(\rho)}$.

We are going to use the fact that if $G = \langle g, h\rangle$ and both g and h have order 2, then $G \cong D_{2s}$, where s is the order of gh.

Since $p = 2$, $\overline{\rho}(\overline{\gamma_2})$ has order 2. By the previous lemma, so does $\overline{\rho}(\overline{\gamma_3})$. Note also that the Jordan canonical form of $\gamma_2\gamma_3$ is

$$\begin{pmatrix} -\zeta_{2a} & 0 \\ 0 & -\zeta_{2a}^{-1} \end{pmatrix},$$

and therefore $\overline{\rho}(\overline{\gamma_2}\ \overline{\gamma_3})$ has order a. ■

LEMMA 2.10. *Suppose $\mathfrak{p}$ is a prime ideal lying above $p\mathbb{Z}$ with $p \geq 3$. Then* $\operatorname{img}(\overline{\rho})$ *is isomorphic to*

(i) $\mathrm{PSL}_2(\mathbb{F}_5)$ *if $p = 3$ and $\mu_a^2 - 2 \in \mathfrak{p}$,*
(ii) $\mathrm{PSL}_2(E)$ *otherwise (where $E = \mathbb{Z}[\lambda_a]/\mathfrak{p}$).*

Proof. Again notice that $\operatorname{img}(\overline{\rho}) = \overline{\operatorname{img}(\rho)}$.

If $p = 3$ and $\mu_a^2 - 2 \in \mathfrak{p}$, Corollary 2.4 says that $\operatorname{img}(\rho) \cong \mathrm{SL}_2(\mathbb{F}_5)$. We have to prove that $\overline{\operatorname{img}(\rho)} \cong \mathrm{PSL}_2(\mathbb{F}_5)$. Notice that

$$\overline{\operatorname{img}(\rho)} = \frac{\operatorname{img}(\rho)}{\{\pm I\} \cap \operatorname{img}(\rho)}.$$

We can verify that $-I \in \operatorname{img}\rho$. In fact, there are only two cases to consider, and they were computed explicitly using Sage.

So, by Fact 2.2,

$$\overline{\operatorname{img}(\rho)} = \frac{\mathrm{SL}_2(\mathbb{F}_5)}{Z(\mathrm{SL}_2(\mathbb{F}_5))} = \mathrm{PSL}_2(\mathbb{F}_5).$$

Otherwise, Corollary 2.4 says that $\operatorname{img}(\rho) = \mathrm{SL}_2(E)$, i.e., ρ is surjective. Hence, $\overline{\operatorname{img}(\rho)} = \mathrm{PSL}_2(E)$. ■

THEOREM 2.11. *Let $a \geq 3$ be an odd integer and $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\lambda_a]$ lying above $p\mathbb{Z}$ where $p \geq 2$. Moreover, let G denote the Galois group of*

$$\varphi : X_{a,\infty,\infty}(\mathfrak{p}) \to X_{a,\infty,\infty}.$$

(i) *If $p = 2$, then $G \cong D_{2a}$, and hence $[\overline{\Gamma_{a,\infty,\infty}} : \overline{\Gamma_{a,\infty,\infty}(\mathfrak{p})}] = 2a$.*
(ii) *If $p = 3$ and $\mu_a^2 - 2 \in \mathfrak{p}$, then $G \cong \mathrm{PSL}_2(\mathbb{F}_5)$, and hence*

$$[\overline{\Gamma_{a,\infty,\infty}} : \overline{\Gamma_{a,\infty,\infty}(\mathfrak{p})}] = 60.$$

(iii) *Otherwise, $G \cong \mathrm{PSL}_2(\mathbb{Z}[\lambda_a]/\mathfrak{p})$, and hence*

$$[\overline{\Gamma_{a,\infty,\infty}} : \overline{\Gamma_{a,\infty,\infty}(\mathfrak{p})}] = (p^m + 1)p^m(p^m - 1)/2.$$

Moreover, $\mathbb{Z}[\lambda_a]/\mathfrak{p} \cong \mathbb{F}_{p^m}$ where m is the smallest positive integer such that $p^m \equiv \pm 1 \pmod{a/p^\nu}$ and p^ν is the greatest power of p dividing a.

Proof. The theorem follows from Lemmas 2.9 and 2.10.

The fact that $\mathbb{Z}[\lambda_a]/\mathfrak{p}$ is a field with p^m elements with m as in the statement of the theorem follows from Proposition 2.6. ■

Remark 3. Recall that, in the classical setting, the Galois group of

$$X(p) \to X(1)$$

is always $\mathrm{PSL}_2(\mathbb{Z}/p)$. The previous theorem shows that it is not always the case for a general triangle group and, in fact, establishes exactly when that happens for the triangle groups $\Gamma_{a,\infty,\infty}$.

3. Genus of $X_{a,\infty,\infty}(\mathfrak{p})$. The proposition below paired with Theorem 2.11 computes the genera of $X_{a,\infty,\infty}(\mathfrak{p})$ for many ideals $\mathfrak{p}$.

Proposition 3.1. *Suppose a is an odd number and $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}[\lambda_a]$ lying above $p\mathbb{Z}$. Suppose also that $p \nmid a$. Then the genus of $X_{a,\infty,\infty}(\mathfrak{p})$ is*

$$1 + \frac{\overline{\mu}}{2}\left(1 - \frac{2}{p} - \frac{1}{a}\right),$$

where $\overline{\mu} = [\overline{\Gamma_{a,\infty,\infty}} : \overline{\Gamma_{a,\infty,\infty}(\mathfrak{p})}]$.

Proof. To simplify notation, let us write $\Gamma = \Gamma_{a,\infty,\infty}$.

We know that the map

$$\varphi : \Gamma(\mathfrak{p})\backslash\mathcal{H}^* \to \Gamma\backslash\mathcal{H}^*$$

is holomorphic and has degree $\overline{\mu}$ (cf. [Shi94, Section 1.5]). So we can use the Riemann–Hurwitz formula to compute the genus g of $\Gamma(\mathfrak{p})\backslash\mathcal{H}^*$:

$$2g - 2 = \overline{\mu}(2 \cdot 0 - 2) + \sum_{P \in \Gamma(J)\backslash\mathcal{H}^*} (e_P - 1) = -2\overline{\mu} + \sum_{P \in \Gamma(J)\backslash\mathcal{H}^*} (e_P - 1)$$

where e_P is the ramification index of φ at P.

By [Shi94, Proposition 1.37], the only points P which may have $e_P > 1$ are those mapped to cusps or elliptic points. Therefore, by Proposition 1.3, the only points P which may have $e_P > 1$ are those mapped to 1, ∞ or $z_0 = e^{i(\pi - \pi/a)}$.

Moreover, it follows from [Bea83, proof of Theorem 10.6.4] that $\overline{\Gamma}_1 = \langle\overline{\gamma_2}\rangle$, $\overline{\Gamma}_\infty = \langle\overline{\gamma_3}\rangle$ and $\overline{\Gamma}_{z_0} = \langle\overline{\gamma_1}\rangle$. In particular, $|\overline{\Gamma_{z_0}}| = a$.

Consider $\{w_1, \ldots, w_{k^{(1)}}\} = \varphi^{-1}(1)$ and let $e_1^{(1)}, \ldots, e_{k^{(1)}}^{(1)}$ be their respective ramification indices. Since $\Gamma(\mathfrak{p}) \trianglelefteq \Gamma$, [Shi94, Proposition 1.37] says that $e_1^{(1)} = \cdots = e_k^{(1)} = [\overline{\Gamma_1} : \overline{\Gamma(\mathfrak{p})_1}]$ and $k^{(1)} e_1^{(1)} = \overline{\mu}$.

Next, $\overline{\Gamma}_1 = \langle\overline{\gamma_2}\rangle$ and $\overline{\Gamma(\mathfrak{p})}_1 = \overline{\Gamma}_1 \cap \overline{\Gamma(\mathfrak{p})}$. Since $\gamma_2^n = \left(\begin{smallmatrix} -n+1 & n \\ -n & n+1 \end{smallmatrix}\right)$ and $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, we have $\overline{\Gamma(\mathfrak{p})}_1 = \langle\gamma_2^p\rangle$. So,

$$e_1^{(1)} = \cdots = e_k^{(1)} = p \quad \text{and} \quad k^{(1)} = \overline{\mu}/p. \tag{3}$$

Let us now compute the ramification indices of $\varphi^{-1}(\infty)$.

Since $p \nmid a$, Lemma 2.8 implies that $\mu_a \notin \mathfrak{p}$. Because $\gamma_3^n = \left(\begin{smallmatrix} 1 & n\mu_q \\ 0 & 1 \end{smallmatrix}\right)$ and $\overline{\Gamma}_\infty = \langle\overline{\gamma_3}\rangle$, we see that $\overline{\Gamma(\mathfrak{p})}_\infty = \langle\overline{\gamma_3{}^p}\rangle$, and hence $[\overline{\Gamma}_\infty : \overline{\Gamma(\mathfrak{p})}_\infty] = p$.

Therefore, if $\{v_1, \ldots, v_{k^{(\infty)}}\} = \varphi^{-1}(\infty)$ and $e_1^{(\infty)}, \ldots, e_{k^{(\infty)}}^{(\infty)}$ are their respective ramification indices, by [Shi94, Proposition 1.37] we get

$$e_1^{(\infty)} = \cdots = e_{k^{(\infty)}}^{(\infty)} = p \quad \text{and} \quad k^{(\infty)} = \overline{\mu}/p. \tag{4}$$

Now we shall compute the ramification indices of $\varphi^{-1}(z_0)$. We need to compute $\overline{\Gamma(\mathfrak{p})}_{z_0}$. Since $\overline{\Gamma(\mathfrak{p})}_{z_0} = \overline{\Gamma}_{z_0} \cap \overline{\Gamma(\mathfrak{p})}$ and $\overline{\Gamma}_{z_0}$ has only elliptic elements (in addition to the identity), the next claim tells us that $|\overline{\Gamma(\mathfrak{p})}_{z_0}| = 1$. Therefore, $[\overline{\Gamma}_{z_0} : \overline{\Gamma(\mathfrak{p})}_{z_0}] = a$.

Claim. *$\Gamma(\mathfrak{p})$ has no elliptic element.*

Since z_0 is the only inequivalent elliptic point and $\overline{\Gamma}_{z_0} = \langle \overline{\gamma_1} \rangle$, we see that any elliptic element of $\overline{\Gamma}$ is conjugate to some (non-trivial) power of $\overline{\gamma_1}$. Since $\Gamma(\mathfrak{p}) \trianglelefteq \Gamma$, if $\overline{\Gamma(\mathfrak{p})}$ contains an elliptic element, it would also contain some (non-trivial) power of $\overline{\gamma_1}$. Now note that

$$\gamma_1 = P \begin{pmatrix} -\zeta_{2a} & 0 \\ 0 & -\zeta_{2a}^{-1} \end{pmatrix} P^{-1} \quad \text{where} \quad P = \begin{pmatrix} -\zeta_{2a} & -\zeta_{2a}^{-1} \\ 1 & 1 \end{pmatrix}.$$

Therefore,

$$\gamma_1^n = \frac{1}{-(\zeta_{2a} - \zeta_{2a}^{-1})} \begin{pmatrix} * & (-1)^{n+1}(\zeta_{2a}^n - \zeta_{2a}^{-n}) \\ * & * \end{pmatrix}.$$

Since $p \nmid a$, the last item of Lemma 2.8 shows that

$$\frac{(-1)^{n+1}(\zeta_{2a}^n - \zeta_{2a}^{-n})}{-(\zeta_{2a} - \zeta_{2a}^{-1})} \not\equiv 0 \pmod{\mathfrak{p}}.$$

Hence, if $\varphi^{-1}(z_0) = \{y_1, \ldots, y_{k^{(z_0)}}\}$ and $e_1^{(z_0)}, \ldots, e_{k^{(z_0)}}^{(z_0)}$ are their respective indices, [Shi94, Proposition 1.37] tells us that

$$e_0^{(z_0)} = \cdots = e_{k^{(z_0)}}^{(z_0)} = a \quad \text{and} \quad k^{(z_0)} = \overline{\mu}/a. \tag{5}$$

Using the Riemann–Hurwitz formula with the information given by (3)–(5), we get

$$\begin{aligned} 2g - 2 &= -2\overline{\mu} + \frac{\overline{\mu}}{p}(p-1) + \frac{\overline{\mu}}{p}(p-1) + \frac{\overline{\mu}}{a}(a-1) \\ &= \overline{\mu}\left(-2 + 2 - \frac{2}{p} + 1 - \frac{1}{a}\right) = \overline{\mu}\left(1 - \frac{2}{p} - \frac{1}{a}\right). \end{aligned}$$

Hence,

$$g = 1 + \frac{\overline{\mu}}{2}\left(1 - \frac{2}{p} - \frac{1}{a}\right). \ \blacksquare$$

4. Genus of $X_{q,\infty,\infty}^{(0)}(\mathfrak{p})$. In order to further understand the triangular modular curves, this section will be devoted to the computation of the genus of $X^{(0)}_{q,\infty,\infty}(\mathfrak{p})$ for a prime number q. The motivation here is a well known result in the $\mathrm{SL}_2(\mathbb{Z})$ case stating that $X_0(p)$ admits an integral model for which the reduction modulo p consists of two copies of $X_0(1)_{\mathbb{F}_p} = \mathbb{P}^1_{\mathbb{F}_p}$ crossing transversally at the supersingular points (cf. [DR73, Theorem 6.9, p. 286]). In particular, in a study conducted in [Tak] to investigate whether a similar structure might exist in the case of the groups $\Gamma_{q,\infty,\infty}$, the knowledge of the genus of $X^{(0)}_{q,\infty,\infty}(\mathfrak{p})$ was crucial.

Recall that $\mathfrak{p}$ denotes a prime above p. In this section, it will be assumed that $p \neq q$ are prime numbers strictly greater than 2, and moreover that $\overline{\Gamma_{q,\infty,\infty}}/\overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})} \cong \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ (which is always true when $p \geq 5$ according to Theorem 2.11).

To compute the genus of $X^{(0)}_{q,\infty,\infty}(\mathfrak{p})$, we use the Riemann–Hurwitz formula and the natural map

$$\psi : X^{(0)}_{q,\infty,\infty}(\mathfrak{p}) \to X_{q,\infty,\infty}(1) = X_{q,\infty,\infty}. \tag{6}$$

It then suffices to compute the ramification indices of ψ.

Recall that

$$(\overline{\Gamma_{q,\infty,\infty}})_\infty = \left\langle \gamma_3 = \begin{pmatrix} 1 & \mu_q \\ 0 & 1 \end{pmatrix} \right\rangle,$$

$$(\overline{\Gamma_{q,\infty,\infty}})_1 = \left\langle \gamma_2 = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \right\rangle,$$

$$(\overline{\Gamma_{q,\infty,\infty}})_{z_0} = \left\langle \gamma_1 = \begin{pmatrix} -\lambda_q & -1 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

It can be shown, with the help of [Shi94, Proposition 1.37], that the monodromy of (6) over ∞ is given by the action of γ_3 on the set of cosets $\overline{\Gamma_{q,\infty,\infty}}/\overline{\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})}$. Similarly, the monodromy of (6) over 1 (resp. z_0) is given by the action of γ_2 (resp. γ_1) on $\overline{\Gamma_{q,\infty,\infty}}/\overline{\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})}$.

Lemma 4.1. *Let $\gamma \in \Gamma_{q,\infty,\infty}$. The action of γ on $\overline{\Gamma_{q,\infty,\infty}}/\overline{\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})}$ is equivalent to the action of $(\gamma \bmod \mathfrak{p}) \in \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ on $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ via fractional linear transformations, i.e., the cycle decomposition of γ (viewed as an element of the group of permutations of $\overline{\Gamma_{q,\infty,\infty}}/\overline{\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})}$) is the same as the cycle structure of $(\gamma \bmod \mathfrak{p})$ (viewed as an element of the group of permutations of $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$).*

Proof. The action of $\overline{\Gamma_{q,\infty,\infty}}$ on $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ via linear fractional transformations is transitive (since $\overline{\Gamma_{q,\infty,\infty}}/\overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})} \cong \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$). Moreover, the stabilizer of $\infty \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ is $\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})$. Hence, by group theory, the action of $\overline{\Gamma_{q,\infty,\infty}}$ on $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ is equivalent to the action of $\overline{\Gamma_{q,\infty,\infty}}$ on $\overline{\Gamma_{q,\infty,\infty}}/\overline{\Gamma^{(0)}_{q,\infty,\infty}(\mathfrak{p})}$. ∎

Lemma 4.2. *The monodromy over* ∞ *is given by*

$$(0)(1\cdots p)(p+1,\ldots,2p)\cdots(p^{f-1}+1,\ldots,p^f),$$

where $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_{p^f}$. *So,* $\psi^{-1}(\infty) = \{w_0, w_1, \ldots, w_{p^{f-1}}\}$ *and*

$$e_{w_0} = 1 \quad \textit{and} \quad e_{w_i} = p \quad \textit{for } 1 \le i \le p^{f-1}.$$

Proof. Notice $(\gamma_3 \bmod \mathfrak{p}) = \left(\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right)$, where $\beta = (\mu_q \bmod \mathfrak{p}) \in \mathbb{F}_{\mathfrak{p}} \setminus \{0\}$ (that $\beta \neq 0$ is part of the proof of Proposition 3.1).

Hence, $\infty \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ is fixed by $(\gamma_3 \bmod \mathfrak{p})$. Furthermore, since

$$(\gamma_3 \bmod \mathfrak{p})^n = \begin{pmatrix} 1 & n\beta \\ 0 & 1 \end{pmatrix}$$

and $\operatorname{char}(\mathbb{F}_{\mathfrak{p}}) = p$, all other points of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ generate an orbit of size p. ∎

Lemma 4.3. *The monodromy over* 1 *has the same cycle decomposition. So,* $\psi^{-1}(1) = \{w_0, w_1, \ldots, w_{p^{f-1}}\}$ *and*

$$e_{w_0} = 1 \quad \textit{and} \quad e_{w_i} = p \quad \textit{for } 1 \le i \le p^{f-1},$$

where $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_{p^f}$.

Proof. Notice that $(\gamma_2 \bmod \mathfrak{p}) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 2 \end{smallmatrix}\right)$.

It is easily seen that the only point of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ fixed by $(\gamma_2 \bmod \mathfrak{p})$ is 1.

Now, consider the natural map

$$\varphi : X_{q,\infty,\infty}(\mathfrak{p}) \to X_{q,\infty,\infty}(1).$$

Since $e_{v,\varphi} = p$ for all $v = \varphi^{-1}(1)$ (part of the proof of Proposition 3.1) and φ factors as

$$X_{q,\infty,\infty}(\mathfrak{p}) \to X^{(0)}_{q,\infty,\infty}(\mathfrak{p}) \xrightarrow{\psi} X_{q,\infty,\infty}(1),$$

we see that $e_{w,\psi} = 1$ or p for all $w \in \psi^{-1}(1)$.

The previous calculation says that there is only one point above 1 having ramification degree 1. Hence, the result follows. ∎

Lemma 4.4. *Let* $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_{p^f}$ *as before. The ramification behavior above* z_0 *is as follows:*

$$\psi^{-1}(z_0) = \{w_1, \ldots, w_n, w'_1, \ldots, w'_m\},$$

where

$$e_{w_i} = q, \quad e_{w'_i} = 1, \quad p^f + 1 = qn + m, \quad m = \begin{cases} 0 & \textit{if } p^f \equiv -1 \pmod{q}, \\ 2 & \textit{if } p^f \equiv 1 \pmod{q}. \end{cases}$$

Proof. Notice that $(\gamma_1 \bmod \mathfrak{p}) = \left(\begin{smallmatrix} \beta & -1 \\ 1 & 0 \end{smallmatrix}\right)$ for some $\beta \in \mathbb{F}_{\mathfrak{p}}$.

As in the proof of the previous lemma, $e_w = 1$ or q for any $w \in \psi^{-1}(z_0)$.

Let n denote the number of points whose ramification degree is q, and let m denote the number of those whose ramification degree is 1. Then m is also the number of points in $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ fixed by $(\gamma_1 \bmod \mathfrak{p})$. Hence $m \le 2$.

Since $\deg(\psi) = p^f + 1$, we have

$$p^f + 1 = nq + m.$$

Since q and p are distinct primes, it follows that $m \neq 1$. Taking the previous equality modulo q and using Proposition 2.6, we obtain the precise value of m in terms of $(p^f \bmod q)$. ■

Theorem 4.5. *Let $p \neq q$ be prime numbers strictly greater than* 2 *and $\mathfrak{p}$ let be a prime ideal of $\mathbb{Z}(\zeta_{2q} + \zeta_{2q}^{-1})$ above $p\mathbb{Z}$. Assume also that $\overline{\Gamma_{q,\infty,\infty}}/\overline{\Gamma_{q,\infty,\infty}(\mathfrak{p})} \cong \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ (always true when $p \geq 5$ by Theorem* 2.11*). Then the genus of the curve $X^{(0)}_{q,\infty,\infty}(\mathfrak{p})$ is*

$$g = \frac{q-1}{2} \cdot \frac{p^f - \delta}{q} - p^{f-1},$$

where

- *f is the smallest positive integer such that $p^f \equiv \pm 1 \pmod{q}$, and*
- *$\delta \in \{\pm 1\}$ is such that $p^f \equiv \delta \pmod{q}$.*

Proof. Follows from the Riemann–Hurwitz formula applied to ψ, the fact that $g(X_{q,\infty,\infty}(1)) = 0$, the previous three lemmas, and Proposition 2.6. ■

5. Computation of the genera. In this section, we will use Theorem 4.5 to compute the genus of $X^{(0)}_{a,\infty,\infty}(\mathfrak{p})$, and Theorem 2.11 and Proposition 3.1 to compute the genus of $X_{a,\infty,\infty}(\mathfrak{p})$ for a few values of a and p. The computations are summarized in Table 1.

Except for the first line, we will assume that $p \geq 5$ and a are prime numbers and $p \neq a$.

As for the first line, note that when $p = 2$ and $a \geq 3$ is an odd integer, Theorem 2.11 implies that $\overline{\mu} = 2a$, and hence by Proposition 3.1 it follows that the genus of $X_{q,\infty,\infty}(\mathfrak{p})$ is 0 for any prime number $q \neq 2$. Then, by the Riemann–Hurwitz formula, the genus of $X^{(0)}_{a,\infty,\infty}(\mathfrak{p})$ has to be 0 as well.

As a last remark, note that, by Theorem 4.5, the genus of $X^{(0)}_{a,\infty,\infty}(\mathfrak{p})$ is always odd. In particular, the smallest possible values are 1 and 3. The proposition below shows that all cases where the genus is 1 or 3 are contained in Table 1.

Proposition 5.1. *Let $q \geq 3$ and $p \geq 5$ be prime numbers such that $q \neq p$, and $g^{(0)}$ be the genus of $X^{(0)}_{q,\infty,\infty}(\mathfrak{p})$. Assume that p and q satisfy one of the following conditions:*

1. *$q = 3$ and $p \geq 17$, or*
2. *$q = 5$ and $p \geq 13$, or*
3. *$q \geq 7$.*

Then $g^{(0)} > 3$.

Proof. By Theorem 4.5, since $f \geq 1$, we obtain

$$g^{(0)} \geq \left(1 - \frac{1}{q}\right)\frac{p-1}{2} - 1.$$

This is enough to prove (1) and (2).

As for (3), we use a similar argument and the fact that if $p \leq q$, then $f \geq 2$. ■

Table 1

a	p	Genus of $X^{(0)}_{a,\infty,\infty}(\mathfrak{p})$	Genus of $X_{a,\infty,\infty}(\mathfrak{p})$
$a \geq 3$ odd	2	0	0
3	5	1	9
3	7	1	33
3	11	3	161
3	13	3	281
3	17	5	673
3	19	5	961
3	23	7	1761
3	29	9	3641
3	31	9	4481
3	37	11	7753
3	41	13	10641
3	43	13	12321
3	47	15	16193
3	53	17	23401
3	59	19	32481
3	61	19	35961
3	67	21	47873
5	7	13	15121
5	11	3	205
5	13	55	779689
5	17	99	4117537
5	19	7	1189
5	23	189	26388913
5	29	11	4453
5	31	11	5473
5	37	511	478473049
5	41	15	12937
5	43	697	1190768041
5	47	837	2041170145
5	53	1071	4223773945
5	59	23	39325
7	5	29	223201
7	11	449	398094841
7	13	5	385
7	17	1817	21923808193
7	19	2579	60655581001
7	23	4685	346805789617
7	29	11	4801
7	31	11807	5239187795521
7	37	20339	26092704504673
7	41	17	13921
7	43	17	16105
7	47	42287	227908029455713

Acknowledgements. I am grateful to Henri Darmon, Eyal Goren and John Voight for helpful discussions and advice. I am also grateful to the anonymous referee who provided invaluable input that allowed me to fix a few mistakes and greatly improve the exposition of the main ideas of this article. Any remaining problems are, of course, my responsibility.

References

[Bea83] A. F. Beardon, *The Geometry of Discrete Groups*, Grad. Texts in Math. 91, Springer, New York, 1983.

[Bel79] G. V. Belyĭ, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. 43 (1979), 267–276 (in Russian).

[CV] P. L. Clark and J. Voight, *Algebraic curves uniformized by congruence subgroups of triangle groups*, arXiv:1506.01371 (2015).

[Dar04] H. Darmon, *A fourteenth lecture on Fermat's last theorem*, in: Number Theory, CRM Proc. Lecture Notes 36, Amer. Math. Soc., Providence, RI, 2004, 103–115.

[DR73] P. Deligne et M. Rapoport, *Les schémas de modules de courbes elliptiques*, in: Modular Functions of One Variable, II (Antwerp, 1972), Lecture Notes in Math. 349, Springer, Berlin, 1973, 143–316.

[DS05] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Grad. Texts in Math. 228, Springer, New York, 2005.

[LLT00] M. L. Lang, C. H. Lim and S. P. Tan, *Principal congruence subgroups of the Hecke groups*, J. Number Theory 85 (2000), 220–230.

[Neu99] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, Berlin, 1999.

[Shi94] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, Princeton, NJ, 1994.

[S$^+$12] W. A. Stein et al., *Sage Mathematics Software* (*Version 4.8*), The Sage Development Team, 2012, http://www.sagemath.org.

[Suz82] M. Suzuki, *Group Theory. I*, Grundlehren Math. Wiss. 247, Springer, Berlin, 1982.

[Tak] L. K. Takei, *The non-ordinary locus of the TTV family of curves*, arXiv:1506.04816 (2015).

[Tak12] L. K. Takei, *On triangle groups and representations of* $\mathrm{PSL}_2(\mathbb{F}_{p^{2n+1}})$, Ann. Sci. Math. Québec 36 (2012), 245–258.

[Tak77] K. Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan 29 (1977), 91–106.

[Was82] L. C. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, New York, 1982.

Luiz Kazuo Takei
Department of Mathematics
John Abbott College
21 275 Lakeshore Road
Sainte-Anne-de-Bellevue, Québec, H9X 3L9 Canada
E-mail: luiz.kazuotakei@johnabbott.qc.ca