DUKE MATHEMATICAL JOURNAL
Vol. 110, No. 2, © 2001

TORSION-FREE GENUS ZERO CONGRUENCE SUBGROUPS OF $\mathrm{PSL}_2(\mathbb{R})$

ABDELLAH SEBBAR

Abstract

We study and classify all the conjugacy classes of the genus zero congruence subgroups of $\mathrm{PSL}_2(\mathbb{R})$ *with no elliptic elements. We show that it suffices to classify those inside the modular group and determine them completely. We also discuss an application to modular curves.*

Contents

1. Introduction

Since the appearance of Moonshine more than two decades ago, much interest has been drawn to genus zero congruence groups. In [13], J. Thompson showed that there are only finitely many conjugacy classes of particular genus zero congruence subgroups of $\mathrm{PSL}_2(\mathbb{R})$ using group-theoretic methods. Using Thompson's results and spectral properties of automorphic functions, P. Zograf [14] showed that there are only finitely many genus zero congruence subgroups of the modular group. However, besides finiteness results and examples, nothing has been explicitly said about the number of these groups (in $\mathrm{PSL}_2(\mathbb{R})$), and no description of their nature has been given. In this paper, we deal with an aspect of this subject; namely, we describe completely

DUKE MATHEMATICAL JOURNAL
Vol. 110, No. 2, © 2001
Received 7 April 2000. Revision received 3 November 2000.
2000 *Mathematics Subject Classification*. Primary 11F06, 20H05; Secondary 11F03.

the genus zero congruence subgroups of $\mathrm{PSL}_2(\mathbb{R})$ that contain no elliptic elements.

This work was motivated by previous papers in collaboration with John McKay [6], [7] in which we studied the action of the Schwarzian derivative on automorphic functions that generate the function field of a genus zero discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$. It turns out that the Schwarzian derivative of such an automorphic function is a weight 4 automorphic form for the normalizer of the discrete subgroup in $\mathrm{PSL}_2(\mathbb{R})$. Moreover, these automorphic forms are holomorphic if and only if the group has no elliptic elements. If we specialize to genus zero congruence subgroups of $\mathrm{PSL}_2(\mathbb{R})$ which do not have elliptic elements, in other words, which are torsion-free, then the automorphic forms obtained coincide with theta-functions of some familiar rank 8 lattices. This phenomenon motivated the present classification to enable a better understanding of the situation.

One of the main results of this paper is the following.

THEOREM 1
There are exactly 15 *conjugacy classes of torsion-free genus zero congruence subgroups of* $\mathrm{PSL}_2(\mathbb{R})$.

These 15 conjugacy classes are explicitly determined in terms of classical congruence groups. This theorem is a consequence of the following.

THEOREM 2
Every torsion-free genus zero discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$ *commensurable with the modular group is conjugate to a subgroup of* $\mathrm{PSL}_2(\mathbb{Z})$.

We then show that if a subgroup of $\mathrm{PSL}_2(\mathbb{R})$ is a congruence group, then any of its conjugates inside $\mathrm{PSL}_2(\mathbb{Z})$ (if it has any) is also a congruence group.

Having transferred the problem inside the modular group, we need to classify torsion-free genus zero congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. We have the following.

THEOREM 3
Up to a modular conjugacy, there are 33 *torsion-free genus zero congruence subgroups of* $\mathrm{PSL}_2(\mathbb{Z})$.

Again, these groups are described explicitly in terms of classical congruence groups. The proof of Theorem 3 is carried out by studying the cusp widths of the groups. Using work of H. Larcher [4], [5], each congruence group has a conjugate by an element of the modular group which contains a simply described group with which it shares the same cusp shape (i.e., set of cusp widths). Furthermore, if the conjugate is

torsion-free and of genus zero, then it coincides with a Larcher group with which it shares the same cusp shape. This makes it easy to classify all the $\mathrm{PSL}_2(\mathbb{Z})$-conjugacy classes of torsion-free and genus zero congruence subgroups of the modular group. We show that the 33 modular conjugacy classes of Theorem 3 are partitioned into the 15 $\mathrm{PSL}_2(\mathbb{R})$ conjugacy classes of Theorem 1.

We also deal with the subgroups that contain a conjugate of $\Gamma_0(n)$ for some n, which occur in Moonshine. Section 9 deals with a special case that leads to a geometric application concerning the modularity of $\mathbb{P}^1 \setminus \{0, 1, \infty, z\}$.

2. Discrete subgroups of $\mathrm{PSL}_2(\mathbb{R})$

The content of this section is common knowledge and is based generally on [9] or [12].

Let $\mathrm{PSL}_2(\mathbb{R})$ be the group of Möbius transformations

$$\tau \to \frac{a\tau + b}{c\tau + d}, \quad a, b, c, d \in \mathbb{R}, \ \ ad - bc > 0.$$

The group $\mathrm{PSL}_2(\mathbb{R})$ acts on $\mathfrak{H}$ by linear fractional transformations, where $\mathfrak{H}$ is the upper half of the complex plane, as well as on the extended real line $\mathbb{R} \cup \{\infty\}$. We represent an element of $\mathrm{PSL}_2(\mathbb{R})$ by a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad ad - bc = 1,$$

with the understanding that A and $-A$ are identified. If A is not the identity element, then it has a single fixed point on $\mathbb{R} \cup \{\infty\}$ if and only if $\mathrm{Tr}(A) = 2$, in which case A is called parabolic. Also, A has a fixed point in $\mathfrak{H}$ if and only if $\mathrm{Tr}(A) < 2$, in which case A is called an elliptic element. The case $\mathrm{Tr}(A) > 2$ is equivalent to A having two fixed points on the real line, and A is called hyperbolic.

Let us now restrict ourselves to a discrete subgroup Γ of $\mathrm{PSL}_2(\mathbb{R})$. A point τ of $\mathfrak{H}$ is called an elliptic point of Γ if it is fixed by an elliptic element of Γ. Similarly, a point of $\mathbb{R} \cup \{\infty\}$ is called a cusp of Γ if it is fixed by a parabolic element of Γ. Every point in the orbit of an elliptic (resp., parabolic) point is elliptic (resp., parabolic). Moreover, the stabilizer in Γ of an elliptic point is a finite cyclic group, and the elements of finite order in Γ consist of the elliptic elements together with the identity element I. Similarly, the stabilizer in Γ of a parabolic point is an infinite cyclic group, and it consists of parabolic elements together with I. If Γ' is a subgroup of $\mathrm{PSL}_2(\mathbb{R})$ commensurable with Γ, then Γ' is discrete and its set of cusps is the same as the set of cusps of Γ.

We denote by $\mathfrak{H}^*$ the union of $\mathfrak{H}$ and the cusps of Γ. The action of Γ on $\mathfrak{H}$ extends to $\mathfrak{H}^*$, and the quotient space $\mathfrak{H}^*/\Gamma$ is a Riemann surface. The group Γ is called a Fuchsian group of the first kind if $\mathfrak{H}^*/\Gamma$ is compact. All the discrete subgroups of

$\mathrm{PSL}_2(\mathbb{R})$ in this paper are assumed to be Fuchsian of the first kind. The genus of such a group Γ is by definition the genus of the compact Riemann surface $\mathfrak{H}^*/\Gamma$. It may occur that $\mathfrak{H}/\Gamma$ is compact; in this case Γ has no parabolic elements. An important property when $\mathfrak{H}^*/\Gamma$ is compact is that the numbers of Γ-inequivalent cusps and elliptic points are finite.

Let g be the genus of Γ, let h be the number of inequivalent cusps, and let r be the number of inequivalent elliptic points. Let $m_1, \dots, m_r$ be the orders of the stabilizers of all conjugacy classes of elliptic points. Then we say that Γ has signature $(g; m_1, \dots, m_r; h)$. The algebraic structure of the group can be determined by its signature. In fact, the group Γ has a presentation:

generators:

$$A_1, B_1, \dots, A_g, B_g; E_1, \dots, E_r; P_1, \dots, P_h; \tag{2.1}$$

relations:

$$E_1^{m_1} = \cdots = E_r^{m_r} = \prod_{i\in 1}^{h} P_i \prod_{i=1}^{r} E_i \prod_{i=1}^{g} A_i B_i A_i^{-1} B_i^{-1} = I. \tag{2.2}$$

The generators P_i are parabolic, the E_i are elliptic, and A_i and B_i are hyperbolic.

3. The torsion-free and genus zero conditions

Let Γ be a Fuchsian group of the first kind. In most cases that occur in practice, Γ is a group commensurable with the modular group $\mathrm{PSL}_2(\mathbb{Z})$. The hyperbolic area of a fundamental domain for Γ acting on $\mathfrak{H}$ is $2\pi\chi(\Gamma)$, where $\chi(\Gamma)$ is the Euler characteristic of the fundamental domain given by

$$\chi(\Gamma) = 2(g-1) + h + \sum_{i=1}^{r}\Big(1 - \frac{1}{m_i}\Big), \tag{3.1}$$

where, as in Section 2, g is the genus, h is the number of inequivalent cusps (or the number of cusps in a fundamental domain), r is the number of inequivalent elliptic points, and $m_1, \dots, m_r$ are their orders. This formula is a consequence of the Riemann-Hurwitz formula.

If Γ is torsion-free (i.e., it has no elliptic elements) and has genus zero, then (3.1) becomes

$$\chi(\Gamma) = h - 2. \tag{3.2}$$

Moreover, from the presentation of Γ by generators and relations, we deduce that Γ can be generated by parabolic elements only, namely, $P_1, \dots, P_h$ with the relation $P_1 \cdots P_h = 1$. Omitting one of the generators makes Γ a free group of rank $h-1$.

PROPOSITION 3.1
If Γ *is a torsion-free genus zero group commensurable with the modular group, then* Γ *is a subgroup of* $\mathrm{PSL}_2(\mathbb{Q})$.

Proof
The set of cusps for the modular group consists of $\mathbb{Q}\cup\{\infty\}$, and the same is true for Γ since it is commensurable with $\mathrm{PSL}_2(\mathbb{Z})$. Assume that Γ is torsion-free and of genus zero so that it can be generated by a set of parabolic elements. Let P be any of these generators, and assume that P is represented by a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $ad - bc = 1$. The image by P of any cusp is also a cusp. In particular, $P \cdot 0$, $P \cdot 1$, and $P \cdot \infty$ are in $\mathbb{Q} \cup \{\infty\}$; that is, b/d, a/c, and $(a + b)/(c + d)$ are in $\mathbb{Q} \cup \{\infty\}$. It is not difficult to see that a, b, c, and d are rational multiples of a real number α. Since $\mathrm{Tr}(P) = \pm 2$, we deduce also that α is rational, so that P is in $\mathrm{PSL}_2(\mathbb{Q})$. □

Examples of Fuchsian groups of the first kind commensurable with the modular group are the so-called congruence groups that contain, as a subgroup of finite index, a principal congruence group $\Gamma(m)$ which is defined for a positive integer m by

$$\Gamma(m) = \{A \in \mathrm{PSL}_2(\mathbb{Z}),\ \ A \equiv \pm I \bmod m\}/\{\pm I\},$$

and the smallest such m is called the level of the group.

Let us now focus on groups of this sort which are subgroups of the modular group. Examples of such groups are

$$\Gamma_1(m) = \left\{A \in \mathrm{PSL}_2(\mathbb{Z}),\ \ A \equiv \pm \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod m\right\}/\{\pm I\},$$

$$\Gamma_0(m) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}),\ \ c \equiv 0 \bmod m\right\}/\{\pm I\}.$$

The indices of these groups in the modular group are given by

$$\left[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma(2)\right] = 2 \times \left[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(2)\right] = 6$$

and

$$\lambda(m) := \big[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma(m)\big] = \frac{m^3}{2} \prod_{\substack{p|m \\ p \text{ prime}}} \Big(1 - \frac{1}{p^2}\Big), \quad m > 2,$$

$$\lambda_1(m) := \big[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(m)\big] = \frac{m^2}{2} \prod_{\substack{p|m \\ p \text{ prime}}} \Big(1 - \frac{1}{p^2}\Big), \quad m > 2,$$

$$\lambda_0(m) := \big[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_0(m)\big] = m \prod_{\substack{p|m \\ p \text{ prime}}} \Big(1 + \frac{1}{p}\Big), \quad m \geq 1.$$

If Γ is subgroup of finite index of $\mathrm{PSL}_2(\mathbb{Z})$, then the hyperbolic area, $2\pi\chi(\Gamma)$, of a fundamental domain for Γ satisfies

$$2\pi\chi(\Gamma) = \lambda \cdot 2\pi\chi\big(\mathrm{PSL}_2(\mathbb{Z})\big),$$

where $\lambda = [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma]$. Since the hyperbolic area of $\mathrm{PSL}_2(\mathbb{Z})$ is $\pi/3$, we deduce from the above formula that $\chi(\Gamma) = \lambda/6$. Also, inside the modular group, elliptic elements have order 2 or 3, and we deduce from (3.1) that

$$\frac{\lambda}{6} = 2(g-1) + h + \frac{\nu_2}{2} + \frac{2\nu_3}{3}, \tag{3.3}$$

where ν_k $(k = 2, 3)$ is the number of inequivalent elliptic elements of order k. It follows that if Γ is torsion-free and of genus zero, then

$$\lambda = 6(h-2). \tag{3.4}$$

The group $\Gamma(m)$ is of genus zero if and only if $1 \leq m \leq 5$, $\Gamma_0(m)$ is of genus zero if and only if $m \in \{1, \ldots, 10, 12, 13, 16, 18, 25\}$, and $\Gamma_1(m)$ is of genus zero if and only if $m \in \{1, \ldots, 10, 12\}$. Meanwhile, $\Gamma(m)$ is torsion-free for $m \geq 2$, $\Gamma_1(m)$ is torsion-free for $m \geq 4$, and a trace argument shows that $\Gamma_0(m)$ is torsion-free if and only if -1 and -3 are not squares modulo m. We also mention that $\Gamma_0(m) = \Gamma_1(m)$ for $m \in \{1, 2, 3, 4, 6\}$.

4. A transfer theorem

The goal of this section is to show that every torsion-free genus zero subgroup of $\mathrm{PSL}_2(\mathbb{R})$ commensurable with $\mathrm{PSL}_2(\mathbb{Z})$ is conjugate to a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ of finite index.

We begin by giving a description of the full normalizer of $\Gamma_0(N)$ inside $\mathrm{PSL}_2(\mathbb{R})$. This description was given originally in [1] and clarified in [2].

Let N be a positive integer, let h be the largest divisor of 24 for which $h^2 \mid N$, and set $N = nh$. The normalizer of $\Gamma_0(N)$ consists of the transformations

$$A = \begin{pmatrix} ae & b/h \\ cn & de \end{pmatrix}, \quad \det(A) = e > 0 \text{ and } e \,||\, n/h, \tag{4.1}$$

where $r \,||\, s$ means $r \mid s$ and $\gcd(r, s/r) = 1$ (r is called an exact divisor of s), and a, b, c, d are integers.

The normalizer can also be described in terms of the Atkin-Lehner involutions that are defined as follows. Let e be an exact positive divisor of N; then the set W_e of matrices

$$B = \begin{pmatrix} ae & b \\ cN & de \end{pmatrix}, \quad \det(B) = e,$$

is a single coset of $\Gamma_0(N)$. This coset, considered as an element of the normalizer quotient of $\Gamma_0(N)$, is called an Atkin-Lehner involution for $\Gamma_0(N)$. The union of all Atkin-Lehner involutions is a subgroup of the normalizer described by (4.1). The Fricke involution $\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ occurs when $e = N$.

Let h be as above, and let $\Gamma_0(n|h)$ be the group of matrices $\left(\begin{smallmatrix} a & b/h \\ cn & d \end{smallmatrix}\right)$ of determinant 1. This group is a conjugate of $\Gamma_0(n/h)$ by $\left(\begin{smallmatrix} h & 0 \\ 0 & 1 \end{smallmatrix}\right)$. The Atkin-Lehner involutions for $\Gamma_0(n|h)$ are the conjugates by $\left(\begin{smallmatrix} h & 0 \\ 0 & 1 \end{smallmatrix}\right)$ of the Atkin-Lehner involutions of $\Gamma_0(n/h)$. The full normalizer of $\Gamma_0(N)$ in $\mathrm{PSL}_2(\mathbb{R})$ is obtained by adjoining to the group $\Gamma_0(N|h)$ its Atkin-Lehner involutions. With this in mind we denote the normalizer of $\Gamma_0(N)$ by $\Gamma_0(n|h)+$; the $+$ sign means that all the Atkin-Lehner involutions are present. If N is square-free, then the normalizer is $\Gamma_0(N)+$.

THEOREM 4.1

Every torsion-free genus zero discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$ *commensurable with the modular group is conjugate to a subgroup of* $\mathrm{PSL}_2(\mathbb{Z})$.

Proof

Let Γ be such a subgroup; then since the group Γ is commensurable with the modular group, using H. Helling's theorem in [3], it is conjugate to a subgroup of $\Gamma_0(m)+$ for a square-free m. Since Γ is torsion-free and of genus zero, its conjugate inside $\Gamma_0(m)+$ is also torsion-free and of genus zero. We may therefore assume without loss of generality that Γ is inside $\Gamma_0(m)+$. Furthermore, Γ can be generated by parabolic elements only. Let P be such a generator. Being an element of $\Gamma_0(m)+$, P has the form (4.1) where $h = 1$ since m is square-free. If we standardize P to have determinant 1, it must have trace equal to ± 2 since it is parabolic. This yields $(a + d)\sqrt{e} = \pm 2$. It follows that $e = 1$ or $e = 4$. The latter is not possible since $e \mid m$ and m is square-free. Therefore P is in $\Gamma_0(m)$. This being true for every parabolic generator of Γ, we deduce that Γ is a subgroup of $\Gamma_0(m)$. □

Theorem 4.1 can be seen as finding a common denominator for elements of the groups in Proposition 3.1. Also, note that the torsion-free and genus zero conditions are essential to the theorem.

5. Larcher congruence groups

In [4], [5], Larcher introduced a large class of congruence subgroups of modular groups of any given level. These groups generalize classical congruence groups like $\Gamma(n)$, $\Gamma_0(n)$, and $\Gamma_1(n)$. To describe them, we follow the treatment of [5]. We first introduce the notion of a cusp width. Let Γ be a subgroup of finite index of $\mathrm{PSL}_2(\mathbb{Z})$; then the stabilizer of a cusp in Γ is a subgroup of finite index in the stabilizer of the same cusp in $\mathrm{PSL}_2(\mathbb{Z})$. This index is called the width of the cusp.

Let m be a positive integer, and let d be a positive divisor of m. Write $m/d = h^2 n$, with n square-free. Let ε and χ be positive integers such that $\varepsilon \mid h$ and $\chi \mid \gcd(d\varepsilon, m/d\varepsilon^2)$, and let $\tau \in \{1, 2, \ldots, \chi\}$. Define the following:

$$\Gamma_\tau(m; m/d, \varepsilon, \chi) = \left\{ \pm \begin{pmatrix} 1 + \frac{m}{\varepsilon\chi}\alpha & d\beta \\ \frac{m}{\chi}\gamma & 1 + \frac{m}{\varepsilon\chi}\delta \end{pmatrix}, \quad \gamma \equiv \tau\alpha \mod \chi \right\}, \tag{5.1}$$

where α, β, γ, and δ are integers. Then, with exceptions $\Gamma_1(4; 2, 1, 2)$ and $\Gamma_1(8; 8, 2, 2)$ which have levels 2 and 4, respectively, the groups $\Gamma_\tau(m; m/d, \varepsilon, \chi)$, which we call Larcher congruence groups, are congruence groups of level m. Moreover, d is the least cusp width and corresponds to the cusp at ∞, while m is the width of the cusp at zero. In particular, if m is square-free, then $\varepsilon = \chi = 1$ and $\Gamma_\tau(m; m/d, \varepsilon, \chi) = \Gamma_1(m) \cap \Gamma(d)$. The cusp widths can be determined in terms of the rational presentation of the cusps and the various data attached to these groups. More interestingly, the Larcher groups describe the cusp widths of any congruence group in the following way. Let Γ be a congruence group of level m, and let d be the least cusp width in Γ. It is possible to conjugate Γ by a matrix in the modular group such that the width of ∞ becomes d and the width of zero becomes m. Note that a modular conjugacy only permutes the cusp widths; however, a nonmodular conjugacy often changes the set of cusp widths. According to [5, Sec. 3], for suitable ε, χ, and τ, the Larcher group $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ is a congruence group having the following properties:

(1) $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ is a subgroup of Γ;

(2) the cusp widths of Γ and $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ coincide.

This means that up to finding the right parameters d, ε, χ, and τ, one is able to describe all the cusp widths in Γ. We refer to $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ as the Larcher group corresponding to Γ.

6. Classification inside the modular group

In this section, we classify all the $\mathrm{PSL}_2(\mathbb{Z})$-conjugacy classes of congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ following [10].

PROPOSITION 6.1

Every torsion-free genus zero congruence subgroup of the modular group is conjugate to a Larcher congruence group.

Proof

Let Γ be a torsion-free genus zero congruence subgroup of level m. Then Γ has a set of parabolic generators. Up to a modular conjugacy, we can assume that the least cusp width d corresponds to ∞, and that the cusp zero has width m. Let $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ be the corresponding Larcher group. According to Section 5, the stabilizers of each cusp with respect to both groups are the same. It follows that every parabolic generator of Γ, which is a generator of the stabilizer of the corresponding cusp, is also in $\Gamma_\tau(m; m/d, \varepsilon, \chi)$. Therefore $\Gamma = \Gamma_\tau(m; m/d, \varepsilon, \chi)$. □

PROPOSITION 6.2

If $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ is of genus zero, then

$$d\varepsilon \leq 5, \qquad \frac{md}{\chi} \leq 25, \qquad \frac{m}{\varepsilon\chi} \leq 12. \tag{6.1}$$

Proof

It is clear that $\Gamma_\tau(m; m/d, \varepsilon, \chi) \subseteq \Gamma_0(m/\chi) \cap \Gamma_1(m/\varepsilon\chi) \cap \Gamma(d)$ since d divides $m/\varepsilon\chi$. Also, $\Gamma_0(m/\chi) \cap \Gamma(d)$ is conjugate to $\Gamma_0(md/\chi) \cap \Gamma_1(d)$, and $\Gamma_0(m/\chi) \cap \Gamma_1(m/\varepsilon\chi) \cap \Gamma(d)$ is conjugate to $\Gamma_1(m/\varepsilon\chi) \cap \Gamma(d\varepsilon)$ since $d\varepsilon$ divides $m/\varepsilon\chi$. A necessary condition to have $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ of genus zero is that the groups $\Gamma_0(md/\chi)$, $\Gamma_1(m/\varepsilon\chi)$, and $\Gamma(d\varepsilon)$ are all of genus zero. This yields (6.1). □

From Proposition 6.2, we see that $1 \leq d \leq 5$, and for each d there are few values of ε such that $d\varepsilon \leq 5$; namely, $\varepsilon = 1$ if $d = 3$, 4, or 5, $\varepsilon = 1$ or 2 if $d = 2$, and $1 \leq \varepsilon \leq 5$ if $d = 1$. This provides us with a (short) list of possible values of χ and τ in each case, and therefore with a (short) list of Larcher groups which contains the genus zero Larcher groups. All the genus zero groups that appear are conjugate to a $\Gamma(m)$, $\Gamma_0(m)$, or $\Gamma_1(m)$, except $\Gamma_1(8) \cap \Gamma(2)$ which can be checked to be of genus zero by finding its signature. The groups obtained which are not of genus zero are easily seen to be so because some conjugate of them is contained in a group of the form $\Gamma(m)$, $\Gamma_0(m)$, or $\Gamma_1(m)$ which is clearly not of genus zero (see [10] for more details). We have the following.

THEOREM 6.3
Up to modular conjugacy, there are exactly 33 *congruence subgroups of the modular group which are torsion-free and of genus zero, all of which are given in Table 1.*

Table 1

Index	*Level*	*Group*
6	2	$\Gamma(2)$
	4	$\Gamma_0(4)$
12	3	$\Gamma(3)$
	4	$\Gamma_0(4) \cap \Gamma(2)$
	5	$\Gamma_1(5)$
	6	$\Gamma_0(6)$
	8	$\Gamma_0(8)$
	9	$\Gamma_0(9)$
24	4	$\Gamma(4)$
	6	$\Gamma_0(3) \cap \Gamma(2)$
	7	$\Gamma_1(7)$
	8	$\Gamma_1(8),\ \Gamma_0(8) \cap \Gamma(2),\ \left\{\pm\left(\begin{smallmatrix} 1+4a & 2b \\ 4c & 1+4d \end{smallmatrix}\right), a \equiv c \mod 2\right\}$
	12	$\Gamma_0(12)$
	16	$\Gamma_0(16),\ \left\{\pm\left(\begin{smallmatrix} 1+4a & b \\ 8c & 1+4d \end{smallmatrix}\right), a \equiv c \mod 2\right\}$
36	6	$\Gamma_0(2) \cap \Gamma(3)$
	9	$\Gamma_1(9),\ \left\{\pm\left(\begin{smallmatrix} 1+3a & 3b \\ 3c & 1+3d \end{smallmatrix}\right), a \equiv c \mod 3\right\}$
	10	$\Gamma_1(10)$
	18	$\Gamma_0(18)$
	27	$\left\{\pm\left(\begin{smallmatrix} 1+3a & b \\ 9c & 1+3d \end{smallmatrix}\right), a \equiv c \mod 3\right\}$
48	8	$\Gamma_1(8) \cap \Gamma(2),\ \left\{\pm\left(\begin{smallmatrix} 1+4a & 4b \\ 4c & 1+4d \end{smallmatrix}\right), a \equiv c \mod 2\right\}$
	12	$\Gamma_1(12),\ \left\{\pm\left(\begin{smallmatrix} 1+6a & 2b \\ 6c & 1+6d \end{smallmatrix}\right), a \equiv c \mod 2\right\}$
	16	$\Gamma_0(16) \cap \Gamma_1(8),\ \left\{\pm\left(\begin{smallmatrix} 1+4a & 2b \\ 8c & 1+4d \end{smallmatrix}\right), a \equiv c \mod 2\right\}$
	24	$\left\{\pm\left(\begin{smallmatrix} 1+6a & b \\ 12c & 1+6d \end{smallmatrix}\right), a \equiv c \mod 2\right\}$
	32	$\left\{\pm\left(\begin{smallmatrix} 1+4a & b \\ 16c & 1+4d \end{smallmatrix}\right), a \equiv c \mod 2\right\}$
60	5	$\Gamma(5)$
	25	$\Gamma_0(25) \cap \Gamma_1(5)$

7. Classification inside $\mathrm{PSL}_2(\mathbb{R})$

In this section, we list all the $\mathrm{PSL}_2(\mathbb{R})$-conjugacy classes of torsion-free genus zero congruence subgroups of $\mathrm{PSL}_2(\mathbb{R})$. According to Theorem 4.1, each such group is conjugate to a subgroup of the modular group. If we establish that this conjugate

is also a congruence group, then it is a modular conjugate of one in the list from Theorem 6.3.

PROPOSITION 7.1
If Γ is a congruence subgroup of $\mathrm{PSL}_2(\mathbb{R})$ which has conjugates inside $\mathrm{PSL}_2(\mathbb{Z})$, then any of these conjugates is a congruence group.

Proof
Let Γ be a congruence subgroup of $\mathrm{PSL}_2(\mathbb{R})$ of level n. Let $C = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $ad - bc = 1$, such that $C^{-1}\Gamma C \subseteq \mathrm{PSL}_2(\mathbb{Z})$. Since $\Gamma(n) \subseteq \Gamma$, the two matrices

$$C^{-1}\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} C = \begin{pmatrix} 1 - abn & -b^2 n \\ a^2 n & 1 + abn \end{pmatrix}$$

and

$$C^{-1}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} C = \begin{pmatrix} 1 + cdn & d^2 n \\ -c^2 n & 1 - cdn \end{pmatrix}$$

have integer entries. We deduce that a^2n, b^2n, c^2n, d^2n, abn, and cdn are in $\mathbb{Z}$. Using this fact and multiplying $ad - bc = 1$ by adn^2, we obtain $adn^2 \in \mathbb{Z}$. Similarly, we have acn^2, bcn^2, $bdn^2 \in \mathbb{Z}$. We are going to show that $\Gamma(n^3) \subseteq C^{-1}\Gamma C$. Let

$$A = \begin{pmatrix} 1 + n^3 x & n^3 y \\ n^3 z & 1 + n^3 t \end{pmatrix} \in \Gamma(n^3);$$

then $CAC^{-1} = \left(\begin{smallmatrix} X & Y \\ Z & T \end{smallmatrix}\right)$, where

$$\begin{aligned} X &= 1 + n^3(adx + bdz - acy - bct), \\ Y &= n^3(a^2 y + abt - abx - b^2 z), \\ Z &= n^3(cdx + d^2 z - c^2 y - cdt), \\ T &= 1 + n^3(acy + adt - bcx - bdz). \end{aligned}$$

It is clear that $CAC^{-1} \in \Gamma(n) \subseteq \Gamma$. This is also true if $A \equiv -I \bmod n^3$. □

Remark 7.1
The same calculations show that if Γ contains $\Gamma_1(n)$ (rather than $\Gamma(n)$), then any of its conjugates inside $\mathrm{PSL}_2(\mathbb{Z})$ contains $\Gamma(n^2)$, and if Γ contains $\Gamma_0(n)$, then its conjugates in $\mathrm{PSL}_2(\mathbb{Z})$ contain $\Gamma(n)$.

In view of Proposition 7.1, any torsion-free genus zero congruence subgroup of $\mathrm{PSL}_2(\mathbb{R})$ is conjugate to a group from the list of Theorem 6.3. Thus, we need only find the $\mathrm{PSL}_2(\mathbb{R})$-conjugacy classes among the groups of Theorem 6.3. Also, we need only look at each index since subgroups of different indices cannot be conjugate.

Index 6. The groups $\Gamma(2)$ and $\Gamma_0(4)$ are conjugate by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Index 12. The groups $\Gamma(3)$ and $\Gamma_0(9)$ are conjugate by $\left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and the groups $\Gamma_0(4) \cap \Gamma(2)$ and $\Gamma_0(8)$ are conjugate by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Index 24. The groups $\Gamma_0(3) \cap \Gamma(2)$ and $\Gamma_0(12)$ are conjugate by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ since $\Gamma_0(3) \cap \Gamma(2) = \Gamma_0(6) \cap \Gamma(2)$. The group $\Gamma(4)$ is conjugate by $\left(\begin{smallmatrix} 4 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ to $\Gamma_0(16)$, and it is conjugate by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ to $\Gamma_0(8) \cap \Gamma(2)$. The group $\Gamma_1(8)$ is conjugate by $\left(\begin{smallmatrix} 1 & 1/2 \\ 0 & 1 \end{smallmatrix}\right)$ to the group

$$\left\{ \pm \begin{pmatrix} 1+4a & b \\ 8c & 1+4d \end{pmatrix}, \ a \equiv c \bmod 2 \right\}$$

which is conjugate by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ to

$$\left\{ \pm \begin{pmatrix} 1+4a & 2b \\ 4c & 1+4d \end{pmatrix}, \ a \equiv c \bmod 2 \right\}.$$

Index 36. The group $\Gamma_0(2) \cap \Gamma(3)$ is conjugate to $\Gamma_0(18)$. The group $\Gamma_1(9)$ is conjugate by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 3 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ to

$$\left\{ \pm \begin{pmatrix} 1+3a & 3b \\ 3c & 1+3d \end{pmatrix}, \ a \equiv c \bmod 3 \right\},$$

and it is conjugate by $\left(\begin{smallmatrix} 1 & \tau/3 \\ 0 & 1 \end{smallmatrix}\right)$, $\tau = \pm 1$, to

$$\left\{ \pm \begin{pmatrix} 1+3a & b \\ 9c & 1+3d \end{pmatrix}, \ a \equiv \tau c \bmod 3 \right\}.$$

Index 48. The group $\Gamma_1(8) \cap \Gamma(2)$ is conjugate by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1/2 \\ 0 & 1 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 1 & 1/4 \\ 0 & 1 \end{smallmatrix}\right)$, respectively, to

$$\Gamma_0(16) \cap \Gamma_1(8),$$

$$\left\{ \pm \begin{pmatrix} 1+4a & 4b \\ 4c & 1+4d \end{pmatrix}, \ a \equiv c \bmod 2 \right\},$$

$$\left\{ \pm \begin{pmatrix} 1+4a & 2b \\ 8c & 1+4d \end{pmatrix}, \ a \equiv c \bmod 2 \right\},$$

and

$$\left\{ \pm \begin{pmatrix} 1+4a & b \\ 16c & 1+4d \end{pmatrix}, \ a \equiv c \bmod 2 \right\}.$$

The group $\Gamma_1(12)$ is conjugate by $\left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ to

$$\left\{ \pm \begin{pmatrix} 1+6a & 2b \\ 6c & 1+6d \end{pmatrix}, \ a \equiv c \bmod 2 \right\}$$

and by $\left(\begin{smallmatrix} 1 & 1/2 \\ 0 & 1 \end{smallmatrix}\right)$ to

$$\left\{ \pm \begin{pmatrix} 1+6a & b \\ 12c & 1+6d \end{pmatrix},\ a \equiv c \bmod 2 \right\}.$$

Index 60. The group $\Gamma(5)$ is conjugate by $\left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ to $\Gamma_0(25) \cap \Gamma_1(5)$.

THEOREM 7.2
There are 15 $\mathrm{PSL}_2(\mathbb{R})$*-conjugacy classes of torsion-free genus zero congruence subgroups of* $\mathrm{PSL}_2(\mathbb{R})$. *Representatives for these classes are* $\Gamma(5)$, $\Gamma_1(8) \cap \Gamma(2)$, $\Gamma_0(n)$ *for* $n = 4, 6, 8, 9, 12, 16, 18$, *and* $\Gamma_1(n)$ *for* $n = 5, 7, 8, 9, 10, 12$.

Proof
In view of the above discussion, the congruence groups listed in this theorem form a set of representatives for the $\mathrm{PSL}_2(\mathbb{R})$-conjugacy classes of torsion-free genus zero congruence subgroups. We need only check that no two of them are conjugate. Since all these groups are in $\mathrm{PSL}_2(\mathbb{Z})$, the proof of Proposition 7.1 provides us with a necessary condition for two such groups to be $\mathrm{PSL}_2(\mathbb{R})$-conjugate; namely, if one contains $\Gamma(n)$ for some n, then the other one must contain $\Gamma(n^3)$. For the groups listed in the theorem, this would imply that if two of them are conjugate, then their levels have the same set of prime divisors. This allows us to see that each two groups of the same index in the list are not conjugate. □

8. Subgroups containing $\Gamma_0(n)$

In this section, as an application of the above, we investigate the groups given in Theorem 7.2 that have a conjugate containing $\Gamma_0(n)$. These groups are of interest in Moonshine and the theory of replicable functions, and they were studied in [6], [7]. Ignoring the groups $\Gamma_0(n)$, we have to deal with the groups $\Gamma_1(n)$, in addition to $\Gamma_1(8) \cap \Gamma(2)$ and $\Gamma(5)$.

Let N be a positive integer such that $\Gamma_1(N)$ contains a conjugate of $\Gamma_0(n)$ for some n. According to Remark 7.1, we must have $\Gamma(n) \subseteq \Gamma_1(N)$. It follows that $N \mid n$. Let $C = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $ad - bc = 1$ (a, b, c, d real numbers), such that $C\Gamma_0(n)C^{-1} \subseteq \Gamma_1(N)$. We have

$$C \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} C^{-1} = \begin{pmatrix} 1-ac & a^2 \\ -c^2 & 1+ac \end{pmatrix} \in \Gamma_1(N)$$

and

$$C \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} C^{-1} = \begin{pmatrix} 1+bdn & -b^2 n \\ d^2 n & 1-bdn \end{pmatrix} \in \Gamma_1(N).$$

It follows that

$$ac \equiv c^2 \equiv bdn \equiv d^2 n \equiv 0 \mod N \qquad \text{and} \qquad a^2, b^2 n \in \mathbb{Z}. \tag{8.1}$$

Let $\alpha \in \mathbb{Z}$ such that $\gcd(\alpha, n) = 1$. There exist β and γ such that $\alpha\gamma - \beta n = 1$, so that $A = \left(\begin{smallmatrix} \alpha & \beta \\ n & \gamma \end{smallmatrix}\right) \in \Gamma_0(n)$. The product $CAC^{-1} = \left(\begin{smallmatrix} X & Y \\ Z & T \end{smallmatrix}\right)$, where

$$\begin{aligned} X &= ad\alpha + bdn - ac\beta - bc\gamma, \\ Y &= a^2\beta + ab\gamma - ab\alpha - b^2 n, \\ Z &= cd\alpha + d^2 n - c^2\beta - cd\gamma, \\ T &= ac\beta + ad\gamma - bc\alpha - bdn \end{aligned}$$

must be in $\Gamma_1(N)$, so that $X \equiv T \equiv \pm 1 \bmod N$, $Z \equiv 0 \bmod N$, and $Y \in \mathbb{Z}$. Using (8.1) we deduce from the expressions of X and T that

$$ad\alpha - bc\gamma \equiv ad\gamma - bc\alpha \equiv \pm 1 \mod N. \tag{8.2}$$

Since $ad - bc = 1$, these equations sum to

$$\alpha + \gamma \equiv \pm 2 \mod N.$$

Since $\det(A) = 1$, we have $\alpha\gamma \equiv 1 \bmod n$ and hence mod N since $N \mid n$. We deduce that $\alpha^2 + 1 \equiv \pm 2\alpha \bmod N$. Meanwhile, because α is an arbitrary element of $(\mathbb{Z}/n\mathbb{Z})^\times$ and $N \mid n$, α can be any element of $(\mathbb{Z}/N\mathbb{Z})^\times$ since the projection $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective. We have shown the following.

PROPOSITION 8.1
If $\Gamma_1(N)$ contains a conjugate of $\Gamma_0(n)$ for some n, then

$$\forall a \in (\mathbb{Z}/N\mathbb{Z})^\times, \quad (a \pm 1)^2 \equiv 0 \mod N. \tag{8.3}$$

PROPOSITION 8.2
The only positive integers N for which (8.3) holds are the divisors of 16 *and* 36.

Proof
Let N be such an integer, and write $N = 2^k N'$ with $\gcd(2, N') = 1$; then the integer $a = 2 + N'$ is relatively prime to N, so that $(a \pm 1)^2 \equiv 0 \bmod N$ and hence mod N'. This implies $N' \mid 9$. Hence, only 2 and 3 may divide N. It follows that 5 is relatively prime to N, so that $(5 \pm 1)^2 \equiv 0 \bmod N$, yielding $N \mid 16$ or $N \mid 36$. Conversely, each positive divisor of 16 or 36 satisfies (8.3). □

Remark 8.1
If we require that $\Gamma_1(N)$ contain some $\Gamma_0(n)$, then a necessary condition is

$$\forall a \in (\mathbb{Z}/N\mathbb{Z})^\times, \quad a \pm 1 \equiv 0 \mod N,$$

which holds if and only if N is a divisor of 4 or 6. Conversely, for each positive divisor N of 4 or 6, we have $\Gamma_1(N) = \Gamma_0(N)$, a fact that was mentioned at the end of Section 3.

Remark 8.2
For the remainder of this section, we implicitly use the following fact: the positive divisors of 24 are the only positive integers r for which

$$\forall x, y, \ xy \equiv 1 \bmod r \Longrightarrow x \equiv y \bmod r.$$

This property is also essential in describing the normalizer of $\Gamma_0(n)$ as in Section 4.

Using Proposition 8.2, the groups $\Gamma_1(N)$ for $N = 5, 7, 10$ do not contain any conjugate of a $\Gamma_0(n)$. This is also true for $\Gamma(5) \subset \Gamma_1(5)$. If $P = \left(\begin{smallmatrix} 9 & -2 \\ 27 & -3 \end{smallmatrix}\right)$, then $P\Gamma_0(81)P^{-1} \subset \Gamma_1(9)$; this uses the simple fact that if $ad \equiv 1 \bmod 9$, then $2a - d \equiv 2d - a \equiv \pm 1 \bmod 9$. For the group $\Gamma_1(8) \cap \Gamma(2)$, we proceed in the following way: the invariance group of the Hauptmodul $\eta(\tau)/\eta(4\tau)$, where η is the Dedekind eta-function, is a modular subgroup with index 48 and level 32. (It can be easily checked that it contains $\Gamma(32)$, which is enough for our purposes.) It must be a conjugate of one of the two representatives of the index 48 subgroups, namely, $\Gamma_1(8) \cap \Gamma(2)$ and $\Gamma_1(12)$. The latter is excluded since its level is divisible by 3. Moreover, the invariance group of $\eta(8\tau)/\eta(32\tau)$ (the conjugate by $\tau \mapsto 8\tau$ of $\eta(\tau)/\eta(4\tau)$) contains $\Gamma_0(2^8)$. Therefore $\Gamma_1(8) \cap \Gamma(2)$ contains a conjugate of $\Gamma_0(2^8)$, and so does $\Gamma_1(8)$. A conjugating matrix is $\left(\begin{smallmatrix} 16 & -1 \\ 32 & 2 \end{smallmatrix}\right)$.

Remark 8.3
The same argument works for $\Gamma_1(9)$ since it is conjugate to the invariance group of $\eta(\tau)/\eta(9\tau)$, and $\eta(3\tau)/\eta(27\tau)$ is invariant under $\Gamma_0(81)$.

It was conjectured in [7] that no other genus zero torsion-free group besides those conjugated to the above ones contains a conjugate of some $\Gamma_0(n)$. To prove this conjecture, we need to eliminate the case of $\Gamma_1(12)$.

PROPOSITION 8.3
Let n be a positive integer divisible by 12, *and let k be an integer. If the equation*

$$x(x + k) \equiv 1 \mod n \tag{8.4}$$

has a solution, then there are four solutions that are distinct modulo 12.

Proof
Assume that the equation (8.4) has a solution x_0; then $-x_0 - k$ is also a solution. Also, $x_0 + k$ is an inverse of x modulo n and hence modulo 12, and therefore k is a multiple of 12 by Remark 8.2. Write $n = 2^\alpha 3^\beta n'$ with $\gcd(6, n') = 1$, and consider the following four systems:

$$\begin{aligned} x &\equiv x_0 \mod n', \\ x &\equiv x_1 \mod 2^\alpha, \\ x &\equiv x_2 \mod 3^\beta, \end{aligned}$$

where x_1 and x_2 take values in $\{x_0, -x_0 - k\}$. By the Chinese remainder theorem, each system provides a solution to equation (8.4). Meanwhile, x_0 and $-x_0 - k$ are distinct modulo 4 and modulo 3 since $k \equiv 0 \bmod 12$. It follows that the four systems yield four solutions to (8.4) that are distinct modulo 12. □

COROLLARY 8.4
There is no positive integer n for which $\Gamma_0(n)$ *has a conjugate inside* $\Gamma_1(12)$.

Proof
Assume there exists a positive integer n and a real matrix $C = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $ad - bc = 1$ such that $C\Gamma_0(n)C^{-1} \subseteq \Gamma_1(12)$. By Remark 7.1, $12 \mid n$. Since the projection $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/12\mathbb{Z})^\times$ is surjective, we can choose $x_0 \in \mathbb{Z}$ with $\gcd(x_0, n) = 1$ and $x_0 \equiv 1 \bmod 12$. Let y_0 and z_0 be such that $x_0 z_0 - n y_0 = 1$. Set $k = z_0 - x_0$ so that x_0 is a solution to the equation $x(x + k) \equiv 1 \bmod n$. Using Proposition 8.3, there exists x_1 such that $x_1(x_1 + k) \equiv 1 \bmod n$ and $x_1 \equiv 7 \bmod 12$. Hence, if we set $z_1 = x_1 + k$, there exists y_1 such that $x_1 z_1 - n y_1 = 1$. The matrices $\left(\begin{smallmatrix} x_0 & y_0 \\ n & z_0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} x_1 & y_1 \\ n & z_1 \end{smallmatrix}\right)$ are in $\Gamma_0(n)$ and hence are conjugated by C into $\Gamma_1(12)$. Using the relations (8.2) with $(\alpha, \gamma) = (x_i, z_i)$, $i = 0, 1$, and taking into account that both matrices have traces congruent to 2 modulo 12 because of the choices of x_0 and x_1, we have

$$adx_0 - bcz_0 \equiv 1 \mod 12, \qquad adx_1 - bcz_1 \equiv 1 \mod 12.$$

Since $ad - bc = 1$ and $z_0 - x_0 = z_1 - x_1 = k$, taking the difference of these two congruences yields $x_0 - x_1 \equiv 0 \bmod 12$, which is a contradiction since x_0 and x_1 were chosen such that $x_0 - x_1 \equiv \pm 6 \bmod 12$. The corollary follows. □

THEOREM 8.5
Any torsion-free genus zero group containing some $\Gamma_0(n)$ *with finite index is conjugate to one of the following groups:*

$$\Gamma_1(8),\ \Gamma_1(9),\ \Gamma_1(8) \cap \Gamma(2),\ \Gamma_0(n) \quad \text{for } n = 4, 6, 8, 9, 12, 16, 18.$$

9. A special case

In this section, we study some properties of the index 12 groups that were found in the previous sections. More interesting properties (geometric and analytic) and details can be found in [11].

The groups described in this paper are all congruence groups. If we drop the congruence condition, then there are infinitely many torsion-free genus zero subgroups of the modular group. In fact, for each λ and h satisfying $\lambda = 6(h-2)$, there is a torsion-free genus zero subgroup of the modular group with index λ and h cusps (see [8]). However, if the number of cusps is arbitrary, this is not true of the cusp widths. The situation is as follows: let X be a set of λ letters, and consider pairings (x, y) of permutations x and y acting on X satisfying $x^2 = y^3 = 1$ and such that the group generated by x and y is transitive on X. We define the equivalence classes (x, y) modulo a conjugation of x and y by a permutation in $\mathfrak{S}_\lambda$. Then there is a one-to-one correspondence between conjugacy classes of subgroups of finite index λ in the modular group and equivalence classes of pairings (x, y) (see [8]). The subgroup is torsion-free if and only if x and y are fixed point free, and it is of genus zero if and only if the total number of disjoint cycles of x, y, and xy is $\lambda + 2$. Moreover, the subgroup has cusp widths $n_1, n_2, \ldots, n_h$, where h is the number of cusps, if and only if the permutation xy consists of h disjoint cycles of lengths $n_1, n_2, \ldots, n_h$.

If we look at the case $\lambda = 12$, we want x and y acting fixed point freely on a set of 12 elements such that $\langle x, y\rangle$ is transitive on these points and such that xy decomposes into 4 cycles of lengths n_1, n_2, n_3, n_4 with $\sum n_i = 12$. It is not difficult to check (by computer or simply using graph theory; see [11]) that the only partitions of 12 into 4 positive integers which are realized are those listed in Table 2 with the corresponding groups. These also account for all the equivalence classes of pairings (x, y).

Notice that the cusp widths of Table 2 give all the possible quadruples of positive integers whose sum is 12 and whose product is a square. This fact has an explanation related to the theory of modular elliptic surfaces (see [11]). We deduce the following from Table 2.

PROPOSITION 9.1

The six congruence subgroups of index 12 *given in Table 1 account for all the torsion-free genus zero subgroups of index* 12 *in* $\mathrm{PSL}_2(\mathbb{Z})$.

If a subgroup of $\mathrm{PSL}_2(\mathbb{R})$ is conjugate to a torsion-free genus zero subgroup of index 12 in $\mathrm{PSL}_2(\mathbb{Z})$, then this group has only four cusps or, equivalently, a fundamental domain for this group has hyperbolic area 4π. Proposition 9.1, together with Theorem 4.1, shows that there are only four conjugacy classes of torsion-free genus zero

Table 2

$\Gamma(3)$	$3-3-3-3$
$\Gamma_0(4)\cap\Gamma(2)$	$4-4-2-2$
$\Gamma_1(5)$	$5-5-1-1$
$\Gamma_0(6)$	$6-3-2-1$
$\Gamma_0(8)$	$8-2-1-1$
$\Gamma_0(9)$	$9-1-1-1$

subgroups of $\mathrm{PSL}_2(\mathbb{R})$ having hyperbolic area 4π which can be represented by only four congruence subgroups of the modular group. Because these groups are torsion-free and of genus zero, the quotient of the upper half-plane $\mathfrak{H}$ by one of these groups is just the projective line $\mathbb{P}^1$ minus four points. To determine these four points, we need to find a Hauptmodul for each group as well as its values at the cusps. For the four $\mathrm{PSL}_2(\mathbb{R})$-conjugacy classes representing the six modular subgroups of index 12, we have Table 3.

Table 3

Group	*Hauptmodul*	*Values at the cusps*
$\Gamma(3)$	$\left(\frac{\eta(\tau/3)}{\eta(3\tau)}\right)^3$	$3, z^2+3z+9, \infty$
$\Gamma_0(4)\cap\Gamma(2)$	$\frac{\eta(2\tau)^{12}}{\eta(\tau)^4\eta(4\tau)^8}$	$4, -4, 0, \infty$
$\Gamma_1(5)$	$\frac{1}{q}\prod_{n=1}^{\infty}(1-q^n)^{-5\left(\frac{n}{5}\right)}$	$z^2-11z-1, 0, \infty$
$\Gamma_0(6)$	$\frac{\eta(\tau)^5\eta(3\tau)}{\eta(2\tau)\eta(6\tau)^5}$	$5, -4, -3, \infty$

In the expression of the Hauptmodul for $\Gamma_1(5)$, $\left(\frac{n}{5}\right)$ denotes the Legendre symbol

and $q = \exp(2\pi i\tau)$. The quadratic polynomials indicate that their roots are values for the Hauptmoduls, and the order in which these values are listed follows the ordering of the cusp widths given in Table 2. The Hauptmoduls are chosen so that their Fourier expansion in q has the form $q^{-1/m}+\mathrm{O}(q^{1/m})$, where m is the cusp width at ∞, except for $\Gamma_1(5)$ which has the form $1/q+5+\mathrm{O}(q)$. The expressions for the Hauptmoduls and their values are found in the Moonshine tables of [2], except for $\Gamma_1(5)$ whose Hauptmodul f is deduced from $\Gamma(5)$ and whose values are deduced from $\Gamma_0(5)$, namely, that the Hauptmodul for $\Gamma_1(5)$ is simply the fifth power of the one for $\Gamma(5)$. If g is a Hauptmodul for $\Gamma_0(5)$ of the form $1/q+\mathrm{O}(q)$, then g takes the values 6 and ∞ at the two cusps of $\Gamma_0(5)$. By desymmetrizing ($\Gamma_1(5)$ has index 2 in $\Gamma_0(5)$), we have

$$g = f - 5 + \frac{1}{f}$$

which leads to the values of f given in Table 3.

Theorem 9.2 determines up to isomorphism all the modular curves, that is, quotients of the upper half-plane $\mathfrak{H}$ by a modular subgroup, which are given by $\mathbb{P}^1$ minus four points. Applying a linear fractional transformation to the four values for each group in Table 3 so that each triple is sent to $0, 1, \infty$, we obtain 17 different values for the fourth cusp. Denoting $\exp(2\pi i/3)$ by ω and the roots of $z^2-125z+125$ by α and β, we have the following.

THEOREM 9.2
The curve $\mathbb{P}^1 \setminus \{0, 1, \infty, z\}$ is a modular curve if and only if z or $1/z$ is a member of

$$\left\{-8, -1, \frac{9}{8}, 2, 9, -\omega, \alpha, \beta, -\frac{\alpha}{\beta}\right\}.$$

Using Theorem 4.1 and Proposition 9.1, we deduce the following.

COROLLARY 9.3
The only values of z for which $\mathbb{P}^1 \setminus \{0, 1, \infty, z\}$ is a quotient of the upper half-plane by a Fuchsian group commensurable with the modular group are those given by Theorem 9.2.

Acknowledgment. I thank John McKay for his support and insights. I also thank Oliver Atkin for helpful discussions.

References

[1] A. O. L. ATKIN and J. LEHNER, *Hecke operators on $\Gamma_0(m)$*, Math. Ann. **185** (1970), 134–160. MR 42:3022 382

[2] J. H. CONWAY and S. P. NORTON, *Monstrous moonshine*, Bull. London Math. Soc. **11** (1979), 308–339. MR 81j:20028 382, 395

[3] H. HELLING, *On the commensurability class of the rational modular group*, J. London Math. Soc. (2) **2** (1970), 67–72. MR 43:3353 383

[4] H. LARCHER, *The cusp amplitudes of the congruence subgroups of the classical modular group*, Illinois J. Math. **26** (1982), 164–172. MR 83a:10040 378, 384

[5] ———, *The cusp amplitudes of the congruence subgroups of the classical modular group, II*, Illinois J. Math. **28** (1984), 312–338. MR 85i:11034 378, 384

[6] J. MCKAY and A. SEBBAR, *Fuchsian groups, Schwarzians, and theta functions*, C. R. Acad. Sci. Paris Sér. I Math. **327** (1998), 343–348. MR 2000a:11059 378, 389

[7] ———, *Fuchsian groups, automorphic functions and Schwarzians*, Math. Ann. **318** (2000), 255–275. MR CMP 1 795 562 378, 389, 391

[8] M. H. MILLINGTON, *Subgroups of the classical modular group*, J. London Math. Soc. (2) **1** (1969), 351–357. MR 39:5477 393

[9] R. A. RANKIN, *Modular Forms and Functions*, Cambridge Univ. Press, Cambridge, 1977. MR 58:16518 379

[10] A. SEBBAR, *Classification of torsion-free genus zero congruence groups*, Proc. Amer. Math. Soc. **129** (2001), 2517–2527. MR CMP1 838 872 385

[11] ———, *Modular subgroups, forms, curves, and surfaces*, to appear in Canad. Math. Bull. http://journals.cms.math.ca/cgi-bin/vault/viewprepub/sebbar8056.prepub 393

[12] G. SHIMURA, *Introduction to the Arithmetic Theory of Automorphic Functions*, Kanô Memorial Lectures **1**, Iwanami Shoten, Tokyo; Publ. Math. Soc. Japan **11**, Princeton Univ. Press, Princeton, 1971. MR 47:3318 379

[13] J. G. THOMPSON, "A finiteness theorem for subgroups of PSL(2, **R**) which are commensurable with PSL(2, **Z**)" in *The Santa Cruz Conference on Finite Groups (Santa Cruz, Calif., 1979)*, Proc. Sympos. Pure Math. **37**, Amer. Math. Soc., Providence, 1980, 533–555. MR 82b:20067 377

[14] P. ZOGRAF, *A spectral proof of Rademacher's conjecture for congruence subgroups of the modular group*, J. Reine Angew. Math. **414** (1991), 113–116. MR 92d:11041 377

Department of Mathematics and Statistics, University of Ottawa, Ottawa, Ontario K1N 6N5, Canada; sebbar@mathstat.uottawa.ca