http://ijgt.ui.ac.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 11 No. 3 (2022), pp. 131-150.

www.ui.ac.ir

ON EFFICIENT PRESENTATIONS OF THE GROUPS PSL($2, m$)

ORLIN STOYTCHEV

Abstract. We exhibit presentations of the Von Dyck groups $D(2,3,m)$, $m \geq 3$, in terms of two generators of order m satisfying three relations, one of which is Artin's braid relation. By dropping the relation which fixes the order of the generators we obtain the universal covering groups of the corresponding Von Dyck groups. In the cases $m = 3, 4, 5$, these are respectively the double covers of the finite rotational tetrahedral, octahedral and icosahedral groups. When $m \geq 6$ we obtain infinite covers of the corresponding infinite Von Dyck groups. The interesting cases arise for $m \geq 7$ when these groups act as discrete groups of isometries of the hyperbolic plane. Imposing a suitable third relation we obtain three-relator presentations of PSL$(2, m)$. We discover two general formulas presenting these as factors of $D(2,3,m)$. The first one works for any odd m and is essentially equivalent to the shortest known presentation of Sunday [J. Sunday, Presentations of the groups SL(2, m) and PSL(2, m), *Canadian J. Math.*, **24** (1972) 1129–1131]. The second applies to the cases $m \equiv \pm 2 \pmod 3$, $m \not\equiv 11 \pmod{30}$, and is substantively shorter. Additionally, by random search, we find many efficient presentations of finite simple Chevalley groups PSL$(2, q)$ as factors of $D(2,3,m)$ where m divides the order of the group. The only other simple group that we found in this way is the sporadic Janko group J_2.

1. Rotations, Braid Groups, Von Dyck Groups and Their Covers

The Von Dyck groups $D(l, n, m)$, which many authors call rotational triangle groups, or just triangle groups, are the finitely presented groups with two generators and three relations as follows [7]:

$$D(l,n,m) := \left\langle x, y \,|\, x^l = y^n = (xy)^m = \mathbf{1} \right\rangle \ , \tag{1.1}$$

where l, n, and m are integers greater than 1. These groups have a geometric realization as discrete subgroups of the groups of isometries of a simply connected Riemann surface with constant positive

Communicated by Alireza Moghaddamfar.
MSC(2010): Primary: 20F05; Secondary: 20G40, 20F36, 20H05.
Keywords: Von Dyck groups, Braid groups, Chevalley groups.
Received: 21 May 2021, Accepted: 14 July 2021.
Article Type: Research Paper.
http://dx.doi.org/10.22108/IJGT.2021.128791.1696 .

curvature (sphere), zero curvature (Euclidean plane), or negative curvature (hyperbolic plane). They are generated by rotations about two of the vertices of a geodesic triangle with angles π/l, π/n, and π/m. The rotations are at angles twice the angle at each vertex. Obviously depending on whether the sum $\frac{1}{l} + \frac{1}{n} + \frac{1}{m}$ is greater than, equal, or less than 1, we get a geodesic triangle on the sphere, the Euclidean plane, or the hyperbolic plane, respectively. Further, in the non-Euclidean cases, if we assume that the curvature has absolute value 1, the Gauss-Bonnet Theorem fixes the size of the defining triangle.

The action of the Von Dyck group defined in this way covers the surface by congruent copies of the defining triangle and its mirror image across one of the sides and produces a tessellation of the surface. The defining triangle and its reflection constitute a fundamental domain for the action of the group. It is quite obvious from the geometric picture that the Von Dyck groups are finite in the spherical case and infinite otherwise.

We concentrate further on the most symmetric cases $D(2,3,m)$, $m \geq 3$, which we call equilateral, as the large triangle obtained by the action of y on the fundamental domain is equilateral. The sum $\frac{1}{2} + \frac{1}{3} + \frac{1}{m}$ is greater than 1 only when $m = 3, 4, 5$. The sphere is tessellated by the equilateral triangles described above and m is the number of triangles that meet at each vertex. Thus, we get a spherical model of the tetrahedron when $m = 3$, of the octahedron when $m = 4$, and of the icosahedron when $m = 5$. The groups of rotational symmetries of these regular polyhedra are precisely the finite groups $D(2,3,3)$ of order 12, $D(2,3,4)$ of order 24 and $D(2,3,5)$ of order 60. The hyperbolic case is of greater interest as many interesting finite groups are obtained as factors of Von Dyck groups.

The geometric picture suggests a different set of generators for $D(2,3,m)$. We consider a regular tessellation with Schläfli symbol $\{3,m\}$ by congruent equilateral geodesic triangles and rotations a and b about two of the vertices (which we also denote by a and b) of one of the triangles at an angle $2\pi/m$, which is the angle at each vertex. It is immediate that $x = aba$ and $y = ab$. However, as shown on Figure 1, we also have $x = bab$, which implies that the two generators satisfy Artin's braid relation $aba = bab$.

Further, a and b satisfy $ab^2a = b^{m-2}$, which is illustrated on Figure 2. Notice that this relation carries information about the number m of triangles that meet at each vertex of the tessellation.

The third relation is a condition on the order of (both) generators, namely $a^m = \mathbf{1}$.

Proposition 1.1. *The group $D_m := \langle a, b \mid aba = bab,\ ab^2a = b^{m-2},\ a^m = \mathbf{1} \rangle$ is isomorphic to the Von Dyck group $D(2,3,m)$.*

Proof. We notice that the group D_m is a factor group of the braid group with three strands B_3. The latter has an obvious automorphism generated by the the map $a \leftrightarrow b$, so any additional relation for a and b automatically implies a symmetric relation with a and b interchanged. This observation shows why having two generators that satisfy Artin's braid relation is economical. In particular it follows that $b^m = \mathbf{1}$ and $ba^2b = a^{m-2}$. We can also see these directly. Indeed, applying Artin's braid relation

http://dx.doi.org/10.22108/IJGT.2021.128791.1696

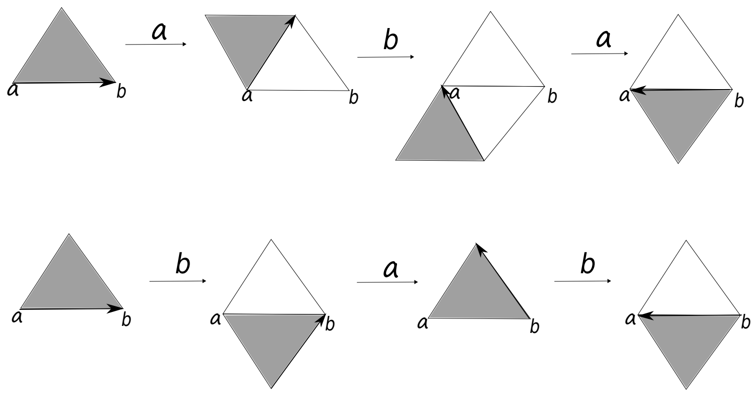

FIGURE 1. An illustration of Artin's relation $aba = bab$

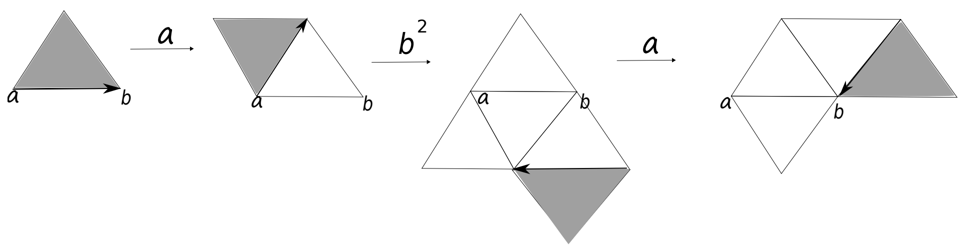

FIGURE 2. The relation $ab^2a = b^{m-2}$

m times we get

$$bab^m a^{-1}b^{-1} = babb^{m-1}a^{-1}b^{-1} = abab^{m-1}a^{-1}b^{-1} = \cdots = a^m baa^{-1}b^{-1} = a^m = \mathbf{1} \ ,$$

which obviously implies $b^m = \mathbf{1}$. In a similar way we write

$$bab^{m-2}a^{-1}b^{-1} = a^{m-2} \ .$$

Now we use the second relation for D_m inside the expression on the left:

$$a^{m-2} = baab^2aa^{-1}b^{-1} = ba^2b \ .$$

Assume now that the group D_m is defined as above and set $x := aba$ and $y := ab$. Then

$$x^2 = abaaba = aa^{m-2}a = a^m = \mathbf{1} \ ,$$
$$y^3 = ababab = abaaba = x^2 = \mathbf{1} \ ,$$
$$(xy)^m = (abaab)^m = (a^{m-1})^m = (a^{-1})^m = \mathbf{1} \ .$$

Conversely, let x and y be the standard generators of $D(2,3,m)$ as in Equation 1.1 and set $a = y^2x$ and $b = xy^2$. Then $aba = y^2xxy^2y^2x = y^6x = x$. At the same time $bab = xy^2y^2xxy^2 = xy^6 = x$, so Artin's braid relation holds for a and b. Next, $a^m = (y^2x)^m = (y^{-1}x^{-1})^m = (xy)^{-m} = \mathbf{1}$ and, as we saw, this implies also $b^m = \mathbf{1}$. Finally, $ab^2a = y^4xy^4x = (yx)^2 = (y^{-2}x^{-1})^2 = (xy^2)^{-2} = b^{-2} = b^{m-2}$. □

http://dx.doi.org/10.22108/IJGT.2021.128791.1696

We now consider the group $\widetilde{D}_m := \langle a, b \mid aba = bab,\, ab^2a = b^{m-2}\rangle$. In other words we drop the condition on the order of a and b. We still have the action of $\widetilde{D}_m$ on the tessellated sphere, Euclidean plane, or hyperbolic plane, except that now the action is not faithful. Further, we can think of continuous motions of the respective surfaces, so that a can be considered as the continuous rotation about the vertex a from angle 0 to angle $2\pi/m$, b is a similar continuous rotation about the vertex b, ab means first performing the motion given by b and then the one given by a, and so on. We can now state that the two relations in the definition of $\widetilde{D}_m$ hold in a stronger, homotopy sense. Namely, the motion determined by aba can be continuously deformed to the one determined by bab and the motion determined by ab^2a can be continuously deformed to the one determined by b^{m-2}. (Notice that the full twists determined by a^m or b^m cannot be deformed to the trivial motion. Notice also that the spherical case is substantially different from the other cases, as a rotation by 4π of the sphere is continuously deformable to the trivial motion, which is not true for the other cases.)

Proposition 1.2. *The group $\widetilde{D}_m$ is the universal central extensions of $D(2,3,m)$. When $m = 3, 4, 5$ the extension is by $\mathbb{Z}_2$ and the group obtained is the binary tetrahedral, binary octahedral, and binary icosahedral group, respectively. We have the short exact sequence*

$$1 \longrightarrow \mathbb{Z}_2 \longrightarrow \widetilde{D}_m \longrightarrow D(2,3,m) \longrightarrow 1 \ . \tag{1.2}$$

In the case $m \geq 6$ we get central extensions by $\mathbb{Z}$ of the infinite Von Dyck group $D(2,3,m)$:

$$1 \longrightarrow \mathbb{Z} \longrightarrow \widetilde{D}_m \longrightarrow D(2,3,m) \longrightarrow 1 \ . \tag{1.3}$$

Proof. We will use a topological argument. First notice that $a^m = b^m$ is central in $\widetilde{D}_m$. Indeed, using the two relations for $\widetilde{D}_m$ we see that

$$ababab = abaaba = a^m \ ,$$

and similarly $b^m = bababa = ababab = a^m$. But the element $(ab)^3$ is central in the braid group B_3 and therefore also in $\widetilde{D}_m$, which can be seen immediately by applying Artin's relation. In the spherical case the group $\widetilde{D}_m$ has the meaning of the group of homotopy classes of paths in $SO(3)$, starting at the identity and ending at some element of the finite tetrahedral, octahedral, or icosahedral subgroup of $SO(3)$. The projection $\widetilde{D}_m \to D(2,3,m)$ obtained by imposing the additional relation $a^m = \mathbf{1}$ is a restriction of the double cover $SU(2) \to SO(3)$ and is therefore a double cover itself. In particular a^m has the meaning of a rotation from 0 to 2π about some axis, which is not topologically trivial, but, as is well known, $(a^m)^2$ is.

The Euclidean case ($m = 6$) and the hyperbolic case ($m > 6$) are essentially the same. The group generated by rotations about two different points is a subgroup of the orientation preserving isometries. In the Euclidean case the latter is the group $E^+(2) = O(2) \ltimes T(2)$, where $T(2)$ denotes the group of translations of $\mathbb{R}^2$. In the hyperbolic case the group is $\mathrm{PSL}(2,\mathbb{R})$. In both cases the topology of these groups is that of $S^1 \times \mathbb{R}^2$ and the universal covering space is topologically $\mathbb{R} \times \mathbb{R}^2$. We have a short exact sequence

$$1 \longrightarrow \mathbb{Z} \longrightarrow \widetilde{\mathrm{PSL}}(2,\mathbb{R}) \longrightarrow \mathrm{PSL}(2,\mathbb{R}) \longrightarrow 1$$

and a similar one for $E^+(2)$. In both cases the covering map $\widetilde{D}_m \to D(2,3,m)$ obtained by imposing the additional relation $a^m = \mathbf{1}$ is a restriction of the universal covering maps just described. In particular a^m has infinite order. □

In the proof of the last proposition we used the fact that the fundamental group of $SO(3)$ is $\mathbb{Z}_2$ to ascertain that $\widetilde{D}_m$ is a double cover of $D(2,3,m)$ when $m = 3,4,5$. This connection between $\pi_1(SO(3))$ and the groups $\widetilde{D}_m$ can be used in the opposite direction. For any one of the three subgroups of $SO(3)$ – rotational tetrahedral, octahedral, or icosahedral group – one can study the group $\widetilde{D}_m$, which is a group of homotopy classes of paths in $SO(3)$ starting at the identity and ending at an element of the respective polyhedral group. Then one shows that the central element $a^m = b^m$, which is the class of closed paths in $SO(3)$, has order two and $\widetilde{D}_m$ is indeed a double (Schur) cover of the respective rotational polyhedral group. This approach has been pursued in detail in [9] for the octahedral case, where the relations for $\widetilde{D}_4$ are derived by considering contractible closed paths. In fact the scheme works for $SO(n)$ with any $n \geq 3$. In all cases we get a group analogous to $\widetilde{D}_4$ – a factor group of the braid group with n strands B_n obtained by imposing the single additional relation $ab^2a = b^2$ for the first two generators.

It may be instructive to see why the relations for $\widetilde{D}_m$ imply that a^m has order two when $m = 3,4,5$. Using $ab^2 = b^{m-2}a^{-1}$ multiple times we can write

$$a^m b^2 = a^{m-1}b^{m-2}a^{-1} = a^{m-1}b^2 a a^{-1} b^{m-4} a^{-1} = \cdots = b^{m-2}a^{-1}b^{m-4}a^{-1}b^{m-4}\cdots a^{-1} \ .$$

As a^m is central, this implies

$$a^m = (b^{m-4}a^{-1})^m \ .$$

For $m = 3$ this reads $a^3 = (b^{-1}a^{-1})^3 = (ab)^{-3}$. But we also know that $a^3 = (ab)^3$, so $a^6 = \mathbf{1}$. For $m = 4$ the formula implies $a^4 = (a^{-1})^4$ and obviously $a^8 = \mathbf{1}$. For $m = 5$ we have $a^5 = (ba^{-1})^5$. Because of the symmetry between a and b we also have $b^5 = (ab^{-1})^5$ and therefore $a^{10} = a^5 b^5 = \mathbf{1}$.

2. Finite Factors of $\widetilde{D}_m$

Many interesting finite groups are obtained as factors of Von Dyck groups. For example, the smallest nonabelian finite simple group is the alternating group A_5 of order 60. It is isomorphic to the rotational icosahedral group, the Von Dyck group $D(2,3,5)$ and the Chevalley group $\mathrm{PSL}(2,5)$. We have the obvious presentation as a factor of $\widetilde{D}_m$:

$$\mathrm{PSL}(2,5) \cong \left\langle a, b \,|\, aba = bab, ab^2a = b^3, a^5 = \mathbf{1} \right\rangle \ .$$

This is, just as the standard one, a presentation with two generators and three relations and is therefore an *efficient presentation*. Recall that a presentation of a finite group is called *efficient* if the difference between the number of relations and the number of generators is equal to the rank of the Schur multiplier group. If a finite group has a nontrivial Schur multiplier it admits a central (Schur) extension, which is also finite. The minimal possible number of relations for the Schur extension is equal to the number of generators for otherwise the group would be infinite. Then, if the Schur multiplier is nontrivial, one needs an additional relation for each of its generators to recover the original group. In our case this is the relation $a^5 = \mathbf{1}$. The Schur multiplier of $D(2,3,5)$ is $\mathbb{Z}_2$ (rank 1) and therefore the presentation is efficient. The Schur extension is the double cover $\mathrm{SL}(2,5)$ (the binary icosahedral group) with (efficient) presentation

$$\mathrm{SL}(2,5) \cong \left\langle a, b \,|\, aba = bab, ab^2a = b^3 \right\rangle \ .$$

The next finite simple group is the group $\mathrm{PSL}(2,7)$ of order 168. It is a Hurwitz group, i.e., a finite factor of the Von Dyck group $D(2,3,7)$. It is the group of automorphisms (orientation-preserving isometries) of a compact Riemann surface of genus 3 known as the Klein quartic. The fact that $\mathrm{PSL}(2,7)$ is a factor of $D(2,3,7)$ has the following geometric interpretation: The hyperbolic plane is tessellated by congruent equilateral geodesic triangles with angles $2\pi/7$. There is a discrete group of motions of the hyperbolic plane preserving this tessellation, which plays the role of a Fuchsian group determining the Klein quartic whose automorphism group is the factor group of the normalizer in $\mathrm{PSL}(2,\mathbb{R})$ of this Fuchsian group by the Fuchsian group itself.

Hurwitz groups have been the subject of considerable interest (see, e.g., [6], [11] for overviews of known facts) for many reasons. Among them is the result of Hurwitz that the biggest automorphism group of a compact Riemann surface of given genus is a Hurwitz group. Also, Hurwitz groups are quite abundant in the Chevalley series $\mathrm{PSL}(2,q)$ and many other finite simple groups, including the Monster group, are known to be of this type.

Some properties of Hurwitz groups are shared by other groups G which are finite factors of Von Dyck groups of type $D(2,3,m)$, $m > 6$. In particular we have the following generalization of a result described in [6]:

Suppose that $\{2,3,m\}$ are pairwise coprime. Then the order of G is divisible by $12m$.

We show this through a simple geometric argument. The Von Dyck group $D(2,3,m)$ acts on the hyperbolic plane preserving the tessellation by congruent equilateral geodesic triangles with angles $2\pi/m$. The action is transitive on the set of triangles and further a given triangle can be mapped to any other in three different ways (cyclic permutations of the three ordered vertices). These properties are inherited by the compact Riemann surface when we factor by the action of a normal subgroup of $D(2,3,m)$. In particular the tessellated surface becomes a generalized regular polyhedron whose faces are the regular triangles. Since there are m triangles meeting at a vertex we have for the number of vertices V and number of faces F the formula $V = 3F/m$ and the relation between number of edges E and number of faces is $E = 3F/2$. We see that the Euler characteristic of the surface is $\chi = F(6-m)/2m$. Using the fact that $|G| = 3F$ and expressing the Euler characteristic in terms of the genus we obtain

$$g = 1 + \frac{|G|(m-6)}{12m} \ . \tag{2.1}$$

Turning this formula around shows that $|G|$ is divisible by $12m$, since $m-6$ has no common factors with 12 or with m.

We looked for finite (simple) groups which are obtained from $\widetilde{D}_m$ by adding one relation, thus producing three-relator presentations. Unless the corresponding Schur multiplier is trivial, these are efficient presentations.

A question of special interest is which finite (simple) groups are *efficient groups*, i.e., admit efficient presentations and whether or not all finite simple groups are in fact efficient. Vast progress has been made in finding experimentally efficient presentations of all simple groups and their covers up to some order (see [2], [3], and [4] for an overview of the results obtained and the literature on the subject). In particular, using extensive computations it is shown in [4] that all finite simple groups of order less than a million, except one, are efficient, and all their covering groups, except one, are efficient.

General theoretical results about efficient presentations of the infinite series of finite simple groups and their covers are relatively scarce. Efficient presentations of $\mathrm{PSL}(2,p)$ for odd primes p (with some exceptions) were first constructed by Zassenhaus [16]. Then Sunday [15] improved this result by finding shorter three-relator presentation for $\mathrm{PSL}(2,m)$ for any odd m. (Note that $\mathrm{PSL}(2,m)$ is the group of 2×2 matrices with determinant 1 over the ring of integers modulo m, factored by its center. When $m = p^n$ with p prime, $n > 1$, $\mathrm{PSL}(2,m)$ is different from the simple Chevalley group $\mathrm{PSL}(2,p^n)$ of matrices over the finite (Galois) field with p^n elements.) Both Zassenhaus and Sunday based their work on a fundamental result of Behr and Mennicke [1] providing a four-relator presentation. Later Campbell and Robertson [5] found efficient (two-relator) presentations of the covering groups $\mathrm{SL}(2,p)$.

The presentations of Sunday are:

$$\begin{aligned} \mathrm{SL}(2,m) \ &\cong \ \left\langle S,T \mid S^m = T^2 = (ST)^3 = (S^{\frac{1}{2}(m+1)}TS^4T)^2 \ \right\rangle \ , \\ \mathrm{PSL}(2,m) \ &\cong \ \left\langle S,T \mid S^m = \mathbf{1},\ T^2 = (ST)^3,\ (S^{\frac{1}{2}(m+1)}TS^4T)^2 = \mathbf{1} \ \right\rangle \ . \end{aligned}$$

In particular $\mathrm{PSL}(2,m)$ is generated by one element of order m and one element (a posteriori) of order 2, whose product is of order 3, so it is not surprising that it is a factor of $D(2,3,m)$.

In our search for interesting finite factors of $\widetilde{D}_m := \langle a,b \mid aba = bab,\, ab^2a = b^{m-2}\rangle$ we observed two general formulas for $\mathrm{PSL}(2,m)$ with odd m. We formulate the results in the next two propositions.

Proposition 2.1. *The groups* $\mathrm{PSL}(2,m)$ *for odd* m *have the presentations*

$$\mathrm{PSL}(2,m) \cong \left\langle a,b \mid aba = bab,\, ab^2a = b^{m-2},\, (a^4b^{-\frac{1}{2}(m-1)})^2 = \mathbf{1} \ \right\rangle \ . \tag{2.2}$$

Proof. We begin by proving a modification of Sunday's result. Namely:

$$\mathrm{PSL}(2,m) \cong G := \left\langle S,T \mid S^{-m} = T^2 = (ST)^3,\ (S^{\frac{1}{2}(m+1)}TS^4T)^2 = \mathbf{1} \ \right\rangle \ . \tag{2.3}$$

Indeed, it is relatively easy to see that the abelianization of G (i.e., when S and T commute) is trivial. If we factor G by the (normal) subgroup generated by the central element T^2 we obtain (see [15]):

$$\left\langle S, T \mid S^{-m} = T^2 = (ST)^3 = (S^{\frac{1}{2}(m+1)}TS^4T)^2 = \mathbf{1} \right\rangle \cong \mathrm{PSL}(2,m) \ .$$

So G is a stem extension of $\mathrm{PSL}(2,m)$ and according to Schur's theory [14] it must be either $\mathrm{PSL}(2,m)$ or $\mathrm{SL}(2,m)$. The latter possibility is excluded by the fact that $(S^{\frac{1}{2}(m+1)}TS^4T)^2 = \mathbf{1}$.

We proceed by showing that the relations in Eq. 2.3 imply and follow from the relations in Eq. 2.2. To this end let $S := b^{-1}$ and $T := bab$. We have seen already that $Z := S^{-n} = b^n = a^n$ is central. We have additionally $T^2 = (bab)^2 = bababa = (ba)^3 = (ST)^3$. Finally $S^{-n} = b^n = b(b^{n-2})b = b(ab^2a)b = T^2$.

The last relation in Eq. 2.2 is equivalent to

$$\mathbf{1} = (b^{-\frac{1}{2}(m-1)}a^4)^2 = (S^{\frac{1}{2}(m-1)}(STS)^4)^2 = (S^{\frac{1}{2}(m+1)}TS^2TS^2TS^2TS)^2 \ .$$

and this is equivalent to $\mathbf{1} = (S^{\frac{1}{2}(m+3)}TS^2TS^2TS^2T)^2$. Since $T^2 = (ST)^3 = (STS)(TST) = Z$ we have $T^{-1} = Z^{-1}T$ and $STS = Z^{-1}TS^{-1}T$. Next we calculate

$$\begin{aligned}
&(S^{\frac{1}{2}(m+3)}TS\,STS\,STS\,ST)^2 = (S^{\frac{1}{2}(m+3)}Z^{-2}TSTS^{-1}T^2S^{-1}TST)^2 \\
&= (S^{\frac{1}{2}(m+3)}Z^{-1}TSTS^{-2}TST)^2 = (S^{\frac{1}{2}(m+3)}Z^{-1}T\,STS\,S^{-4}\,STS\,T)^2 \\
&= (S^{\frac{1}{2}(m+3)}Z^{-3}T^2S^{-1}TS^{-4}TS^{-1}T^2)^2 = (S^{\frac{1}{2}(m+3)}Z^{-1}S^{-1}TS^{-4}TS^{-1})^2 \ .
\end{aligned}$$

Therefore our relation becomes equivalent to the following sequence of relations:

$$\begin{aligned}
&\mathbf{1} = (S^{\frac{1}{2}(m-1)}Z^{-1}TS^{-4}T)^2 \ , \quad \mathbf{1} = (T^{-1}S^4T^{-1}ZS^{-\frac{1}{2}(m-1)})^2 \ , \\
&\mathbf{1} = (S^{-\frac{1}{2}(m-1)}Z^{-1}TS^4T)^2 = (S^{\frac{1}{2}(m+1)}TS^4T)^2 \ .
\end{aligned}$$

□

Proposition 2.2. *The groups* $\mathrm{PSL}(2,m)$ *for* m *odd,* $m \equiv 2 \pmod 3$*,* $m \not\equiv 11 \pmod{30}$*, have the presentations*

$$\mathrm{PSL}(2,m) \cong \left\langle a, b \mid aba = bab,\ ab^2a = b^{m-2},\ (a^3b^{-\frac{1}{3}(m-2)})^2 = \mathbf{1} \right\rangle \ . \tag{2.4}$$

The groups $\mathrm{PSL}(2,m)$ *for* m *odd,* $m \equiv -2 \pmod 3$*, have the presentations*

$$\mathrm{PSL}(2,m) \cong \left\langle a, b \mid aba = bab,\ ab^2a = b^{m-2},\ (a^3b^{\frac{1}{3}(m+2)})^2 = \mathbf{1} \right\rangle \ . \tag{2.5}$$

Proof. In their paper [1] Behr and Mennicke proved that $\mathrm{PSL}(2,m)$ for odd m has a presentation with two generators and the following set of relations:

$$S^m = T^2 = (ST)^3 = (S^2TS^{\frac{1}{2}(m+1)}T)^3 = \mathbf{1} \ .$$

Their proof uses the authors' general results about Ihara's modular groups $\mathrm{SL}(2, \mathbb{Z}^{(p)})$ and complete sets of relations for them. Here $\mathrm{SL}(2, \mathbb{Z}^{(p)})$ stands for the group of 2×2 matrices over the ring $\mathbb{Z}^{(p)} := \{x/p^t,\ x, t \in \mathbb{Z}\}$, p a fixed prime number, with unit determinant. First $\mathrm{SL}(2, \mathbb{Z}^{(p)})$ is presented in terms of three generators and a relatively large complete set of relations, not all of them independent. In all cases the relations include

(2.6) $$T^2 = (ST)^3,\ T^4 = \mathbf{1},\ \text{(the relations for the subgroup SL}(2,\mathbb{Z}))$$

(2.7) $$U^{-1}SU = S^{p^2},\ (UT)^2 = T^2\ ,$$

and a set of additional relations which have to be made more concrete for each specific p. Then Behr and Mennicke specify their results to the case $p = 2$ where the additional relations reduce to just $(US^2T)^3 = T^2$. Finally, excluding the generator U and adding the additional relations $S^m = T^2 = \mathbf{1}$ they arrive at the relations for $\mathrm{PSL}(2, m)$ cited above.

The fact that our formulas for $\mathrm{PSL}(2, m)$ involve exponents like $\frac{1}{3}(m \pm 2)$ suggests an attempt to repeat the analysis of Behr and Mennicke with $p = 3$. For $\mathrm{SL}(2,\ \mathbb{Z}^{(3)})$ we have of course the relations (2.6) and (2.7) with $p^2 = 9$. Notice that the following matrices satisfy them:

$$S' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ T' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ U' = \begin{pmatrix} 3 & 0 \\ 0 & \frac{1}{3} \end{pmatrix}\ .$$

A complete set of relations is obtained by adding relations (D), (G), (I), (L), and (M) as specified in [1], p. 1437. Performing the straightforward but tedious task of specifying these for $p = 3$ showed that there are only two (seemingly) independent relations coming from (D) (note that each formula on p. 1437 involves several relations):

(D_1) $$U = TS^{-3}T^{-1}S^{-\frac{1}{3}}T^{-1}S^{-3} \quad \Longleftrightarrow \quad (US^3T)^3 = T^2\ ,$$

(D_2) $$U = TS^{-2}T^{-1}S^{-2}T^{-1}S^{-\frac{2}{3}}T^{-1}S^{-6} \quad \Longleftrightarrow \quad (US^6T)^2US^2TS^2T = T^2\ .$$

As an illustration we show the derivation of (D_1). Formula (D) in [1] for $p = 3$ becomes

$$S^xU^{-1}T^{-1}S^{-3y}U^{-1}T^{-1}S^{-3y'}U^{-1} = \begin{pmatrix} (yy'-1)3^{-1} & -y \\ x(yy'-1)3^{-1} + y' & -xy-3 \end{pmatrix}\ .$$

where in general $x = 0, 1, \ldots, p^2-1$ and $y,\ y' \in \{1, 2, \ldots, p-1\}$ and in this particular case additionally $yy' \equiv 1 \pmod 3$. The two possibilities are $y = y' = 1$ giving (D_1) and $y = y' = 2$ (giving (D_2)). The right-hand side is always a matrix in $\mathrm{SL}(2,\ \mathbb{Z})$ and can be written as a product of powers of S and T. For $y = y' = 1$ we obtain

$$S^xU^{-1}T^{-1}S^{-3}U^{-1}T^{-1}S^{-3}U^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & -x-3 \end{pmatrix} = S^{x+3}T^{-1}\,.$$

From this and the relations (2.7) (note that the second one is equivalent to $UT = TU^{-1}$) we arrive at (D_1). An explanation is due of the rational exponents of S in (D_1) and (D_2). For now we can simply define $S^{\frac{1}{3}} := US^3U^{-1}$. Notice that

$$(S')^{\frac{1}{3}} = \begin{pmatrix} 1 & 0 \\ \frac{1}{3} & 1 \end{pmatrix}$$

looks very natural. The conclusion is that relations (2.6), (2.7), (D_1), and (D_2) form a complete set of relations for $SL(2, \mathbb{Z}^{(3)})$.

Next we impose the additional relation

$$S^m = \mathbf{1}\ . \tag{2.8}$$

Mennicke [13] has shown that the normal closure of S^m in $SL(2, \mathbb{Z}^{(p)})$ is the full congruence subgroup modulo m provided that $(m,p) = 1$, which is satisfied in our case since $p = 3$ and $m \equiv \pm 2 \pmod 3$. Using relation (2.8) we can modify the first relation in (2.7), namely, we replace $U^{-1}SU = S^9$ by the equivalent relation $U^{-1}S^{1+m}U = S^9$ in the case $m \equiv 2 \pmod m$ and by $U^{-1}S^{1-m}U = S^9$ in the case $m \equiv -2 \pmod m$. This leads to $S^{\frac{1}{3}(1\pm m)} = US^3U^{-1}$ and to replacing the rational exponents of S in (D_1) and (D_2) by integer ones. For the sake of brevity we will keep the rational exponents and add $\pm m$ as appropriate in the final formulas. With this in mind we proceed to exclude the generator U. First, from (D_1) and (D_2) it follows that

$$(S^3TS^{\frac{2}{3}}T)^2 = T^2\ . \tag{2.9}$$

Next, substituting (D_1) in $(UT)^2 = T^2$ and using that T^2 is central and $T^4 = \mathbf{1}$, we obtain

$$(S^6TS^{\frac{1}{3}}T)^2 = T^2\ . \tag{2.10}$$

Finally we substitute U from (D_1) in the relation $US^6U^{-1} = S^{\frac{2}{3}}$ and after some manipulations and applying (2.10) we arrive at $(S^3TS^{\frac{2}{3}}T)^2 = T^2$, which is relation (2.9). Therefore relations (2.6), (2.7), (2.8), (D_1), and (D_2) imply (2.6), (2.8), (2.9), and (2.10). Conversely, it is easy to see that the second set of relations implies the first one. We obtain a group generated by two generators S and T, subject to the relations

$$S^m = \mathbf{1},\ (ST)^3 = (S^3TS^{\frac{1}{3}(2\mp m)}T)^2 = (S^6TS^{\frac{1}{3}(1\pm m)}T)^2 = T^2,\ T^4 = \mathbf{1}\,, \tag{2.11}$$

for the two separate cases $m \equiv \pm 2 \pmod 3$, respectively. This is obviously a quotient of $SL(2, \mathbb{Z})$ by a normal subgroup containing the principal congruence subgroup $\Gamma(m)$, because of the way it was constructed. The group cannot be smaller than $SL(2, m)$ because the matrices S' and T', which generate $SL(2, \mathbb{Z})$ fulfill relations (2.11) modulo m. Therefore it must be $SL(2, m)$.

Imposing additionally $T^2 = \mathbf{1}$ leads to the following presentation for $PSL(2, m)$:

$$S^m = (ST)^3 = (S^3TS^{\frac{1}{3}(2\mp m)}T)^2 = (S^6TS^{\frac{1}{3}(1\pm m)}T)^2 = T^2 = \mathbf{1}\,, \tag{2.12}$$

We proceed by rewriting the presentation (2.12) in terms of two generators a and b of order m. As before, we set $S := b^{-1}$ and $T := bab$. We have already seen in the proof of the previous proposition that the relations $S^m = (ST)^3 = T^2 = \mathbf{1}$ are equivalent to the relations $aba = bab$, $ab^2a = b^{m-2}$, $a^m (= b^m) = \mathbf{1}$. Next we calculate

$$\mathbf{1} = (S^3TS^{\frac{1}{3}(2\mp m)}T)^2 = (b^{-3}babb^{-\frac{1}{3}(2\mp m)}bab)^2\,.$$

Using a few transformations the last relation is shown to be equivalent to

$$(a^3 b^{\frac{1}{3}(2\mp m)})^2 = \mathbf{1}\,.$$

Similarly

$$(S^6 T S^{\frac{1}{3}(1\pm m)} T)^2 = \mathbf{1} \quad \Longleftrightarrow \quad (a^6 b^{\frac{1}{3}(1\pm m)})^2 = \mathbf{1}\ .$$

We arrive at the following presentation for $\mathrm{PSL}(2,m)$ in terms of two generators of order m:

$$aba = bab,\ ab^2a = b^{m-2},\ a^m = (a^3 b^{\frac{1}{3}(2\mp m)})^2 = (a^6 b^{\frac{1}{3}(1\pm m)})^2 = \mathbf{1}\ . \tag{2.13}$$

The last relation in (2.13) is redundant. In order to show this we first observe that the following two matrices fulfill (2.13) modulo m:

$$a' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\ ,\quad b' = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\ .$$

Both matrices are parabolic, i.e., their trace is 2. Parabolic elements act on the upper complex half-plane via fractional linear transformations without fixed points. They fix only ∞. Any automorphic image of the pair a' and b' must have the same property, i.e they must be parabolic too. It is known (see, e.g., [10]) that all parabolic elements in $\mathrm{PSL}(2,\mathbb{Z})$ fall in infinitely many conjugacy classes, each class containing a representative $b = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$. Therefore we can assume that our generators a and b are represented by

$$a = \begin{pmatrix} x & y \\ z & w \end{pmatrix}\ \text{, where } xw - yz = 1\ , \qquad b = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\ . \tag{2.14}$$

The braid relation $aba = bab$ imposes the following additional conditions on the entries:

$$\begin{aligned} &x^2 + z(kx + y) = kz + x \\ &xy + (kx + y)w = k(x + kz) + y + kw \\ &xz + (kz + w)z = z \\ &zy + (kz + w)w = kz + w \end{aligned}$$

Considering first the case $z \neq 0$ it easily follows that $x + w = 2$ and then $kz = -1$. Taking $k = 1$ and $z = -1$ leads to $y = (x-1)^2$ and the matrices a and b become

$$a = \begin{pmatrix} x & (x-1)^2 \\ -1 & 2 - x \end{pmatrix}\ ,\quad b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\ .$$

We check that $ab^2a = \begin{pmatrix} -1 & 2 \\ 0 & -1 \end{pmatrix} \sim b^{-2}$. It remains to consider $(a^3 b^{\frac{1}{3}(2\mp m)})^2$ and $(a^6 b^{\frac{1}{3}(1\pm m)})^2$. Since we are looking at the condition that these two are congruent to $\pm I$, it is enough to do the calculation

http://dx.doi.org/10.22108/IJGT.2021.128791.1696

for $m = 0$. The calculation, somewhat miraculously, shows that

$$(a^3 b^{\frac{2}{3}})^2 = (a^6 b^{\frac{1}{3}})^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

independent of x. The other solution is $k = -1,\ z = 1$ which leads to the following expressions for a and b:

$$a = \begin{pmatrix} x & (x-1)^2 \\ 1 & 2-x \end{pmatrix}, \quad b = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

This time calculating $C := (a^3 b^{\frac{2}{3}})^2$ produces entries which are polynomials in x. We have a congruence condition $C_{21} = \frac{1}{3}(64x^4 - 256x^3 + 480x^2 - 448x + 160) = 0$ and this has a unique solution $x = 1$. This means that $a = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and a direct calculation confirms that $(a^3 b^{\frac{2}{3}})^2 = (a^6 b^{\frac{1}{3}})^2 = -I$.

Considering the case $z = 0$ easily implies $a = b = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, which is incompatible with $ab^2a = b^{-2}$.

We conclude that $\mathrm{PSL}(2, m)$ for the specified values of m is defined by the relations

$$aba = bab,\ ab^2a = b^{m-2},\ a^m = (a^3 b^{\frac{1}{3}(2\mp m)})^2 = \mathbf{1}\ . \tag{2.15}$$

It is also evident from the derivation that $\mathrm{SL}(2, m)$ is defined by the relations

$$aba = bab,\ ab^2a = b^{m-2},\ a^m = (a^3 b^{\frac{1}{3}(2\mp m)})^2,\ a^{2m} = \mathbf{1}\ . \tag{2.16}$$

The final step is to use Schur's theory and drop the condition $a^m = \mathbf{1}$ in (2.15). Considering the group $G = \left\langle a, b \mid aba = bab,\ ab^2a = b^{m-2},\ (a^3 b^{\frac{1}{3}(2\mp m)})^2 = \mathbf{1} \right\rangle$ we recall that a^m belongs to its center. We have that $G/\langle a^m \rangle \cong \mathrm{PSL}(2, m)$, so the former is a central extension of the latter. It will be a stem extension if a^m belongs to the commutator subgroup of G, which will be satisfied if G is perfect, or, equivalently, if the abelianization of G is trivial. In the abelanization Artin's braid relation implies $a = b$ while the second and third relations for G impose conditions on the order of a. The order will be different from 1 iff $\gcd(m-6, 2(\frac{1}{3}(2\mp m)+3)) \neq 1$. The greatest common divisor is 1 in all cases except for $m = 11 + 30n,\ n = 0, 1, 2, \ldots$, when it becomes 5. Excluding these cases, we infer that G, being a stem extension of $\mathrm{PSL}(2, m)$, must be either $\mathrm{PSL}(2, m)$ itself, or $\mathrm{SL}(2, m)$. The latter possibility is excluded by the fact that $(a^3 b^{\frac{1}{3}(2\mp m)})^2 = \mathbf{1}$. □

There are various criteria when comparing different presentations of a group. Generally, the smaller the number of generators and relations, the "nicer" the presentation is considered. In this respect efficient presentations with two generators are most economical and aesthetic. Another criterion is the length of the relations, defined as the sum of the absolute values of the exponents in all the words in the relations. Our presentation (2.2) has length $2m + 15$ and is nominally shorter than Sunday's presentation having length $2m+21$. Still, the two can be considered as essentially the same presentation expressed in different generators. On the other hand the presentations (2.4) and (2.5) are substantively shorter, the first one having length $2m - \frac{m}{3} + 13 - \frac{1}{3}$ and the second $2m - \frac{m}{3} + 15 + \frac{1}{3}$. Last but not least, presentations are evaluated with respect to their computational efficiency, i.e., the processor time needed to complete a coset enumeration algorithm and the maximal size of the coset enumeration table before reduction. We tested how the different presentations behave for several values of m using the standard algorithm of GAP [8] on a work station with CPUs at 3.28 GHz under Linux. In the table that follows we have recorded the computer resources used by GAP for calculating the order of four different groups with four different presentations for each one. The data represents the CPU time in milliseconds and the memory used in gigabytes by the program in each case. By "S" we denote the standard presentation of Sunday, by "S′ " – the modification of Sunday's presentation described in Eq.2.3, by "2.2" is denoted our presentation (2.2), and by "2.4/2.5" – our presentation (2.4) or (2.5) (depending on the value of m).

group	order	S	S′	2.2	2.4/2.5
PSL(2,31)	14880	11.7×10^3 ms 0.38 GB	0.585×10^3 ms 0.018 GB	8.76×10^3 ms 0.23 GB	0.827×10^3 ms 0.02 GB
PSL(2,37)	25308	196×10^3 ms 3 GB	5.5×10^3 ms 0.15 GB	84×10^3 ms 1.9 GB	3.9×10^3 ms 0.087 GB
PSL(2,43)	39732	3276×10^3 ms 21 GB	31×10^3 ms 0.77 GB	819×10^3 ms 15.5 GB	10.6×10^3 ms 0.237 GB
PSL(2,47)	51888	8727×10^3 ms 28 GB	52.5×10^3 ms 1.27 GB	3203×10^3 ms 61 GB	46.1×10^3 ms 1.07 GB

As expected, presentation (2.2) is computationally a little more efficient when compared to Sunday's presentation while presentations (2.4) or (2.5) are significantly more efficient. What came as a complete surprise was how much better the modification of Sunday's presentation behaves computationally compared to the original one.

The presentations discussed so far may be called *standard* in the sense that $\mathrm{PSL}(2, m)$ is generated by two generators, at least one of which is of order m and the relations obey a general formula. We can also say that in this case $\mathrm{PSL}(2, m)$ is presented as a factor of $D(2, 3, m)$ by adding one additional relation.

In addition to the standard presentations, we found essentially by a random search many presentations of $\mathrm{PSL}(2, q)$ as factors of $\widetilde{D}_m$ with $m \leq q$ dividing the order of the group. In practice we started with the relations for $\widetilde{D}_m$ and tested with GAP a third relation that would produce a finite group, then tried to identify that group. We selected the cases in which a simple group was obtained. It turned out that with one exception the groups obtained in this way were of type $\mathrm{PSL}(2, q)$. We could call these presentations *nonstandard*. For large q and (relatively) small m these are generally much shorter and computationally more efficient. In fact the experiments showed that even with the shortest standard presentations (2.4/2.5) our work station with 64 GB RAM could barely handle the coset enumeration of GAP for m greater than, say, 71. Note that $\mathrm{PSL}(2, 71)$ has order just 178920. At the same time the Hurwitz group $\mathrm{PSL}(2, 379)$ with 27219780 elements has presentation $\langle a, b \mid aba = bab,\, ab^2a = b^5,\, (a^2b^{-2}(a^3b^{-2})^5)^2 = \mathbf{1} \rangle$ and the coset enumeration with respect to the trivial subgroup used 4.4 GB memory and 2.8×10^6 ms CPU time. $\mathrm{PSL}(2, 991)$ with presentation $\langle a, b \mid aba = bab,\, ab^2a = b^{29},\, (a^3b^{-9})^2 = \mathbf{1} \rangle$ has order 486620640 and the coset enumeration with respect to the subgroup $\langle a \rangle$ required 20 GB and 8.9×10^6 ms .

Campbell et al. [3], [4] provided efficient presentations for all but one simple group of order less than a million, excluding the simple groups $\mathrm{PSL}(2, p)$ for prime p. The reason was that their main goal was to establish the efficiency of all simple groups up to this order and Sunday's presentation already established this for the latter family. At the same time they mention that the standard presentations for $\mathrm{PSL}(2, p)$ are (perhaps) by far not the shortest. They also argue that finding "nice", i.e., short and computationally efficient, presentations can be useful as input for further investigations into these groups.

In the following table we list all simple groups $\mathrm{PSL}(2, q)$ of order less than ten million and the shortest nonstandard presentations we have found for each q and m. We specify m and the word that gives the third relation, which should be added to the relations for $\widetilde{D}_m$. Thus for example we have $\mathrm{PSL}(2, 181) \cong \langle a, b \mid aba = bab,\, ab^2a = b^5,\, ((a^3b^{-4})^3(a^2b^{-1})^5)^2 = \mathbf{1} \rangle$. When $q = 2^n$ an efficient presentation has two relations. The word listed gives the relation that should replace the second relation for $\widetilde{D}_m$. For example for $\mathrm{PSL}(2, 16)$ we have the presentation $\mathrm{PSL}(2, 16) \cong \langle a, b \mid aba = bab,\, ab^2ab^{-15}(a^3b^{-9})^{-2} = \mathbf{1} \rangle$. One exception, marked by daggers is $\mathrm{PSL}(2, 32)$, for which we could not find efficient presentations and the words listed give a third relation. In the few cases where there are two words listed separated by a comma, they give the second and third relation, e.g., $\mathrm{PSL}(2, 47) \cong \langle a, b \mid aba = bab,\, ab^2ab^{-6}(ab^{-2}a^2b^{-2})^{\pm 3} = \mathbf{1}, a^8 = \mathbf{1} \rangle$. The cases marked by an asterisk are those for which the group has been identified based on its order and it being perfect but the GAP routine "IsSimple" could not be completed in a reasonable time, i.e., several months, so these should be treated as (very plausible) conjectures.

group	order			
PSL(2,5)	$60{=}2^2 \cdot 3 \cdot 5$	$m = 5$ a^5		
PSL(2,7)	$168 = 2^3 \cdot 3 \cdot 7$	$m = 7$ $(ab^{-1})^4$		
PSL(2,9)	$360 = 2^3 \cdot 3^2 \cdot 5$			
PSL(2,8)	$504 = 2^3 \cdot 3^2 \cdot 7$	$m = 7$ ab^2ab^{-5} $\cdot(a^2b^{-2}ab^{-2})^{-2}$		
PSL(2,11)	$660 = 2^3{\cdot}3{\cdot}5{\cdot}11$	$m = 11$ $(ab^{-1}a^2b^{-1})^3$		
PSL(2,13)	$1092 = 2^2{\cdot}3{\cdot}7{\cdot}$ 13	$m = 7$ $(ab^{-1})^6$	$m = 13$ $(a^3b^{-1}ab^{-1})^2$	
PSL(2,17)	$2448 = 2^4 \cdot 3^2 \cdot$ 17	$m = 9$ $(ab^{-2})^4$		
PSL(2,19)	$3420 = 2^2 \cdot 3^2 \cdot$ $5 \cdot 19$	$m = 9$ $(a^3b^{-3}ab^{-3})^2$	$m = 10$ $ab^2ab^{-8}(a^2b^{-3})^{-3}$, a^{10}	$m = 19$ $(ab^{-1}ab^{-5})^2$
PSL(2,16)	$4080 = 2^4{\cdot}3{\cdot}5{\cdot}$ 17	$m = 15$ ab^2ab^{-13} $\cdot(ab^{-2}ab^{-5})^{-2}$	$m = 17$ $ab^2ab^{-15}(a^3b^{-9})^{-2}$	
PSL(2,23)	$6072 = 2^3 \cdot 3 \cdot$ $11 \cdot 23$	$m = 11$ $(a^2b^{-1}ab^{-3})^3$		
PSL(2,25)	$7800 = 2^3 \cdot 3 \cdot$ $5^2 \cdot 13$	$m = 13$ $(a^3b^{-4})^2$		
PSL(2,27)	$9828 = 2^2 \cdot 3^3 \cdot$ $7 \cdot 13$	$m = 7$ $((ab^{-1})^3b^{-1}$ $\cdot(ab^{-1})^2a)^2$	$m = 13$ $(a^2b^{-3})^3$	
PSL(2,29)	$12180 = 2^2 \cdot 3 \cdot$ $5 \cdot 7 \cdot 29$	$m = 7$ $((ab^{-1})^4b^{-1})^3$	$m = 15$ $(a^3b^{-8})^2$	
PSL(2,31)	$14880 = 2^5 \cdot 3 \cdot$ $5 \cdot 31$	$m = 8$ $ab^2ab^{-2}a^8(ab^{-2})^5$, a^8	$m = 15$ $(ab^{-2}ab^{-4})^2$	
PSL(2,37)	$25308 = 2^2{\cdot}3^2{\cdot}$ $19 \cdot 37$	$m = 9$ $(a^2b^{-2}a^2b^{-3})^2$	$m = 19$ $(a^3b^{-4})^2$	
PSL(2,32)	$32736 = 2^5 \cdot 3 \cdot$ $11 \cdot 31$	$m = 11$ † $(a^4b^{-2}a^4b^{-1})^2a^{11}$	$m = 31$ † $(a^3b^{-7})^2$	
PSL(2,41)	$34440 = 2^3 \cdot 3 \cdot$ $5 \cdot 7 \cdot 41$	$m = 7$ $(a^2b^{-1}ab^{-2})^4$	$m = 10$ ab^2ab^{-8} $\cdot(ab^{-1}ab^{-2})^{\pm 3}$, a^{10}	$m = 21$ $(a^3b^{-7})^2$
PSL(2,43)	$39732 = 2^2 \cdot 3 \cdot$ $7 \cdot 11 \cdot 43$	$m = 7$ $(a^3b^{-2}a^2b^5)^3$	$m = 11$ $((ab^{-1})^3b^{-1}ab^{-2})^2$	$m = 21$ $(a^5b^{-7})^2$
PSL(2,47)	$51888 = 2^4 \cdot 3 \cdot$ $23 \cdot 47$	$m = 8$ $ab^2ab^{-6}(ab^{-2}$ $\cdot a^2b^{-2})^{\pm 3}$, a^8	$m = 23$ $(a^3b^{-12})^2$	

PSL(2,49)	$58800 = 2^4 \cdot 3 \cdot 5^2 \cdot 7^2$	$m = 25$ $(a^3b^7)^2$		
PSL(2,53)	$74412 = 2^2 \cdot 3^3 \cdot 13 \cdot 53$	$m = 13$ $(a^3b^{-1}a^3b^{-2})^2$	$m = 27$ * $(a^6b^{-13})^2a^{54}$	
PSL(2,59)	$102660 = 2^2 \cdot 3 \cdot 5 \cdot 29 \cdot 59$	$m = 10$ $ab^2ab^{-8}(a^4b^{-5})^{-3}$, a^{10}	$m = 15$ $(a^3b^{-4})^2$	$m = 29$ $(a^3b^{-7})^2$
PSL(2,61)	$113460 = 2^2 \cdot 3 \cdot 5 \cdot 31 \cdot 61$	$m = 15$ $(a^4b^{-5})^2$	$m = 31$ * $(a^3b^{-24})^2$	
PSL(2,67)	$150348 = 2^2 \cdot 3 \cdot 11 \cdot 17 \cdot 67$	$m = 11$ $((ab^{-1})^3b^{-1}a^2 \cdot b^{-2})^2$	$m = 17$ $(a^3b^{-4})^2$	
PSL(2,71)	$178920 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 71$	$m = 7$ $((ab^{-1})^3b^{-1})^4$	$m = 9$ * $(a^2b^{-2}a^2b^{-2}a^2b^{-6})^2$	
PSL(2,73)	$194472 = 2^3 \cdot 3^2 \cdot 37 \cdot 73$	$m = 9$ $((ab^{-1})^3(ab^{-2})^2)^2$		
PSL(2,79)	$246480 = 2^4 \cdot 3 \cdot 5 \cdot 13 \cdot 79$	$m = 13$ $(a^2b^{-1})^4$		
PSL(2,64)	$262080 = 2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$			
PSL(2,81)	$265680 = 2^4 \cdot 3^4 \cdot 5 \cdot 41$			
PSL(2,83)	$285852 = 2^2 \cdot 3 \cdot 7 \cdot 41 \cdot 83$	$m = 7$ $((ab^{-1})^5b^{-1} \cdot (ab^{-1})^2a)^2$	$m = 21$ $(a^3b^{-5})^2$	
PSL(2, 89)	$352440 = 2^3 \cdot 3^2 \cdot 5 \cdot 11 \cdot 89$	$m = 11$ $(a^4b^{-3}a^4b^{-1})^2$		
PSL(2,97)	$456288 = 2^5 \cdot 3 \cdot 7 \cdot 97$	$m = 7$ $(a^2b^{-2}ab^{-2}(ab^{-1})^2 \cdot a^2b^{-3}ab^{-1})^2$		
PSL(2,101)	$515100 = 2^2 \cdot 3 \cdot 5^2 \cdot 17 \cdot 101$	$m = 17$ $(ab^{-2}ab^{-5})^2$	$m = 25$ $(a^3b^{-7})^2$	
PSL(2,103)	$546312 = 2^3 \cdot 3 \cdot 13 \cdot 17 \cdot 103$	$m = 13$ $(ab^{-2}a^2b^{-2})^2$	$m = 17$ $((ab^{-1})^2b^6)^2$	
PSL(2,107)	$612468 = 2^2 \cdot 3^3 \cdot 53 \cdot 107$	$m = 9$ $((ab^{-2})^2(ab^{-1})^2 \cdot a^2b^{-2})^2$	$m = 27$ $(a^3b^-5)^2$	
PSL(2,109)	$647460 = 2^2 \cdot 3^3 \cdot 5 \cdot 11 \cdot 109$	$m = 27$ $(ab^{-1}ab^{-6})^2$		
PSL(2,113)	$721392 = 2^4 \cdot 3 \cdot 7 \cdot 19 \cdot 113$	$m = 7$ $((ab^{-1})^3b^{-1} \cdot (a^2b^{-1})^4b^{-1})^2$	$m = 8$ $ab^2ab^{-6} \cdot (a^2b^{-2}a^2b^{-3})^{\pm 3}$, a^8	$m = 19$ $(ab^{-2}ab^{-5})^2$
PSL(2,121)	$885720 = 2^3 \cdot 3 \cdot 5 \cdot 11^2 \cdot 61$			
PSL(2,125)	$976500 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 31$	$m = 7$ $((ab^{-3})^4(a^2b^{-2})^2 \cdot (a^3b^{-1})^4)^2$	$m = 21$ $(a^4b^7)^2$	

PSL(2,127)	$1024128 = 2^7 \cdot 3^2 \cdot 7 \cdot 127$	$m = 7$ $(ab^{-1}(a^2b^{-3})^3 \cdot(a^3b^{-1})^2)^2$	$m = 21$ * $(ab^{-2}ab^{-4})^2$	
PSL(2,131)	$1123980 = 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 131$	$m = 11$ $(a^{-4}b^4a^2b^{-2}ab^{-3})^2$		
PSL(2,137)	$1285608 = 2^3 \cdot 3 \cdot 17 \cdot 23 \cdot 137$	$m = 17$ $(ab^{-3}a^{-5}b^{-3})^2$	$m = 23$ * $(a^3b^{-14})^2$	
PSL(2,139)	$1342740 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 23 \cdot 139$	$m = 7$ * $(a^2b^{-2}a \cdot(ab^{-1})^6b^{-2})^2$	$m = 23$ * $(a^3b^{-16})^2$	
PSL(2,149)	$1653900 = 2^2 \cdot 3 \cdot 5^2 \cdot 37 \cdot 149$	$m = 25$ * $(a^3b^{-13})^2$	$m = 37$ * $(a^3b^8)^2$	
PSL(2,151)	$1721400 = 2^3 \cdot 3 \cdot 5^2 \cdot 19 \cdot 151$	$m = 19$ * $(a^{-6}(ab^{-1})^2)^2$	$m = 25$ * $(a^3b^{-5})^2$	
PSL(2,157)	$1934868 = 2^2 \cdot 3 \cdot 13 \cdot 79 \cdot 157$	$m = 13$ $(ab^{-3}a^3b^{-3})^2$		
PSL(2,128)	$2097024 = 2^7 \cdot 3 \cdot 43 \cdot 127$			
PSL(2,163)	$2165292 = 2^2 \cdot 3^4 \cdot 41 \cdot 163$			
PSL(2,167)	$2328648 = 2^3 \cdot 3 \cdot 7 \cdot 83 \cdot 167$	$m = 7$ * $((a^3b^{-1})^3(ab^{-1})^7)^2$		
PSL(2,169)	$2413320 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13^2 \cdot 17$	$m = 17$ * $(ab^{-1}(ab^{-3})^2)^2$		
PSL(2,173)	$2588772 = 2^2 \cdot 3 \cdot 29 \cdot 43 \cdot 173$	$m = 29$ * $(a^3b^{11})^2$		
PSL(2,179)	$2867580 = 2^2 \cdot 3^2 \cdot 5 \cdot 89 \cdot 179$			
PSL(2,181)	$2964780 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 181$	$m = 7$ * $((a^3b^{-4})^3 \cdot(a^2b^{-1})^5)^2$	$m = 13$ * $(a^2b^{-1}a^2b^{-4})^2$	
PSL(2,191)	$3483840 = 2^6 \cdot 3 \cdot 5 \cdot 19 \cdot 191$	$m = 19$ * $((ab^{-1})^2a^5b^{-1})^2$		
PSL(2,193)	$3594432 = 2^6 \cdot 3 \cdot 97 \cdot 193$			
PSL(2,197)	$3822588 = 2^2 \cdot 3^2 \cdot 7^2 \cdot 11 \cdot 197$			
PSL(2,199)	$3940200 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 199$	$m = 25$ * $(a^5b^{-11})^2$		
PSL(2,211)	$4696860 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 53 \cdot 211$	$m = 7$ * $((a^3b^{-3})^4 \cdot(a^3b^{-1})^2)^2$		
PSL(2,223)	$5544672 = 2^5 \cdot 3 \cdot 7 \cdot 37 \cdot 223$	$m = 7$ * $((a^2b^{-2})^3(a^2b^{-3})^2 \cdot(a^3b^{-1})^2)^2$		
PSL(2,227)	$5848428 = 2^2 \cdot 3 \cdot 19 \cdot 113 \cdot 227$			

http://dx.doi.org/10.22108/IJGT.2021.128791.1696

PSL(2,229)	$6004380 = 2^2 \cdot 3 \cdot 5 \cdot 19 \cdot 23 \cdot 229$	$m = 19$ * $(a^2b^{-3}ab^{-2})^2$	$m = 23$ * $(a^3b^{-8})^2$	
PSL(2,233)	$6324552 = 2^3 \cdot 3^2 \cdot 13 \cdot 29 \cdot 233$	$m = 29$ * $(a^4b^7)^2$		
PSL(2,239)	$6825840 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 239$	$m = 7$ * $((ab^{-2})^3(ab^{-1})^5 \cdot(ab^{-3})^3)^2$	$m = 17$ * $((ab^{-1})^2ab^{-5})^2$	
PSL(2,241)	$6998640 = 2^4 \cdot 3 \cdot 5 \cdot 11^2 \cdot 241$			
PSL(2,243)	$7174332 = 2^2 \cdot 3^5 \cdot 11^2 \cdot 61$			
PSL(2,251)	$7906500 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 251$	$m = 7$ * $((ab^{-1})^3ab^{-2} \cdot(a^3b^{-2})^3)^2$		
PSL(2,257)	$8487168 = 2^8 \cdot 3 \cdot 43 \cdot 257$			
PSL(2,263)	$9095592 = 2^3 \cdot 3 \cdot 11 \cdot 131 \cdot 263$			
PSL(2,269)	$9732420 = 2^2 \cdot 3^3 \cdot 5 \cdot 67 \cdot 269$			
PSL(2,271)	$9951120 = 2^4 \cdot 3^3 \cdot 5 \cdot 17 \cdot 271$	$m = 27$ * $(a^3b^{-7})^2$		

It seems intriguing to find out for which m dividing the order of the group there exist presentations for $\mathrm{PSL}(2,q)$ of the above type. This would imply having a presentation with two generators, one of order two and one of order three, whose product has order m. This is often referred to as having a generating triple $(2,3,m)$ and is of course the same as saying that we have a factor group of $D(2,3,m)$. An analysis due to Macbeath [12] shows that $\mathrm{PSL}(2,q)$ has a generating triple $(2,3,7)$, i.e., it is a Hurwitz group, if and only if $q = p$ is prime and $p = 7$ or $p \equiv \pm 1 \pmod 7$ or $q = p^3$ and p is prime with $p \equiv \pm 2 \pmod 7$ or $p \equiv \pm 3 \pmod 7$. We see that our table contains presentations with $m = 7$ for all groups $\mathrm{PSL}(2,q)$ which are Hurwitz, except $\mathrm{PSL}(2,197)$ for which we could not find any nonstandard presentation. Of course it may be that $\mathrm{PSL}(2,197)$ does not admit a presentation with generating triple $(2,3,7)$ and three relations. We are not aware of analyses similar to Macbeath's for $m \neq 7$.

The only finite simple group outside the series $\mathrm{PSL}(2,q)$ for which our search has yielded an efficient presentation is the sporadic Janko group J_2 of order 604800. We have

$$J_2 \cong \left\langle a, b \mid aba = bab,\, ab^2a = b^5,\, (a^3b^{-2}a^2b^4)^3 = \mathbf{1} \right\rangle .$$

This has length 48 and is by far not the shortest known efficient presentation for J_2. Campbell et al. [4] have found the following presentation of length 22:

$$J_2 \cong \left\langle a, b \mid a^3 = b^5 = abab^2a^{-1}b^{-1}a^{-1}b^2abab^{-1} = \mathbf{1} \right\rangle .$$

In terms of computational efficiency, however, when performing coset enumeration with respect to the trivial subgroup, the former presentation required 3.5×10^3 ms CPU time and 72 MB memory, while the latter needed 23×10^3 ms and 263 MB.

All presentations described in this study have a simple geometric interpretation. Excluding $m = 5$, each one can be rewritten as a presentation with two generators and four relations, the first three being the relations for $D(2,3,m)$ (according to Proposition 1.1). Recall that the generators a and b act on the hyperbolic plane, tessellated by congruent equilateral geodesic triangles with angles $2\pi/m$, as rotations about two of the vertices of a triangle. The fourth relation ensures finiteness. The normal closure in $D(2,3,m)$ of the subgroup generated by the word giving this fourth relation is a Fuchsian group. Thus the group obtained appears as an automorphism group of the corresponding compact Riemann surface. The genus of the surface is calculated according to Equation 2.1. We observe that a group $\mathrm{PSL}(2,q)$ may occur as a factor group of $D(2,3,m)$ for several different values of m, so we may have several different surfaces with the same automorphism group.

Acknowledgments

The author is grateful to Christopher Parker for helpful information.

References

[1] H. Behr and J. Mennicke, A presentation of the groups PSL(2, p), *Canadian J. Math.*, **20** (1968) 1432–1438.

[2] C. M. Campbell, E. F. Robertson and P. D. Williams, *Efficient presentations for finite simple groups and related groups*, Groups - Korea 1988, Lecture Notes in Math., 1398, Springer, Berlin, 1989 65–72.

[3] C. M. Campbell, G. Havas, C. Ramsay and E. F. Robertson, Nice efficient presentations for all small simple groups and their covers, *LMS J. Comput. Math.*, **7** (2004) 266–283.

[4] C. M. Campbell, G. Havas, C. Ramsay and E. F. Robertson, On the efficiency of the simple groups of order less than a million and their covers, *Experimental Math.*, **16** (2007) 347–358.

[5] C. M. Campbell and E. F. Robertson, A deficiency zero presentation for SL(2, p), *Bull. London Math. Soc.*, **12** (1980) 17–20.

[6] M. D. E. Conder, Hurwitz groups: a brief survey, *Bull. Amer. Math. Soc.* (N.S.), **23** (1990) 359–370.

[7] H. S. M. Coxeter and W. 0. J. Moser, *Generators and relations for discrete groups*, Springer-Verlag, Berlin-Gottingen-Heidelberg, 1957.

[8] GAP - Groups, Algorithms, Programming-a System for Computational Discrete Algebra, https://www.gap-system.org/.

[9] I. Hajdini and O. Stoytchev, The Fundamental Group of $SO(n)$ Via Quotients of Braid Groups, Preprint (2016). https://arxiv.org/abs/1607.05876.

[10] F. Klein, *On the order-seven transformation of elliptic functions*, Translated from the German and with an introduction by Silvio Levy. Math. Sci. Res. Inst. Publ., **35**, The eightfold way, Cambridge Univ. Press, Cambridge, 1999 287–331.

[11] A. M. Macbeath, *Hurwitz groups and surfaces*, The eightfold way, Math. Sci. Res. Inst. Publ., **35**, Cambridge Univ. Press, Cambridge, 1999 103–113.

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

[13] J. Mennicke, On Ihara's modular group, *Invent. Math.*, **4** (1967) 202–228.

[14] J. Schur, Untersuchungen uber die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, *J. Reine Angew. Math.*, **132** (1907) 85–137.

[15] J. Sunday, Presentations of the groups SL(2, m) and PSL(2, m), *Canadian J. Math.*, **24** (1972) 1129–1131.

[16] H. Zassenhaus, A presentation of the groups PSL(2, p) with three defining relations, *Can. J. Math.*, **21** (1969) 310–311.

Orlin Stoytchev

Department of Mathematics and Science, American University in Bulgaria, 2700 Blagoevgrad, Bulgaria

Email: ostoytchev@aubg.edu