CONFORMAL GEOMETRY AND DYNAMICS
An Electronic Journal of the American Mathematical Society
Volume 6, Pages 33–60 (May 30, 2002)
S 1088-4173(02)00073-5

SOME PRESENTATIONS FOR $\overline{\Gamma}_0(N)$

ANTONIO LASCURAIN ORIVE

Abstract. Some presentations of the Fuchsian groups defined by the Hecke congruence subgroups

$$\Gamma_0(N) \;=\; \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \;\middle|\; c \equiv 0 \mod N \right\}$$

are given. The first is one obtained by the Reidemeister-Schreier rewriting process, thereby completing and correcting Chuman's work on the subject. The main result (Theorem 3) is the reduction of this huge presentation into another one which is simple and useful. In the process, $\mathbb{Z}_N$ is partitioned into three subsets that exhibit many cyclic and dual properties of its ring structure. For some cases, a *minimal* presentation derived from the Ford domains is given explicitly in terms of the units and its inverses.

1. Introduction

The Fuchsian groups $\overline{\Gamma}_0(N)$ play an important role in number theory. Moreover, the properties of these groups seem to be closely related to the structure of the rings $\mathbb{Z}_N$. The exhibition of presentations for these groups is very useful to computational number theorists, however, those which are known are far from simple.

Using the Reidemeister-Schreier rewriting process, Radamacher [9] got a presentation for $\overline{\Gamma}_0(p)$, p a prime number. Chuman [3] generalized this presentation for an arbitrary number; nevertheless, his presentation is incomplete and therefore incorrect in most cases. The main problem is that a crucial relator, denoted in this paper by $\overline{R}_{14}$, is not included in his presentation. The importance of this relator is described at the end of this article, where an explicit presentation of $\overline{\Gamma}_0(30)$ is given.

Although Chuman's work pioneers the field, it fails in key results such as those already mentioned and in the formula of the rank of these groups in the torsion cases; furthermore, he does not exhibit a simplified presentation. His article also contains far too many misprints, making it virtually unaccessible to the reader.

The object of this paper is to produce some presentations for $\overline{\Gamma}_0(N)$, accessible and useful. One of the main results is the exhibition of a presentation arising from the Reidemeister-Schreier rewriting process which can be applied to specific cases (see Theorem 3 and the examples that follow it). The huge presentation given by Theorem 1 is developed in great detail, with the aim of simplifying it.

In the process of obtaining the relators derived from the Reidemeister-Schreier rewriting process, a whole set of results on the structure of the rings $\mathbb{Z}_N$ arises. The

Received by the editors January 8, 2001 and, in revised form, April 11, 2002.
2000 *Mathematics Subject Classification.* Primary 11F06, 20H05, 30F35, 51M10, 52C22; Secondary 13M05, 22E40.

cyclic and dual nature of distinct collections of numbers becomes apparent (see the remark after Theorem 1, Lemmas 3, 4 and 7 and the long proof of Theorem 1, Cases 1 through 7). Most of these properties are derived when considering the different proper divisors d of N and the units in $\mathbb{Z}_w$, $w = (d, \frac{N}{d})$. For instance, it follows from Subcase 1a, that if N is a prime number and $N \equiv 2 \mod 3$, then the set $\mathbb{Z}_N - \{\overline{0}, \overline{1}\}$ may be partitioned into *cycles* of length three.

One more explicit presentation derived from geometric methods is given for a large collection of groups $\overline{\Gamma}_0(N)$. This one is obtained by applying one of Poincaré's theorems for fundamental polygons to the Ford domains (see Theorem 4). The virtue of this presentation is that it is given by an explicit and simple expression in terms of the units and their inverses.

Kulkarni has also exhibited presentations derived from fundamental domains (see [4]); however, his polygons are not Ford regions. Finally, I would like to thank Troels Jørgensen for introducing me to this area of research.

2. Preliminaries

We will denote by Γ the classical modular group $SL(2, \mathbb{C})$; the corresponding group of transformations $\mathrm{PSL}(2, \mathbb{Z})$ will be written as $\overline{\Gamma}$. In general, we will put bars to symbols representing matrices, to denote the corresponding transformations. It is well known that $\overline{\Gamma}$ has the following presentation,

$$\left\langle \overline{T}, \overline{S};\ \overline{S}^2,\ (\overline{S}\,\overline{T})^3 \right\rangle, \tag{2.1}$$

where

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

One way to prove this is by applying one of Poincaré's theorems for fundamental domains to the Dirichlet polygon with center at $2i$ (see [7], pp. 230–234).

Let $\Gamma_0(N)$ denote the Hecke congruence subgroup of Γ of level N, consisting of the matrices

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \quad \middle| \quad c \equiv 0 \mod N \right\}.$$

The election of representatives for the right cosets is necessary to apply the Reidemeister-Schreier rewriting process to exhibit a presentation of $\overline{\Gamma}_0(N)$, derived from the presentation of $\overline{\Gamma}$ defined by (2.1).

Lemma 1. *Let $\overline{\Gamma}_\infty$ denote the subgroup of translations of $\overline{\Gamma}$; then, every double coset*

$$\overline{\Gamma}_0(N)\,\overline{V}\,\overline{\Gamma}_\infty, \qquad \overline{V} \in \overline{\Gamma},$$

contains an element of the form

$$\overline{S}\,\overline{T}^{\,n}\,\overline{S}, \qquad n \in \mathbb{Z}.$$

Proof. One may find a matrix $U \in \Gamma_0(N)$, for which

$$U\,V = \begin{pmatrix} 1 & * \\ * & * \end{pmatrix}.$$

Hence for suitable n,

$$U\,V\,T^{\,n} = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}.$$

Since

$$S\,T^{\,m}S = \begin{pmatrix} -1 & 0 \\ m & -1 \end{pmatrix},$$

the lemma follows. A more detailed proof may be found in [3], p. 382. □

Lemma 2. *The double cosets defined by* $\overline{S}\,\overline{T}^{\,m}\,\overline{S}$ *and* $\overline{S}\,\overline{T}^{\,n}\,\overline{S}$, $n, m \in \mathbb{Z}$, *are equal if and only if the following conditions hold:*

(a) $(n, N) = (m, N) = d$,
(b) $\dfrac{n}{d} \equiv \dfrac{m}{d} \mod w, \quad w = \left(d, \frac{N}{d}\right)$.

Proof. Using matrices, a calculation shows that $\overline{S}\,\overline{T}^{\,m}\,\overline{S}$ and $\overline{S}\,\overline{T}^{\,n}\,\overline{S}$ belong to the same double coset if and only if

$$m - n + mnu \;\equiv\; 0 \mod N, \tag{2.2}$$

for some $u \in \mathbb{Z}$. It is also not difficult to prove that condition (2.2) is equivalent to the hypotheses (a) and (b). For more details see [3], p. 382. □

It is a remarkable fact that conditions (a) and (b) in Lemma 2 are exactly those that define the distribution of parabolic vertices of the Ford polygon into cusps (see [5]).

An application of Lemmas 1 and 2 will yield representatives for double cosets, but first one has to define a set of numbers. For each proper divisor d of N, let

$$A_d = \{m_{d,1},\ m_{d,2}, \ldots, m_{d,\phi(w)}\}$$

be a complete set of representatives for $\mathbb{Z}_w^*$, where $w = \left(d, \frac{N}{d}\right)$ and ϕ denotes the Euler function.

We make this selection so that $0 < m_{d,j} < \frac{N}{d}$ and $(m_{d,j},\ \frac{N}{d}) = 1$, for all $j \in \{1, 2, \ldots, \phi(w)\}$. This is possible because the Chinese Remainder Theorem implies that the natural map from $\mathbb{Z}_{\frac{N}{d}}^*$ to $\mathbb{Z}_w^*$ is surjective.

For example, if $N = 9000$ and $d = 100$, one has $\frac{N}{d} = 90$, $w = 10$ and we may choose

$$A_{100} = \{1, 13, 7, 19\}.$$

Having fixed the sets A_d, one defines

$$M_d = \{d\, m_{d,j} \mid m_{d,j} \;\in\; A_d\}$$

and

$$\boldsymbol{M} \;=\; \bigcup_{\substack{d|N \\ 1<d<N}} M_d.$$

It follows from the definition that $Md \cap Md' = \emptyset$, if $d \neq d'$.

Chuman's definition of $\boldsymbol{M}$ requires $(m_{d,j},\ N) = 1$, instead of $(m_{d,j},\ \frac{N}{d}) = 1$, however this is not consistent with Proposition 2 in his paper. This can be seen with $N = 36$ and $d = 12$, since for this case $w = 3$ and the class of $\overline{2}$ is represented with a number which is at least 5, but then $\boldsymbol{M}$ has elements bigger than 36.

Proposition 1. *The set of transformations,*

$$\overline{\boldsymbol{F}} = \{\overline{I},\ \overline{S},\ \overline{S}\ \overline{T}^{\,m}\,\overline{S},\quad m \in \boldsymbol{M}\},$$

forms a complete set of representatives of double cosets in

$$\overline{\Gamma}_0(N) \setminus \overline{\Gamma} \,/\, \overline{\Gamma}_\infty.$$

Proof. This result is a direct consequence of the previous lemmas and the definition of $\boldsymbol{M}$:

It follows from Lemma 2 that

$$\overline{S}\,\overline{T}^{\,k\,N}\,\overline{S},\quad k \in \mathbb{Z},$$

belongs to the identity class. This lemma also implies that

$$\overline{S}\,\overline{T}^{\,k}\,\overline{S},\quad (k,\,N) = 1,$$

defines the same double coset as

$$\overline{\Gamma}_0(N)\,\overline{T}\,\overline{\Gamma}_\infty.$$

Since

$$S\,T\,S = T^{\,-1}\,S\,T^{\,-1},$$

these classes are represented by $\overline{S}$.

Clearly, all other double classes are determined by the elements in $\boldsymbol{M}$. □

The next step is to distribute the double coset classes into right coset classes defined by $\overline{\Gamma}_0(N)$. Observe that for fixed $\overline{U} \in \overline{\boldsymbol{F}}$, given

$$\overline{V}_1\,\overline{U}\,\overline{T}^{\,l}\ \in\ \overline{\Gamma}_0(N)\,\overline{U}\,\overline{\Gamma}_\infty,\quad \overline{V}_1\ \in\ \overline{\Gamma}_0(N);$$

if we could write $\overline{T}^{\,l}$ as

$$(\overline{U}^{\,-1}\,\overline{V}_2\,\overline{U})\ \overline{T}^{\,j},\quad \overline{V}_2 \in \overline{\Gamma}_0(N),$$

we would have

$$\overline{V}_1\,\overline{U}\,\overline{T}^{\,l}\ =\ \overline{V}_1\,\overline{V}_2\,\overline{U}\,\overline{T}^{\,j}\ \in\ \overline{\Gamma}_0(N)\,\overline{U}\,\overline{T}^{\,j}.$$

Hence, the key to the decomposition of double cosets will be the subgroups of translations defined by

$$\left(\overline{U}\,\overline{\Gamma}_0(N)\,\overline{U}^{\,-1}\right) \bigcap \overline{\Gamma}_\infty.$$

If $\overline{U}$ is of the form $\overline{S}\,\overline{T}^{\,m}\,\overline{S}$, one has

$$U\,T^{\,n}\,U^{\,-1} = \begin{pmatrix} * & * \\ m\,n^2 & * \end{pmatrix}\ \in \Gamma_0(N), \tag{2.3}$$

provided $m\,n^2 \equiv 0 \mod N$.

On the other hand, if $\overline{U} = \overline{S}$,

$$S\,T^{\,n}\,S = \begin{pmatrix} -1 & 0 \\ n & -1 \end{pmatrix} \in \Gamma_0(N),$$

whenever $n \equiv 0 \mod N$.

In the first cases, if we take the smallest integer n for which

$$mn^2 \equiv 0 \mod N,$$

we get the coset decomposition for

$$\left[\left(\overline{U}^{-1}\overline{\Gamma}_0(N)\,\overline{U}\right)\bigcap\overline{\Gamma}_\infty,\ \overline{\Gamma}_\infty\right]$$

with the representatives

$$\overline{I},\,\overline{T},\,\overline{T}^2,\ldots,\overline{T}^{n(m)-1};$$

whereas, in the second case the representatives are

$$\overline{I},\,\overline{T},\,\overline{T}^2,\ldots,\overline{T}^{N-1}.$$

These ideas lead to the election of representatives for $[\overline{\Gamma}_0(N),\overline{\Gamma}]$.

Proposition 2. *A complete set of representatives for right cosets in* $[\,\overline{\Gamma}_0(N),\overline{\Gamma}\,]$ *is given by the following set* $\overline{\boldsymbol{W}}$ *of transformations*

$$\left\{\overline{I},\ \overline{S}\ \overline{T}^k,\ 0\le k\le N-1,\ \ \overline{S}\,\overline{T}^m\,\overline{S}\,\overline{T}^j,\ m\in\boldsymbol{M},\ \ 0\le j\le n(m)-1\right\},$$

where $n(m)$ *is the smallest integer for which*

$$n(m)\,m^2\equiv 0\quad mod\ N.$$

One may easily deduce this result from the previous remarks. For other details, we refer to Chuman's paper.

Sometimes we will write simply n for $n(m)$. It turns out that

$$n\ =\ \frac{N}{dw},$$

where $w=\left(d,\frac{N}{d}\right)$ and $d=(m,N)$. This is not hard to prove by writing the prime decompositions of $d,\ \frac{N}{d},\ N,\ m$ and w. This equality also shows that the number n does not depend on m, but only on d. It is also true that the condition

$$n(m)=1$$

implies that m is uniquely determined. This follows because under such hypothesis $w=\frac{N}{d}$, and each integer in $\{1,2,\ldots,\frac{N}{d}\}$ represents a different class in $\mathbb{Z}_w$.

We describe briefly the Reidemeister-Schreier rewriting process: given a transformation $\overline{V}\in\overline{\Gamma}$, we will denote by $\overline{\overline{V}}$ the corresponding element in $\overline{\boldsymbol{W}}$ representing $\overline{V}$. In our context, the Reidemeister-Schreier method states that the set

$$\overline{\boldsymbol{G}}\ =\ \left\{\overline{V}\,\overline{T}\,\overline{\left(\overline{V}\,\overline{T}\right)}^{-1},\ \overline{V}\,\overline{S}\,\overline{\left(\overline{V}\,\overline{S}\right)}^{-1},\quad \overline{V}\in\overline{\boldsymbol{W}}\right\}$$

generates $\overline{\Gamma}_0\,(N)$ (cf. [8], p. 89).

Giving a reduced word in the letters $\overline{T},\ \overline{T}^{-1}$ and $\overline{S}$, say

$$\overline{V}\ =\ \overline{V}_1^{\,\epsilon_1}\,\overline{V}_2^{\,\epsilon_2}\cdots\overline{V}_m^{\,\epsilon_m},$$

where each $\overline{V}_j$ equals $\overline{T}$ or $\overline{S}$ and $\epsilon_j=\pm1$. Let $\overline{U}_j$ denote the preceding segment in the word $\overline{V}$ of the letter $\overline{V}_j$ and

$$\overline{W}_j\ =\ \overline{\overline{U}}_j\ \overline{V}_j^{\,\epsilon_j}\ \left(\overline{\overline{U}_j\ \overline{V_j}^{\,\epsilon_j}}\right)^{-1},$$

then

$$\tau\left(\overline{V}_1^{\,\epsilon_1}\ \overline{V}_2^{\,\epsilon_2}\cdots\overline{V}_m^{\,\epsilon_m}\right)\ =\ \overline{W}_1\,\overline{W}_2\cdots\overline{W}_m$$

is the Reidemeister-Schreier rewriting process with respect to the set of generators $\overline{\boldsymbol{G}}$ (cf. [8], Corollary 2.7.2 and proof, pp. 90–91).

One concludes that $\overline{\Gamma}_0(N)$ has a presentation with the family $\overline{\boldsymbol{G}}$ as the set of generators and

$$\overline{\boldsymbol{R}} \,=\, \left\{\tau\left(\overline{V}\,\overline{S}^{2}\,\overline{V}^{-1}\right),\, \tau\left(\overline{V}\,(\overline{S}\,\overline{T})^{3}\,\overline{V}^{-1}\right),\quad \overline{V}\in\overline{\boldsymbol{W}}\right\},$$

the set of relators. This is the Reidemeister theorem (cf. [8], p. 91).

3. Some algebraic presentations

It will be convenient to partition the first $N-1$ integers into three sets, which we will denote by $\boldsymbol{M}$, $\boldsymbol{K}$ and $\boldsymbol{P}$. The set $\boldsymbol{M}$ was defined in the preliminaries,

$$\boldsymbol{K}=\left\{k\in\{1,2,\ldots,N-1\}\;\middle|\;(k,N)>1,\; k\notin\boldsymbol{M}\right\}$$

and

$$\boldsymbol{P}=\left\{k\in\{1,2,\ldots,N-1\}\;\middle|\;(k,N)=1\right\}.$$

In order to exhibit the set of generators $\overline{\boldsymbol{G}}$, we need to determine the representatives in $\overline{\boldsymbol{W}}$ of certain transformations.

Lemma 3. *Given $k\in\boldsymbol{K}$, one has that*

$$\overline{\overline{S}\,\overline{T}^{k}\,\overline{S}}\;=\;\overline{S}\,\overline{T}^{m}\,\overline{S}\,\overline{T}^{j},\quad m\in\boldsymbol{M},\quad 1\le j\le n(m)-1$$

and

$$k\,(1-mj)\equiv m\mod N. \tag{3.1}$$

Proof. Calculation yields

$$S\,T^{k}\,S\,T^{-j}\,S^{-1}\,T^{-m}\,S^{-1}\;=\;\begin{pmatrix}* & *\\ -k+mk\,j+m & *\end{pmatrix}.$$

Hence the result follows, provided the congruence (3.1) holds for $1\le j\le n-1$. We observe that (3.1) is the same congruence as (2.2) in the proof of Lemma 2, so there exists $m\in\boldsymbol{M}$ such that $(k,N)=(m,N)=d$ and $\frac{k}{d}\equiv\frac{m}{d}\mod w$, where $w=\left(d,\frac{N}{d}\right)$. Under this notation

$$m-k+mk\,u\;\equiv\;0\mod N,\quad u\in\mathbb{Z}.$$

Since $(N,mk)=dw$, it follows easily from the basic theory of Diophantine equations, that one may choose $0<u<\frac{N}{dw}-1=n-1$. □

It is clear from Lemma 3 that the pair $(m,\,j)$ is unique. We will write

$$k\;\sim\;(m,\,j)\quad\text{or}\quad(m,\,j)\;\sim\;k,$$

to describe the congruence (3.1). Observe that if (3.1) arises

$$(1-mj,\,N)=1.$$

Moreover, this last condition implies the existence of $k\in\boldsymbol{K}$ such that $(m,\,j)\;\sim\;k$.

Lemma 4. *Given $m\in\boldsymbol{M}$ and $j\in\{1,2,\ldots,n(m)-1\}$, such that $(1-mj,N)>1$, then there exists another pair $(m',\,j')$, $m'\in\boldsymbol{M}$, $1\le j'\le n(m')-1$, for which*

$$\overline{\overline{S}\,\overline{T}^{m}\,\overline{S}\,\overline{T}^{j}\,\overline{S}}\;=\;\overline{S}\,\overline{T}^{m'}\,\overline{S}\,\overline{T}^{j'}$$

and

$$(1-mj)(1-m'j')\;\equiv\;-m\,m'\mod N. \tag{3.2}$$

Proof. Using Lemma 3 and calculating some products of matrices defined by other transformations in $\overline{\boldsymbol{W}}$, the first assertion is a consequence of Proposition 2 and the hypothesis on $1 - mj$.

Since

$$S\,T^{\,m}\,S\,T^{\,j}\,S\,T^{\,-j'}\,S^{\,-1}\,T^{\,-m'}\,S^{\,-1} \;=\; \begin{pmatrix} * & * \\ (1-mj)(1-m'j') + mm' & * \end{pmatrix} \in \Gamma_0(N),$$

the second assertion also follows. □

Again the pair $(m',\, j')$ is unique. We will refer to the congruence (3.2) simply as

$$(m,\, j) \;\sim\; (m',\, j').$$

It follows from (3.2) that if $(m,\, j) \sim (m',\, j')$, one necessarily has that

$$(1 - m\,j,\, N) > 1.$$

Observe that given $m \in \boldsymbol{M}$ and $0 \;<\; j \;<\; n(m) - 1$, either $(m,\, j) \;\sim\; k$, or $(m,\, j) \;\sim\; (m',\, j')$.

Before exhibiting the generators it is necessary to get the representatives of all words of the form

$$\overline{V}\,\overline{S},\; \overline{V}\,\overline{T}, \quad \overline{V} \in \overline{\boldsymbol{W}}.$$

Lemma 5. *For the following transformations in $\overline{\Gamma}$, one gets representatives in $\overline{\boldsymbol{W}}$, as follows:*

1. $\overline{\overline{I}\,\overline{T}} = \overline{I}.$
2. $\overline{\overline{S}\,\overline{T}^{\,k}\,\overline{T}} \;=\; \overline{S}\,\overline{T}^{\,k+1}, \qquad k = 0,\, 1,\, 2, \ldots, N-2.$
3. $\overline{\overline{S}\,\overline{T}^{\,N-1}\,\overline{T}} \;=\; \overline{S}.$
4. $\overline{\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,j}\,\overline{T}} \;=\; \overline{S}\,\overline{T}^{\,m}\overline{S}\,\overline{T}^{\,j+1}, \qquad m \in \boldsymbol{M}, \quad 0 \;\le\; j \;\le\; n(m) - 2.$
5. $\overline{\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,n-1}\,\overline{T}} \;=\overline{S}\,\overline{T}^{\,m}\,\overline{S}, \qquad m \in \boldsymbol{M}, \;\; n = n(m).$
6. $\overline{\overline{I}\,\overline{S}} \;=\; \overline{S}.$
7. $\overline{\overline{S}\,\overline{S}} \;=\; \overline{I}.$
8. $\overline{\overline{S}\,\overline{T}^{\,m}\,\overline{S}} \;=\; \overline{S}\,\overline{T}^{\,m}\,\overline{S}, \qquad m \in M.$
9. $\overline{\overline{S}\,\overline{T}^{\,k}\,\overline{S}} \;=\; \overline{S}\,\overline{T}^{\,k^*}, \qquad (k, N) = 1, \;\; k\,k^* \equiv -1 \quad \mathit{mod}\ N.$
10. $\overline{\overline{S}\,\overline{T}^{\,k}\,\overline{S}} \;=\; \overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,j}, \qquad k \;\sim\; (m,\, j).$
11. $\overline{\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{S}} \;=\; \overline{S}\,\overline{T}^{\,m}, \qquad m \in M.$
12. $\overline{\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,j}\,\overline{S}} \;=\; \overline{S}\,\overline{T}^{\,k}, \qquad (m,\, j) \;\sim\; k.$
13. $\overline{\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,j}\,\overline{S}} \;=\; \overline{S}\overline{T}^{\,m'}\,\overline{S}\,\overline{T}^{\,j'}, \qquad (m,\, j) \;\sim\; (m',\, j').$

Proof. Assertions *1, 2, 4, 6, 7, 8, 10, 11* and *13* are either trivial or have been proved in Lemmas 3 and 4. Assertion *3* follows because

$$S\,T^{\,N}\,S = \begin{pmatrix} -1 & 0 \\ N & -1 \end{pmatrix},$$

whereas using (2.3) one may prove Assertion *5*.

Also, since

$$S\,T^{\,k}\,S\,T^{\,-k^*}\,S=\begin{pmatrix} * & * \\ 1+k\,k^* & * \end{pmatrix},$$

Assertion *9* follows. Finally, Assertion *12* is the dual situation to Assertion *10* and may be proved by taking the inverse of the matrix in the proof of Lemma 3. □

The exhibition of the generators for $\overline{\Gamma}_0(N)$ is now a direct consequence of Lemma 5 and the Reidemeister-Schreier method.

Proposition 3. *The Hecke congruence subgroup $\overline{\Gamma}_0(N)$ is generated by the set of transformations*

$$\overline{\boldsymbol{G}}\;=\;\left\{\overline{T},\;\overline{U},\;\overline{V}_k,\;\;1\,\leq\,k\,\leq\,N-1,\;\;\overline{V}_{m,\,j},\;\;m\in\boldsymbol{M},\;\;1\,\leq\,j\,\leq\,n(m)-1\right\},$$

where

$$\begin{aligned}
&\overline{U}\;=\;\overline{S}\,\overline{T}^{\,N}\,\overline{S},\\
&\overline{V}_k\;=\;\overline{S}\,\overline{T}^{\,k}\,\overline{S}\,\overline{T}^{\,-k^*}\,\overline{S}, && k\,k^*\equiv -1 \quad mod\,N,\\
&\overline{V}_k\;=\;\overline{S}\,\overline{T}^{\,k}\,\overline{S}\,\overline{T}^{\,-j}\,\overline{S}\,\overline{T}^{\,-m}\,\overline{S}, && k\,\sim\,(m,\,j),\\
&\overline{V}_m\;=\;\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,n}\,\overline{S}\,\overline{T}^{\,-m}\,\overline{S}, && m\in\boldsymbol{M},\;\;n=n(m),\\
&\overline{V}_{m,\,j}\;=\;\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,j}\overline{S}\,\overline{T}^{\,-k}\,\overline{S}, && (m,\,j)\;\sim\;k,\\
&\overline{V}_{m,\,j}\;=\;\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,j}\overline{S}\,\overline{T}^{\,-j'}\,\overline{S}\,\overline{T}^{\,-m'}\,\overline{S}, && (m,\,j)\;\sim\;(m',\,j').
\end{aligned}$$

Most of the generators in the set $\overline{\boldsymbol{G}}$ appear together with their inverses. However, these repetitions will be eliminated using the relators defined by the rewriting of the words

$$\overline{V}\,\overline{S}^{\,2}\,\overline{V}^{\,-1},\qquad \overline{V}\in\overline{\boldsymbol{K}}.$$

Lemma 6. *Up to a cyclic permutation, the relators derived from $\tau\left(\overline{V}\,\overline{S}^{\,2}\,\overline{V}^{\,-1}\right)$, $\overline{V}\in\overline{\boldsymbol{K}}$, in the Reidemeister presentation are:*

$$\begin{aligned}
&\overline{R}_1=\overline{V}_{\,k}\,\overline{V}_{\,k^*}, && k\in\boldsymbol{P},\\
&\overline{R}_2=\overline{V}_{\,k}\,\overline{V}_{\,m,\,j}, && k\,\sim\,(m,\,j),\\
&\overline{R}_3=\overline{V}_{\,m,\,j}\,\overline{V}_{\,m',\,j'}, && (m,\,j)\;\sim\;(m',\,j').
\end{aligned}$$

Proof. One easily checks that

$$\tau\left(\overline{V}\,\overline{S}^{\,2}\,\overline{V}^{\,-1}\right)\;=\;\overline{I},$$

for the cases $\overline{V}\,=\,\overline{I},\;\overline{S},\;\overline{S}\,\overline{T}^{\,m}\,\overline{S},\;\overline{S}\,\overline{T}^{\,m},\;m\in\boldsymbol{M}$.

If $\overline{V}\;=\;\overline{S}\;\overline{T}^{\,k},\quad k\in\boldsymbol{P}$, using Assertion *9* in Lemma 5, the rewriting of the segment $\overline{S}\,\overline{T}^{\,k}\,\overline{S}$ yields $\overline{V}_k$ and that one of the segment $\overline{S}\,\overline{T}^{\,k}\,\overline{S}\,\overline{S}$ is $\overline{V}_{\,k^*}$. Since the rewriting of all other segments is the identity, one gets relator $\overline{R}_1$.

Similarly, if $k\;\sim\;(m,\,j)$, using Assertions *10* and *12* in Lemma 5, one obtains relator $\overline{R}_2$

$$\tau\left(\overline{S}\,\overline{T}^{\,k}\,\overline{S}^{\,2}\,(\overline{S}\,\overline{T}^{\,k})^{\,-1}\right)\;=\;\overline{V}_{\,k}\,\overline{V}_{\,m,\,j}.$$

The dual case

$$\tau\left(\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,j}\,\overline{S}^{\,2}\,(\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,j}\,)^{\,-1}\right),\qquad (m,\,j)\;\sim\;k,$$

yields $\overline{V}_{m,\,j}\,\overline{V}_k$, a cyclic permutation of $\overline{R}_2$.

Finally, if $(m,\,j) \sim (m',\,j')$, using Assertion *13* in Lemma 5, one gets relator $\overline{R}_3$,

$$\tau\left(\overline{S}\,\overline{T}^{m}\,\overline{S}\,\overline{T}^{j}\,\overline{S}^{2}\,(\overline{S}\,\overline{T}^{m}\,\overline{S}\,\overline{T}^{j}\,)^{-1}\right) \;=\; \overline{V}_{m,\,j}\,\overline{V}_{m',\,j'}.$$

□

The calculations of the relators derived from $\overline{S}\,\overline{T}^{3}$ will prove one of the main results. This analysis will also exhibit some properties of the rings $\mathbb{Z}_N$. In particular, the cyclic and dual nature of the distribution of these numbers into the sets $\boldsymbol{M}$, $\boldsymbol{K}$ and $\boldsymbol{P}$.

Theorem 1. *The group $\overline{\Gamma}_0(N)$ may be presented as*

$$\left\{\overline{\boldsymbol{G}};\quad \overline{R}_1,\,\overline{R}_2,\,\overline{R}_3,\ldots,\overline{R}_{14}\right\},$$

where $\overline{R}_1$, $\overline{R}_2$, $\overline{R}_3$ are as defined in Lemma 6, and the other relators are given by:

$$\begin{aligned}
\overline{R}_4 &= \overline{V}_1\,\overline{U}\,\overline{T}, && \\
\overline{R}_5 &= \overline{V}_{k_1}\,\overline{V}_{k_2}\,\overline{V}_{k_3}, && (k_{i+1}) = k_i^* + 1,\ \ i = 1, 2,\\
& && k_3^* + 1 = k_1,\\
\overline{R}_6 &= \overline{V}_k\,\overline{V}_{k-1}, && k \in \boldsymbol{P},\ \ k-1 \in \boldsymbol{M},\\
& && k^* + 1 = k - 1,\ \ n(k-1) = 1,\\
\overline{R}_7 &= \overline{V}_k\,\overline{V}_{k_1,\,1}, && k \in \boldsymbol{P},\ \ k_1 = k^* + 1,\\
& && (k_1, 1) \sim k - 1,\\
\overline{R}_8 &= \overline{V}_k\,\overline{V}_{k_1}\,\overline{V}_{m,\,j}\,, && k \in \boldsymbol{P},\ \ k_1 = k^* + 1,\\
& && k_1 \sim (m,\,j-1),\ \ (m,\,j) \sim k - 1,\\
\overline{R}_9 &= \overline{V}_k\,\overline{V}_{k_1}\,\overline{V}_{k-1}, && k \in \boldsymbol{P},\ \ k_1 = k^* + 1,\\
& && k_1 \sim (k-1,\,n-1),\ \ n = n(k-1),\\
\overline{R}_{10} &= \overline{V}_{m,\,1}\,\overline{V}_{m-1}, && (m,\,1) \sim (m-1,\,n-1),\\
& && n = n(m-1),\ \ n(m) > 1,\\
\overline{R}_{11} &= \overline{V}_{m,\,1}\,\overline{V}_{m',\,j'+1}, && (m,\,1) \sim (m',\,j'),\\
& && (m',\,j'+1) \sim m - 1,\ \ n(m) > 1,\\
\overline{R}_{12} &= \overline{V}_k\,\overline{V}_{m,\,j+1}\,\overline{V}_{m',\,j'+1}, && k \sim (m,\,j),\\
& && (m,\,j+1) \sim (m',\,j'),\\
& && (m',\,j'+1) \sim k - 1,\\
\overline{R}_{13} &= \overline{V}_k\,\overline{V}_{m,\,j+1}\,\overline{V}_{k-1}, && k \sim (m,\,j),\ n = n(k-1),\\
& && (m,\,j+1) \sim (k-1,\,n-1),\\
\overline{R}_{14} &= \overline{V}_{m_1,\,j_1}\,\overline{V}_{m_2,\,j_2+1}\,\overline{V}_{m_3,\,j_3+1}, && (m_1,\,j_1) \sim (m_2,\,j_2),\\
& && (m_2,\,j_2+1) \sim (m_3,\,j_3),\\
& && (m_3,\,j_3+1) \sim (m_1,\,j_1-1).
\end{aligned}$$

Before proving the theorem, we note that all relators from $\overline{R}_4$ to $\overline{R}_{14}$ follow a cyclic pattern of the numbers, or pairs of numbers, that defined them. Namely, the

elements of the set

$$A \;=\; \{0,1,2,\dots,N\} \bigcup \{(m,j) \mid m \in M,\; 1 \le j \le n(m)-1\}$$

may be paired, given $u \in A$ one defines its dual u^* as follows:

if $u \in \boldsymbol{P}$, u^* is the standard one (as in Assertion *9* in Lemma 5),
if $u \in \boldsymbol{K}$, $u^* = (m,j)$, where $u \sim (m,\, j)$,
if $u \in \boldsymbol{M}$, $u = N$, or $u = 0$, $u^* = u$,
if $u = (m,\, j)$, $u^* = (m',\, j')$, where $(m,\, j) \sim (m',\, j')$.

On the other hand, for each element $u \in A$ one may define its successor $u+1$ as follows:

if $u = (m,\, j)$, $u+1 = (m,\, j+1)$, $j < n-1$,
if $u = (m, n-1)$, $u+1 = m$,
if $u = N$, $u+1 = 0$, and so on.

Under this interpretation all relators from $\overline{R}_4$ to $\overline{R}_{14}$ follow the next rule:

(a) it appears the generator that is associated to u, as a factor;
(b) the next factor is the generator associated to u^*+1;
(c) the next factor is the generator associated to $(u^*+1)^*+1$, and so on.

In all cases one returns to the original generator. The generator associated to $u \in \boldsymbol{M}$ might be either $\overline{V}_m$ or $\overline{V}_{m,\,1}$. $\overline{T}$ is associated to 0 and $\overline{U}$ to N.

Relator $\overline{R}_{14}$ is essential to get a presentation of $\overline{\Gamma}_0(N)$, as it will be shown later with the example $N = 30$. Since Chuman does not include this relator, his presentation is not correct.

The proof of Theorem 1 consists of all calculations

$$\tau\left(\overline{V}\,(\overline{S}\,\overline{T})^3\,\overline{V}^{-1}\right), \qquad \overline{V} \in \overline{\boldsymbol{W}}.$$

We will consider different cases depending on the types of representatives and check that the only relators appearing are those from $\overline{R}_4$ to $\overline{R}_{14}$.

Case 0. $\overline{V} \;=\; \overline{I},\; \overline{S},\; \overline{S}\,\overline{T}$.

Using Assertion *9* in Lemma 5, in all these cases one gets

$$\tau\left(\overline{V}\,(\overline{S}\,\overline{T})^3\,\overline{V}^{-1}\right) \;=\; \overline{V}_1\,\overline{U}\,\overline{T} \;=\; \overline{R}_4,$$

up to a cyclic permutation.

Case 1. $\overline{V} \;=\; \overline{S}\,\overline{T}^{\,k}, \quad k \in \boldsymbol{P}, \quad k > 1.$

One has to calculate

$$\tau\left(\overline{S}\,\overline{T}^{\,k}(\overline{S}\,\overline{T})^3\,(\overline{S}\,\overline{T}^{\,k})^{-1}\right).$$

Using Assertion *9* in Lemma 5, we see that the rewriting of the segments $\overline{S},\; \overline{S}\,\overline{T}, \dots,\; \overline{S}\,\overline{T}^{\,k}$ and $\overline{S}\,\overline{T}^{\,k}\,\overline{S}\,\overline{T}$ is the identity; whereas, that one of $\overline{S}\,\overline{T}^{\,k}\,\overline{S}$ is the generator $\overline{V}_k$.

To calculate the rewriting of other segments, we will consider subcases in accordance with k_1 and $k-1$ being in $\boldsymbol{P}$, $\boldsymbol{M}$ or $\boldsymbol{K}$, where $k_1 = k^* + 1$. First, we make some remarks under the hypothesis $k \in \boldsymbol{P}$.

Remark 1. $k\,k_1 \equiv k-1 \mod N$.

Remark 2.

(a) $(k_1,\, N) = (k-1,\, N)$.

(b) $\dfrac{k_1}{d} \equiv \dfrac{k-1}{d} \quad mod\ w$, where $d = (k-1,\, N)$ and $w = (d, \frac{N}{d})$. Therefore if $k_1 \neq k-1$, only one of them might be in $\boldsymbol{M}$.

Remark 3. One has that $n(k-1) = 1$ if and only if $k-1 = k_1$.

The first remark is evident and implies Remark 2(a). Remark 2(b) follows because

$$k\left(\frac{k_1}{d}\right) \equiv \frac{k-1}{d} \quad mod\ \left(\frac{N}{d}\right)$$

and

$$k\left(\frac{k_1}{d}\right) \equiv \frac{k_1}{d} \quad mod\ d.$$

Finally, Remark 3 arises since

$$(k-1)^2 \equiv 0 \quad mod\ N$$

if and only if

$$k\,(k-1) \equiv k\,k^* + k \quad mod\ N.$$

Now we may proceed with the subcases of Case 1.

Subcase 1a. $k_1 \in \boldsymbol{P}$ or $k-1 \in \boldsymbol{P}$.

Under either hypothesis, both numbers are in $\boldsymbol{P}$. Moreover, in this case a cyclic situation arises. Namely, let $k_2 = k_1^* + 1$, then

$$k_1\, k_2 \equiv k_1 - 1 \quad mod\ N$$

and

$$k_1\, k_2 \;\equiv\; k^* \quad mod\ N,$$

so

$$k\, k_1\, k_2 \;\equiv\; -1 \quad mod\ N.$$

Thus

$$(k-1)\, k_2 \;\equiv\; -1 \quad mod\ N$$

and

$$k_2 \;=\; (k-1)^*.$$

Using this remark, calculation yields

$$\overline{\overline{S}\,\overline{T}^{\,k}\,\overline{S}\,\overline{T}\,\overline{S}} \;=\; \overline{S}\,\overline{T}^{\,k_1^*}.$$

Hence, the rewriting of the segment $\overline{S}\,\overline{T}^{\,k}\,\overline{S}\,\overline{T}\,\overline{S}$ is the generator $\overline{V}_{k_1}$.

Finally, using again the cyclic relation described above, the rewriting of the segment $\overline{S}\;\overline{T}^{\,k}\;\overline{S}\;\overline{T}\;\overline{S}\;\overline{T}\;\overline{S}$ is the generator $\overline{V}_{k_2}$. Since other segments yield the identity, one gets relator $\overline{R}_5$

$$\tau\left(\overline{S}\,\overline{T}^{\,k}(\overline{S}\,\overline{T})^3\,(\overline{S}\,\overline{T}^{\,k})^{-1}\right) \;=\; \overline{V}_k\,\overline{V}_{k_1}\,\overline{V}_{k_2}.$$

Subcase 1b. $k_1 \in \boldsymbol{M},\ k-1 \in \boldsymbol{K}$.

Under these hypotheses

$$k-1 \ \sim \ (k_1,\, 1).$$

This follows because Remark 1 implies that

$$k \ - \ k\, k_1 \equiv 1 \quad mod\ N.$$

Using Assertion *10* in Lemma 5, we see that

$$\overline{\overline{S}\,\overline{T}^{\,k}\,\overline{S}\,\overline{T}\,\overline{S}} = \overline{S}\,\overline{T}^{\,k_1}\,\overline{S}$$

and

$$\tau\left(\overline{S}\,\overline{T}^{\,k}(\overline{S}\,\overline{T})^3\,(\overline{S}\,\overline{T}^{\,k})^{-1}\right) \ = \ \overline{V}_k\,\overline{V}_{k_1,\,1} \ = \ \overline{R}_7.$$

Subcase 1c. $k_1 \in \boldsymbol{K}, \quad k-1 \in \boldsymbol{M}$.

In this case, it turns out that

$$k_1 \ \sim \ (k-1,\, n-1), \quad n = n(k-1).$$

This follows because

$$\begin{aligned}
&[\ 1-(k-1)\,(n-1)\ ]\ k_1 \ \equiv \ k-1 \quad mod\ N \\
&\quad \Leftrightarrow k_1 - k_1\,(k-1)\,n + k_1\,(k-1) \ \equiv \ k-1 \quad mod\ N \\
&\quad \Leftrightarrow k\,k_1 - k\,k_1\,(k-1)\,n + k\,k_1\,(k-1) \ \equiv \ (k-1)\,k \quad mod\ N \\
&\quad \Leftrightarrow k-1+(k-1)^2 \ \equiv \ (k-1)\,k \quad mod\ N.
\end{aligned}$$

Using this remark and

$$\overline{\overline{S}\,\overline{T}^{\,k}\overline{S}\,\overline{T}\,\overline{S}} \ = \ \overline{\overline{S}\,\overline{T}^{k_1}\,\overline{S}},$$

one gets

$$\overline{R}_9 = \overline{V}_k\,\overline{V}_{k_1}\,\overline{V}_{k-1}.$$

Subcase 1d. $k_1,\, k-1 \in \boldsymbol{M}$.

It follows from Remark 2 that $k_1 = k-1$ and from Remark 3 that $n(k-1) = 1$. Using this fact and the techniques of the previous subcases, one easily gets

$$\overline{R}_6 = \overline{V}_k\,\overline{V}_{k-1}.$$

Subcase 1e. $k_1,\, k-1 \in \boldsymbol{K}$.

Under these hypotheses, it turns out that

$$k-1 \ \sim \ (m,\, j) \ \Leftrightarrow \ k_1 \ \sim \ (m,\, j-1).$$

This follows because

$$\begin{aligned}
&m\ [\ (k-1)\,j+1\ ] \ \equiv \ k-1 \quad mod\ N \\
&\quad \Leftrightarrow m\ [\ (k-1)\,(j-1)+k\ ] \ \equiv \ k-1 \quad mod\ N \\
&\quad \Leftrightarrow m\ [\ k\,k_1\,(j-1)+k\ ] \ \equiv \ k\,k_1 \quad mod\ N \\
&\quad \Leftrightarrow m\ [\ k_1\,(j-1)+1\ ] \ \equiv \ k_1 \quad mod\ N.
\end{aligned}$$

Observe that since $k_1 \in \boldsymbol{K}$, $j \ > \ 1$. Using these remarks and Assertion *10* in Lemma 5, one gets a new relator

$$\overline{R}_8 \ = \ \overline{V}_k\,\overline{V}_{k_1}\,\overline{V}_{m,\,j}.$$

Case 2. $\overline{V} = \overline{S}\,\overline{T}^{\,m}, \quad m \in \boldsymbol{M}$.

The different subcases will be defined by putting conditions on $n(m)$ and on $(m, 1)$.

Subcase 2a. $n(m) = 1$.

Observe that $m-1$ and $m+1$ are units since

$$m^2 \equiv 0 \quad mod\ N \quad \Leftrightarrow \quad (m-1)\,(m+1) \equiv -1 \quad mod\ N.$$

So $(m-1)^* = m+1$.

Putting $k = m+1$, one recognizes the same conditions as in Subcase 1d. In fact, using Assertion *5* in Lemma 5 one gets

$$\tau\left(\overline{S}\,\overline{T}^{\,m}\,(\overline{S}\,\overline{T})^3\,(\overline{S}\,\overline{T}^{\,m})^{-1}\right) = \overline{V}_m\,\overline{V}_{m+1},$$

which is a cyclic permutation of $\overline{R}_6$.

Subcase 2b. $n(m) > 1, \quad$ and $(m, 1) \sim k$.

Under the first hypothesis, the last condition is equivalent to $m-1 \in \boldsymbol{P}$. This follows because

$$(k+1)\,(m-1) \equiv -1 \quad mod\ N \ \Leftrightarrow\ k\,(1-m) \equiv m \quad mod\ N.$$

Observe also that $(k+1) = (m-1)^*$. Furthermore, putting $t = k+1$, one has that $t \in \boldsymbol{P}$ and $t_1 = m$, which is the situation of Subcase 1b.

Using these remarks and Assertion *5* and *12* in Lemma 5, calculation yields

$$\overline{V}_{m,\,1}\,\overline{V}_{k+1}.$$

Renaming and applying a cyclic permutation, this relator is $\overline{R}_7$.

Subcase 2c. $n(m) > 1, \quad (m, 1) \sim (m', j'), \quad j' = n(m') - 1$.

In this case it turns out that

$$m' = m - 1,$$

so $(m, 1) \sim (m-1, n-1), \quad n = n(m-1)$. To prove this, let $n(m')$ be n'. One has that

$$(1-m)\,(1-m'\,(n'-1)) \equiv -m\,m' \quad mod\ N$$

if and only if

$$(m-1)\,m'\,n' + m' \equiv m-1 \quad mod\ N. \tag{3.3}$$

Multiplying by m', one gets

$$(m')^2 \equiv m'\,(m-1) \quad mod\ N.$$

Finally, replacing the last expression in (3.3), one obtains $m' = m-1$.

An example of this situation is given by $N = 3^2 \cdot 2^4 \cdot 5^2 = 3600,\ d_1 = 15,\ d_2 = 16$. One may take $15, 16 \in M$, so $n(15) = 16$, and we have

$$(1-16)\,(1-15^2) \equiv -16 \cdot 15 \quad mod\ 3600.$$

Using the remark above and Assertion *13* in Lemma 5, one gets a new relator

$$\tau\left(\overline{S}\,\overline{T}^{\,m}(\overline{S}\,\overline{T})^3\,(\overline{S}\,\overline{T}^{\,m})^{-1}\right) = \overline{V}_{\,m,\,1}\,\overline{V}_{m-1} = \overline{R}_{10}.$$

Subcase 2d. $n(m) > 1, \quad (m, 1) \sim (m', j'), \quad j' < n(m') - 1$.

It turns out that these hypotheses hold if and only if

$$m-1 \in \boldsymbol{K}, \quad (m-1) \sim (m',\, j'+1).$$

This follows because

$$\begin{aligned} -m\,m' &\equiv m\,m'\,j' - m + 1 - m'\,j' \mod N \\ &\Leftrightarrow -m\,m'\,(j'+1) + m - 1 + m'\,(j'+1) \equiv m' \mod N \\ &\Leftrightarrow (m-1)\,(1 - m'\,(j'+1)) \equiv m' \mod N. \end{aligned}$$

Using this remark, one has

$$\overline{\overline{S}\,\overline{T}^{\,m}\overline{S}\,\overline{T}\,\overline{S}} = \overline{\overline{S}\,\overline{T}^{\,m-1}\,\overline{S}\,\overline{T}^{\,-1}} = \overline{\overline{S}\,\overline{T}^{\,m'}\,\overline{S}\,\overline{T}^{\,j'}}.$$

Thus

$$\tau\left(\overline{S}\,\overline{T}^{\,m}(\overline{S}\,\overline{T})^3\,(\overline{S}\,\overline{T}^{\,m})^{-1}\right) = \overline{V}_{m,\,1}\,\overline{V}_{m',\,j'+1},$$

a new relator that we denote by $\overline{R}_{11}$.

This finishes Case 2. Observe that the condition $m-1 \in \boldsymbol{M}$ defines Subcase 2c. Moreover, under these hypotheses, one has that $(m,\,1) \sim (m-1,\,n-1)$. Similar results hold for $m-1 \in \boldsymbol{K}$ (Subcase 2d) and $m-1 \in \boldsymbol{P}$ (Subcases 2a and 2b).

Case 3. $\overline{V} = \overline{S}\,\overline{T}^{\,k}, \quad k \in \boldsymbol{K}$.

One has that $k \sim (m,\,j)$. Either $j = n(m)-1$, or $j < n(m)-1$. In the latter case, one gives conditions on $(m,\,j+1)$ to get the different subcases. Once all subcases are discussed, it will be clear that they only depend on $k-1$ being in $\boldsymbol{P}, \boldsymbol{K}$, or $\boldsymbol{M}$.

Subcase 3a. $k \sim (m,\,n-1)$.

In this subcase it turns out that

$$k - 1 = (m+1)^*.$$

This follows because by hypothesis one has that

$$k - m - k\,m\,n + k\,m \equiv 0 \mod N \tag{3.4}$$

and multiplying by m

$$m\,k - m^2 + k\,m^2 \equiv 0 \mod N.$$

Replacing this last expression in (3.4), one gets

$$k - m + k\,m \equiv 0 \mod N.$$

Thus

$$(k-1)\,(m+1) \equiv -1 \mod N.$$

Observe that this is exactly the same situation as in Subcase 1c. Moreover, using the above remark, Lemma 5 and the identity

$$\overline{\overline{S}\,\overline{T}^{\,k}\,\overline{S}\,\overline{T}\,\overline{S}} = \overline{\overline{S}\,\overline{T}^{\,k-1}\,\overline{S}\,\overline{T}^{\,-1}} = \overline{S}\,\overline{T}^{\,(k-1)^*-1},$$

one gets

$$\tau\left(\overline{S}\,\overline{T}^{\,k}(\overline{S}\,\overline{T})^3\,(\overline{S}\,\overline{T}^{\,k})^{-1}\right) = \overline{V}_k\,\overline{V}_m\,\overline{V}_{(k-1)^*},$$

which is a cyclic permutation of $\overline{R}_9$.

Subcase 3b. $j \,<\, n(m)-1, \qquad (1-m\,(j+1),\, N) \,=\, 1.$

The assumption on $(m,\, j+1)$ implies the existence of a number $k' \in \boldsymbol{K}$, for which $(m,\, j+1) \,\sim\, k'$. In fact, these hypotheses imply that

$$(k-1)^* \,=\, k'+1.$$

To prove this, write $a = (1-m\,j)$. By hypothesis one has

$$k\,a \,\equiv\, m \mod N \tag{3.5}$$

and

$$k'\,a - k'\,m \,\equiv\, m \mod N.$$

Replacing (3.5) in this last expression, one gets

$$k'\,a - k\,k'\,a \,\equiv\, k\,a \mod N.$$

Thus

$$k' - k\,k' \,\equiv\, k \mod N$$

and

$$(k'+1)\,(k-1) \,\equiv\, -1 \mod N.$$

Writing $t = k'+1$, one has $t_1 = k$, which is the situation in Subcase 1e. As in that subcase, the usual techniques yield

$$\tau\left(\overline{S}\,\overline{T}^{\,k}(\overline{S}\,\overline{T})^3\,(\overline{S}\,\overline{T}^{\,k})^{-1}\right) \,=\, \overline{V}_k\,\overline{V}_{m,\,j+1}\,\overline{V}_{k'+1},$$

a cyclic permutation of $\overline{R}_8$.

Subcase 3c. $j \,<\, n(m)-1, \quad (1-m\,(j+1),\; N) \,>\, 1, \quad (m,\, j+1) \,\sim\, (m',\, j'),$ $m' \,\neq\, k-1.$

Under these conditions, one has that

$$k-1 \,\sim\, (m',\, j'+1).$$

To check this, write $a = 1-m\,j$ and $b = 1-m'\,j'$, by hypothesis

$$b\,a - b\,m \,\equiv\, -m\,m' \mod N.$$

Replacing (3.5) in this expression, one obtains

$$b\,a - k\,a\,b \,\equiv\, -k\,a\,m' \mod N.$$

Therefore

$$b - k\,b \,\equiv\, -k\,m' \mod N$$

and

$$k-1 \,\sim\, (m',\, j'+1).$$

Using this data, one gets a new relator

$$\tau\left(\overline{S}\,\overline{T}^{\,k}(\overline{S}\,\overline{T})^3\,(\overline{S}\,\overline{T}^{\,k})^{-1}\right) \,=\, \overline{V}_k\,\overline{V}_{m,\,j+1}\,\overline{V}_{m',\,j'+1} \,=\, \overline{R}_{12}.$$

Subcase 3d. $j \,<\, n(m)-1, \quad (1-m\,(j+1),\, N) \,>\, 1, \quad (m,\, j+1) \,\sim\, (m',\, j'),$ $m' \,=\, k-1.$

These hypotheses imply that

$$j' \;=\; n(m') - 1.$$

To prove this, write $n = n(k-1)$. So

$$-j\,m\,n\,(k-1)^2 + n\,(k-1)^2 \;\equiv\; 0 \quad mod\ N.$$

Thus

$$j\,m\,n\,(k-1) + (k - k\,m\,j)\,n\,(k-1) - n\,(k-1) \;\equiv\; 0 \quad mod\ N.$$

Using

$$k - j\,m\,k \;\equiv\; m \quad mod\ N,$$

the above expression becomes

$$j\,m\,n\,(k-1) + m\,n\,(k-1) - n\,(k-1) \;\equiv\; 0 \quad mod\ N,$$

which one may rewrite as

$$j\,m\,n\,(k-1) - j\,m\,k + m\,n\,(k-1) - m\,k - n\,(k-1) + k \;\equiv\; -m\,k + m \quad mod\ N.$$

Finally, since this last congruence is the same as

$$(j\,m + m - 1)\;(n\,(k-1) - k) \;\equiv\; -m\,(k-1) \quad mod\ N,$$

one has

$$(m,\, j+1) \;\sim\; (k-1,\, n-1).$$

Using this result one gets

$$\tau\left(\overline{S}\,\overline{T}^{\,k}(\overline{S}\,\overline{T})^3\,(\overline{S}\,\overline{T}^{\,k})^{-1}\right) \;=\; \overline{V}_k\,\overline{V}_{m,\,j+1}\,\overline{V}_{k-1},$$

a new relator that we denote by $\overline{R}_{13}$.

Observe that the study of Case 3 provides information on the numbers preceding k. For instance, if $k-1 \in \boldsymbol{K}$, one necessarily has that

$$(k-1) \;\sim\; (m',\, j'+1),$$

where $k \;\sim\; (m,\, j)$ and $(m,\, j) \;\sim\; (m',\, j')$.

Case 4. $\overline{V} \;=\; \overline{S}\,\overline{T}^{\,m}\,\overline{S}, \quad m \in \boldsymbol{M}$.

We consider subcases accordingly with $m+1$ being in $\boldsymbol{P}$, $\boldsymbol{M}$, or $\boldsymbol{K}$.

Subcase 4a. $n(m) = 1$.

This situation was studied in Subcases 1d and 2a. Thus

$$(m-1)\,(m+1) \equiv -1 \quad mod\ N.$$

As in those subcases, one gets relator R_6,

$$\tau\left(\overline{S}\,\overline{T}^{m}\,\overline{S}\,(\overline{S}\,\overline{T})^3\,(\overline{S}\,\overline{T}^{m}\,\overline{S})^{-1}\right) \;=\; \overline{V}_{m+1}\,\overline{V}_m.$$

Subcase 4b. $n(m) > 1, \quad m+1 \in \boldsymbol{P}$.

Putting $t = m+1$, one gets the same situation as in Subcase 1c. Moreover, calculation yields

$$\tau\left(\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,(\overline{S}\,\overline{T})^3\,(\overline{S}\,\overline{T}^{\,m}\,\overline{S})^{-1}\right) \;=\; \overline{V}_t\,\overline{V}_{t_1}\,\overline{V}_{t-1} \;=\; \overline{R}_9,$$

the relator obtained in that subcase.

Subcase 4c. $n(m) > 1, \quad m+1 \in \boldsymbol{M}$.

The hypothesis are those of Subcase 2c, also the rewriting is

$$\tau\left(\overline{S}\,\overline{T}^{m}\,\overline{S}\,(\overline{S}\,\overline{T})^{3}\,(\overline{S}\,\overline{T}^{m}\,\overline{S})^{-1}\right) \;=\; \overline{V}_{m+1,\,1}\,\overline{V}_{m} \;=\; \overline{R}_{10}.$$

Subcase 4d. $n(m) > 1, \quad m+1 \in \boldsymbol{K}$.

Since $m+1 \in \boldsymbol{K}$ and $m \in \boldsymbol{M}$, the hypothesis of Subcase 3d must be accomplished. Thus, $m+1 \;\sim\; (m',\, j')$ and $(m',\, j'+1) \;\sim\; (m,\, n(m)-1)$. As in that case, one gets

$$\tau\left(\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,(\overline{S}\,\overline{T})^{3}\,(\overline{S}\,\overline{T}^{\,m}\,\overline{S})^{-1}\right) \;=\; \overline{V}_{m+1}\,\overline{V}_{m',\,j'+1}\,\overline{V}_{m} \;=\; \overline{R}_{13}.$$

Case 5. $\overline{V} \;=\; \overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}$.

One considers three subcases depending on $(m,\,1)$, as it was done in Case 2. If $(m,\,1) \;\sim\; k$, calculation yields a cyclic permutation of $\overline{R}_7$. For the case $(m,\,1) \;\sim\; (m', j')$, $j' < n(m') - 1$, one gets $\overline{R}_{11}$. If $j' = n(m') - 1$, the rewriting is relator $\overline{R}_{10}$.

Case 6. $\overline{V} \;=\; \overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,j}, \quad j \;>\; 1, \quad (m,\,j) \;\sim\; k$.

One considers subcases accordingly with $k+1$ being an element in $\boldsymbol{M}$, $\boldsymbol{P}$ or $\boldsymbol{K}$. It comes out that these hypotheses establish the situations of Subcases 2d, 1e and 3c, respectively. Furthermore, up to a cyclic permutation, the rewriting process yields relators $\overline{R}_{11}$, $\overline{R}_8$ and $\overline{R}_{12}$, as in those subcases.

We consider the last case that will finish the proof of Theorem 1.

Case 7. $\overline{V} \;=\; \overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,j}, \quad j \;>\; 1, \quad (m,\,j) \sim (m',\,j')$.

We take subcases putting conditions on $(m',\,j')$.

Subcase 7a. $j' \;=\; n(m') - 1$.

We claim that under this hypothesis, one has that

$$(m,\,j-1) \;\sim\; m'+1.$$

To prove the claim, let a denote $1 - m\,(j-1)$ and write n' for $n(m')$. By hypothesis

$$(a-m)\,(m'+1-m'\,n') \;\equiv\; -m\,m' \quad mod\ N,$$

hence

$$a\,(1+m') - a\,m'\,n' + m\,m'\,n' \;\equiv\; m \quad mod\ N. \tag{3.6}$$

Multiplying this last congruence by m', one obtains

$$a\,m'\,(1+m') \;\equiv\; m\,m' \quad mod\ N.$$

Finally, replacing this congruence in (3.6) one gets

$$a\,(1+m') \;\equiv\; m \quad mod\ N.$$

Observe that these are the same hypotheses as in Subcase 3d. Moreover, calculation yields

$$\tau\left(\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,j}(\overline{S}\,\overline{T})^{3}\,(\overline{S}\,\overline{T}^{\,m}\,\overline{S}\,\overline{T}^{\,j})^{-1}\right) \;=\; \overline{V}_{m,\,j}\,\overline{V}_{m'}\,\overline{V}_{m'+1},$$

a cyclic permutation of $\overline{R}_{13}$, the relator obtained in that subcase.

Subcase 7b. $j' < n(m') - 1, \quad (m', j'+1) \sim k.$

We claim that under these conditions one has that

$$k+1 \sim (m, j-1).$$

To prove this, one applies a similar argument to the one in Subcase 3c. Using the claim, one gets a cyclic permutation of $\overline{R}_{12}$,

$$\tau\left(\overline{S}\,\overline{T}^{m}\,\overline{S}\,\overline{T}^{j}(\overline{S}\,\overline{T})^{3}\,(\overline{S}\,\overline{T}^{m}\,\overline{S}\,\overline{T}^{j})^{-1}\right) = \overline{V}_{m,j}\,\overline{V}_{m',j'+1}\,\overline{V}_{k+1}.$$

Subcase 7c. $j' < n(m') - 1, \quad (m, j) \sim (m', j'), \quad (m', j'+1) \sim (m'', j'').$

To treat this case, we need the following lemma.

Lemma 7. *Under the hypothesis of Subcase 7c, one has that*

$$(m'', j''+1) \sim (m, j-1).$$

Proof. We denote $a = 1 - m\,j$, $b = 1 - m'\,j'$ and $c = 1 - m''\,j''$. By hypothesis

$$a\,b \equiv -m\,m' \mod N \tag{3.7}$$

and

$$(b - m')\,c \equiv -m'\,m'' \mod N. \tag{3.8}$$

It follows from (3.8) that

$$a\,b\,c - a\,m'\,c + m'\,m''\,a \equiv 0 \mod N,$$

using (3.7), this last congruence may be written as

$$m'\,(m''\,a - a\,c - m\,c) \equiv 0 \mod N. \tag{3.9}$$

Applying a similar argument and multiplying the congruence (3.8) by m, one gets

$$-b\,(m''\,a - a\,c - m\,c) \equiv 0 \mod N. \tag{3.10}$$

Now, since $(m', b) = 1$, it follows from the congruences (3.9) and (3.10) that $m''\,a - a\,c - m\,c \equiv 0 \mod N$. Thus

$$(a+m)\,(c - m'') \equiv -m\,m'' \mod N. \tag{3.11}$$

We still have to prove that $j'' < n(m'') - 1$. Let $n'' = n(m'')$, if $j''+1 = n''$, the congruence (3.11) may be rewritten as

$$(1 - m''\,n'')\,(a+m) \equiv -mm'' \mod N.$$

Multiplying this last congruence by m'', one gets

$$m''\,(a+m) + (m'')^2\,m \equiv 0 \mod N.$$

Finally, it follows from this last congruence that if t is a common proper divisor of m and N, one has that t is also a factor of m''. However, this assumption contradicts (3.11). □

Using the lemma, it is not difficult to calculate

$$\tau\left(\overline{S}\,\overline{T}^{m}\,\overline{S}\,\overline{T}^{j}(\overline{S}\,\overline{T})^{3}\,(\overline{S}\,\overline{T}^{m}\,\overline{S}\,\overline{T}^{j})^{-1}\right) = \overline{V}_{m,j}\,\overline{V}_{m',j'+1}\,\overline{V}_{m'',j''+1},$$

our last relator, which we denote by $\overline{R}_{14}$. This finishes the proof of Theorem 1.

The presentation in Theorem 1 is huge, however it may be substantially simplified. The next step is to eliminate most of the generators and relators, and one gets a fairly simple presentation (Theorem 3).

Proposition 4. *In the case of no torsion, all generators in relators $\overline{R_4}$ to $\overline{R}_{14}$ appear exactly once.*

Proof. One checks that each group of generators has this property. Certainly, each of the generators of type $\overline{V}_k,\ k \in \boldsymbol{P}$, appears in relators $\overline{R}_4$ to $\overline{R}_9$. They do so once, because of the exclusive conditions of Case 0 and the subcases of Case 1.

Each generator of type $V_m,\ m \in \boldsymbol{M}$, also appears exactly once in $\overline{R}_6,\ \overline{R}_9,\ \overline{R}_{10}$ and $\overline{R}_{13}$. If $n(m) = 1$, it only appears in $\overline{R}_6$. Otherwise, it appears in $\overline{R}_9, \overline{R}_{10}$ and $\overline{R}_{13}$, in accordance with $m+1$ being in $\boldsymbol{P},\ \boldsymbol{M}$ or $\boldsymbol{K}$.

It follows immediately from Case 3 that all generators $\overline{V}_k,\ k \in \boldsymbol{K}$, appear exactly once in $\overline{R}_8,\ \overline{R}_9,\ \overline{R}_{12}$ and $\overline{R}_{13}$. From Case 5, the result also follows for generators of type $V_{m,1}$, they appear once in $\overline{R}_7,\ \overline{R}_{10}$ and $\overline{R}_{11}$.

Using the cyclic and dual nature of the numbers defining the relators, one may also check without difficulty that Cases 6 and 7 yield all possible and distinct appearances of all generators of type $\overline{V}_{m,j},\quad j > 1$. They appear exactly once in relators $\overline{R}_8,\ \overline{R}_{11},\ \overline{R}_{12},\ \overline{R}_{13}$ and $\overline{R}_{14}$. □

We observe that in relator $\overline{R}_5$, either the three generators are equal, or the three are distinct. This follows because $k = k_1$ if and only if $(k-1)^* = k$.

Proceeding with the elimination, we will get in the case of no torsion a free group of rank

$$\frac{\mu\ +\ 6}{6},$$

where μ is the index of $\overline{\Gamma}_0(N)$ in $\overline{\Gamma}$ (Theorem 2).

Lemma 8. *In the no torsion case one may eliminate*

$$\frac{|\overline{\boldsymbol{G}}|\ -\ (|\boldsymbol{M}|+2)}{2}$$

generators with relators $\overline{R}_1,\ \overline{R}_2,\ \overline{R}_3$ and

$$\frac{|\overline{\boldsymbol{G}}|+|\boldsymbol{M}|}{3}$$

generators with relators $\overline{R}_4, \overline{R}_5, \ldots, \overline{R}_{14}$.

Proof. In $\overline{R}_1$, one may eliminate $\overline{V}_k$, where $k < k^*$. The generators of the form $\overline{V}_k,\quad k \in \boldsymbol{K}$, might be withdrawn, using the relator $\overline{R}_2$. Also in $\overline{R}_3$, one may discard the generators $\overline{V}_{m,j}$, where $j < j'$, or $j = j'$ and $m < m'$. Thus, using the first three relators, one may eliminate

$$\frac{|\overline{\boldsymbol{G}}|\ -\ (|\boldsymbol{M}|+2)}{2}$$

generators. This follows because $\overline{T},\ \overline{U}$ and the elements $\overline{V}_m,\ m \in \boldsymbol{M}$, are not paired to other generators.

The elimination may be continued in a systematic way. Generator $\overline{U}$ might be withdrawn using $\overline{R}_4$. With relator $\overline{R}_5$, one discards $\overline{V}_k,\ k > k^*$ (certainly one of the factors has this property). The next step is the use of relators $\overline{R}_7,\ \overline{R}_8,\ \overline{R}_{11}$ and $\overline{R}_{12}$, to eliminate all generators of type $\overline{V}_{m,j},\ (m,\, j) \sim k$.

Also, one may withdraw all generators of type $\overline{V}_m,\ m \in \boldsymbol{M}$, with relators $\overline{R}_6,\ \overline{R}_9,\ \overline{R}_{10}$ and $\overline{R}_{13}$. Finally, with $\overline{R}_{14}$ one may eliminate some generators of

type $\overline{V}_{m,j}$, $(m,j) \sim (m',j')$, for which $j > j'$. This is possible because one of the factors has this property.

The result now follows from Proposition 4 and the fact that those relators which have two factors instead of three are exactly $|\boldsymbol{M}|$, namely $\overline{R}_6$, $\overline{R}_7$, $\overline{R}_{10}$ and $\overline{R}_{11}$ (see Case 2). □

In the torsion cases it turns out that each elliptic conjugacy class of subgroups of order two is in a one-to-one correspondence with solutions in $\mathbb{Z}_n$ to the congruence

$$t^2 \equiv -1 \mod N,$$

and those of order 3 with

$$t(t+1) \equiv -1 \mod N$$

(see [5], p. 8 and p. 10).

It is now clear from Theorem 1 that all elliptic conjugacy classes of subgroups of order two are represented by the relators

$$\overline{R}_1 = (\overline{V}_k)^2, \quad k^2 \equiv -1 \mod N,$$

and those of order three by the relators

$$\overline{R}_5 = (\overline{V}_k)^3, \quad k(k-1) \equiv -1 \mod N.$$

One denotes the number of these elliptic classes by ν_2 and ν_3, respectively. These numbers are well known.

Given $N = 2^r p_1^{r_1} \cdots p_m^{r_m}$, $r = 0,1$, $p_j \equiv 1 \mod 4$, $j \in \{1,2,\ldots,m\}$, the number of conjugacy classes of elliptic subgroups of order 2 in $\overline{\Gamma}_0(N)$ is 2^m. For other numbers with a different prime decomposition, $\overline{\Gamma}_0(N)$ does not have elements of order 2. A similar result holds for classes of order 3: $\overline{\Gamma}_0(N)$ has 2^m classes provided $N = 3^r p_1^{r_1} \cdots p_m^{r_m}$, $r = 0,1$, $p_j \equiv 3 \mod N$, $j \in \{1,2,\ldots,m\}$, otherwise it has none (cf. [10] or [11]).

Hence, it follows from Lemma 8 that in all cases one may eliminate

$$\frac{1}{2}\left(|\overline{\boldsymbol{G}}| - (|\boldsymbol{M}|+2) - \nu_2\right)$$

generators using relators $\overline{R}_1$, $\overline{R}_2$, $\overline{R}_3$, and

$$\frac{1}{3}\left(|\overline{\boldsymbol{G}}| + |\boldsymbol{M}| - \nu_3\right)$$

generators using relators $\overline{R}_4$ to $\overline{R}_{14}$.

Putting together this information, we get the next result.

Theorem 2. *The group $\overline{\Gamma}_0(N)$ is generated by a subset $\overline{\boldsymbol{G}}_0$ of $\overline{\boldsymbol{G}}$ of cardinality*

$$\frac{1}{6}(\mu + 6 + 3\nu_2 + 2\nu_3).$$

There are ν_2 relators of the form $(\overline{V}_k)^2$ and ν_3 of the form $(\overline{V}_k)^3$. Furthermore, there are no other relators among the generators of $\overline{\boldsymbol{G}}_0$.

Proof. First observe that

$$|\overline{\boldsymbol{G}}| + |\boldsymbol{M}| = \mu.$$

This is clear from the association:

$\overline{T} \to \overline{I}$, $\overline{U} \to \overline{S}$, $\overline{V}_k \to \overline{S}\,\overline{T}^k$, $k \geq 1$, $\overline{V}_{m,j} \to \overline{S}\,\overline{T}^m\,\overline{S}\,\overline{T}^j$ and $m \to \overline{S}\,\overline{T}^m\,\overline{S}$, where $m \in \boldsymbol{M}$.

Thus, it follows from Lemma 8 and the remarks before the theorem that the number of generators left after the elimination is given by

$$|\overline{\boldsymbol{G}}| - \frac{1}{2}\left(|\overline{\boldsymbol{G}}| - (|\boldsymbol{M}|+2) - \nu_2\right) - \frac{1}{3}\left(|\overline{\boldsymbol{G}}| + |\boldsymbol{M}| - \nu_3\right) = \frac{\mu + 6 + 3\nu_2 + 2\nu_3}{6}.$$

We still have to prove that we may delete all relators except those in $\overline{R}_1$ and $\overline{R}_5$ that define elliptic elements.

Using Tietze's fourth movement (see [8], p. 50), one may delete generators and relators in the following order:

(1) all generators $\overline{V}_k$ and all relators $\overline{R}_1$, where $k \in \boldsymbol{P}$, $k < k^*$;
(2) all generators $\overline{V}_k$ and all relators $\overline{R}_2$, where $k \in \boldsymbol{K}$;
(3) all generators $\overline{V}_{m,\,j}$, where $(m,\,j) \sim (m',\,j')$ and $j < j'$, or $j = j'$ and $m < m'$, together with all relators $\overline{R}_3$;
(4) generator $\overline{U}$ and relator $\overline{R}_4$;
(5) some generators $\overline{V}_k$, where $k > k^*$, and all relators $\overline{R}_5$ which are not of the form $(\overline{V}_k)^3$;
(6) all generators V_m, where $m \in \boldsymbol{M}$, and all relators $\overline{R}_6$, $\overline{R}_9$, $\overline{R}_{10}$ and $\overline{R}_{13}$;
(7) all generators $\overline{V}_{m,\,j}$, where $(m,\,j) \sim k$, and all relators $\overline{R}_7$, $\overline{R}_8$, $\overline{R}_{11}$ and $\overline{R}_{12}$.
(8) Finally, one may delete some generators $\overline{V}_{m,\,j}$, for which $(m,j) \sim (m',\,j')$ and $j > j'$, together with all relators $\overline{R}_{14}$. □

We remark that the equivalent result in Chuman's article (Proposition 4) is false in the torsion cases. On the other hand, Theorem 2 does not provide a method to get presentations for $\overline{\Gamma}_0(N)$. However, our next and main result yields such an algorithm and it also simplifies, substantially, the presentation in Theorem 1. Observe that the only generators left after the elimination are: $\overline{T}$, some of type $\overline{V}_k$, where $k \in \boldsymbol{P}$, $k > k*$, some of type $\overline{V}_{m,\,j}$, where $(m,j) \sim (m',\,j')$, $j \geq j'$ and those of orders two and three (in the torsion cases).

Theorem 3. *The group $\overline{\Gamma}_0(N)$ may be presented as*

$$\left\{\overline{T},\ \overline{V}_k,\ k \in P,\ \overline{V}_{m,\,j},\ (1 - m\,j,\,N) > 1;\quad \overline{R}_1,\ \overline{R}_3,\ \overline{R}_5,\ \overline{R}_{14}\right\}.$$

Proof. The order of elimination of generators and relators in the proof of Theorem 2 may be altered as follows: one just eliminates the generators and relators in steps (2), (4), (6) and (7). Thus, getting the above presentation. □

This last theorem actually provides a simple method to get presentations for $\overline{\Gamma}_0(N)$. Using Tietze's fourth movement, one deletes all generators $\overline{V}_k$, where $k < k^*$, and all relators $\overline{R}_1$, which are not of the form $(\overline{V}_k)^2$. Then, one withdraws all relators $\overline{R}_3$ and all generators $\overline{V}_{m,\,j}$, where $(m,\,j) \sim (m',\,j')$ and $j < j'$, or $j = j'$ and $m < m'$. The next step is to delete all relators $\overline{R}_5$, which do not define elements of order three, and some of the generators $\overline{V}_k$, where $k > k^*$. Finally, one eliminates all relators $\overline{R}_{14}$ and some generators $\overline{V}_{m,\,j}$, for which $(m,\,j) \sim (m',\,j')$ and $j > j'$. As examples of this method, we give presentations of $\overline{\Gamma}_0(16)$ and $\overline{\Gamma}_0(30)$.

For $\overline{\Gamma}_0(16)$, one may choose $\boldsymbol{M}$ to be $\{2, 4, 8, 12\}$, it is easily checked that there are no generators of the form $\overline{V}_{m,\,j}$, $(1 - m\,j,\,16) > 1$.

Since $3 \cdot 5 \equiv -1 \mod 16$, $7 \cdot 9 \equiv -1 \mod 16$ and $11 \cdot 13 \equiv -1 \mod 16$, $\overline{\Gamma}_0(16)$ is a free group of rank five, which may be presented as

$$\left\{\overline{T},\ \overline{V}_5,\ \overline{V}_9,\ \overline{V}_{13},\ \overline{V}_{15}\right\}.$$

For $\overline{\Gamma}_0(30)$, the set $\boldsymbol{M}$ may be selected to be $\{2,3,5,6,10,15\}$. Observe also that $1 \cdot 29 \equiv -1 \mod 30$, $7 \cdot 17 \equiv -1 \mod 30$, $11 \cdot 19 \equiv -1 \mod 30$ and $13 \cdot 23 \equiv -1 \mod 30$. One also has that $n(2) = 15,\ n(5) = 6,\ n(6) = 5,\ n(10) = 3$, and $n(15) = 2$.

Calculation yields that the pairs $(m,\, j)$, for which $(1 - m\, j,\, 30) > 1$, are $(2.,2), (2,3), (2,5), (2,8), (2,11), (2,13), (2,14), (3,1), (3,2), (3,3), (3,5), (3,7), (3,9), (5,1), (5,2), (5,3), (5,5), (6,1), (10,1)$ and $(15,1)$.

Solving the congruence (3.2) described at the beginning of this section, one gets

$$\begin{aligned}
(2,2) &\sim (3,3),\\
(2,3) &\sim (5,1),\\
(2,5) &\sim (3,9),\\
(2.8) &\sim (15,1),\\
(2,11) &\sim (3,5),\\
(2,13) &\sim (5,3),\\
(2,14) &\sim (3,1),\\
(3,2) &\sim (5,2),\\
(3,7) &\sim (10,1),\\
(5,5) &\sim (6,1).
\end{aligned}$$

In solving these congruences, it is convenient to observe that m' must be different to m and also that $(m\, j - 1,\, N)$ is a factor of m'. This last remark follows because the congruence (3.2) may be expressed as

$$m' \left[\, (m\, j - 1)\, j' + m \,\right] \equiv m\, j - 1 \mod N.$$

The next step is to check which of the relators defined by the above pairs of numbers satisfy the cyclic condition stated in Lemma 7, in reference to relator $\overline{R}_{14}$. One easily checks that there are two relators of type $\overline{R}_{14}$ given by the following sequences of pairs of numbers:

$$\begin{aligned}
(5,3) &\sim (2,13),\\
(2,14) &\sim (3,1),\\
(3,2) &\sim (5,2),
\end{aligned}$$

and

$$\begin{aligned}
(2,3) &\sim (5,1),\\
(5,2) &\sim (3,2),\\
(3,3) &\sim (2,2).
\end{aligned}$$

The corresponding relators are:

$$\overline{V}_{2,\,14}\, \overline{V}_{3,\,2}\, \overline{V}_{5,\,3}, \qquad \overline{V}_{2,\,3}\, \overline{V}_{5,\,2}\, \overline{V}_{3,\,3}.$$

Now we proceed with the elimination, using relator $\overline{R}_1$ one may discard $\overline{V}_1,\ \overline{V}_7,\ \overline{V}_{11},\ \overline{V}_{13}$. Also by relator $\overline{R}_3$ we may remove $\overline{V}_{2,\,2},\ \overline{V}_{5,\,1},\ \overline{V}_{2,\,5},\ \overline{V}_{15,\,1},\ \overline{V}_{3,\,5}, \overline{V}_{5,\,3},\ \overline{V}_{3,\,1},\ \overline{V}_{3,\,2},\ \overline{V}_{10,\,1}$ and $\overline{V}_{6,\,1}$. Finally, with the elimination of $\overline{V}_{2,\,14}$ and $\overline{V}_{2,\,3}$ using $\overline{R}_{14}$, one gets a presentation of $\overline{\Gamma}_0(30)$ as a free group of rank thirteen:

$$\{\overline{T},\ \overline{V}_{17},\ \overline{V}_{19},\ \overline{V}_{23},\ \overline{V}_{29},\ \overline{V}_{2,\,8},\ \overline{V}_{2,\,11},\ \overline{V}_{2,\,13},\ \overline{V}_{3,\,3},\ \overline{V}_{3,\,7},\ \overline{V}_{3,\,9},\ \overline{V}_{5,\,2},\ \overline{V}_{5,\,5}\}.$$

4. A geometric method

Hyperbolic geometry is a useful tool to study modular groups. Particularly, in the construction of fundamental domains for the groups $\overline{\Gamma}_0(N)$, substantial information evolves (see [4], [5] and [6]).

We will discuss only the specific case

$$N \;=\; 2^{k_1}\, p^{k_2},$$

where, $k_1 \in \mathbb{N}$, k_2 is a nonnegative integer and p is a prime number. For these cases, one may exhibit in a simple and direct way a presentation of $\overline{\Gamma}_0(N)$. These presentations are the smallest possible, in the sense that the only relators are those of order two, one for each conjugacy class. As we mentioned before, these groups do not have elements of order three.

This method is derived from the Ford domains. The isometric circle of a transformation $\overline{V}$ in $PSL(2,\mathbb{C})$, which does not fix infinity, is the unique circle where $\overline{V}$ acts as a Euclidean isometry. Namely, this circle is defined by

$$\left\{ z \in \mathbb{C} \;\mid\; |\,\overline{V}^{\,\prime}\,(z)\,| \;=\; 1 \right\}.$$

Thus, if

$$V \;=\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{C}),$$

the isometric circle of $\overline{V}$ is the circle with center at $-\frac{d}{c}$ and radius $\frac{1}{|c|}$. The symbol $I(\overline{V})$ will denote the isometric circle of this transformation. These circles provide a description of the geometry of the transformations. It follows easily from the chain rule that

$$\overline{V}\,\big(\,I(\overline{V}\,)\big) \;=\; I(\,\overline{V}^{-1}\,).$$

Also, one gets

$$\overline{V}\,\big(\,ext\; I(\overline{V})\big) \;=\; int\; I(\overline{V}^{-1}), \qquad \overline{V}\,\big(\,int\; I(\overline{V})\big) \;=\; ext\; I(\overline{V}^{-1}),$$

where $ext\; I(\overline{V})$ denotes the unbounded component in $\mathbb{C} - I(\overline{V})$ and $int\; I(\overline{V})$ the bounded one.

The transformations in $PSL(2,\mathbb{R})$ act as hyperbolic isometries in $\mathbb{H}^2$, and one may think of the isometric circles as a collection of geodesics.

Let R_∞ be the infinite, open rectangle defined by $0, 1$ and ∞ in $\mathbb{H}^2$. Given $\overline{H}$ a discrete subgroup of $PSL(2,\mathbb{R})$, whose group of translations is generated by $z \to z+1$, the Ford polygon for $\overline{H}$ is defined to be set

$$R_\infty \;\cap\; (\bigcap_{\overline{V}}\; ext\; I(\overline{V})\;),$$

where the intersection runs over all transformations $\overline{V} \in \overline{H}$, which are not translations.

These are convex polygons bounded by two vertical lines and a collection of arcs. If $\overline{H}$ is finitely generated, the polygon has a finite number of sides (cf. [1] or [2]). In the particular cases of the groups $\overline{\Gamma}_0(N)$, $N \in \mathbb{N}$, we will denote by F_N these Ford domains.

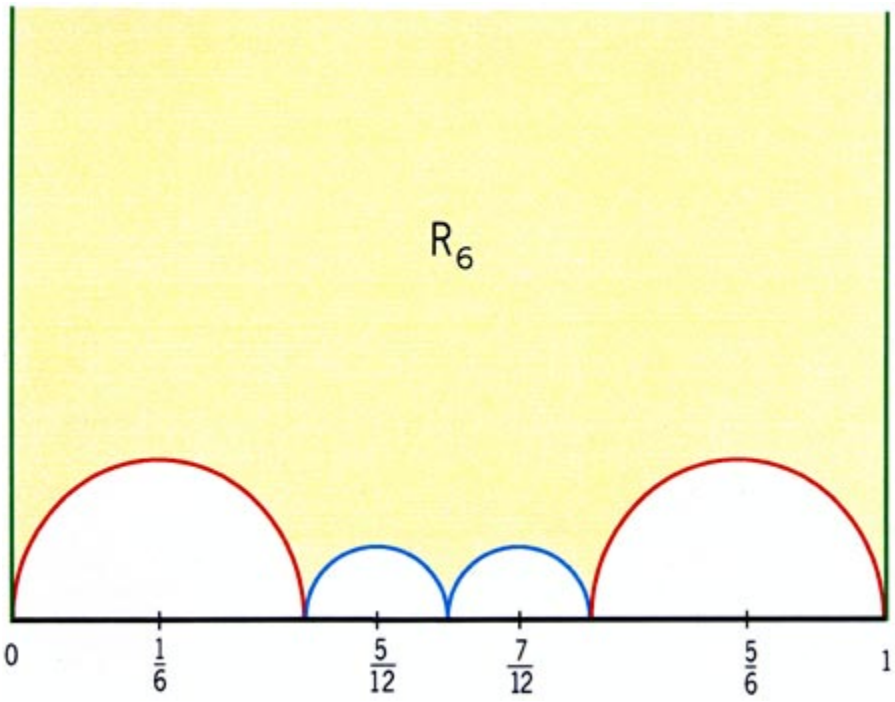

FIGURE 1. The Ford polygon for $\Gamma_0(6)$.

The shape of F_N is described essentially by $F_{\overline{N}}$, where $\overline{N}$ is the square free part of N. Specifically, if $\rho = \frac{N}{\overline{N}}$ and $\overline{B}(z) = \frac{z}{\rho}$, one has that

$$\overline{F}_N = \bigcup_{m=0}^{\rho-1} \overline{B}\,\overline{T}^m\,(\overline{F}_{\overline{N}}),$$

where $\overline{F}_N$ and $\overline{F}_{\overline{N}}$ denote the Euclidean closures of F_N and $F_{\overline{N}}$ in the complex plane, respectively (cf. [5], Theorem 3). See also Figures 1, 2 and 4. On the other hand, elliptic vertices of order 2 in F_N have coordinates

$$\frac{t}{N} + \frac{i}{N}, \qquad t^2 \equiv -1 \quad mod\ N$$

(cf. [5], p. 8). For more information on the Ford domains for $\overline{\Gamma}_0(N)$, we refer to [5] and [6].

Using the properties of isometric circles, one may prove that the Ford polygon $F_{2p},\ p$ a prime number, consists of two vertical lines, together with $p-1$ semicircles of radius $\frac{1}{N}$ and two semicircles of radius $\frac{1}{2N}$, distributed exactly as in Figures 1 and 3 (cf. [6], proof of Corollary 2).

The pairing of sides of F_{2p} consists of translation by one, together with the pairing of sides given by the transformations defined by the matrices

$$A_k = \begin{pmatrix} k^* & * \\ N & -k \end{pmatrix}, \qquad 1 < k \leq k^* < N, \quad (k, N) = 1,$$

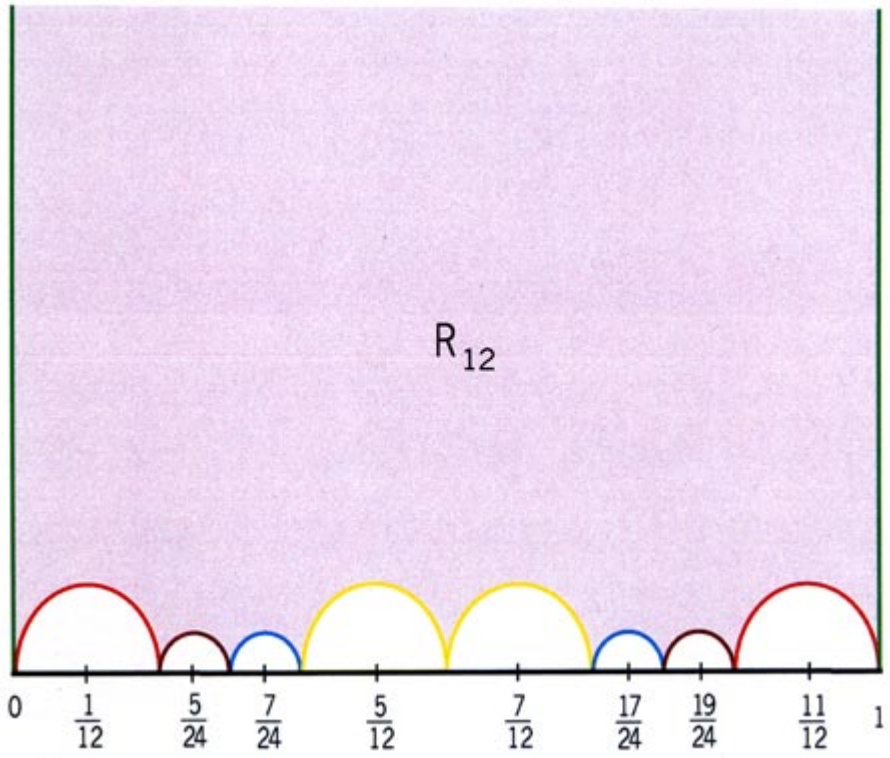

FIGURE 2. The Ford polygon for $\Gamma_0(12)$.

and by the matrix

$$B = \begin{pmatrix} 2p+1 & * \\ 2N & -(2p-1) \end{pmatrix}.$$

This follows again from the geometry of isometric circles. Our next result is now a direct consequence of Poincaré's Theorem (cf. [7], pp. 230–234).

Proposition 5. *The group* $\overline{\Gamma}_0(2p)$ *may be presented as*

$$\left\{\overline{T},\ \overline{A}_k,\ \overline{B};\ \ \overline{A}_e^{\,2}\right\},$$

where $k \leq k^*,\ \ 1 < e < N$ *and* $e^{\,2} \equiv -1 \mod N$.

For example, $\overline{\Gamma}_0(6)$ may be presented as $\{\overline{T},\ \overline{A_1},\ \overline{B}\}$, a free group of rank three (see Figure 1). Also, $\overline{\Gamma}_0(14)$ is presented as a free group of rank five $\{\overline{T},\ \overline{A_1},\ \overline{A_3},\ \overline{A_5},\ \overline{B}\}$ (see Figure 3).

For the general case, we have to apply the result which relates the shape of F_N, to that one of $F_{\overline{N}}$. First, we need to introduce some notation. Let

$$A_{k,\,t} = \begin{pmatrix} (w_{k,\,t})^* & * \\ N & -w_{k,\,t} \end{pmatrix},$$

where $w_{k,\,t} = k + 2\,p\,t,\ \ 1 < k < 2\,p,\ \ (k,\,2\,p) = 1$ and $t \in \mathbb{Z}$.

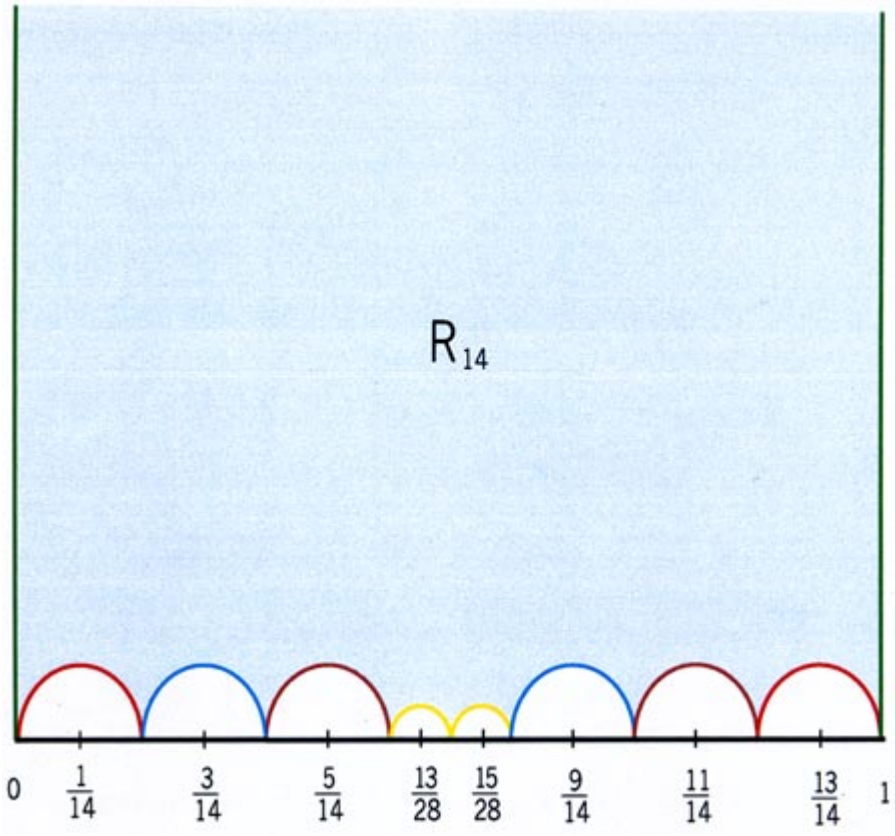

FIGURE 3. The Ford polygon for $\Gamma_0(14)$.

Let also

$$B_{+t} = \begin{pmatrix} (s_{+t})^* & * \\ 2N & -s_{+t} \end{pmatrix}, \quad B_{-t} = \begin{pmatrix} (s_{-t})^* & * \\ 2N & -s_{-t} \end{pmatrix},$$

where $s_{+t} = 2p + 1 + 2pt$, $s_{-t} = 2p - 1 + 2pt$ and $t \in \mathbb{Z}$. Under this notation, one gets the next and last result.

Theorem 4. *Let N be $2^{k_1} p^{k_2}$, where $k_1 \in \mathbb{N}$ and k_2 is a nonnegative integer, then $\overline{\Gamma}_0(N)$ may be presented as*

$$\left\{\overline{T},\ \overline{A}_{k,t},\ \overline{B}_{+t},\ \overline{B}_{-t};\quad \overline{A}_e^{\,2}\right\},$$

where $w_{k,t} \leq (w_{k,t})^*$, $s_{+t} < (s_{+t})^*$, $s_{-t} < (s_{-t})^*$, $0 \leq t < 2^{k_1-1}p^{k_2-1} - 1$ and $e^2 \equiv -1 \mod N$, $1 < e < N$.

This result follows from the previous remarks and the properties of isometric circles. For example, $\overline{\Gamma}_0(12)$ may be presented as $\{\overline{T}, \overline{A}_{1,0}, \overline{A}_{5,0}, \overline{B}_{-0}, \overline{B}_{+0}\}$, a free group of rank five (see Figure 2). The group $\overline{\Gamma}_0(18)$ may be presented as $\{\overline{T}, \overline{A}_{1,0}, \overline{A}_{5,0}, \overline{A}_{5,1}, \overline{B}_{-0}, \overline{B}_{-2}, \overline{B}_{-4}\}$, a free group of rank seven (see Figure 4).

Observe that these new presentations are more easily obtained than those in Theorem 3, since one is only required to calculate the inverses of the units involving

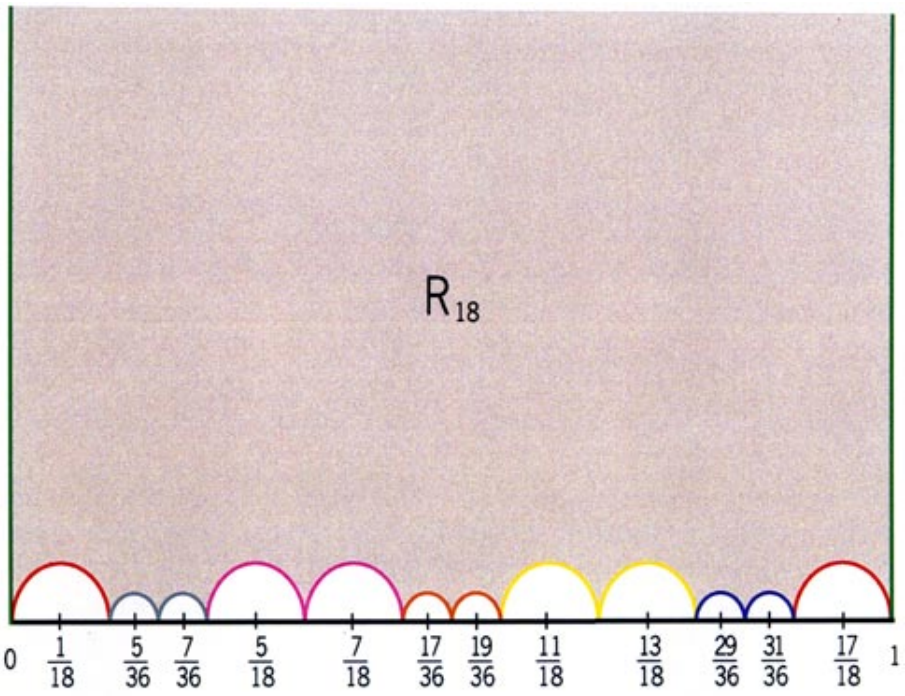

FIGURE 4. The Ford polygon for $\Gamma_0(18)$.

certain isometric circles. For example, the generators of $\overline{\Gamma}_0(12)$ are defined by the following matrices

$$T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad A_{1,0} = \begin{pmatrix} 11 & -1 \\ 12 & -1 \end{pmatrix}, \qquad B_{-0} = \begin{pmatrix} 19 & -4 \\ 24 & -5 \end{pmatrix},$$
$$B_{+0} = \begin{pmatrix} 17 & -5 \\ 24 & -7 \end{pmatrix}, \qquad A_{5,0} = \begin{pmatrix} 7 & -3 \\ 12 & -5 \end{pmatrix}.$$

These matrices are completely determined by the *visible* isometric circles, described in Figure 2 with different colors. The pairing is described by putting the same color to the isometric circle of a transformation and to that one of its inverse.

This method for getting presentations from the Ford domains is not very efficient for numbers with a different prime decomposition to that one in Theorem 4. This happens because in all of these cases the Ford domains contain accidental vertices, and this fact makes the presentation arising from the side pairing very cumbersome (see Figure 3 in [5]).

REFERENCES

[1] A.F. BEARDON, The Geometry of Discrete Groups, Springer-Verlag, 1983. MR **85d:**22026
[2] A.F. BEARDON AND T. JØRGENSEN, *Fundamental Domains for Finitely Generated Kleinian Groups,* Mathematica Scandinavica, **36** (1975), 21–26. MR **52:**8416
[3] Y. CHUMAN, *Generators and Relations for* $\Gamma_0(N)$, J. Math. Kyoto Univ., **13-2** (1973), pp. 381–390. MR **50:**499
[4] R. KULKARNI, *An Arithmetic-Geometric Method in the Study of the Subgroups of the Modular Group,* American Journal of Mathematics, **113** (1991), 1053–1133. MR **92i:**11046

[5] A. Lascurain, *Ford Polygons for* $\Gamma_0(N)$, Boletín de la Sociedad Matemática Mexicana, Vol. **39**, pp. 1-18, 1994. MR **96g:**11038
[6] A. Lascurain, *The Shape of the Ford Domains for* $\Gamma_0(N)$, Conformal Geometry and Dynamics, Vol. **3**, pp. 1-23, 1999. MR **2000a:**11058
[7] J. Lehner, Discontinuous Groups and Automorphic Functions, *Mathematical Surveys, Number VIII,* American Math. Soc., Providence, RI, 1964. MR **29:**1332
[8] W. Magnus, A. Karrass, and D. Solitar, Combinatorial Group Theory, Dover, 1976. MR **54:**10423
[9] H. Radamacher, *Uber die Erzeungenden von Kongruenzuntergruppen der Modulgruppe,* Ham. Abh. **7**, pp.139-148, 1929.
[10] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Tokyo Iwanami Shoten and Princeton University Press, 1971. MR **47:**3318
[11] B. Schoeneberg, Elliptic Modular Functions, Springer-Verlag, 1974. MR **54:**236

Havre 101, Colonia Villa Verdun, Mexico D.F. 01810 Mexico
E-mail address: lasc@hp.fciencias.unam.mx