THE GROUP STRUCTURE OF THE NORMALIZER OF $\Gamma_0(N)$ AFTER ATKIN-LEHNER

FRANCESC BARS

ABSTRACT. We determine the group structure of the normalizer of $\Gamma_0(N)$ in $SL_2(\mathbb{R})$ modulo $\Gamma_0(N)$. These results correct the Atkin-Lehner statement [1, Theorem 8].

1. Introduction

The modular curves $X_0(N)$ contain deep arithmetical information. These curves are the Riemann surfaces obtained by completing with the cusps the upper half plane modulo the modular subgroup

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in SL_2(\mathbb{Z}) | c \in \mathbb{Z}\}.$$

It is clear that the elements in the normalizer of $\Gamma_0(N)$ in $SL_2(\mathbb{R})$ induce automorphisms of $X_0(N)$ and moreover one obtains in that way all automorphisms of $X_0(N)$ for $N \neq 37$ and 63 [3]. This is one reason coming from the modular world that shows the interest in computing the group structure of this normalizer modulo $\Gamma_0(N)$.

Morris Newman obtains a result for this normalizer in terms of matrices [5],[6], see also the work of Atkin-Lehner and Newman [4]. Moreover, Atkin-Lehner state without proof the group structure of this normalizer modulo $\Gamma_0(N)$ [1, Theorem 8]. In this paper we correct this statement and we obtain the right structure of the normalizer modulo $\Gamma_0(N)$. The results are a generalization of some results noticed in [2].

2. The Normalizer of $\Gamma_0(N)$ in $SL_2(\mathbb{R})$

Denote by $\mathrm{Norm}(\Gamma_0(N)$ the normalizer of $\Gamma_0(N)$ in $SL_2(\mathbb{R})$.

Theorem 1 (Newman)**.** *Let $N = \sigma^2 q$ with $\sigma, q \in \mathbb{N}$ and q square-free. Let ϵ be the* gcd *of all integers of the form $a - d$ where a, d are integers such that $\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_0(N)$. Denote by $v := v(N) := \gcd(\sigma, \epsilon)$. Then $M \in \mathrm{Norm}(\Gamma_0(N))$ if and only if M is of the form*

$$\sqrt{\delta} \begin{pmatrix} r\Delta & \frac{u}{v\delta\Delta} \\ \frac{sN}{v\delta\Delta} & l\Delta \end{pmatrix}$$

Date: Revised version: July 16th, 2007.

Work partially supported by MTM2006-11391. MSC: 20H05(19B37,11G18).

After the paper were accepted we learned that a similar result was obtained by M. Akbas and D. Singerman in *The normalizer of* $\Gamma_0(N)$ *in* $PSL(2, \mathbb{R})$ with a different proof. See the postscript.

with $r,u,s,l\in\mathbb{Z}$ *and* $\delta|q$, $\Delta|\frac{\sigma}{v}$. *Moreover* $v=2^{\mu}3^{w}$ *with* $\mu=min(3,[\frac{1}{2}\upsilon_2(N)])$ *and* $w=min(1,[\frac{1}{2}\upsilon_3(N)])$ *where* $\upsilon_{p_i}(N)$ *is the valuation at the prime* p_i *of the integer* N.

This theorem is really proved (and not only stated) by Morris Newman in [5] [6], see also [2, p.12-14].

Observe that if $\gcd(\delta\Delta,6)=1$ we have $\gcd(\delta\Delta^2,\frac{N}{\delta\Delta^2})=1$ because the determinant is one .

3. The group structure of $\mathrm{Norm}(\Gamma_0(N))/\Gamma_0(N)$

In this section we obtain some partial results on the group structure of $\mathrm{Norm}(\Gamma_0(N))$. Let us first introduce some particular elements of $SL_2(\mathbb{R})$.

Definition 1. *Let* N *be fixed. For every divisor* m' *of* N *with* $\gcd(m',N/m')=1$ *the Atkin-Lehner involution* $w_{m'}$ *is defined as follows,*

$$w_{m'}=\frac{1}{\sqrt{m'}}\begin{pmatrix} m'a & b\\ Nc & m'd\end{pmatrix}\in SL_2(\mathbb{R})$$

with $a,b,c,d\in\mathbb{Z}$.

Denote by $S_{v'}=\begin{pmatrix}1 & \frac{1}{v'}\\ 0 & 1\end{pmatrix}$ with $v'\in\mathbb{N}\setminus\{0\}$. Atkin-Lehner claimed in [1] the following:

Claim 2 (Atkin-Lehner)**.** [1, Theorem 8] *The quotient* $\mathrm{Norm}(\Gamma_0(N))/\Gamma_0(N)$ *is the direct product of the following groups:*

(1) $\{w_{q^{\upsilon_q(N)}}\}$ *for every prime* q, $q\geq 5$ $q\mid N$.
(2) (a) *If* $\upsilon_3(N)=0$, $\{1\}$
   (b) *If* $\upsilon_3(N)=1$, $\{w_3\}$
   (c) *If* $\upsilon_3(N)=2$, $\{w_9,S_3\}$*; satisfying* $w_9^2=S_3^3=(w_9S_3)^3=1$ *(factor of order 12)*
   (d) *If* $\upsilon_3(N)\geq 3$*;* $\{w_{3^{\upsilon_3(N)}},S_3\}$*; where* $w^2_{3^{\upsilon_3(N)}}=S_3^3=1$ *and* $w_{3^{\upsilon_3(N)}}S_3w_{3^{\upsilon_3(N)}}$ *commute with* S_3 *(factor group with 18 elements)*
(3) *Let be* $\lambda=\upsilon_2(N)$ *and* $\mu=\min(3,[\frac{\lambda}{2}])$ *and denote by* $v''=2^{\mu}$ *the we have:*
   (a) *If* $\lambda=0$ *;* $\{1\}$
   (b) *If* $\lambda=1$*;* $\{w_2\}$
   (c) *If* $\lambda=2\mu$*;* $\{w_{2^{\upsilon_2(N)}},S_{v''}\}$ *with the relations* $w^2_{2^{\upsilon_2(N)}}=S_{v''}^{v''}=(w_{2^{\upsilon_2(N)}}S_{v''})^3=1$*, where they have orders 6,24, and 96 for* $v=2,4,8$ *respectively. (One needs to warn that for* $v=8$ *the relations do not define totally this factor group).*
   (d) *If* $\lambda>2\mu$*;* $\{w_{2^{\upsilon_2(N)}},S_{v''}\}$*;* $w^2_{2^{\upsilon_2(N)}}=S_{v''}^{v''}=1$*. Moreover,* $S_{v''}$ *commutes with* $w_{2^{\upsilon_2(N)}}S_{v''}w_{2^{\upsilon_2(N)}}$ *(factor group of order* $2{v''}^2$*).*

Let us give some partial results first.

Proposition 3. *Suppose that* $v(N)=1$ *(thus* $4\nmid N$ *and* $9\nmid N$*). Then the Atkin-Lehner involutions generate* $\mathrm{Norm}(\Gamma_0(N)/\Gamma_0(N)$ *and the group structure is*

$$\cong\prod_{i=1}^{\pi(N)}\mathbb{Z}/2\mathbb{Z}$$

where $\pi(N)$ *is the number of prime numbers* $\leq N$.

Proof. This is classically known already in the 1970's. We recall only that $w_{mm'} = w_m w_{m'}$ for $(m, m') = 1$ and easily $w_m w_{m'} = w_{m'} w_m$; the the result follows by a straightforward computation from Theorem 1, see also [2, p.14]. □

When $v(N) > 1$ it is clear that some element $S_{v'}$ appears in the group structure of $\mathrm{Norm}(\Gamma_0(N))/\Gamma_0(N)$ from Theorem 1.

Lemma 4. *If $4|N$ the involution $S_2 \in \mathrm{Norm}(\Gamma_0(N))$ commutes with the Atkin-Lehner involutions w_m with $\gcd(m,2) = 1$ and with the other $S_{v'}$.*

Proof. By the hypothesis the following matrix belongs to $\Gamma_0(N)$

$$w_m S_2 w_m S_2 = \begin{pmatrix} \frac{2mk^2+2Nt+mkNt}{2m} & \frac{(2+2m)(2m+2mk+Nt)}{4m} \\ \frac{Nt(2m+2mk+Nt)}{2m} & m + Nt + \frac{Nt}{m} + \frac{kNt}{2} + \frac{Nt^2}{4m} \end{pmatrix}.$$

□

Proposition 5. *Let $N = 2^{v_2(N)} \prod_i p_i^{n_i}$, with p_i different odd primes and assume that $v_2(N) \leq 3$, $v_3(N) \leq 1$. Then Atkin-Lehner's Claim 2 is true.*

For the proof we need two lemmas.

Lemma 6. *Let $\tilde{u} \in \mathrm{Norm}(\Gamma_0(N))$ and write it as:*

$$\tilde{u} = \frac{1}{\sqrt{\delta\Delta^2}} \begin{pmatrix} \Delta^2\delta r & \frac{u}{2} \\ \frac{sN}{2} & l\Delta^2\delta \end{pmatrix},$$

following the notation of Theorem 1. Then:

$$w_{\Delta^2\delta}\tilde{u} = \begin{pmatrix} r' & \frac{u'}{2} \\ \frac{s'N}{2} & v' \end{pmatrix}, \ if \ \gcd(\delta, 2) = 1,$$

$$w_{\Delta^2\frac{\delta}{2}}\tilde{u} = \frac{1}{\sqrt{2}} \begin{pmatrix} 2r'' & \frac{u''}{2} \\ \frac{s''N}{2} & 2v'' \end{pmatrix}, \ if \ \gcd(\delta, 2) = 2.$$

Proof. This is an easy calculation. □

We study now the different elements of the type

$$a(r', u', s', v') = \begin{pmatrix} r' & \frac{u'}{2} \\ \frac{s'N}{2} & v' \end{pmatrix},$$

$$b(r'', u'', s'', v'') = \frac{1}{\sqrt{2}} \begin{pmatrix} 2r'' & \frac{u''}{2} \\ \frac{s''N}{2} & 2v'' \end{pmatrix}.$$

Observe that $b(,,,)$ only appears when $N \equiv 0 (mod\ 8)$.

Lemma 7. *For $N \equiv 4(mod\ 8)$ all the elements of the normalizer of type $a(r', u', s', v')$ belong to the order six group $\{S_2, w_4 | S_2^2 = w_4^2 = (w_4 S_2)^3 = 1\}$.*

Proof. Straightforward from the equalities:

$$a(r', u', s', v') \in \Gamma_0(N) \Leftrightarrow s' \equiv u' \equiv 0(mod\ 2)$$
$$a(r', u', s', v')S_2 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv \ u' \equiv 1 \ s' \equiv 0(mod\ 2)$$
$$a(r', u', s', v')w_4 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv 0 \ u' \equiv s' \equiv 1(mod\ 2)$$
$$a(r', u', s', v')w_4 S_2 \in \Gamma_0(N) \Leftrightarrow r' \equiv u' \equiv s' \equiv 1 \ v' \equiv 0(mod\ 2)$$

$$a(r',u',s',v')S_2w_4 \in \Gamma_0(N) \Leftrightarrow v' \equiv u' \equiv s' \equiv 1 \ r' \equiv 0 (mod\ 2)$$
$$a(r',u',s',v')S_2w_4S_2 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv s' \equiv 1 \ u' \equiv 0 (mod\ 2)$$

□

Lemma 8. *Let N be a positive integer with $\upsilon_2(N)=3$. Then all the elements of the form $a(r',u',s',v')$ and $b(r'',u'',s'',v'')$ correspond to some element of the following group of 8 elements*

$$\{S_2, w_8 | S_2^2 = w_8^2 = 1, S_2w_8S_2w_8 = w_8S_2w_8S_2\}$$

Proof. If follows from the equalities:

$$a(r',u',s',v') \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv 1, u' \equiv s' \equiv 0 (mod\ 2)$$
$$a(r',u',s',v')S_2 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv u' \equiv 1, s' \equiv 0 (mod\ 2)$$
$$a(r',u',s',v')w_8S_2w_8 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv s' \equiv 1, u' \equiv 0 (mod\ 2)$$
$$a(r',u',s',v')S_2w_8S_2w_8 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv s' \equiv v' \equiv 1 (mod\ 2)$$
$$b(r'',u'',s'',v'')w_8 \in \Gamma_0(N) \Leftrightarrow r'' \equiv v'' \equiv 0, u'' \equiv s'' \equiv 1 (mod\ 2)$$
$$b(r'',u'',s'',v'')S_2w_8S_2 \in \Gamma_0(N) \Leftrightarrow r'' \equiv v'' \equiv u'' \equiv s'' \equiv 1 (mod\ 2)$$
$$b(r'',u'',s'',v'')S_2w_8 \in \Gamma_0(N) \Leftrightarrow r'' \equiv 0, u'' \equiv s'' \equiv v'' \equiv 1 (mod\ 2)$$
$$b(r'',u'',s'',v'')w_8S_2 \in \Gamma_0(N) \Leftrightarrow v'' \equiv 0, u'' \equiv s'' \equiv r'' \equiv 1 (mod\ 2)$$

□

We can now proof Proposition 5].

Proof. [of Proposition 5] Let $N = 2^{\upsilon_2(N)}\prod_i p_i^{n_i}$, with p_i different primes and assume that $9 \nmid N$. If $\upsilon_2(N) \leq 1$ we are done by proposition 3. Suppose $\upsilon_2(N)=2$ and let $\tilde{u} \in \text{Norm}(\Gamma_0(N))$. By lemmas 6 and 7, $w_\delta \tilde{u} = \alpha$, $\alpha \in \{S_2, w_4 | S_2^2 = w_4^2 = (w_4S_2)^3 = 1$ and it follows that $\tilde{u} = w_\delta \alpha$. Since w_δ $((\delta,2)=1)$ commutes with S_2 and the Atkin-Lehner involutions commute one to each other, we are already done. In the situation $8||N$ the proof is exactly the same but using lemmas 6 and 8 instead. □

4. Counterexamples to Claim 2.

In the above section we have seen that Atkin-Lehner's claim is true if $v(N) \leq 2$ i.e. for $v_2(N) \leq 3$ and $v_3(N) \leq 1$. Now we obtain counterexamples when $v_2(N)$ and/or $v_3(N)$ are bigger.

Lemma 9. *Claim 2 for $N=48$ is wrong.*

Proof. We know by Ogg [7] that $X_0(48)$ is an hyperelliptic modular curve with hyperelliptic involution not of Atkin-Lehner type. The hyperelliptic involution always belongs to the center of the automorphism group. We know by [3] that $\text{Aut}(X_0(48)) = \text{Norm}(\Gamma_0(48))/\Gamma_0(N)$. Now if Claim 2 where true this group would be isomorphic to $\mathbb{Z}/2 \times \Pi_4$ where Π_n is the permutation group of n elements. It is clear that the center of this group is $\mathbb{Z}/2 \times \{1\}$, generated by the Atkin-Lehner involution w_3, but this involution is not the hyperelliptic one. □

The problem of $N=48$ is that S_4 does not commute with the Atkin-Lehner involution w_3; thus the direct product decomposition of Claim 2 is not possible.

This problem appears also for powers of 3 one can prove,

Lemma 10. *Let $N = 3^{v_3(N)} \prod_i p_i^{n_i}$ where p_i are different primes of $\mathbb{Q}$. Impose that $S_3 \in \mathrm{Norm}(\Gamma_0(N))$. Then S_3 commutes with $w_{p_i^{n_i}}$ if and only if $p_i^{n_i} \equiv 1(modulo\ 3)$. Therefore if some $p_i^{n_i} \equiv -1(modulo\ 3)$ the Claim 2 is not true.*

Proof. Let us show that S_3 does not commute with $w_{p_i^{n_i}}$ if and only if $p_i^{n_i} \equiv -1(mod\ 3)$. Observe the equality $w_{p_i^{n_i}} = \frac{1}{\sqrt{p_i^{n_i}}} \begin{pmatrix} p_i^{n_i}k & 1 \\ Nt & p_i^{n_i} \end{pmatrix}$:

$$w_{p_i^{n_i}} S_3 w_{p_i^{n_i}} S_3^2 =$$

$$\frac{1}{p_i^{n_i}} \begin{pmatrix} (p_i^{n_i}k)^2 + Nt(1+\frac{p_i^{n_i}k}{3}) & p_i^{n_i}k(\frac{2p_i^{n_i}k}{3}+1) + (\frac{p_i^{n_i}k}{3}+1)(\frac{2Nt}{3}+p_i^{n_i}) \\ Nt(p_i^{n_i}k) + Nt(\frac{Nt}{3}+p_i^{n_i}) & Nt(\frac{2p_i^{n_i}k}{3}+1) + p_i^{n_i}(\frac{Nt}{3}+p_i^{n_i})(\frac{2Nt}{3}+p_i^{n_i}) \end{pmatrix}.$$

For this element to belong to $\Gamma_0(N)$ one needs to impose $\frac{2k^2p_i^{n_i}}{3} + \frac{p_i^{n_i}k}{3} \in \mathbb{Z}$. Since $p_i^{n_i} \equiv 1\ o\ -1(mod\ 3)$ it is needed that $k \equiv 1(mod\ 3)$. Now from $\det(w_{p_i}) = 1$ we obtain that $p_i^{n_i}k \equiv 1(mod\ 3)$; therefore $p_i^{n_i} \equiv 1(mod\ 3)$. □

5. The group structure of $\mathrm{Norm}(\Gamma_0(N))/\Gamma_0(N)$ revisited.

In this section we correct Claim 2. We prove here that the quotient

$$\mathrm{Norm}(\Gamma_0(N))/\Gamma_0(N)$$

is the product of some groups associated every one of them to the primes which divide N. See for the explicit result theorem 16.

Theorem 11. *Any element $w \in \mathrm{Norm}(\Gamma_0(N))$ has an expression of the form*

$$w = w_m\Omega,$$

where w_m is an Atkin-Lehner involution of $\Gamma_0(N)$ with $(m, 6) = 1$ and Ω belongs to the subgroup generated by $S_{v(N)}$ and the Atkin Lehner involutions $w_{2^{v_2(N)}}$, $w_{3^{v_3(N)}}$. Moreover for $\gcd(v(N), 2^3) \leq 2$ the group structure for the subgroup $< S_{v_2(v(N))}, w_{2^{v_2(N)}} >$ and $< S_{v_3(v(N))}, w_{3^{v_3(N)}} >$ of $< S_{v(N)}, w_{2^{v_2(N)}}, w_{3^{v_3(N)}} >$ is the predicted by Atkin-Lehner at Claim 2, but these two subgroups do not necessary commute withe each other element-wise.

Proof. Let us take any element w of the $\mathrm{Norm}(\Gamma_0(N))$. By Theorem 1 we can express w as follows,

$$w = \sqrt{\delta} \begin{pmatrix} r\Delta & \frac{u}{v\delta\Delta} \\ \frac{sN}{v\delta\Delta} & l\Delta \end{pmatrix} = \frac{1}{\Delta\sqrt{\delta}} \begin{pmatrix} r\delta\Delta^2 & \frac{u}{v} \\ \frac{sN}{v} & l\delta\Delta^2 \end{pmatrix}$$

Let us denote by $U = 2^{v_2(N)}3^{v_3(N)}$. Write $\Delta' = \gcd(\Delta, N/U)$ and $\delta' = \gcd(\delta, N/U)$; then we obtain

$$w_{\delta'\Delta'^2} w = \frac{1}{\frac{\Delta}{\Delta'}\sqrt{\delta/\delta'}} \begin{pmatrix} r'\frac{\delta}{\delta'}\frac{\Delta^2}{\Delta'^2} & \frac{u'}{v(N)} \\ \frac{Nt'}{v(N)} & v'\frac{\delta}{\delta'}\frac{\Delta^2}{\Delta'^2} \end{pmatrix}$$

Observe that if $v(N) = 1$ we already finish and we reobtain proposition 3. This is clear if $\gcd(N, 6) = 1$; if not, the matrix $ww_{\delta'\Delta'^2}$ is the Atkin-Lehner involution at $(\frac{\Delta}{\Delta'})^2\frac{\delta}{\delta'} \in \mathbb{N}$.

Now we need only to check that any matrix of the form

$$\Omega = \frac{1}{\frac{\Delta}{\Delta'}\sqrt{\delta/\delta'}}\begin{pmatrix} r'\frac{\delta}{\delta'}(\frac{\Delta}{\Delta'})^2 & \frac{u'}{v(N)} \\ \frac{Nt'}{v(N)} & v'\frac{\delta}{\delta'}(\frac{\Delta}{\Delta'})^2 \end{pmatrix} \tag{1}$$

is generated by $S_{v(N)}$ and the Atkin-Lehner involutions at 2 and 3 which are the factors of $\frac{\delta}{\delta'}(\frac{\Delta}{\Delta'})^2$. To check this observe that $\Omega = \Omega_2\Omega_3$ with

$$\Omega_2 = \frac{1}{2^{v_2(\frac{\Delta}{\Delta'}\sqrt{\delta/\delta'})}}\begin{pmatrix} r''2^{v_2(\frac{\delta}{\delta'}(\frac{\Delta}{\Delta'})^2)} & \frac{u''}{2^{v_2(v(N))}} \\ \frac{Nt''}{2^{v_2(v(N))}} & v''2^{v_2(\frac{\delta}{\delta'}(\frac{\Delta}{\Delta'})^2)} \end{pmatrix} \tag{2}$$

$$\Omega_3 = \frac{1}{3^{v_3(\frac{\Delta}{\Delta'}\sqrt{\delta/\delta'})}}\begin{pmatrix} r'''3^{v_3(\frac{\delta}{\delta'}(\frac{\Delta}{\Delta'})^2)} & \frac{u'''}{3^{v_3(v(N))}} \\ \frac{Nt'''}{3^{v_3(v(N))}} & v'''3^{v_3(\frac{\delta}{\delta'}(\frac{\Delta}{\Delta'})^2)} \end{pmatrix}.$$

We only consider the case for Ω_2, the case for the Ω_3 is similar. We can assume that $2^{v_2(\frac{\Delta}{\Delta'}\sqrt{\delta/\delta'})} = 1$ substituting Ω_2 by $w_{2^{v_2(N)}}\Omega_2$ if necessary. Thus, we are reduced to a matrix of the form $\tilde{\Omega_2} = \begin{pmatrix} r' & \frac{u'}{2^{v_2(v(N))}} \\ \frac{Nt'}{2^{v_2(v(N))}} & v' \end{pmatrix}$. Now for some i we can obtain $S^i_{2^{v_2(v(N))}}\tilde{\Omega_2} = \begin{pmatrix} r' & u' \\ \frac{Nt'}{2^{v_2(v(N))}} & v' \end{pmatrix}$; name this matrix by $\overline{\Omega_2}$. Then, it is easy to check that $w_{2^{v_2(N)}}S^i_{2^{v_2(v(N))}}w_{2^{v_2(N)}}\overline{\Omega_2} \in \Gamma_0(N)$ for some i.

Similar argument as above are obtained if we multiply w by w_m on the right, i.e. ww_m is also some Ω as above obtaining similar conclusion.

Let us see now that the group generated by $S_{v_2(v(N))}$ and the Atkin-Lehner involutions at 2, and the group generated by $S_{v_3(v(N))}$ and the Atkin-Lehner involution at 3 have the structure predicted in Claim 2 when $\gcd(v(N), 2^3) \leq 2$. We only need to check when $v(N)$ is a power of 2 or 3 by (2). For $v(N) = 1$ the matrix (1) is $w_{\frac{\delta}{\delta'}(\frac{\Delta}{\Delta'})^2}$ (we denote $w_1 := id$) (we have in this case a much deeper result, see proposition 3). Take now $v(N) = 2$. If $l = gcd(3, \delta/\delta')$ let $\Omega = w_l\Omega'$; the matrix Ω' is as (1) but with $\gcd(3, \delta/\delta') = 1$, and $\frac{\delta}{\delta'}\frac{\Delta^2}{\Delta'^2}$ is only a power of 2. Then $\Omega' \in < S_2, w_{2^{v_2(N)}} >$, let us to precise the group structure. For $v(N) = 2$ we have $v_2(N) = 2$ or 3, and we have already proved the group structure of Claim [1] in lemmas 7,8 (we have moreover that Claim 2 is true because S_2 commutes with the Atkin-Lehner involutions $w_{p_i^{n_i}}$ if $(p_i, 2) = 1$, see proposition 5). Assume now $v(N) = 3$. If $l = gcd(2, \delta/\delta')$ and $\Omega = w_l\Omega'$ then Ω' is as (1) but with $gcd(2, \delta/\delta') = 1$, and $\frac{\delta}{\delta'}\frac{\Delta^2}{\Delta'^2}$ is only a power of 3. Then $\Omega' \in < S_3, w_{3^{v_3(N)}} >$, let us to precise the group structure. For $v(N) = 3$ we have $v_3(N) \geq 2$. Let us begin with $v_3(N) = 2$, then Ω' is of the form

$$\Omega' = \begin{pmatrix} r' & \frac{u'}{3} \\ \frac{Nt'}{3} & v' \end{pmatrix} =: a(r', u', t', v')$$

(from the formulation of Theorem 1 we can consider $\frac{\Delta}{\Delta'} = 1 = \frac{\delta}{\delta'}$ because the factors outside 3 does not appear if we multiply for a convenient Atkin-Lehner involution, and for 3 observe that under our condition $\Delta = 1$) and we have

$$a(r', u', t', v') \in \Gamma_0(N) \Leftrightarrow t' \equiv u' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')w_9 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')S_3 \in \Gamma_0(N) \Leftrightarrow r' + u' \equiv t' \equiv 0(mod\ 3)$$

$$a(r',u',t',v')S_3^2 \in \Gamma_0(N) \Leftrightarrow 2r'+u' \equiv t' \equiv 0(mod\ 3)$$
$$a(r',u',t',v')S_3w_9 \in \Gamma_0(N) \Leftrightarrow r' \equiv qt'+v' \equiv 0(mod\ 3)$$
$$a(r',u',t',v')S_3^2w_9 \in \Gamma_0(N) \Leftrightarrow r' \equiv 2qt'+v' \equiv 0(mod\ 3)$$
$$a(r',u',t',v')w_9S_3^2 \in \Gamma_0(N) \Leftrightarrow r'+u' \equiv v' \equiv 0(mod\ 3)$$
$$a(r',u',t',v')w_9S_3 \in \Gamma_0(N) \Leftrightarrow r'+2u' \equiv v' \equiv 0(mod\ 3)$$
$$a(r',u',t',v')w_9S_3^2w_9 \in \Gamma_0(N) \Leftrightarrow u' \equiv qt'+v' \equiv 0(mod\ 3)$$
$$a(r',u',t',v')S_3^2w_9S_3^2 \in \Gamma_0(N) \Leftrightarrow u' \equiv 2qt'+v' \equiv 0(mod\ 3)$$
$$a(r',u',t',v')S_3^2w_9S_3 \in \Gamma_0(N) \Leftrightarrow r'+u' \equiv 2t'q+v' \equiv 0(mod\ 3)$$
$$a(r',u',t',v')S_3w_9S_3^2 \in \Gamma_0(N) \Leftrightarrow 2r'+u' \equiv qt'+v' \equiv 0(mod\ 3)$$

and these are all the possibilities, proving that the group is $\{S_3, w_9 | S_3^3 = w_9^2 = (w_9S_3)^3 = 1\}$ of order 12. Observe that S_3 does not commute with w_2 (see for example lemma 7).

Suppose now that $v_3(N) \geq 3$. We distinguish the cases $v_3(N)$ odd and $v_3(N)$ even. Suppose $v_3(N)$ is even, then $\frac{\delta}{\delta'} = 1$ and Ω' has the following form

$$\frac{1}{\frac{\Delta}{\Delta'}} \begin{pmatrix} r'(\frac{\Delta}{\Delta'})^2 & \frac{u'}{3} \\ \frac{Nt'}{3} & v'(\frac{\Delta}{\Delta'})^2 \end{pmatrix}$$

with $\alpha := \Delta/\Delta'$ dividing $3^{[v_3(N)/2]-1}$. Since this last matrix has determinant 1 we see that α satisfies $\gcd(\alpha, N/(3^2\alpha^2)) = 1$; thus $\alpha = 1$ or $\alpha = 3^{[v_3(N)/2]-1}$. Write $a(r',u',t',v') = \begin{pmatrix} r' & \frac{u'}{3} \\ \frac{Nt'}{3} & v' \end{pmatrix}$ when we take $\alpha = 1$ and $b(r',u',t',v') = \begin{pmatrix} r'(3^{[v_3(N)/2]-1}) & \frac{u'}{3^{[v_3(N)/2]}} \\ \frac{Nt'}{3^{[v_3(N)/2]}} & v'(3^{[v_3(N)/2]-1}) \end{pmatrix}$ when $\alpha = 3^{[v_3(N)/2]-1}$. It is easy to check that $b(r',u',t',v') = w_{3^{v_3(N)}}a(r',u',t',v')$ and that the group structure is the predicted in a similar way as the one done above for $v(N) = 2$. Suppose now that $v_3(N)$ is odd, then $\frac{\delta}{\delta'}$ is 1 or 3 and $\frac{\Delta}{\Delta'}$ divides $3^{[v_3(N)/2]-1}$. Now from $\det() = 1$ we obtain that the only possibilities are $\frac{\delta}{\delta'} = 1 = \frac{\Delta}{\Delta'}$ name the matrices for this case following equation 1 by $a(r',u',t',v')$, and the other possibility is $\frac{\delta}{\delta'} = 3$ and $\frac{\Delta}{\Delta'} = 3^{[v_3(N)/2]-1}$, write the matrices for this case following equation 1 by $c(r',u',t',v')$. It is also easy to check that $c(r',u',t',v') = w_{3^{v_3(N)}}a(r'',u'',t'',v'')$, and that the group structure is the predicted.

□

Corollary 12. *Let $N = 3^{v_3(N)}\prod_i p_i^{n_i}$, with p_i different primes such that $\gcd(p_i, 6) = 1$. Suppose that $v(N) = 3$ and $p_i^{n_i} \equiv 1(mod\ 3)$ for all i. Then Claim 2 is true.*

Proof. From the proof of the above theorem 11 for $v(N) = 3$ with $v_3(N) \geq 2$, lemma 10, and that the general observation that the Atkin-Lehner involutions commute one with each other we obtain that the direct product decomposition of Claim 2 is true obtaining the result. □

Now we shows the corrections to Claim 2 for $v(N) = 4$ and $v(N) = 8$, about the group structure of the subgroup of $\mathrm{Norm}(\Gamma_0(N))/\Gamma_0(N)$ generated for S_{2^k} and the Atkin-Lehner involution at prime 2.

Proposition 13. *Suppose $v(N)=4$, observe that in this situation $v_2(N)=4$, or 5. Then the group structure of the subgroup $< w_{2^{v_2(N)}}, S_4 >$ of $\mathrm{Norm}(\Gamma_0(N))/\Gamma_0(N)$ is given by the relations:*

1. *For $v_2(N)=4$ we have $S_4^4=w_{16}^2=(w_{16}S_4)^3=1$.*
2. *For $v_2(N)=5$ we have $S_4^4=w_{32}^2=(w_{32}S_4)^4=1$.*

Proof. It is a straightforward computation. Observe that for $v_2(N)=4$ the statement coincides with Claim 2 but not for $v_2(N)=5$, where one checks that S_4 does not commute with $w_{32}S_4w_{32}$. □

Proposition 14. *Suppose $v(N)=8$ and $v_2(N)$ even (this is the case (3)(c) in Claim 2). Then the group $< w_{2^{v_2(N)}}, S_8 >\subseteq \mathrm{Norm}(\Gamma_0(N))/\Gamma_0(N)$ satisfies the following relations: $S_8^8=w_{2^{v_2(N)}}^2=1$, and*

1. *for $v_2(N)=6$ we have $(w_{64}S_8)^3=1$,*
2. *for $v_2(N)\geq 8$ we do not have the relation $(w_{2^{v_2(N)}}S_8)^3=1$,*
3. *for $v_2(N)\geq 10$ we have the relation: S_8 commutes with $w_{2^{v_2(N)}}S_8w_{2^{v_2(N)}}$,*
4. *for $v_2(N)=6$ or 8 we do not have the relation: S_8 commutes with the element $w_{2^{v_2(N)}}S_8w_{2^{v_2(N)}}$.*
5. *For $v_2(N)=8$ we have the relation: $w_{256}S_8w_{256}S_8w_{256}S_8^3w_{256}S_8^3=1$.*

Proof. Straightforward. □

Proposition 15. *Suppose $v(N)=8$ and $v_2(N)$ odd (this is the case (3)(d) in Claim 2). Then the group $< w_{2^{v_2(N)}}, S_8 >\subseteq \mathrm{Norm}(\Gamma_0(N))/\Gamma_0(N)$ satisfies the following relations: $S_8^8=w_{2^{v_2(N)}}^2=1$, and*

1. *for $v_2(N)=7$ $(w_{128}S_8)^4=1$,*
2. *for $v_2(N)\geq 9$ we do not have the relation $(w_{2^{v_2(N)}}S_8)^4=1$,*
3. *for $v_2(N)\geq 9$ we have the Atkin-Lehner relation: S_8 commutes with $w_{2^{v_2(N)}}S_8w_{2^{v_2(N)}}$,*
4. *for $v_2(N)=7$ we do not have that S_8 commutes with $w_{128}S_8w_{128}$.*

Proof. Straightforward. □

Let us finally write the revisited results concerning Claim 2 that we prove;

Theorem 16. *The quotient $\mathrm{Norm}(\Gamma_0(N))/\Gamma_0(N)$ is a product of the following groups:*

1. *$\{w_{q^{v_q(N)}}\}$ for every prime q, $q\geq 5$ $q\mid N$.*
2. (a) *If $v_3(N)=0$, $\{1\}$*
   (b) *If $v_3(N)=1$, $\{w_3\}$*
   (c) *If $v_3(N)=2$, $\{w_9,S_3\}$; satisfying $w_9^2=S_3^3=(w_9S_3)^3=1$ (factor of order 12)*
   (d) *If $v_3(N)\geq 3$; $\{w_{3^{v_3(N)}},S_3\}$; where $w_{3^{v_3(N)}}^2=S_3^3=1$ and $w_{3^{v_3(N)}}S_3w_{3^{v_3(N)}}$ commute with S_3 (factor group with 18 elements)*
3. *Let be $\lambda=v_2(N)$ and $\mu=\min(3,[\frac{\lambda}{2}])$ and denote by $v''=2^\mu$ the we have:*
   (a) *If $\lambda=0$; $\{1\}$*
   (b) *If $\lambda=1$; $\{w_2\}$*
   (c) *If $\lambda=2\mu$ and $2\leq\lambda\leq 6$; $\{w_{2^{v_2(N)}},S_{v''}\}$ with the relations $w_{2^{v_2(N)}}^2=S_{v''}^{v''}=(w_{2^{v_2(N)}}S_{v''})^3=1$, where they have orders 6,24, and 96 for $v=2,4,8$ respectively.*

(d) *If* $\lambda > 2\mu$ *and* $2 \leq \lambda \leq 7$; $\{ w_{2^{v_2(N)}}, S_{v''}\}$; $w_{2^{v_2(N)}}^2 = S_{v''}^{v''} = 1$. *Moreover,* $(w_{2^{v_2(N)}}S_{v''})^4 = 1$.

($\tilde{c}$),($\tilde{d}$) *If* $\lambda \geq 9$; $\{w_{2^{v_2(N)}}, S_8\}$ *with the relations* $w_{2^{v_2(N)}}^2 = S_8^8 = 1$ *and* S_8 *commutes with* $w_{2^{v_2(N)}}S_8w_{2^{v_2(N)}}$.

($\hat{c}$) *If* $\lambda = 8$; $\{w_{2^{v_2(N)}}, S_8\}$ *with relations given by* $w_{2^{v_2(N)}}^2 = S_8^8 = 1$ *and* $w_{256}S_8w_{256}S_8w_{256}S_8^3w_{256}S_8^3 = 1$.

Observation 17. *One needs to warn that for the situations* $v(N) = 8$ *or* $\lambda = 5$ *possible the relations does not define totally the factor group, but it is a computation more.*

Observation 18. *The product between the different groups appearing in theorem 16 is easily computable. Effectively, we know that the Atkin-Lehner involutions commute, and* $S_{2^{v_2(v(N))}}$ *commutes with* $S_{3^{v_3(v(N))}}$. *Moreover* S_2 *commutes with any element different from Atkin-Lehner involutions involving the prime 2 from lemma 4. Consider* w_{p^n} *an Atkin-Lehner involution for* $X_0(N)$ *with* p *a prime. One obtains the following results by using the same arguments appearing in the proof of lemma 10;*

1. *let* p *be coprime with* 3 *and* $3|v(N)$. S_3 *commutes with* w_{p^n} *if and only if* $p^n \equiv 1(modulo\ 3)$. *If* $p^n \equiv -1(modulo\ 3)$ *then* $w_{p^n}S_3 = S_3^2w_{p^n}$.
2. *Let* p *be coprime with* 2 *and* $4|v(N)$. S_4 *commutes with* w_{p^n} *if and only if* $p^n \equiv 1(modulo\ 4)$. *If* $p^n \equiv -1(modulo\ 4)$ *then* $w_{p^n}S_4 = S_4^3w_{p^n}$.
3. *Let* p *be coprime with* 2 *and* $8|v(N)$. *Then,* $w_{p^n}S_8 = S_8^kw_{p^n}$ *if* $p^n \equiv k(modulo\ 8)$, *in particular* S_8 *commutes with* w_{p^n} *if and only if* $p^n \equiv 1(modulo\ 8)$.

6. Postcript

The normalizer of $\Gamma_0(N)$ in $SL_2(\mathbb{R})$ has conjecturally deep interest in group theory for the Monster simple group. Let j be the j-invariant function for elliptic curves, the field $\mathbb{C}(j)$ corresponds to the function field of the compactification of $\mathbb{H}/SL_2(\mathbb{Z})$, where $\mathbb{H}$ is the Poincaré semi-half plane, which has genus zero. We usually write this function as a $q(= e^{2\pi i})$-series, $j = q^{-1} + 744 + 196884q + \ldots$. A q-series is normalized for group theory specialists in this field when the constant term is zero, thus take $J := j - 744 = q^{-1} + 0 + H_1q + ...$ where the H_r are conjecturally related with certain representations for the Monster, called the head representations. Thompson replaces H_r with what he calls character values $H_r(m)$. This gives another normalized series $T_m = q^{-1}+0+H_1(m)q+\ldots$. Roughly speaking, the conjecture claims some sort of relation between the function field generated for the normalizer function T_m and the generating normalized function for a genus 0 curve arising from a group between $\Gamma_0(N)$ and its normalizer in $PSL_2(\mathbb{R})$.

Conway and Norton in the paper "Monstrous moonshine" (Bull. London Mat. Soc., 11,(1979),308-339) gives a very nice exposition of the subject from a group theorical point of view. Conway and Norton take the matrices for the normalizer of $\Gamma_0(N)$ given by the last theorem in [1] (we observed in this paper that this theorem is wrong, but Conway and Norton use the matrix statement of Atkin-Lehner paper which is from Newmann, which is correct) and express the normalizer of $\Gamma_0(N)$ in a better form for the above conjecture. This new formulation of the normalizer is used for obtaining the normalizer of $\Gamma_0(N)$ in $PSL_2(\mathbb{R})$ by Akbas-Singerman (*The* *normalizer of* $\Gamma_0(N)$ *in* $PSL(2,\mathbb{R})$; Glasgow Math. J. 32 (1990), no.3, 317-327) correcting the Atkin-Lehner statement, and the Conway-Norton matrix formulation for the normalizer is also used to obtain in particular some normalizers for modular subgroups as $\Gamma_0(N) + some\ Atkin-Lehner\ involution$: results of Lang (*Normalizers of the congruence subgroups of the Hecke groups* G_4 *and* G_6: J. Number Theory 90 (2001), no.1, 31-43; *Groups commensurable with the modular group*: J. Algebra 274 (2004), no.2, 804-821) and Chua-Lang (*Congruence subgroups associated to the monster*: Experiment. Math. 13 (2004), no.3, 343-360).

Our approach follows the old Newmann formulation for the normalizer, and the results obtained agree with those obtained by Akbas-Singerman. We only mention that the claimed relation $w_{256}S_8^2w_{256}S_8 = S_8^2w_{256}S_8w_{256}$ when $N = 256$ at Akbas-Singerman result in p.324 (loc. cit.) is not true, (the others relations at this result in p.324 are true).

I thank John McKay for drawing these references to my attention.

References

[1] Atkin, A.O.L., Lehner, J.: Hecke operator on $\Gamma_0(N)$. Math.Ann.185, 134-160 (1970).

[2] Bars, F.: Determinació de les corbes $X_0(N)$ biel.líptiques. Tesina Universitat Autònoma de Barcelona. September 1997. Find a copy at http://mat.uab.es/~francesc/publicac.html

[3] Kenku, M.A.,Momose, F.: Automorphisms groups of the modular curves $X_0(N)$. Compositio Math. 65, 51-80, (1988).

[4] Lehner, J., Newman, M.: Weierstrass points of $\Gamma_0(N)$. Ann. of Math. 79, 360-368 (1964).

[5] Newman, M.: Structure theorem for modular subgroups. Duke Math. J.22, 25-32 (1955).

[6] Newman, M.: Conjugacy, genus and class numbers. Math.Ann.196m 198-217 (1975).

[7] Ogg, A.P.: Hyperelliptic modular curves. Bull.Soc.math. France 102,449-462 (1974).

Francesc Bars Cortina, Depart. Matemàtiques, Universitat Autònoma de Barcelona, 08193 Bellaterra. Catalonia. Spain. E-mail: francesc@mat.uab.cat