THE GROUP STRUCTURE OF THE NORMALIZER OF $\Gamma_0(N)$

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

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

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 obtained in [2].

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

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

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

$$\sqrt{\delta} \left( \frac{r\Delta}{\nu^2\Delta} \frac{s\Delta}{\nu^3\Delta} \frac{l\Delta}{\nu^3\Delta} \right)$$

with $r, u, s, l \in \mathbb{Z}$ and $\delta | q$, $\Delta | \frac{\sigma}{\epsilon}$. Moreover $\nu = 2^\mu 3^w$ with $\mu = \text{min}(3, \left\lfloor \frac{1}{2} \nu_2(N) \right\rfloor)$ and $w = \text{min}(1, \left\lfloor \frac{1}{2} \nu_3(N) \right\rfloor)$ where $\nu_p(N)$ is the valuation at the prime $p_i$ of the integer $N$.

Date: First version: December 22th, 2006.
MSC: 20H05(19B37,11G18).
This theorem is proved by Morris Newman in [5], see also [2] p.12-14.

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

3. THE GROUP STRUCTURE OF \( \text{Norm}(\Gamma_0(N))/\Gamma_0(N) \)

In this section we obtain some partial results on the group structure of \( \text{Norm}(\Gamma_0(N)) \).

Let us first introduce some particular elements of \( \text{SL}_2(\mathbb{R}) \).

**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,

\[
w_{m'} = \frac{1}{\sqrt{m'}} \begin{pmatrix} m'a & b \\ Nc & m'd \end{pmatrix} \in \text{SL}_2(\mathbb{R})
\]

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 \( \text{Norm}(\Gamma_0(N))/\Gamma_0(N) \) is the direct product of the following groups:

1. \( \{w_{p^q(N)}\} \) 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 \( v_3(N) = 2 \), \( \{w_3, S_3\} \); satisfying \( w_3^2 = S_3^2 = (w_9S_3)^3 = 1 \) (factor of order 12)
   (d) If \( v_3(N) \geq 3 \), \( \{w_{3^v(N)}, S_3\} \); where \( w_{3^v(N)}^2 = S_3^2 \) and \( w_{3^v(N)}S_3w_{3^v(N)} \) commute with \( S_3 \) (factor group with 18 elements)
3. Let be \( \lambda = v_2(N) \) and \( \mu = \min(3, [\frac{N}{2}]) \) and denote by \( v'' = 2^\mu \) the we have:
   (a) If \( \lambda = 0 \), \( \{1\} \)
   (b) If \( \lambda = 1 \), \( \{w_2\} \)
   (c) If \( \lambda = 2 \mu \); \( \{w_{2^v(N)}, S_{v''}\} \) with the relations \( w_{2^{v(N)}}^2 = S_{v''}^2 = (w_{2^{v(N)}}S_{v''})^3 = 1 \), 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 \( \lambda > 2 \mu \); \( \{w_{2^{v(N)}}, S_{v''}\} \); \( w_{2^{v(N)}}^2 = S_{v''}^{v''} = 1 \). Moreover, \( S_{v''} \) commutes with \( w_{2^{v(N)}}S_{v''}w_{2^{v(N)}} \) (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 \( \text{Norm}(\Gamma_0(N))/\Gamma_0(N) \) 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. We recall only that \( w_{mm'} = w_mw_{m'} \) for \( (m, m') = 1 \) and easily \( w_mw_{m'} = w_{m'w_m} \); the the result follows by a straightforward computation from Theorem[1] see also [2] p.14. \( \square \)
When $v(N) > 1$ it is clear that some element $S_w$ appears in the group structure of $\text{Norm}(\Gamma_0(N))/\Gamma_0(N)$ from Theorem 1.

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

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

$$w_m S_2 w_m S_2 = \begin{pmatrix} \frac{2mk^2 + 2Nt + mkNt}{N(2m + 2mk + Nt)} & (2 + 2m)(2m + 2mk + Nt) \\ \frac{2m}{2m} & m + Nt + \frac{N_1}{m} + \frac{kN_1}{2} + \frac{N_1^2}{4m} \end{pmatrix}.$$ 

$\square$

**Proposition 5.** Let $N = 2^{v_2(N)} \prod p_i^{v_i}$, 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 $\hat{u} \in \text{Norm}(\Gamma_0(N))$ and write it as:

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

following the notation of Theorem 1. Then:

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

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

**Proof.** This is an easy calculation. $\square$

We study now the different elements of the type

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

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

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

**Lemma 7.** For $N \equiv 4(\text{mod } 8)$ all the elements of the normalizer of type $a(r', u', s', v')$ belong to the order six group $\{S_2, w_4S_2^2 = w_4^2 = (w_4S_2)^3 = 1\}$.

**Proof.** Straightforward from the equalities:

$$a(r', u', s', v') \in \Gamma_0(N) \iff s' \equiv u' \equiv 0(\text{mod } 2)$$

$$a(r', u', s', v') S_2 \in \Gamma_0(N) \iff r' \equiv v' \equiv u' \equiv 1 s' \equiv 0(\text{mod } 2)$$

$$a(r', u', s', v') w_4 \in \Gamma_0(N) \iff r' \equiv v' \equiv u' \equiv s' \equiv 1(\text{mod } 2)$$

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

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

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

$\square$
Lemma 8. Let $N$ be a positive integer with $v_2(N) = 3$. Then all the elements of the form $a(r', u', s', v')$ and $b(v'', u'', s'', v'')$ 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:

- $a(r', u', s', v') \in \Gamma_0(N) \iff r' \equiv v' \equiv 1, u' \equiv s' \equiv 0 \mod 2$
- $a(r', u', s', v')S_2 \in \Gamma_0(N) \iff r' \equiv v' \equiv u' \equiv 1, s' \equiv 0 \mod 2$
- $a(r', u', s', v')w_8S_2w_8S_2 \in \Gamma_0(N) \iff r' \equiv v' \equiv s' \equiv v' \equiv 0 \mod 2$
- $b(v'', u'', s'', v'') \in \Gamma_0(N) \iff v'' \equiv u'' \equiv s'' \equiv v'' \equiv 1 \mod 2$

We can now proof Proposition 5.

Proof. [ of Proposition 5] Let $N = 2^{v_2(N)} \prod p_i^{v_i}$, with $p_i$ different primes and assume that $9 \not| N$. If $v_2(N) \leq 1$ we are done by proposition 4. Suppose $v_2(N) = 2$ and let $u \in \text{Norm}(\Gamma_0(N))$. By lemmas 6 and 7 $w_8u = \alpha, \alpha \in \{S_2, w_8|S_2^2 = w_8^2 = (w_8S_2)^3 = 1\}$ and it follows that $u = w_8\alpha$. Since $w_8 ((5, 2) = 1)$ 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 $v_2(N) \leq 2$ 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 [8] 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 $\mathbb{Z}/2 \times \Pi_k$ where $\Pi_k$ 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 $N = 3^{v_3(N)} \prod p_i^{v_i}$ where $p_i$ are different primes of $\mathbb{Q}$. Impose that $S_3 \in \text{Norm}(\Gamma_0(N))$. Then $S_3$ commutes with $w_3p_i^{v_i}$ if and only if $p_i^{v_i} \equiv 1 \mod 3$. Therefore if some $p_i^{v_i} \equiv -1 \mod 3$ the Claim 2 is not true.
Proof. Let us show that $S_3$ does not commute with $w_{p_i}$, if and only if $p_i^{n_i} \equiv -1 (\text{mod } 3)$. Observe the equality $w_{p_i} = \frac{1}{\sqrt{p_i}} \begin{pmatrix} p_i^{n_i} & 1 \\ Nt & p_i^{n_i} \end{pmatrix}$:

$$w_{p_i} S_3 w_{p_i} S_3^2 = \frac{1}{p_i^{n_i}} \begin{pmatrix} (p_i^{n_i} k)^2 + Nt(1 + \frac{p_i^{n_i} k}{p_i^{n_i}}) & p_i^{n_i} k(2p_i^{n_i} k + 1) + (\frac{p_i^{n_i} k}{p_i^{n_i}} + 1)(\frac{2Nt}{3} + p_i^{n_i}) \\ Nt(p_i^{n_i} k) + Nt(\frac{Nt}{3} + p_i^{n_i}) & Nt(2p_i^{n_i} k + 1) + p_i^{n_i}(\frac{Nt}{3} + p_i^{n_i})(\frac{2Nt}{3} + p_i^{n_i}) \end{pmatrix}.$$ 

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

\section*{5. The Group Structure of $\text{Norm}(\Gamma_0(N))/\Gamma_0(N)$ revisited.}

In this section we correct Claim 2. We prove here that the quotient $\text{Norm}(\Gamma_0(N))/\Gamma_0(N)$ is the product of some groups associated every one of them to the primes which divide $N$. See for the explicit result theorem 10.

Theorem 11. Any element $w \in \text{Norm}(\Gamma_0(N))$ 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 $\Omega$ belongs to the subgroup generated by $S_3(N)$ and the Atkin Lehner involutions $w_{2^{\nu_2}(N)}, w_{3^{\nu_3}(N)}$. Moreover for $\gcd(v(N), 2^3) \leq 2$ the group structure for the subgroup $< S_{v_2(v(N))}, w_{2^{\nu_2}(N)} >$ and $< S_{v_3(v(N))}, w_{3^{\nu_3}(N)} >$ of $< S_{v(N)}, w_{2^{\nu_2}(N)}, w_{3^{\nu_3}(N)} >$ is the predicted by Atkin-Lehner at Claim 2, but these two subgroups do not necessarily commute with each other element-wise.

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

$$w = \sqrt{\frac{r \Delta}{N}} \begin{pmatrix} \frac{r \Delta}{N} & \frac{w}{\Delta} \\ \frac{w}{\Delta} & \frac{l \delta (\Delta^2)}{\Delta} \end{pmatrix} = \frac{1}{\Delta \sqrt{\delta}} \begin{pmatrix} r \delta \Delta^2 & \frac{w}{l \delta (\Delta^2)} \\ \frac{w}{l \delta (\Delta^2)} & \frac{v(N)}{\delta} \end{pmatrix}.$$ 

Let us denote by $U = 2^\nu(N)3^{\nu_3(N)}$. Write $\Delta' = \gcd(\Delta, N/U)$ and $\delta' = \gcd(\delta, N/U)$; then we obtain

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

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

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

(1)
is generated by $S_{v(N)}$ and the Atkin-Lehner involutions at 2 and 3 which are the factors of $\frac{\sqrt{\Delta}}{\Delta}$.

To check this observe that $\Omega = \Omega_2 \Omega_3$ with

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

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

We only consider the case for $\Omega_2$, the case for the $\Omega_3$ is similar. We can assume that $2^{v_2(N)} \sqrt{\Delta/\delta} = 1$ substituting $\Omega_2$ by $w_{2^2(N)} \Omega_2$ if necessary. Thus, we are reduced to a matrix of the form $\Omega_2 = \begin{pmatrix} r' & N' \cdot \frac{2^{v_2(N)}}{\sqrt{\Delta/\delta}} \\ \sqrt{\Delta/\delta} & v' \cdot \frac{2^{v_2(N)}}{\sqrt{\Delta/\delta}} \end{pmatrix}$. Now for some $i$ we can obtain $S_{2^2(N)} \Omega_2 = \begin{pmatrix} r' & N' \cdot \frac{2^{v_2(N)}}{\sqrt{\Delta/\delta}} \\ \sqrt{\Delta/\delta} & v' \cdot \frac{2^{v_2(N)}}{\sqrt{\Delta/\delta}} \end{pmatrix}$ (we denote $w_1 := \text{id}$) (we have in this case a much deeper result, see proposition $\text{B}$). Take now $v(N) = 2$. If $l = \gcd(3, \delta/\delta')$ let $\Omega = w_l \Omega'$; the matrix $\Omega'$ is as $\text{B}$ but with $\gcd(3, \delta/\delta') = 1$, and $\frac{\Delta}{2\Delta_2}$ is only a power of 2. Then $\Omega' \in S_2^1(\omega(N))$, 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 $\text{B}$ in lemmas $\text{B}$ (we have moreover that Claim $\text{B}$ is true because $S_2$ commutes with the Atkin-Lehner involutions $w_{p_i^m}$ if $(p_i, 2) = 1$, see proposition $\text{B}$). Assume now $v(N) = 3$. If $l = \gcd(2, \delta/\delta')$ and $\Omega = w_l \Omega'$ then $\Omega'$ is as $\text{B}$ but with $\gcd(2, \delta/\delta') = 1$, and $\frac{\Delta}{2\Delta_2}$ is only a power of 3. Then $\Omega' \in S_3(\omega_3(N))$, 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 $\Omega'$ is of the form

$$\Omega' = \begin{pmatrix} r' & N' \cdot \frac{\Delta}{\Delta_2} \\ \Delta & v' \cdot \frac{\Delta}{\Delta_2} \end{pmatrix} =: a(r', u', t', v')$$

(from the formulation of Theorem $\text{B}$ we can consider $\frac{\Delta}{\Delta_2} = 1 = \frac{\delta}{\delta'}$ 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

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

$$a(r', u', t', v') w_3 \in \Gamma_0(N) \iff r' \equiv v' \equiv 0(\mod 3)$$

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

$$a(r', u', t', v') S_3^2 \in \Gamma_0(N) \iff 2r' + u' \equiv t' \equiv 0(\mod 3)$$

$$a(r', u', t', v') w_3 S_3 \in \Gamma_0(N) \iff r' \equiv qt' + v' \equiv 0(\mod 3)$$

$$a(r', u', t', v') S_3^2 w_3 \in \Gamma_0(N) \iff r' \equiv 2qt' + v' \equiv 0(\mod 3)$$

$$a(r', u', t', v') w_3 S_3^2 \in \Gamma_0(N) \iff r' + u' \equiv v' \equiv 0(\mod 3)$$
\[
\begin{align*}
a(r', u', t', v')w_9S_3 & \in \Gamma_0(N) \iff r' + 2u' \equiv v' \equiv 0 \mod{3} \\
a(r', u', t', v')w_9S_3^2w_9 & \in \Gamma_0(N) \iff u' \equiv qt' + v' \equiv 0 \mod{3} \\
a(r', u', t', v')S_3^2w_9S_3^2 & \in \Gamma_0(N) \iff u' \equiv 2qt' + v' \equiv 0 \mod{3} \\
a(r', u', t', v')S_3^2w_9S_3 & \in \Gamma_0(N) \iff r' + u' \equiv 2t'q + v' \equiv 0 \mod{3}
\end{align*}
\]
and these are all the possibilities, proving that the group is \(\{S_3, w_9S_3^3 = w_9^3 = (w_9S_3)^3 = 1\}\) 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 \(\Omega'\) has the following form

\[
\frac{1}{\Delta}
\begin{pmatrix}
\frac{r'}{\Omega'} & \frac{u'}{\Omega'} & \frac{v'}{\Omega'} \\
\frac{N_3}{\Omega'} & \frac{3}{\Omega'} & \frac{3}{\Omega'} \\
\frac{N_3^2}{\Omega'} & \frac{3}{\Omega'} & \frac{3}{\Omega'}
\end{pmatrix}
\]

with \(\alpha := \Delta/\Delta'\) dividing \(3^{[v_3(N)/2] - 1}\). Since this last matrix has determinant 1 we see that \(\alpha\) satisfies \(\gcd(\alpha, N(3^2\alpha^2)) = 1\); thus \(\alpha = 1\) or \(3^{[v_3(N)/2] - 1}\).

Write \(a(r', u', t', v') = \begin{pmatrix} \frac{r'}{\Omega'} & \frac{u'}{\Omega'} & \frac{v'}{\Omega'} \\ \frac{N_3}{\Omega'} & \frac{3}{\Omega'} & \frac{3}{\Omega'} \\ \frac{N_3^2}{\Omega'} & \frac{3}{\Omega'} & \frac{3}{\Omega'} \end{pmatrix}\) when we take \(\alpha = 1\) and \(b(r', u', t', v') = \begin{pmatrix} \frac{r'}{\Omega'} & \frac{u'}{\Omega'} & \frac{v'}{\Omega'} \\ \frac{N_3}{\Omega'} & \frac{3}{\Omega'} & \frac{3}{\Omega'} \\ \frac{N_3^2}{\Omega'} & \frac{3}{\Omega'} & \frac{3}{\Omega'} \end{pmatrix}\) when \(\alpha = 3^{[v_3(N)/2] - 1}\). It is easy to check that \(b(r', u', t', v') = w_{3v_3(N)}a(r', u', t', v')\) 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 \(\frac{\Delta}{\Delta'} = 1\) or 3 and \(\frac{\Delta}{\Delta'}\) divides \(3^{[v_3(N)/2] - 1}\). Now from \(\det() = 1\) we obtain that the only possibilities are \(\frac{\Delta}{\Delta'} = 1\), 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 \(c(r', u', t', v') = w_{3v_3(N)}a(r', u', t', v')\), and that the group structure is the predicted.

\[\square\]

**Corollary 12.** Let \(N = 3^{v_3(N)} \prod p_i^{n_i}\), 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 \(1\) 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 \(\text{Norm}(\Gamma_0(N))/\Gamma_0(N)\) generated for \(S_2\) 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 \(<w_{2v_2(N)}, S_4>\) of \(\text{Norm}(\Gamma_0(N))/\Gamma_0(N)\) is given by the relations:

1. For \(v_2(N) = 4\) we have \(S_4^4 \equiv w_4^2 = (w_4S_4)^3 = 1\).
2. For \(v_2(N) = 5\) we have \(S_4^4 \equiv w_{10}^2 = (w_{10}S_4)^3 = 1\).
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 \(w_{2^2} S_4 w_{32}\).

\(\square\)

**Proposition 14.** Suppose \(v(N) = 8\) and \(v_2(N)\) even (this is the case (3)(c) in Claim 2). Then the group \(G_{2^{v_2(N)}, S_8} > \subseteq \text{Norm}(\Gamma_0(N))/\Gamma_0(N)\) satisfies the following relations: \(S_8^2 = w_{2^2} = 1\), 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 \((w_{2^2} S_8)^3 = 1\),
3. for \(v_2(N) \geq 10\) we have the relations: \(S_8\) commutes with \(w_{2^2} S_8 w_{2^2} = 1\),
4. for \(v_2(N) = 6\) or \(8\) we do not have the relation: \(S_8\) commutes with the element \(w_{2^2} S_8 w_{2^2}\).
5. For \(v_2(N) = 8\) we have the relation: \(w_{2^5} S_8 w_{2^5} S_8 w_{2^5} S_8^3 = 1\).

Proof. Straightforward. \(\square\)

**Proposition 15.** Suppose \(v(N) = 8\) and \(v_2(N)\) odd (this is the case (3)(d) in Claim 2). Then the group \(G_{2^{v_2(N)}, S_8} > \subseteq \text{Norm}(\Gamma_0(N))/\Gamma_0(N)\) satisfies the following relations: \(S_8^2 = w_{2^2} = 1\), 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 \((w_{2^2} S_8)^4 = 1\),
3. for \(v_2(N) \geq 9\) we have the Atkin-Lehner relation: \(S_8\) commutes with \(w_{2^2} S_8 w_{2^2}\),
4. for \(v_2(N) = 7\) we do not have that \(S_8\) commutes with \(w_{128} S_8 w_{128}\).

Proof. Straightforward. \(\square\)

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

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

1. \(\{w_{2^q(N)}\}\) 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 \(w_9^2 = S_3^2 = (w_9 S_3)^3 = 1\) (factor of order 12)
   (d) If \(v_3(N) \geq 3, \{w_3^{3^{v_3(N)}}, S_3\}\); where \(w_9^2 = S_3^3 = 1\) and \(w_3^{3^{v_3(N)}}, S_3 w_3^{3^{v_3(N)}}\) commute with \(S_3\) (factor group with 18 elements)
3. Let be \(\lambda = v_2(N)\) and \(\mu = \min(3, \lceil \frac{\lambda}{2} \rceil)\) 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 \(2 \leq \lambda \leq 6; \{w_2^{2^v(N)}, S_{v''}\}\) with the relations \(w_2^{2^v(N)} = S_{v''}^{v''} = (w_2^{2^v(N)} S_{v''})^3 = 1\), where they have orders 6, 24, and 96 for \(v = 2, 4, 8\) respectively.
   (d) If \(\lambda > 2\mu\) and \(2 \leq \lambda \leq 7, \{w_2^{2^v(N)}, S_{v''}\}; w_2^{2^v(N)} = S_{v''}^{v''} = 1\). Moreover, \((w_2^{2^v(N)}, S_{v''})^4 = 1\).
   (c), (d) If \(\lambda \geq 9; \{w_2^{2^v(N)}, S_8\}\) with the relations \(w_2^{2^v(N)} = S_8^8 = 1\) and \(S_8\) commutes with \(w_2^{2^v(N)} S_8 w_2^{2^v(N)}\).
   (c) If \(\lambda = 8; \{w_2^{2^v(N)}, S_8\}\) with the relations \(w_2^{2^v(N)} = S_8^8 = 1\) and \(w_2^{256} S_8 w_2^{256} S_8 w_2^{256} S_8^3 w_2^{256} S_8^3 = 1\).
Observation 17. One needs to warn that for the situation \( v(N) = 8 \) 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 \( S_{2^2(N)} \) commutes with \( S_{3^2(N)} \). Moreover \( S_2 \) commutes with any element from lemma 3. 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 III:

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 \( w_{p^n} S_3 = S_3^2 w_{p^n} \).

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 \( w_{p^n} S_4 = S_4^3 w_{p^n} \).

3. Let \( p \) be coprime with 2 and \( 8 | v(N) \). Then, \( w_{p^n} S_8 = S_8^k w_{p^n} \) 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).

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·liptiques. Tesina Universitat Autònoma de Barcelona. September 1997. Find a copy at [http://mat.uab.es/~francesc/publicac.html](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, 369-368 (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