Open Mathematics **Open Access**

Research Article

Bo-Hae Im, Daeyeol Jeon*, and Chang Heon Kim

Normalizers of intermediate congruence subgroups of the Hecke subgroups

DOI 10.1515/math-2017-0066
Received January 20, 2017; accepted April 26, 2017.

Abstract: For a square-free positive integer N, we study the normalizer of $\Gamma_\Delta(N)$ in $\mathrm{PSL}_2(\mathbb{R})$ and investigate the group structure of its quotient by $\Gamma_\Delta(N)$ under certain conditions.

Keywords: Normalizers, Hecke subgroups, Modular curves, Automorphism groups

MSC: 20H05, 19B37, 11G18

1 Introduction

For each positive integer N, we let $\Gamma_0(N)$ be the Hecke subgroup of the full modular group $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,|\, c \equiv 0 \pmod{N} \right\}.$$

We denote by $\mathfrak{N}_0(N)$ the normalizer of $\Gamma_0(N)$ in $\mathrm{PSL}_2(\mathbb{R})$. Newman [14, 17, 18] obtained a result about $\mathfrak{N}_0(N)$. This normalizer has acquired its importance in several areas of mathematics. For instance, the genus zero subgroups of $\mathfrak{N}_0(N)$ have a mysterious correspondence to the conjugacy classes of the monster simple group [6, 7]. Moreover, the normalizer $\mathfrak{N}_0(N)$ played an important role in the work on Weierstrass points on the modular curve $X_0(N)$ associated to $\Gamma_0(N)$ [14] and on ternary quadratic forms [15].

The automorphism group of the modular curve $X_0(N)$ is closely related to the quotient group $\mathfrak{N}_0(N)/\Gamma_0(N)$. Kenku and Momose [12] determined the full automorphism group for $X_0(N)$ with $N \neq 63$ and Elkies [8] completed the problem by treating the case $N = 63$. And recently Harrison [9] corrected the statement in [12] for the case $N = 108$. According to their results, there are exceptional automorphisms (not coming from the elements in the quotient group $\mathfrak{N}_0(N)/\Gamma_0(N)$) only for the case $N = 37, 63, 108$. Meanwhile, as for the quotient group $\mathfrak{N}_0(N)/\Gamma_0(N)$, Atkin and Lehner [2] stated its structure without proof. But the list in [2] turned out to contain several errors and later was corrected by Akbas and Singerman [1] and Bars [4].

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and $X(\Gamma)$ the modular curve associated to Γ. Motivated by the importance of the normalizer of $\Gamma_0(N)$ and the automorphism group of $X_0(N)$, there have been several works on the normalizer of Γ and the automorphism group of $X(\Gamma)$. When $\Gamma = \Gamma_1(N)$, the group of elements of $\mathrm{SL}_2(\mathbb{Z})$ that are congruent to $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ modulo N, the third author and Koo [11], and Lang [13] independently determined its normalizer in $\mathrm{PSL}_2(\mathbb{R})$. Furthermore for the modular curve $X_1(N) := X(\Gamma_1(N))$ with N square-free, Momose [16] proved that there are no exceptional automorphisms. Let $\Gamma(N)$ be the principal congruence subgroup which consists of the elements of $\mathrm{SL}_2(\mathbb{Z})$ that are congruent to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ modulo N, and let $X(N) := X(\Gamma(N))$. Recently

Bo-Hae Im: Department of Mathematical Sciences, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, South Korea, E-mail: bhim@kaist.ac.kr
***Corresponding Author: Daeyeol Jeon:** Department of Mathematics education, Kongju National University, 56 Gongjudaehak-ro, Gongju-si, Chungcheongnam-do 314-701, South Korea, E-mail: dyjeon@kongju.ac.kr
Chang Heon Kim: Department of Mathematics, Sungkyunkwan University, Suwon 440-746, South Korea, E-mail: chhkim@skku.edu

Bars, Knotogeorgis, and Xarles [5] considered the automorphism group of $X(N)$ and proved that it is equal to the group $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$, which is isomorphic to the normalizer of $\Gamma(N)$ in $\mathrm{PSL}_2(\mathbb{R})$ modulo $\pm\Gamma(N)$.

Let $\Gamma_\Delta(N)$ be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$\Gamma_\Delta(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \bmod N, (a \bmod N) \in \Delta \right\},$$

where Δ is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ and we always assume that $-1 \in \Delta$. We note that $\Gamma_\Delta(N)$ is an intermediate subgroup between $\Gamma_0(N)$ and $\Gamma_1(N)$. In particular, if $\Delta = (\mathbb{Z}/N\mathbb{Z})^*$ (respectively $\Delta = \{\pm 1\}$), then we have $\Gamma_\Delta(N) = \Gamma_0(N)$ (respectively $\Gamma_\Delta(N) = \pm\Gamma_1(N)$). In this article, we are concerned with the normalizer of $\Gamma_\Delta(N)$ in $\mathrm{PSL}_2(\mathbb{R})$ and its underlying group structures.

After the preprint was ready, we recognized the results in the paper [19], which independently obtained a criterion of normalizers (compare Corollary 2.6 of that reference with our Theorem 2.1). The reference aims only for determining the normalizers, while we also investigate the structure of quotient groups in case N is square-free.

This paper is organized as follows. In Section 2 we investigate the normalizer $\mathfrak{N}_\Delta(N)$ of $\Gamma_\Delta(N)$ in $\mathrm{PSL}_2(\mathbb{R})$. In Section 3 we find the group structures of the quotient group $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ for square-free N when the exact sequence

$$1 \to \Gamma_0(N)/\Gamma_\Delta(N) \xrightarrow{f} \mathfrak{N}_\Delta(N)/\Gamma_\Delta(N) \xrightarrow{g} \mathfrak{N}_\Delta(N)/\Gamma_0(N) \to 1 \tag{1}$$

splits. In fact, the sequence (1) is not well-defined in general, since $\Gamma_0(N)$ will not always be a normal subgroup of $\mathfrak{N}_\Delta(N)$. However, $\Gamma_0(N)$ is a normal subgroup of $\mathfrak{N}_\Delta(N)$ for square-free N. We prove that in this case,

$$\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N) \cong ((\mathbb{Z}/N\mathbb{Z})^*/\Delta) \rtimes (\mathbb{Z}/2\mathbb{Z})^r,$$

where r is the number of distinct prime divisors of N, and we give some examples of such quotient groups for nontrivial Δ. Finally, in Section 4 we study the case of composite N, which is a product of two distinct primes and find out what happens in the cases when the exact sequence (1) does not split. In these cases we investigate the group structures of the quotient groups $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ by describing their group presentations (see Theorem 4.1, Theorem 4.2, Theorem 4.3, Theorem 4.4, and Remark 4.6).

We use the following notations through this paper.

Notations.

1. For integers $a, b \in \mathbb{Z}$ such that $a \neq 0$, we use $a \parallel b$ to mean that $a|b$ and $\gcd(a, \frac{b}{a}) = 1$.
2. For a prime p and an integer a such that $\gcd(a, p) = 1$, we let $\left(\frac{a}{p}\right)$ denote the Legendre symbol if $p \neq 2$, and we define $\left(\frac{a}{2}\right) = 1$ conventionally.
3. By abuse of notation, for an integer a, we use $a \in \Delta$ to mean that the congruence class of a belongs to Δ.
4. For a positive integer n and an integer a prime to n, we let $\mathrm{ord}_n(a)$ denote the order of a modulo n, i.e. the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

2 Normalizers of intermediate congruences subgroups

Let σ^2 be the largest square dividing N so that $q := \frac{N}{\sigma^2}$ is square-free. Define ϵ to be the *gcd* of the elements in the set

$$\left\{ a - d \mid \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_\Delta(N) \right\},$$

and define $h = \gcd(\sigma, \epsilon)$.

Let $\mathfrak{N}_\Delta(N)$ be the normalizer of $\Gamma_\Delta(N)$. Note that

$$\mathrm{PSL}_2(\mathbb{R}) \cong \mathrm{SL}_2(\mathbb{R})/\{\pm I\} \cong \mathrm{PGL}_2^+(\mathbb{R}).$$

We can modify Theorem 1 of [14] as follows:

Theorem 2.1. *A matrix M is contained in $\mathfrak{N}_\Delta(N)$ only if M is represented in $\mathrm{PGL}_2^+(\mathbb{R})$ as*

$$M = \begin{pmatrix} Qx & \frac{y}{h} \\ \frac{N}{h}z & Qw \end{pmatrix}$$

where $Q||\frac{N}{h^2}$ and $x, y, z, w \in \mathbb{Z}$ such that $\det(M) = Q$.

If $h = 1$, then we denote M by W_Q in Theorem 2.1. Such a matrix W_Q is contained in the normalizer of the group $\Gamma_0(N)$ and it defines a unique automorphism on the modular curve $X_0(N)$ which is called *the Atkin-Lehner involution*. However, the uniqueness doesn't hold for general congruence groups $\Gamma_\Delta(N)$.

We investigate when W_Q belongs to $\mathfrak{N}_\Delta(N)$. Each $\gamma \in \Gamma_\Delta(N)$ is of the form

$$\begin{pmatrix} a & b \\ c & \bar{a} \end{pmatrix}$$

where $a \in \Delta$ and $\bar{a}$ is an integer with $a\bar{a} \equiv 1 \pmod N$. For $W_Q = \begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix}$ and $\gamma = \begin{pmatrix} a & b \\ c & \bar{a} \end{pmatrix} \in \Gamma_\Delta(N)$, one can easily compute that $W_Q \gamma W_Q^{-1} \in \Gamma_\Delta(N)$ if and only if the following condition holds:

$$Qxwa - \frac{N}{Q}yz\bar{a} \in \Delta. \tag{2}$$

From $Q^2xw - Nyz = Q$, we have that $Qxw - \frac{N}{Q}yz = 1$ and hence the following holds:

$$Qxwa - \frac{N}{Q}yz\bar{a} \equiv \begin{cases} a \pmod{\frac{N}{Q}}, \\ \bar{a} \pmod Q. \end{cases}$$

Note that $\bar{a}$ is the multiplicative inverse of a modulo Q. Now we define an isomorphism $t_Q : (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/N\mathbb{Z})^*$ by

$$t_Q(a) \equiv \begin{cases} a \pmod{\frac{N}{Q}}, \\ \bar{a} \pmod Q. \end{cases}$$

Since $(\mathbb{Z}/N\mathbb{Z})^*$ is isomorphic to the direct product $(\mathbb{Z}/Q\mathbb{Z})^* \times (\mathbb{Z}/\frac{N}{Q}\mathbb{Z})^*$, one can show that the condition (2) holds if and only if $t_Q(a) \in \Delta$. Therefore we have the following result:

Proposition 2.2. *$W_Q \in \mathfrak{N}_\Delta(N)$ if and only if $t_Q(\Delta) = \Delta$.*

If $M \in \mathfrak{N}_\Delta(N)$, then

$$M \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} M^{-1} = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_\Delta(N). \tag{3}$$

Taking the trace, we see that $2 = a + d$. Since d is a multiplicative inverse of a in $(\mathbb{Z}/N\mathbb{Z})^*$,

$$(a-1)^2 \equiv 0 \pmod N,$$

and hence

$$a \equiv 1 \pmod{\sigma q}. \tag{4}$$

Now consider the natural homomorphism

$$\phi : (\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\} \to (\mathbb{Z}/\sigma q\mathbb{Z})^*/\{\pm 1\}. \tag{5}$$

Then $\ker(\phi) = \{1, \sigma q + 1, 2\sigma q + 1, ..., (\sigma - 1)\sigma q + 1\}$ is the cyclic group of order σ generated by $\sigma q + 1$. Thus equation (4) is equivalent to that $a \in \ker(\phi)$.

In [11], the third author and Koo prove that $\mathfrak{N}_\Delta(N)$ is generated by the elements of $\Gamma_0(N)$ and W_Q for all $Q||N$ when $N \neq 4$ and $\Delta = \{\pm 1\}$, and its proof mainly depends on the following two conditions:

$$M \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} M^{-1} \in \pm\Gamma_1(N), \tag{6}$$

$$M \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} M^{-1} \in \pm\Gamma_1(N). \tag{7}$$

If $(\Delta/\{\pm 1\}) \cap \ker(\phi) = \{1\}$ holds, then Eq. (3) is the same as Eq. (6). Similarly Eq. (7) is the same as the following condition:

$$M \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} M^{-1} \in \Gamma_\Delta(N).$$

By exactly the same arguments as those in [11], we have the following result:

Theorem 2.3. *If $(\Delta/\{\pm 1\}) \cap \ker(\phi) = \{1\}$, then $\mathfrak{N}_\Delta(N)$ is generated by the elements of $\Gamma_0(N)$ and W_Q with $t_Q(\Delta) = \Delta$ for each $Q \parallel N$.*

From Theorem 2.3, one can easily obtain the following result:

Corollary 2.4. *If N is square-free, then $\mathfrak{N}_\Delta(N)$ is generated by the elements of $\Gamma_0(N)$ and W_Q with $t_Q(\Delta) = \Delta$ for $Q|N$.*

Proof. If N is square-free, then ϕ defined in (5) is an isomorphism, and hence $\ker(\phi)$ is trivial. □

3 The group structures of the quotient group $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ for square-free N: the split case

In this section, we assume that N is square-free and for simplicity we assume that $t_Q(\Delta) = \Delta$ for all $Q||N$. As the main result of this section, we find a condition for Δ so that the exact sequence (1) splits. For that, we state a well-known result as follows:

Lemma 3.1.

$$\Gamma_0(N)/\Gamma_\Delta(N) \cong (\mathbb{Z}/N\mathbb{Z})^*/\Delta.$$

Proof. For an integer a prime to N, let $[a]$ denote a matrix represented by $\gamma \in \Gamma_0(N)$ such that $\gamma \equiv \left(\begin{smallmatrix} a & * \\ 0 & * \end{smallmatrix}\right) \mod N$. Consider the natural surjective homomorphism

$$\phi : \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*/\Delta$$

defined by $\phi([a]) = a$. One can prove that the kernel of ϕ is equal to $\Gamma_\Delta(N)$, and the result follows from the first isomorphism theorem. □

By Corollary 2.4, $\mathfrak{N}_\Delta(N)$ is the same as $\mathfrak{N}_0(N)$ for square-free N. Then the Atkin–Lehner involutions modulo $\Gamma_0(N)$ generate $\mathfrak{N}_\Delta(N)/\Gamma_0(N)$ which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ where r is the number of prime divisors of N. Now we investigate when the exact sequence (1) splits, in which case, we have the following isomorphism:

$$\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N) \cong \left((\mathbb{Z}/N\mathbb{Z})^*/\Delta\right) \rtimes (\mathbb{Z}/2\mathbb{Z})^r.$$

For that we should find a group homomorphism $h : \mathfrak{N}_\Delta(N)/\Gamma_0(N) \to \mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ so that $g \circ h$ is the identity map, where g appears in (1). Note that the generators of $\mathfrak{N}_\Delta(N)/\Gamma_0(N)$ are the Atkin-Lehner involutions W_p for

each prime divisor p of N, and so are their preimages of g in (1). Therefore the exact sequence (1) splits if and only if there exists an elementary abelian 2-subgroup of $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ generated by W_p with prime divisors p of N. Put $N = p_1 p_2 \cdots p_r$ with distinct primes $p_1, p_2, ..., p_r$. Then the exact sequence (1) splits if and only if one can find W_{p_i} for all i so that the following two conditions hold:

$$\left(\frac{1}{\sqrt{p_i}} W_{p_i}\right)^2 \in \Gamma_\Delta(N), \tag{8}$$

$$W_{p_i} W_{p_j} W_{p_i}^{-1} W_{p_j}^{-1} \in \Gamma_\Delta(N), \text{ for any } i, j. \tag{9}$$

We give necessary and sufficient conditions for the splitting property of the sequence (1) in turn when $r = 1, 2$ and $r \geq 3$.

3.1 The case when $N = p$

First, we consider the case when N is a prime p.

In this case W_p is always contained in $\mathfrak{N}_\Delta(N)$, and hence we have the following result:

Theorem 3.2. *Let $\Delta \leq (\mathbb{Z}/p\mathbb{Z})^*$ then the sequence* (1) *splits and*

$$\mathfrak{N}_\Delta(p)/\Gamma_\Delta(p) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } m = 1, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \text{if } m = 2, \\ D_m, & \text{if } m \geq 3, \end{cases}$$

where $m = \frac{p-1}{|\Delta|}$ and D_m is a dihedral group of order $2m$.

Proof. One can easily check that $\left(\frac{1}{\sqrt{p}} W_p\right)^2 = -1$, and hence the conditions (8) and (9) hold. Since $((\mathbb{Z}/p\mathbb{Z})^*/\Delta)$ is a cyclic group of order m, $\mathfrak{N}_\Delta(p)/\Gamma_\Delta(p) \cong \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Also one can easily prove that the following holds:

$$[a] W_p \equiv W_p [a^{-1}] \pmod{p}.$$

Our result comes from this relation. □

3.2 The case when $N = pq$

Next, we consider the case when $N = pq$ for two distinct primes p and q.

Theorem 3.3. *Let $\Delta \leq (\mathbb{Z}/pq\mathbb{Z})^*$. Then, the sequence* (1) *splits if and only if there exist $a, b \in \Delta$ such that $\left(\frac{aq}{p}\right) = 1$, $a \equiv -1 \pmod{q}$, $\left(\frac{bp}{q}\right) = 1$, and $b \equiv -1 \pmod{p}$. In this case,*

$$\mathfrak{N}_\Delta(pq)/\Gamma_\Delta(pq) \cong ((\mathbb{Z}/pq\mathbb{Z})^*/\Delta) \rtimes (\mathbb{Z}/2\mathbb{Z})^2,$$

which is of order $4m$ where $m = \frac{(p-1)(q-1)}{|\Delta|}$.

Proof. Suppose there exist $a, b \in \Delta$ such that $\left(\frac{aq}{p}\right) = 1$, $a \equiv -1 \pmod{q}$, $\left(\frac{bp}{q}\right) = 1$, and $b \equiv -1 \pmod{p}$. Then, there exist $x, x' \in \mathbb{Z}$ such that

$$a \equiv \begin{cases} qx'^2 & (\text{mod } p) \\ -1 & (\text{mod } q), \end{cases} \quad b \equiv \begin{cases} -1 & (\text{mod } p) \\ px^2 & (\text{mod } q). \end{cases}$$

Note that $\gcd(x, q) = 1$ and $\gcd(x', p) = 1$. Hence there exist $y, z, y', z' \in \mathbb{Z}$ such that

$$(px)z - qy = 1, \ (qx')z' - py' = 1.$$

Then by the uniqueness of a and b modulo pq,

$$a \equiv qx'^2 + py' \pmod{pq},\ b \equiv px^2 + qy \pmod{pq}.$$

Let

$$W_p = \begin{pmatrix} px & y \\ pq & pz \end{pmatrix},\ W_q = \begin{pmatrix} qx' & y' \\ pq & qz' \end{pmatrix}.$$

Then $\det(W_p) = p$ and $\det(W_q) = q$ and the first component of $(\frac{1}{\sqrt{p}}W_p)^2$ is $px^2 + qy \equiv b \in \Delta$ and the first component of $(\frac{1}{\sqrt{q}}W_q)^2$ is $qx'^2 + py' \equiv a \in \Delta$. Hence the condition (8) holds.

Note that if we let $a', b' \in \mathbb{Z}$ such that

$$a' \equiv \begin{cases} qz'^2 & (\mathrm{mod}\ p) \\ -1 & (\mathrm{mod}\ q), \end{cases} \quad b' \equiv \begin{cases} -1 & (\mathrm{mod}\ p) \\ pz^2 & (\mathrm{mod}\ q), \end{cases}$$

then $a' \equiv a^{-1} \pmod{pq}$ and $b' \equiv b^{-1} \pmod{pq}$, so $a', b' \in \Delta$. Now the first component of $W_pW_qW_p^{-1}W_q^{-1}$ is

$$pq(xx'+y)(zz'+y) + (pxy' + qyz')(-qz' - px) \equiv \begin{cases} qz'^2 \equiv a' \equiv -a'b & (\mathrm{mod}\ p) \\ px^2 \equiv b \equiv -a'b & (\mathrm{mod}\ q) \end{cases},$$

hence it is $-a'b \pmod{pq}$, which is in Δ since $a', b, -1 \in \Delta$. So the condition (9) holds. Hence the sequence (1) splits.

Conversely, suppose the sequence (1) splits. Then there exist $W_p = \begin{pmatrix} px & y \\ pqz & pw \end{pmatrix}$ and $W_q = \begin{pmatrix} qx' & y' \\ pqz' & qw' \end{pmatrix}$ satisfying the conditions (8) and (9). By a similar computations of the first components of $\left(\frac{1}{\sqrt{p}}W_p\right)^2$ and $\left(\frac{1}{\sqrt{q}}W_q\right)^2$, we can show that there exist $a, b \in \Delta$ such that $\left(\frac{aq}{p}\right) = 1$, $a \equiv -1 \pmod{q}$, $\left(\frac{bp}{q}\right) = 1$, and $b \equiv -1 \pmod{p}$.

In this case, by Lemma 3.1 and the exact sequence (1),

$$\mathfrak{N}_\Delta(pq)/\Gamma_\Delta(pq) \cong \Gamma_0(pq)/\Gamma_\Delta(pq) \rtimes \mathfrak{N}_\Delta(pq)/\Gamma_0(pq) \cong ((\mathbb{Z}/pq\mathbb{Z})^*/\Delta) \rtimes (\mathbb{Z}/2\mathbb{Z})^2. \qquad \square$$

Corollary 3.4. *Suppose p and q are distinct two primes with $p < q$. If $\Delta = \{\pm 1\} \leq (\mathbb{Z}/pq\mathbb{Z})^*$, then the sequence (1) splits if and only if*
(1) *for $p = 2$ and an odd prime q, $q \equiv 1, 3, 7 \pmod 8$ or*
(2) *for distinct odd primes p and q, $p \equiv q \equiv 1 \pmod 4$ and $\left(\frac{q}{p}\right) = 1$.*

Proof. By using the quadratic reciprocity law, we can prove that the conditions (1) and (2) are equivalent to that

$$\begin{cases} \left(\frac{2}{q}\right) = 1 \text{ or } \left(\frac{-2}{q}\right) = 1, & \text{if } p = 2 \\ \left(\frac{-q}{p}\right) = \left(\frac{-p}{q}\right) = 1, & \text{otherwise.} \end{cases} \tag{10}$$

It is based on a having to be -1, and the same value must be attained by b if $p > 2$. $\square$

Remark 3.5. *There exist infinitely many pairs of distinct primes satisfying conditions (1) and (2) of Corollary 3.4. For example, $p = 5$ and $q \equiv 1$ or $9 \pmod{20}$ satisfy (10).*

3.3 The case when N is a square-free integer with more than 2 prime divisors

Theorem 3.6. *Let $p_1, \ldots, p_r$ be distinct primes where $r \geq 3$ and let $N = \prod_{i=1}^{r} p_i$. Let $\Delta \leq (\mathbb{Z}/N\mathbb{Z})^*$.*

Then, the sequence (1) *splits if and only if the following holds;*

(1) *For $i = 1, \dots, r$, the class modulo N of the elements $a_i \in \mathbb{Z}$ satisfying*

$$\begin{cases} a_i \equiv -1 \pmod{p_i} \\ \left(\frac{a_i p_i}{p_k}\right) = 1, \text{ for each } k \neq i, \end{cases}$$

lies in Δ.

(2) *For each $1 \leq i < j \leq r$, the class modulo N of the elements $b_{ij} \in \mathbb{Z}$ satisfying*

$$b_{ij} \equiv \begin{cases} a_j^{-1} & \pmod{p_i} \\ a_i & \pmod{p_j} \\ 1 & \pmod{p_k} \text{ for all } k \neq i, j, \end{cases}$$

lies in Δ.

In this case,

$$\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N) \cong ((\mathbb{Z}/N\mathbb{Z})^*/\Delta) \rtimes (\mathbb{Z}/2\mathbb{Z})^r,$$

which is of order $2^r m$ where $m = \frac{\prod_{i=1}^{r}(p_i - 1)}{|\Delta|}$.

Proof. Suppose there exist $a_i, b_{ij} \in \Delta$ satisfying conditions (1) and (2). Then by the condition (1), for each $i = 1, \dots, r$, there exist $x_i \in \mathbb{Z}$ such that

$$a_i \equiv \begin{cases} -1 & \pmod{p_i} \\ p_i x_i^2 & \pmod{\frac{N}{p_i}}. \end{cases}$$

Note that $\gcd(p_i x_i, \frac{N}{p_i}) = 1$ since $a_i \in \Delta$. So there exist $y_i, z_i \in \mathbb{Z}$ such that

$$(p_i x_i) z_i - \frac{N}{p_i} y_i = 1.$$

For each $i = 1, \dots, r$, let

$$W_{p_i} = \begin{pmatrix} p_i x_i & y_i \\ N & p_i z_i \end{pmatrix}.$$

Then $\det(W_{p_i}) = p_i$, and the first component of $(\frac{1}{\sqrt{p_i}} W_{p_i})^2$ is

$$p_i x_i^2 + \frac{N}{p_i} y_i \equiv \begin{cases} \frac{N}{p_i} y_i \equiv -1 \equiv a_i & \pmod{p_i} \\ p_i x_i^2 \equiv a_i & \pmod{p_k} \text{ for all } k \neq i, \end{cases}$$

which is in Δ by condition (1). Hence the condition (8) holds.

Note that if we let $a_i' \in \mathbb{Z}$ such that

$$a_i' \equiv \begin{cases} -1 & \pmod{p_i} \\ p_i z_i^2 & \pmod{\frac{N}{p_i}}, \end{cases}$$

then $a_i' \equiv a_i^{-1} \pmod{N}$. Now, for each $1 \leq i < j \leq r$, the first component of $W_{p_i} W_{p_j} W_{p_i}^{-1} W_{p_j}^{-1}$ is

$$(p_i p_j x_i x_j + N y_i)\Big(z_i z_j + \frac{N}{p_i p_j} y_i\Big) - (p_i x_i y_j + p_j y_i z_j)\Big(\frac{N}{p_i} z_j + \frac{N}{p_j} x_i\Big)$$

$$\equiv \begin{cases} -p_j z_j^2 (\frac{N}{p_i} y_i) \equiv p_j z_j^2 \equiv a_j' \equiv a_j^{-1} \equiv b_{ij} & \pmod{p_i} \\ -p_i x_i^2 (\frac{N}{p_j} y_j) \equiv p_i x_i^2 \equiv a_i \equiv b_{ij} & \pmod{p_j} \\ (p_i x_i z_i)(p_j x_j z_j) \equiv 1 \equiv b_{ij} & \pmod{p_k} \text{ for all } k \neq i, j, \end{cases}$$

which is in Δ by condition (2). Thus the condition (9) holds, and hence the sequence (1) splits.

Suppose the sequence (1) splits. As explained in the proof of Theorem 3.3, we can show that the conditions (1) and (2) hold.

In this case, again by Lemma 3.1 and the exact sequence (1),

$$\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N) \cong \Gamma_0(N)/\Gamma_\Delta(N) \rtimes \mathfrak{N}_\Delta(N)/\Gamma_0(N) \cong ((\mathbb{Z}/N\mathbb{Z})^*/\Delta) \rtimes (\mathbb{Z}/2\mathbb{Z})^r. \qquad \square$$

Remark 3.7. *For $N = p_1 p_2 \cdots p_r$ with $r \geq 3$, if $\Delta = \{\pm 1\} \leq (\mathbb{Z}/N\mathbb{Z})^*$, then the sequence (1) does not split since otherwise the condition (1) in Theorem 3.6 implies that $a_i \equiv -1 \pmod N$ for all i, which shows that there is no $b_{ij} \in \{\pm 1\}$ satisfying the condition (2) in Theorem 3.6. This is a different phenomenon from the case when $r = 1$ or 2 referring to Theorem 3.2 and Corollary 3.4.*

Now we give some examples in the split case.

Example 3.8. *Let $N = 21 = 3 \cdot 7$ and $\Delta = \{\pm 1, \pm 8\} \leq (\mathbb{Z}/N\mathbb{Z})^*$. In this case, the maps t_3 and t_7 are the identity map, and so they preserve Δ. Indeed, Δ consists precisely of those residues that are congruent to ± 1 modulo 7; hence it will make it immediately evident that Δ is a subgroup and that it is preserved under the involutions t_3 and t_7. If we let $a = -8$ and $b = -1$, then a and b satisfy the conditions of Theorem 3.3 when we take $p = 3$ and $q = 7$, and hence*

$$\mathfrak{N}_\Delta(21)/\Gamma_\Delta(21) \cong (\mathbb{Z}/3\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})^2.$$

More precisely, we take $[2] = \left(\begin{smallmatrix} 2 & 1 \\ 21 & 11 \end{smallmatrix}\right)$, $W_3 = \left(\begin{smallmatrix} 9 & -4 \\ 21 & -9 \end{smallmatrix}\right)$ and $W_7 = \left(\begin{smallmatrix} 7 & 2 \\ 21 & 7 \end{smallmatrix}\right)$. Then $\langle [2] \rangle = \mathbb{Z}/3\mathbb{Z}$ and $\langle W_3, W_7 \rangle = (\mathbb{Z}/2\mathbb{Z})^2$, and we can check that

$$\begin{aligned} [2]W_3 &= W_3[2], \\ [2]W_7 &= W_7[2]^{-1}, \\ [2]W_3W_7 &= W_3W_7[2]^{-1}, \end{aligned}$$

i.e. exactly one involution of $(\mathbb{Z}/2\mathbb{Z})^2$ operates tirivally on $\mathbb{Z}/3\mathbb{Z}$, and the other two operate nontrivially on $\mathbb{Z}/3\mathbb{Z}$. Thus $[2]W_3$ has order 6 and $W_7([2]W_3) = ([2]W_3)^{-1}W_7$ in $\mathfrak{N}_\Delta(21)/\Gamma_\Delta(21)$, and hence $\mathfrak{N}_\Delta(21)/\Gamma_\Delta(21)$ is isomorphic to the dihedral group D_6 of order 12.

Example 3.9. *Let $N = 105 = 3 \cdot 5 \cdot 7$ and $p_1 = 3, p_2 = 5, p_3 = 7$. Let $\Delta = \{\pm 1, \pm 8, \pm 13, \pm 22, \pm 29, \pm 34, \pm 41, \pm 43\}$. As mentioned in Example 3.8, Δ consists precisely of those residues that are congruent to ± 1 modulo 7; hence t_3, t_5 and t_7 preserve Δ. Put $a_1 = -43, a_2 = -1, a_3 = 13$, then $b_{12} = -13, b_{23} = -8, b_{13} = -29$, and they are all contained in Δ. From our criterion of Theorem 3.6, we can conclude that*

$$\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N) \cong \mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^3.$$

4 The group structures of the quotient group $\mathfrak{N}_\Delta(pq)/\Gamma_\Delta(pq)$ for primes p, q: the non-split case

Usually it is not easy to determine the group structure of $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ for N, if the short exact sequence (1) does not split. In this section we find the group structure of $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ when $N = pq$ with distinct primes p, q for which the exact sequence (1) does not split, and $\Delta = \{\pm 1\} \leq (\mathbb{Z}/N\mathbb{Z})^*$.

If we take

$$W_p = \begin{pmatrix} px_1 & y_1 \\ N & pz_1 \end{pmatrix}, \ W_q = \begin{pmatrix} qx_2 & y_2 \\ N & qz_2 \end{pmatrix},$$

then one can easily check that

$$\left(\frac{1}{\sqrt{p}}W_p\right)^2 = [px_1^2 + qy_1], \ \left(\frac{1}{\sqrt{q}}W_q\right)^2 = [qx_2^2 + py_2]. \tag{11}$$

Put $w_1 = px_1^2 + qy_1$ and $w_2 = qx_2^2 + py_2$. Then from the fact that $\det(W_p) = p$ and $\det(W_q) = q$ the following holds:

$$w_1 \equiv \begin{cases} -1 \pmod p \\ px_1^2 \pmod q, \end{cases} \quad w_2 \equiv \begin{cases} qx_2^2 \pmod p \\ -1 \pmod q. \end{cases} \tag{12}$$

By using the fact that $\det(W_p) = p$ and $\det(W_q) = q$ again, we can show that the $(1,1)$-component of $\frac{1}{N}W_qW_pW_qW_p$ is as follows:

$$\frac{1}{N}W_qW_pW_qW_p[1,1] \equiv qy_1 + py_2 \equiv \begin{cases} -1 \pmod{p}, \\ -1 \pmod{q}, \end{cases} \tag{13}$$

and hence $\frac{1}{N}W_qW_pW_qW_p[1,1] \equiv -1 \pmod{N}$, which shows its triviality in the quotient group $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$.

Now as the complement of Corollary 3.4, consider the non-split cases for $N = pq$ with distinct two primes p, q which can be divided into the following five sub-cases depending on the congruences of p and q:

(i) $p = 2$ and $q \equiv 5 \pmod 8$.
(ii) $p \equiv q \equiv 3 \pmod 4$, in which case we choose p and q such that $\left(\frac{p}{q}\right) = -1$.
(iii) $p \equiv 1$ and $q \equiv 3 \pmod 4$ with $\left(\frac{p}{q}\right) = -1$.
(iv) $p \equiv 1$ and $q \equiv 3 \pmod 4$ with $\left(\frac{p}{q}\right) = 1$.
(v) $p \equiv q \equiv 1 \pmod 4$ with $\left(\frac{p}{q}\right) = -1$.

For the non-split case for $N = pq$, we have the following group presentations of the quotient group $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ where $\Delta = \{\pm 1\}$.

Theorem 4.1. *Let $N = 2q$ where q is a prime with $q \equiv 5 \pmod 8$. Then,*

$$\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N) \cong \langle a, b \mid a^{q-1} = b^2 = (ab)^2 = 1\rangle.$$

In this case, $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ is isomorphic to the Dihedral group D_{q-1} of order $2(q-1)$.

Proof. From (10) and Euler's criterion, we have

$$\left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} \equiv -1 \pmod{q}. \tag{14}$$

Let $d = \mathrm{ord}_q(2)$. Then $\frac{q-1}{d}$ should be odd. Suppose that $\frac{q-1}{d}$ is even, then $d \mid \frac{q-1}{2}$ which is a contradiction to (14). Take a primitive root $r \in (Z/N\mathbb{Z})^*$ of q so that $2 \equiv r^{\frac{q-1}{d}} \pmod q$, and put x_1 to be an integer satisfying $x_1 \equiv r^m \pmod q$ where m is the integer with $\frac{q-1}{d} + 2m = 1$. Then $2x_1^2 \equiv r \pmod q$, and $\mathrm{ord}_q(2x_1^2) = q-1$. If we take $W_2 = \begin{pmatrix} 2x_1 & y_1 \\ N & 2z_1 \end{pmatrix}$ for some y_1, z_1, and let $w_1 = 2x_1^2 + qy_1$, then $W_2^2 = [w_1]$ in $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ by (11). Since $\mathrm{ord}_N(w_1) = \mathrm{ord}_q(2x_1^2) = q-1$ and $w_1^{\frac{q-1}{2}} \equiv -1 \pmod N$, the order of W_2 in $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ is equal to $q-1$. We recall that we work modulo $\Delta = \{\pm 1\}$, so that the order $q-1$ of w_1 means an order of $\frac{q-1}{2}$ of W_2^2, whence an order of $q-1$ of W_2 itself.

If we take $W_q = \begin{pmatrix} qx_2 & y_2 \\ N & qz_2 \end{pmatrix}$ and let $w_2 = qx_2^2 + 2y_2$, then $W_q^2 = [w_2]$ in $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ by (11). Since $w_2 \equiv -1 \pmod N$ from (12), the order of W_q in $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ is equal to 2.

Since w_1 generate $(\mathbb{Z}/N\mathbb{Z})^*$, $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ can be generated by W_2 and W_q. From (13) we know that $(W_2W_q)^2 = 1$.

Let $G = \langle a, b \mid a^{q-1} = b^2 = (ab)^2 = 1\rangle$. Then the map $a \mapsto W_2$ and $b \mapsto W_q$ can be extended to a unique homomorphism from G to $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ because W_2 and W_q satisfy all the relations in G if we replace a and b by W_2 and W_q . Clearly, the order $|G|$ of G is equal to $2(q-1)$ which is the same as $|\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)|$. Thus G is isomorphic to $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$. □

Theorem 4.2. *Let $N = pq$ where p and q are primes satisfying one of the following:*
(a) $p \equiv q \equiv 3 \pmod 4$*, in which case we choose p and q such that* $\left(\frac{p}{q}\right) = -1$.

(b) $p \equiv 1 \pmod 4$ *and* $q \equiv 3 \pmod 4$ *with* $\left(\frac{p}{q}\right) = -1$.
Then,

$$\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N) \cong \langle a, b \mid a^{q-1} = b^{2(p-1)} = (ba)^2 = ba^2b^{-1}a^2 = 1\rangle.$$

Proof. Let us consider the case when $p \equiv q \equiv 3 \pmod 4$ by choosing the notation for p and q such that $\left(\frac{p}{q}\right) = -1$. By the same reason as in the proof of Theorem 4.1, $\frac{q-1}{d_1}$ is odd where $d_1 := \mathrm{ord}_q(p)$. Thus we can take a primitive root $r \in (Z/N\mathbb{Z})^*$ of q and an integer x_1 so that $px_1^2 \equiv r \pmod q$, and hence $\mathrm{ord}_q(px_1^2) = q-1$. Take $W_p = \begin{pmatrix} px_1 & y_1 \\ N & pz_1 \end{pmatrix}$ for some y_1, z_1, and let $w_1 = px_1^2 + qy_1$. By the Chinese Remainder Theorem, we know that

$$(\mathbb{Z}/N\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*,$$

and hence $\mathrm{ord}_N(w_1) = \mathrm{lcm}(\mathrm{ord}_q(px_1^2), \mathrm{ord}_p(qy_1)) = \mathrm{lcm}\{q-1, 2\} = q-1$ by (12). From (12), we also know that $w_1^{\frac{q-1}{2}} \equiv -1 \pmod N$ because $\frac{q-1}{2}$ is odd, and hence the order of W_p in $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ is equal to $q-1$.

On the other hand, $\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \equiv 1 \pmod p$. Thus $d_2 := \mathrm{ord}_p(q) | \frac{p-1}{2}$, and $\frac{p-1}{d_2}$ is even. Take a primitive root $s \in (Z/N\mathbb{Z})^*$ of p so that $q \equiv s^{\frac{q-1}{d_2}} \pmod p$, and put x_2 to be an integer satisfying $x_2 \equiv s^{m_2} \pmod p$ where m_2 is the integer with $\frac{q-1}{d_1} + 2m_2 = 2$. Then $px_2^2 \equiv s^2 \pmod p$, and $\mathrm{ord}_p(qx_2^2) = \frac{p-1}{2}$. In fact, we cannot take x_2 so that $\mathrm{ord}_p(qx_2^2) = p-1$. Now we take $W_q = \begin{pmatrix} qx_2 & y_2 \\ N & qz_2 \end{pmatrix}$ for some y_2, z_2, and let $w_2 = qx_2^2 + py_2$. From (12), we know $\mathrm{ord}_N(w_2) = \mathrm{lcm}(\frac{p-1}{2}, 2)$; hence it is equal to $p-1$ because $\frac{p-1}{2}$ is odd by our assumption about p. From (12) again,

$$w_2^{\frac{p-1}{2}} \equiv \begin{cases} 1 & \pmod p \\ -1 & \pmod q \end{cases},$$

and hence $w_2^{\frac{p-1}{2}} \not\equiv \pm 1 \pmod N$. Thus the order of w_2 modulo $\Delta = \{\pm 1\}$ is equal to $p-1$; hence the order of W_q in $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ is equal to $2(p-1)$.

Now we will show that W_p and W_q generate $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$. For that it suffices to show that w_1 and w_2 generate $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$. Since

$$(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\} \cong \left[(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*\right]/\{\pm(1,1)\},$$

from (12), we can view w_1 and w_2 as the elements $(-1, r)$ and $(s^2, -1)$ of $[(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*]/\{\pm(1,1)\}$, respectively . Since $\frac{p-1}{2}$ is odd, $-s^2$ is a primitive root modulo$p$. Thus $(1, r) = (-1, 1)(-1, r) = (-s^2, 1)^{\frac{p-1}{2}}(-1, r)$, and hence $(1, r)$ and $(-s^2, 1)$ are expressed by $\pm(-1, r)$ and $\pm(s^2, -1)$. Since $(1, r)$ and $(-s^2, 1)$ generate $[(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*]/\{\pm(1,1)\}$, so do $(-1, r)$ and $(s^2, -1)$. Thus w_1 and w_2 generate $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$.

From (13) we know that $(W_qW_p)^2 = 1$. For $u \in (\mathbb{Z}/N\mathbb{Z})^*$, by the action of the Atkin-Lehner involution W_q on $(\mathbb{Z}/N\mathbb{Z})^*$ via the t_q operator which is in correspondence with conjugation by the W_q on $\Gamma_0(N)$ modulo $\Gamma_1(N)$, we have the following:

$$W_q[u]W_q^{-1}[u][1,1] \equiv 1 \pmod q. \tag{15}$$

Thus $W_q[w_1]W_q^{-1}[w_1][1,1] \equiv 1 \pmod q$, and clearly $W_q[w_1]W_q^{-1}[w_1][1,1] \equiv 1 \pmod p$ because $w_1 \equiv -1 \pmod p$. Therefore, $W_qW_p^2W_q^{-1}W_p^2 = 1$ holds.

Let $G = \langle a, b \mid a^{q-1} = b^{2(p-1)} = (ba)^2 = ba^2b^{-1}a^2 = 1\rangle$. Then there is a unique homomorphism from G to $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ determined by the map $a \mapsto W_p$ and $b \mapsto W_q$. From the relations in G, we know that

$$a^{-1} = a^{q-2},\ b^{-1} = b^{2(p-1)-1},\ ba = a^{-1}b^{-1},\ ba^2 = a^{-2}b,$$

and hence every element of G can be expressed as a^ib^j with $0 \le i < q-1$ and $0 \le j < 2(p-1)$. Thus the order $|G|$ of G is less than or equal to $2(p-1)(q-1)$. Since $|\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)| \le |G|$ and $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ is of order $2(p-1)(q-1)$, G is isomorphic to $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$.

Next consider the case when $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ with $\left(\frac{p}{q}\right) = -1$. By the quadratic reciprocity law, $\left(\frac{q}{p}\right) = -1$ too. Under the exact same notations as in the previous case, we know that $\mathrm{ord}_q(w_1) = q-1$ and $\mathrm{ord}_p(w_2) = p-1$. The fact that $\mathrm{ord}_q(w_1) = q-1$ comes from two conditions $q \equiv 3 \pmod 4$ and $\left(\frac{p}{q}\right) = -1$ which is the same as in the previous case. Since $\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \equiv -1 \pmod p$, $\frac{p-1}{d_2}$ should be odd. Thus one can take x_2 so that qx_2^2 is a primitive root modulo p, and hence $\mathrm{ord}_p(w_2) = p-1$.

From (12), $w_1^{\frac{q-1}{2}} \equiv -1 \pmod N$ because $\frac{q-1}{2}$ is odd, but $w_2^{\frac{p-1}{2}} \not\equiv -1 \pmod N$ because $\frac{p-1}{2}$ is even. Thus the order of W_p and W_q in $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ are equal to $q-1$ and $2(p-1)$ respectively.

In this case we can view w_1 and w_2 as the elements $(-1, r)$ and $(s, -1)$ in $[(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*]/\{\pm(1,1)\}$. Since $\frac{p-1}{2}$ is even, $-s$ is a primitive root modulo p too. By the similar argument as in the previous case, $(1, r)$ can be expressed by $(-1, r)$ and $(-s, 1)$. Since $(-s, 1)$ and $(1, r)$ generate $[(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*]/\{\pm(1,1)\}$, so w_1 and w_2 generate $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$. Thus the result follows. □

Theorem 4.3. *Let $N = pq$ where p and q are primes satisfying $p \equiv q \equiv 1 \pmod 4$ with $\left(\frac{p}{q}\right) = -1$, Then,*

$$\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N) \cong \langle a, b \mid a^{2(q-1)} = b^{2(p-1)} = (ba)^2 = ba^2b^{-1}a^2 = a^{q-1}b^{p-1} = 1\rangle.$$

Proof. The notations are exactly the same as in the proof of Theorem 4.2. By quadratic reciprocity law, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = -1$; hence $p^{\frac{q-1}{2}} \equiv -1 \pmod q$ and $q^{\frac{p-1}{2}} \equiv -1 \pmod p$, and hence $\frac{q-1}{d_1}$ and $\frac{p-1}{d_2}$ are odd. Thus we can take x_1 and x_2 so that px_1^2 and qx_2^2 are primitive roots of q and p, respectively. Thus $\mathrm{ord}_N(w_1) = q-1$ and $\mathrm{ord}_N(w_2) = p-1$. Since $\frac{q-1}{2}$ and $\frac{p-1}{2}$ are even, $w_1^{\frac{q-1}{2}} \not\equiv \pm 1 \pmod N$ and $w_2^{\frac{p-1}{2}} \not\equiv \pm 1 \pmod N$ from (12), and hence the orders of W_p and W_q in $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ are equal to $2(q-1)$ and $2(p-1)$ respectively.

Since

$$w_1^{\frac{q-1}{2}} \equiv \begin{cases} 1 & (\mathrm{mod}\ p) \\ -1 & (\mathrm{mod}\ q) \end{cases}, \quad w_2^{\frac{p-1}{2}} \equiv \begin{cases} -1 & (\mathrm{mod}\ p) \\ 1 & (\mathrm{mod}\ q) \end{cases},$$

$w_1^{\frac{q-1}{2}} w_2^{\frac{p-1}{2}} \equiv -1 \pmod N$, and hence $W_p^{q-1} W_q^{p-1} = 1$. It holds that $(W_q W_p)^2 = 1$ and $W_q W_p^2 W_q^{-1} W_p^2 = 1$ as before.

In this case we can view w_1 and w_2 as the elements $(-1, r)$ and $(s, -1)$ in $[(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*]/\{\pm(1,1)\}$, and $-s$ and $-r$ are primitive roots of p and q. Thus $-(1, -r)$ and $-(-s, 1)$ generate $[(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*]/\{\pm(1,1)\}$, and so w_1 and w_2 generate $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$.

Finally consider the isomorphism. Let $G = \langle a, b \mid a^{2(q-1)} = b^{2(p-1)} = (ba)^2 = ba^2b^{-1}a^2 = a^{q-1}b^{p-1} = 1\rangle$. From the first four relations, we know that any element of G can be expressed as $a^i b^j$ with $0 \le i < 2(q-1)$ and $0 \le j < 2(p-1)$. However due to the relation $a^{q-1}b^{p-1} = 1$, it can be boiled down to be $a^i b^j$ with $0 \le i < q-1$ and $0 \le j < 2(p-1)$. Thus $|G| \le 2(p-1)(q-1)$, and hence the result follows by the same argument as in the proof of Theorem 4.2. □

Theorem 4.4. *Let $N = pq$ where p and q are primes satisfying $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ with $\left(\frac{p}{q}\right) = 1$. Then,*

$$\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N) \cong \begin{cases} \langle a, b, c \mid a^{2(q-1)} = b^{p-1} = c^{p-1} = (ba)^2 = ba^2b^{-1}a^2 = a^{q-1}b^{\frac{p-1}{2}} \\ \qquad = a^{q-1}b^2c^{-2} = aca^{-1}c = bcb^{-1}c^{-1} = 1\rangle, & \text{if } p \equiv 1 \pmod 8, \\ \langle a, b, c \mid a^{2(q-1)} = b^{\frac{p-1}{2}} = c^{p-1} = (ba)^2 = ba^2b^{-1}a^2 \\ \qquad = a^{q-1}b^2c^{-2} = aca^{-1}c = bcb^{-1}c^{-1} = 1\rangle, & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

Proof. The notations are exactly the same as in the proof of Theorem 4.2. Since $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$, $p^{\frac{q-1}{2}} \equiv 1 \pmod q$ and $q^{\frac{p-1}{2}} \equiv 1 \pmod p$, and hence $\frac{q-1}{d_1}$ and $\frac{p-1}{d_2}$ are even. Thus we can take x_1 and x_2 so that

$\mathrm{ord}_q(px_1^2) = \frac{q-1}{2}$ and $\mathrm{ord}_p(qx_2^2) = \frac{p-1}{2}$. Since $\frac{q-1}{2}$ is odd and $\frac{p-1}{2}$ is even, $\mathrm{ord}_N(w_1) = q-1$ and $\mathrm{ord}_N(w_2) = \frac{p-1}{2}$ by (12). Then the order of W_p in $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ is equal to $2(q-1)$ because $w_1^{\frac{q-1}{2}} \not\equiv \pm 1 \pmod N$ from (12). However, the order of W_q in $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ is equal to $p-1$ (resp. $\frac{p-1}{2}$) if $p \equiv 1 \pmod 8$ (resp. $p \equiv 5 \pmod 8$), because $w_2^{\frac{p-1}{4}} \not\equiv \pm 1 \pmod N$ if $\frac{p-1}{4}$ is even but $w_2^{\frac{p-1}{4}} \equiv -1 \pmod N$ if $\frac{p-1}{4}$ is odd from (12).

First consider the case $p \equiv 1 \pmod 8$. Then $w_1^{\frac{q-1}{2}} w_2^{\frac{p-1}{4}} \equiv 1 \pmod N$, and hence $W_p^{q-1} W_q^{\frac{p-1}{2}} = 1$. It holds that $(W_q W_p)^2 = 1$ and $W_q W_p^2 W_q^{-1} W_p^2 = 1$ as before.

In this case we can view w_1 and w_2 as the elements $(-1, r^2)$ and $(s^2, -1)$ in $[(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*]/\{\pm(1,1)\}$. Then $-r^2$ is a primitive root modulo q, but $\mathrm{ord}_p(-s^2) = \frac{p-1}{2}$. Thus $\pm(s,1)$ cannot be expressed by $(-1, r^2)$ and $(s^2, -1)$, and then $[(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\} : \langle w_1, w_2\rangle] = 2$ and $[\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N) : \langle W_p, W_q\rangle] = 2$. If we take $u \in (\mathbb{Z}/N\mathbb{Z})^*$ so that $u \equiv s \pmod p$ and $u \equiv 1 \pmod q$, then $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N) = \langle W_p, W_q, [u]\rangle$. As explained for the equation (15), we have

$$W_p[u]W_p^{-1}[u][1,1] \equiv 1 \pmod p,$$

and clearly $W_p[u]W_p^{-1}[u][1,1] \equiv 1 \pmod q$. Thus $W_p[u]W_p^{-1}[u] = 1$ in $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$. We can compute

$$W_q[u]W_q^{-1}[u]^{-1}[1,1] \equiv \begin{cases} uu^{-1}qx_2z_2 \equiv 1 \pmod p, \\ -u^2py_2 \equiv 1 \pmod q, \end{cases}$$

and hence $W_q[u]W_q^{-1}[u]^{-1} = 1$ in $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$. Let $G = \langle a, b, c \mid a^{2(q-1)} = b^{p-1} = c^{p-1} = (ba)^2 = ba^2b^{-1}a^2 = a^{q-1}b^{\frac{p-1}{2}} = a^{q-1}b^2c^{-2} = aca^{-1}c = bcb^{-1}c^{-1} = 1\rangle$. Then there is a unique homomorphism from G to $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ determined by the map $a \mapsto W_p$, $b \mapsto W_q$, and $c \mapsto [u]$. By the same reason as in the proof of Theorem 4.3, all the products of a, b can be expressed as $a^i b^j$ with $0 \le i < (q-1)$, $0 \le j < (p-1)$. From the relations $a^{\frac{q-1}{2}}b^2c^{-2} = aca^{-1}c = bcb^{-1}c^{-1} = 1$, we can check that every element of G can be expressed as $a^i b^j c^k$ with $0 \le i < (q-1)$, $0 \le j < (p-1)$, and $k = 0, 1$. Thus $|G| \le 2(p-1)(q-1)$, and hence we have an isomorphism.

Let us consider the case $p \equiv 5 \pmod 8$. We can take W_p, W_q, and $[u]$ as the same as in the case $p \equiv 1 \pmod 8$. Then they satisfy all the relations in $G := \langle a, b, c \mid a^{2(q-1)} = b^{\frac{p-1}{2}} = c^{p-1} = (ba)^2 = ba^2b^{-1}a^2 = a^{q-1}b^2c^{-2} = aca^{-1}c = bcb^{-1}c^{-1} = 1\rangle$ if we replace a, b, and c by W_p, W_q, and $[u]$, respectively. By the same argument as in the case $p \equiv 1 \pmod 8$, we can show that G is isomorphic to $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$. □

Corollary 4.5. *For the non-split cases for $N = pq$ with distinct two primes p, q, we have*

$$|\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)| = 2(p-1)(q-1).$$

Proof. It follows from the proofs of Theorem 4.1, Theorem 4.2, Theorem 4.3, and Theorem 4.4. □

Remark 4.6. *(1) In Theorem 4.4, $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ cannot have two generators. Suppose it can be generated by two elements, say α and β. In the sequence* (1)*, they map to generators of $\mathfrak{N}_\Delta(N)/\Gamma_0(N)$ under the map g. Since $\mathfrak{N}_\Delta(N)/\Gamma_0(N)$ is the Klein four-group and it is generated by W_p and W_q, we can assume α and β are same as W_p and W_q. In fact, if one of $g(\alpha)$ and $g(\beta)$ is equal to W_N, say $g(\beta)$, we can take α and $\alpha\beta$ as generators of $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$, and then $g(\alpha)$ and $g(\alpha\beta)$ are equal to W_p and W_q. However, W_p and W_q cannot generate $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ as shown in the proof of Theorem 4.4.*

(2) Consider the non-split cases for $N = pq$ and let $\Delta \le (\mathbb{Z}/N\mathbb{Z})^*$. Suppose $t_Q(\Delta) = \Delta$ for all $Q||N$. Then one can obtain a group presentation of $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ by using the methods used in the proofs of Theorem 4.1, Theorem 4.2, Theorem 4.3, and Theorem 4.4. Since $\mathfrak{N}_\Delta(N) = \mathfrak{N}_{\{\pm 1\}}(N)$, there is a natural projection $\mathfrak{N}_{\{\pm1\}}(N)/\Gamma_{\{\pm1\}}(N) \to \mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$, and hence we can take the same generators of $\mathfrak{N}_\Delta(N)/\Gamma_\Delta(N)$ as of $\mathfrak{N}_{\{\pm1\}}(N)/\Gamma_{\{\pm1\}}(N)$. Thus it suffices to change the order of generators and the relations between them for getting a group presentation.

We give an example in the non-split case which shows the orders that generators W_p and W_q can have and their relations depending on Δ.

Example 4.7. *Let* $N = 35$*, which is in the case of Theorem 4.2, and let* $\Delta_1 = \{\pm 1, \pm 6\}$ *and* $\Delta_2 = \{\pm 1, \pm 11, \pm 16\}$*. Take*

$$W_5 = \begin{pmatrix} 5 & 2 \\ 35 & 15 \end{pmatrix}, \; W_7 = \begin{pmatrix} 7 & 4 \\ 35 & 21 \end{pmatrix},$$

then $w_1 = 19$ *and* $w_2 = 27$*. Since* $w_1^3 \equiv -1 \pmod{35}$*, the order of* W_5 *in* $\mathfrak{N}_{\Delta_1}(N)/\Gamma_{\Delta_1}(35)$ *is* 6*, and since* $w_2^2 \equiv -6 \pmod{35}$*, the order of* W_7 *in* $\mathfrak{N}_{\Delta_1}(N)/\Gamma_{\Delta_1}(35)$ *is* 4*. Consider the group* $G_1 = \langle a, b \mid a^6 = b^4 = (ba)^2 = ba^2b^{-1}a^2 = 1\rangle$*. Then* W_5 *and* W_7 *satisfy all the relations of* G_1 *in* $\mathfrak{N}_{\Delta_1}(N)/\Gamma_{\Delta_1}(35)$ *if we replace* a *and* b *by* W_5 *and* W_7*. Clearly* $|G_1| = 24$ *which is the same as the order of* $\mathfrak{N}_{\Delta_1}(N)/\Gamma_{\Delta_1}(35)$*, and hence* $\mathfrak{N}_{\Delta_1}(N)/\Gamma_{\Delta_1}(35)$ *is isomorphic to* G_1*.*

Since $w_1 \in \Delta_2$*, the order of* W_5 *in* $\mathfrak{N}_{\Delta_2}(N)/\Gamma_{\Delta_2}(35)$ *is* 2*, and since* $w_2^4 \equiv 1 \pmod{35}$*, the order of* W_7 *in* $\mathfrak{N}_{\Delta_2}(N)/\Gamma_{\Delta_2}(35)$ *is* 8*. Consider the group* $G_2 = \langle a, b \mid a^2 = b^8 = (ba)^2 = 1\rangle$*. Since the order of* a *is* 2*, we can remove the relation* $ba^2b^{-1}a^2 = 1$*. Then one can easily confirm that* $\mathfrak{N}_{\Delta_2}(N)/\Gamma_{\Delta_2}(35)$ *is isomorphic to* G_2 *which is a dihedral group of order* 16*.*

Acknowledgement: We would like to thank KIAS (Korea Institute for Advanced Study) for its hospitality while we have worked on this result. Also we thank Shaul Zemel for giving comments on the sequence (1) in the earlier version. We would like to thank the referees for their valuable comments and suggestions on the revision.

Bo-Hae Im was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning(NRF-2017R1A2B4002619). Daeyeol Jeon was supported by the Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (NRF-2014R1A1A2056390). Chang Heon Kim was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government (MSIP) (NRF-2015R1D1A1A01057428 and 2016R1A5A1008055).

References

[1] Akbas M., Singerman D., The normalizer of $\Gamma_0(N)$ in $\mathrm{PSL}_2(\mathbb{R})$, Glasgow Math. J., 1990, 32, 317-327
[2] Atkin A.O.L., Lehner J., Hecke operator on $\Gamma_0(N)$, Math. Ann., 1970, 185, 134-160
[3] Baker M., Hasegawa Y., Automorphisms of $X_0^*(p)$, J. Number Theory, 2003, 100, 72-87
[4] Bars F., The group structure of the normalizer of $\Gamma_0(N)$ after Atkin-Lehner, Comm. Algebra, 2008, 36, 2160-2170
[5] Bars F., Kontogeorgis A., Xarles X., Bielliptic and hyperelliptic modular curves $X(N)$ and the group $\mathrm{Aut}(X(N))$, Acta Arith., 2013, 161, 283-299
[6] Borcherds R.E., Monstrous moonshine and monstrous Lie superalgebras, Invent. Math., 1992, 109, 405-444
[7] Conway C., Norton S., Monstrous moonshine, Bull. London Math. Soc., 1979, 11, 308-339
[8] Elkies N.D., The automorphism group of the modular curve $X_0(63)$, Compositio Math., 1990, 74, 203-208
[9] Harrison M., A new automorphism of $X_0(108)$, arXiv:1108.5595 [math.NT]
[10] Jeon D., Kim C.H., Bielliptic modular curves $X_1(N)$, Acta Arith., 2004, 112, 75–86
[11] Kim C.H., Koo J.K., The normalizer of $\Gamma_1(N)$ in $\mathrm{PSL}_2(\mathbb{R})$, Comm. Algebra, 2000, 28, 5303–5310
[12] Kenku M.A., Momose F., Automorphism groups of the modular curves $X_0(N)$, Compositio Math., 1988, 65, 51-80
[13] Lang M.L., Normalizers of $\Gamma_1(m)$, J. Number Theory, 2001, 86, 50-60
[14] Lehner J., Newman M., Weierstrass points of $\Gamma_0(N)$, Ann of Math. (2), 1964, 79, 260-368
[15] Maclachlan C., Groups of units of zero ternary quadratic forms, Proc. Roy. Soc. Edinburgh Sect. A, 1981, 88, 141-157
[16] Momose F., Automorphism groups of the modular curves $X_1(N)$, Preprint
[17] Newman M., Structure theorem for modular subgroups, Duke Math. J., 1955, 22, 25-32
[18] Newman M., Conjugacy, genus and class numbers, Math. Ann., 1975, 196, 198-217
[19] Zemel S., Normalizers of Congruence Groups in $\mathrm{SL}_2(\mathbb{R})$ and Automorphisms of Lattices, to appear in Int. J. Number Theory