*Konuralp Journal of Mathematics*, 9 (1) (2021) 60-64

**Konuralp Journal of Mathematics**

*Research Paper*

https://dergipark.org.tr/en/pub/konuralpjournalmath

e-ISSN: 2147-625X

# Index and Equality Conditions of the Subgroups $\Gamma_{0,n}(N)$ and $\Lambda_n(N)$

**Aziz Büyükkaragöz[1*], Erdal Ünlüyol[1] and Mehmet Akbaş[2]**

[1] *Department of Mathematics, Faculty of Science and Arts, Ordu University, Ordu, Turkey*
[2] *Department of Mathematics, Faculty of Science, Karadeniz Technical University, Trabzon, Turkey*
[*] *Corresponding author*

**Abstract**

In this paper, we find conditions on the natural number $n$ that the subgroups $\Gamma_{0,n}(N)$ and $\Lambda_n(N)$ of modular group are different. And then, by defining an $\Lambda_n(N)$ invariant equivalence relation on the subset $\hat{\mathbb{Q}}_n(N)$, we calculate the index formula for $\Gamma_{0,n}(N)$ in $\Lambda_n(N)$.

***Keywords:*** *Congruence subgroup of modular group, transitivity, conjugateness, stabilizing, infinite cycle group, index formula*
***2010 Mathematics Subject Classification:*** *05C20, 20E07, 20F38.*

## 1. Introduction

**Definition 1.1.** *[1] Let $G$ be a group and also a topology. If the functions $F : G \times G \longrightarrow G$, $F(x,y) := xy$ and $f : G \longrightarrow G$, $f(x) := x^{-1}$ functions are continuous, then $G$ is called a topological group.*

**Definition 1.2.** *[2] Let $G$ be a group and $X \neq \emptyset$ be a set. In this case, if the function $\Psi : G \times X \longrightarrow X$ satisfies the following conditions,*

*i.)* $\Psi(g_1g_2,x) = \Psi(g_1,\Psi(g_2,x))$ *for* $g_1,g_2 \in G$ *and* $x \in X$,
*ii.)* $\Psi(1,x) = x$ *for* $1 \in G$ *is unit element and* $x \in X$,

*then $G$ is called an act group according to the left product on $X$.*

*Here, we shortly write $gx$ instead of $\Psi(g,x)$. Hence, $(g_1g_2)x = g_1(g_2x)$ and $1x = x$. An act group expression will mean an act group with respect to the left product. Moreover, if $G$ is a topological group, $X$ is a topology and the transformation $\Psi$ is continuous, then the pair of $[G,X]$ is called topological transformation group.*

**Definition 1.3.** *[2] Let $[G,X]$ be a topological transformation group. If $Gx = X$ for $x \in X$, then the pair of $[G,X]$ is called transitive topological transformation group. It is clearly, if there is a element $g \in G$, such that $gx = y$ for $x,y \in X$, then the pair of $[G,X]$ is transitive topological transformation group.*

**Definition 1.4.** *[3] Let $[G,X]$ be any topological transformation group. In this case,*

*i.) For $x \in X$, the set of $Sb_G(x) = G_x := \{g \in G : gx = x\}$ is called stabilizing $x$ in $G$.*
*ii.) For $g \in G$, the set of $Sb(g;X) := \{x \in X : gx = x\}$ is called constant point set $g$ in $X$.*

Now, we give some information for subgroups act.

$$\mp\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad a,b,c,d \in \mathbb{Z}, ad - bc = 1. \tag{1.1}$$

Here we omit the symbol $\mp$, and identify each matrix with its negatives. As usual, $\Gamma$ and its subgroups act on the extended rational $\hat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ by

$$z \to \frac{az+b}{cz+d},$$

***Email addresses***: azizbk@windowslive.com (Aziz Büyükkaragöz), eunluyol@yahoo.com (Erdal Ünlüyol), akbas@ktu.edu.tr (Mehmet Akbaş)

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is as in (1.1).
Throughout the paper we use the following subgroups

$$\Gamma_{0,n}(N) = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma : a^2 \equiv 1 \ mod \ n \right\}$$

and

$$\Lambda_n(N) = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma : a^4 \equiv 1 \ mod \ n \right\}.$$

where $N, n$ be positive integers with $n \mid N$. Then We now give the notion, as in [3], an imprimitive action for a permutation group $(G, \Omega)$, where $G$ is the group acting on the set $\Omega$ transitively. The equivalence relation $\approx$ is called $G$-invariant if and only if

$$x \approx y \qquad \text{gives} \qquad g(x) \approx g(y) \qquad \text{for all } g \in G.$$

Then we immediately have two trivial equivalence relations $\Omega$ as

i.) For all $x, y \in \Omega \quad x \approx y$,
ii.) For all $x \in \Omega \quad x \approx x$.

If there is an equivalence relation on $\Omega$ other than the above two we say that the group $G$ acts on $\Omega$ imprimitively.

Let $H$ be a subgroup of $G$ with $H \neq G$ and $G_\alpha$ be stabilizer of $\alpha \in \Omega$ and that $G_\alpha \lneqq H \lneqq G$. In this case we define a $G$-invariant imprimitive action as follows. Since $G$ acts on $\Omega$ transitively there exist $g, h \in G$ such that, for any given $x$ and $y$ in $\Omega$

$$x = g(\alpha), y = h(\alpha).$$

Let $x \approx y \Leftrightarrow gh^{-1} \in H$. Then the relation $\approx$ on $\Omega$ is a $G$-invariant primitive equivalence relation. As in [3], in this case the index $\mid G : H \mid$ is the number of equivalence classes. You can find the fundamental concepts and information in [4]-[8].

**Lemma 1.5.** *[6] Let $n \in \mathbb{Z}^+, x \leq n$ and $(x, n) = 1$. In this case, the solution of the congruence $x^2 \equiv 1 \ mod \ n$ consists of $2^{r+s}$ values for*

$$n = 2^{\alpha_1} p_2^{\alpha_2} \dots p_{r+1}^{\alpha_{r+1}} \text{ and } s = \begin{cases} 0, & if \ \alpha_1 = 1 \\ 1, & if \ \alpha_1 = 2 \\ 2, & if \ \alpha_1 \geq 3 \end{cases}$$

The paper is organized as follows.

First of all we will get conditions on the natural number $n$ so that the equality

$$\Lambda_n(N) = \Gamma_{0,n}(N)$$

is satisfied. Then we calculate the index

$$\mid \Lambda_n(N) : \Gamma_{0,n}(N) \mid.$$

## 2. Main Calculations

We again write the groups as

$$\Gamma_{0,n}(N) = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma : a^2 \equiv 1 \ mod \ n \quad \text{or} \quad a \equiv d \ mod \ n \right\}$$

and

$$\Lambda_n(N) = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma : a^4 \equiv 1 \ mod \ n \quad \text{or} \quad a^2 \equiv d^2 \ mod \ n \right\}.$$

Then it is clear that $\Gamma_{0,n}(N) \leq \Lambda_n(N)$.

Let us define the subset of $\hat{\mathbb{Q}}$ as

$$\hat{\mathbb{Q}}_n(N) = \left\{ \frac{a}{cN} \in \hat{\mathbb{Q}} : a^4 \equiv 1 \ mod \ n \quad \text{and} \quad (a, cN) = 1 \right\}.$$

Then it is easily seen that this is one of the largest subset of $\hat{\mathbb{Q}}$ on which the group $\Lambda_n(N)$ acts transitively.

**Theorem 2.1.** *We suppose that $m, N \in \mathbb{Z}^+$, $p \in \mathbb{P}$, $p|N$ and $p \neq 4m+1$. Then*

$$\Lambda_p(N) = \Gamma_{0,p}(N).$$

*Proof.* If $a \equiv d \mod p$, then $a^2 \equiv d^2 \mod p$. From this, it is clear that $\Gamma_{0,p}(N) \subset \Lambda_p(N)$. Now, let we show that $\Lambda_p(N) \subset \Gamma_{0,p}(N)$. Firstly, let we take $\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Lambda_p(N)$. Then, we obtain $ad - bcN = 1$ and $a^2 \equiv d^2 \mod p$. Hence, we establish $ad \equiv 1 \mod p$ according to $p|N$. Therefore, $d \equiv a^{-1} \mod p$. And then $a^4 \equiv 1 \mod p$ from $a^2 \equiv (a^{-1})^2 \mod p$. If $m \in \mathbb{Z}^+$ and $p \neq 4m+1$, then we have $a^2 \equiv 1 \mod p$. Namely, we find $a \equiv d \mod p$ in the group $\Gamma_{o,p}(N)$. This is also means that $\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_{0,p}(N)$. Thus, we get $\Lambda_p(N) \subset \Gamma_{0,p}(N)$. Consequently, we obtain $\Lambda_p(N) = \Gamma_{0,p}(N)$ under the conditions of $p \neq 4m+1$ and $m \in \mathbb{Z}^+$. Clearly, if $p \equiv -1 \mod 4$, then we prove $\Lambda_p(N) = \Gamma_{0,p}(N)$. □

As a start we now give the following important theorem.

**Theorem 2.2.** *Let $p$ be a prime with $p > 2$ and suppose that $\left(\frac{-1}{p}\right)$, namely there exists an $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \mod p$. Then, with the same understanding, $\left(\frac{-1}{p^n}\right) = 1$ if and only if $p \equiv 1 \mod 4$ for all $n \in \mathbb{N}$.*

*Proof.* Take $n$ to be 1, we get $\left(\frac{-1}{p}\right) = 1$. Then, $p \equiv 1 \mod 4$. Conversely, suppose $p \equiv 1 \mod 4$ and $n$ is an arbitrary natural number. We here use the principle of Mathematical Induction.

It is true for $n = 1$. Suppose it is true for $\ell \in \mathbb{N}$, that is, there exists $y \in \mathbb{Z}$ such that $y^2 \equiv -1 \mod p^\ell$. We will show that the claim is true for the number $\ell + 1$.

Since $(y, p) = 1$, then there exists $z \in \mathbb{Z}$ such that $2yz \equiv 1 \mod p$. Then

$$\frac{1+y^2}{p^\ell} - 2yz\frac{1+y^2}{p^\ell} \equiv 0 \mod p.$$

So, $1 + y^2 - 2yz(1+y^2) \equiv 0 \mod p^{\ell+1}$. Let $k = -z\frac{1+y^2}{p^\ell}$. Then we get

$$1 + y^2 + 2ykp^\ell \equiv 0 \mod p^{\ell+1}.$$

Therefore we have $\left(y + kp^\ell\right)^2 \equiv -1 \mod p^{\ell+1}$. That is, $\left(\frac{-1}{p^{\ell+1}}\right) = 1$, which completes the proof. □

**Theorem 2.3.** *Let $n = 2^\alpha . p_1^{\alpha_1} . p_2^{\alpha_2} . p_3^{\alpha_3} . \cdots . p_r^{\alpha_r}$ be the prime power decomposition of $n$ with $n \mid N$. Then, for $\alpha \leq 3$ and $1 \leq k \leq r$,*

$$p_k \equiv -1 \mod 4 \quad \Leftrightarrow \quad \Gamma_{0,n}(N) = \Lambda_n(N).$$

*Proof.* It is already known that $\Gamma_{0,n}(N) \leq \Lambda_n(N)$. Now we take an arbitrary $T = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Lambda_n(N)$. Thus, we have $a^4 \equiv 1 \mod n$. So, we find $n \mid (a^2-1)(a^2+1)$. This gives that $p_k^{\alpha_k} \mid (a^2-1)(a^2+1)$ for $1 \leq k \leq r$. Since $p \equiv -1 \mod 4$, $p_k \nmid (a^2+1)$. Therefore we have $p_k^{\alpha_k} \mid (a^2-1)$ for $1 \leq k \leq r$. On the other hand we know that $a^2 \equiv 1 \mod 2^\alpha$ with $\alpha \leq 3$. Consequently, $n \mid (a^2-1)$, that is, $a^2 \equiv 1 \mod n$ which gives that $T \in \Gamma_{0,n}(N)$. Hence, $\Gamma_{0,n}(N) = \Lambda_n(N)$.

Conversely, we will show that $\alpha \leq 3$ and $p \equiv -1 \mod 4$ for $1 \leq k \leq r$.

Suppose that, $\alpha \geq 4$. Let $n = 2^\alpha n_1$ and $N = 2^\beta N_1$ with $(2, N_1) = 1$. Take $a = 2^{\alpha-2}N_1 + 1$. Then, there exist $b$ and $d$ in $\mathbb{Z}$ due to $(a, N) = 1$, so that $A = \begin{pmatrix} a & b \\ N & d \end{pmatrix}$ is in $\Gamma_0(N)$. Because $\alpha \geq 4$ it is easily seen that $a^4 \equiv 1 \mod n$ and $a^2 \not\equiv 1 \mod n$. Hence $A \in \Lambda_n(N)$ but $A \notin \Gamma_{0,n}(N)$. This shows that $\alpha \leq 3$.

Now, we suppose that $n = p^\alpha n_0$ with $(p, n_0) = 1$, and that $p \equiv 1 \mod 4$. In this case, by theorem 2.2, there exists $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \mod p^\alpha$.

Let $N = p^\beta . p_1^{\beta_1} . p_2^{\beta_2} . \cdots p_r^{\beta_r}$ and $n = p^\alpha . p_1^{\alpha_1} . p_2^{\alpha_2} . \cdots p_\ell^{\alpha_\ell}$ be the prime power decomposition of $N$ and $n$ respectively, and $n \mid N$.

i.) Let $(a, N_0) = 1$, where $N_0 = p_1^{\beta_1} . \cdots p_r^{\beta_r}$. Due to $(ap^\alpha, N_0) = 1$, there exists $k \in \mathbb{Z}$ such that

$$kap^\alpha \equiv 1 - a \mod N_0 \qquad \text{or} \qquad a + kap^\alpha \equiv 1 \mod N_0.$$

It is clear that

$$(a + kap^\alpha)^2 \equiv 1 \mod p^\alpha \qquad \text{and} \qquad (a + kap^\alpha)^4 \equiv 1 \mod p^\alpha.$$

Hence $(a + kap^\alpha)^2 \equiv -1 \mod p^\alpha$ we have $(a + kap^\alpha)^2 \not\equiv 1 \mod n$. In this case, again, there exist $u, v \in \mathbb{Z}$ such that

$$\begin{pmatrix} a + kap^\alpha & u \\ N & v \end{pmatrix} \in \Lambda_n(N) \backslash \Gamma_{0,n}(N).$$

This contradicts the equality of the groups $\Gamma_{0,n}(N)$ and $\Lambda_n(N)$. Therefore, we must have $p \equiv -1 \mod 4$.

ii.) Let $(a,N_0)\neq 1$ and $N_0=p_1^{\beta_1}\dots p_r^{\beta_r}$. Suppose that, $p_1\mid a,\cdots,p_\ell\mid a$ and $p_{\ell+1}\nmid a,\cdots,p_r\nmid a$. Let $b=a+p_{\ell+1}\dots p_r p^{\alpha}$. Then

$$b^2\equiv a^2\equiv -1 \; mod \; p^{\alpha} \quad \text{and} \quad (b,N_0)=1.$$

So, if we repeat the calculations as in *i.*), we get a contradiction as $\Gamma_{0,n}(N)\neq\Lambda_n(N)$. Hence, in this case as well, we have $p\equiv -1 \; mod \; 4$. Consequently, the proof of theorem 2.3 is completed.

□

We now continue to define a $\Lambda_n(N)$-invariant equivalence relation on the set

$$\hat{\mathbb{Q}}_n(N)=\left\{\frac{a}{cN}\in\hat{\mathbb{Q}}: a^4\equiv 1 \; mod \; n \quad \text{and} \quad (a,cN)=1\right\}.$$

This will be used in the index calculation of $\Gamma_{0,n}(N)$ in $\Lambda_n(N)$.

Let $n=2^{\alpha}.p_1^{\alpha_1}\dots p_\ell^{\alpha_\ell}$, $\alpha\geq 4$ or $p_i\equiv 1 \; mod \; 4$ for some $1\leq i\leq\ell$. Only, in this case, we have $\Gamma_{0,n}(N)\subsetneqq\Lambda_n(N)$ with $n>1$. The stabilizer $\Lambda_n(N)_\infty$ of $\infty$ in $\Lambda_n(N)$ is the group $\left\langle\begin{pmatrix}1&1\\0&1\end{pmatrix}\right\rangle$. Then, we get

$$\Lambda_n(N)_\infty\subsetneqq\Gamma_{0,n}(N)\subsetneqq\Lambda_n(N).$$

Let $\frac{r}{sN},\frac{x}{yN}$ be in $\hat{\mathbb{Q}}_n(N)$. Since $\Lambda_n(N)$ act transitively on $\hat{\mathbb{Q}}_n(N)$, there exist $g,h\in\Lambda_n(N)$ such that $g(\infty)=\frac{r}{sN}$ and $h(\infty)=\frac{x}{yN}$. In this case, we can define an equivalence relation as

$$\frac{r}{sN}\underset{n}{\approx}\frac{x}{yN}\Leftrightarrow gh^{-1}\in\Gamma_{0,n}(N).$$

So, If we take the $T$ and $M$ for the convenient $g=\begin{pmatrix}r&k\\sN&\ell\end{pmatrix}$ and $h=\begin{pmatrix}x&t\\yN&m\end{pmatrix}$ respectively, then we get

$$TM^{-1}=\begin{pmatrix}rm-kyN&*\\ *&*\end{pmatrix}.$$

$TM^{-1}\in\Gamma_{0,n}(N)$ if $(rm-kyN)^2\equiv r^2m^2\equiv 1 \; mod \; n$. Since $detM=1$, $xm\equiv 1 \; mod \; n$ or $x\equiv m^{-1} \; mod \; n$. Therefore,

$$r^2x^{-2}\equiv 1 \; mod \; n \; or \; r^2\equiv x^2 \; mod \; n.$$

Hence,

$$\frac{r}{sN}\underset{n}{\approx}\frac{x}{yN}\quad\Leftrightarrow\quad r^2\equiv x^2 \; mod \; n.$$

The relation $\underset{n}{\approx}$ is a $\Gamma$-invariant primitive equivalence relation. Then, the number of equivalence classes, denoted by $\Psi_N(n)$, will give the index

$$\mid\Lambda_n(N):\Gamma_{0,n}(N)\mid.$$

Therefore, we must calculate the number $\Psi_N(n)$. First of all we give the following theorem.

**Theorem 2.4.** *The function $\Psi_N:E\to\mathbb{N}$ is a multiplicative function. That is, let $E$ be the exact divisors of $n:=k.\ell$ for $k,\ell\in E$ with $(k,\ell)=1$. Then*

$$\Psi_N(n)=\Psi_N(k.\ell)=\Psi_N(k).\Psi_N(\ell).$$

*Proof.* Without loss of generality, it is sufficient to prove only the case, where $n=k.\ell$ for $k,\ell\in E$ with $(k,\ell)=1$. It is clear that if $x\underset{n}{\approx}y$, then $x\underset{k}{\approx}y$ and $x\underset{\ell}{\approx}y$.

Conversely, we show that if $a\underset{k}{\approx}b$ and $c\underset{\ell}{\approx}d$, then exists $x\underset{n}{\approx}y$, such that

$$\begin{cases}x\equiv a & mod \; k,\\ y\equiv b & mod \; k,\end{cases}\quad and\quad\begin{cases}x\equiv c & mod \; \ell,\\ y\equiv d & mod \; \ell.\end{cases}$$

Therefore, let $a\underset{k}{\approx}b$ and $c\underset{\ell}{\approx}d$. Then, $a\underset{k}{\approx}b$ and $c\underset{\ell}{\approx}d$. Then

$$\begin{cases}a^4\equiv 1 & mod \; k,\\ b^4\equiv 1 & mod \; k,\end{cases}\quad and\quad\begin{cases}c^4\equiv 1 & mod \; \ell,\\ d^4\equiv 1 & mod \; \ell.\end{cases}$$

Since $(k,\ell)=1$, then there exist $x,y\in\mathbb{Z}$ such that $a+kx=c+\ell y$.

$$(a+kx)^4\equiv a^4\equiv 1 \; mod \; k \quad and \quad (a+kx)^4\equiv(c+\ell y)^4\equiv c^4\equiv 1 \; mod \; \ell.$$

So, we get that $(a+kx)^4\equiv 1 \; mod \; n$. Therefore, if $[a]_k$ and $[c]_\ell$ are the equivalence classes of $a$ and $c$ respectively, then we get a unique equivalence class $[a+kx]_n$ with respect to the number $n$. Consequently, this means that $\Psi_N(n)=\Psi_N(k).\Psi_N(\ell)$. This proves the theorem. □

Now we give the below important theorem.

**Theorem 2.5.** *Let $N,n \in \mathbb{N}$ with $n|N$ and $n = 2^{\alpha}.p_1^{\alpha_1}.\cdots.p_r^{\alpha_r}.q_1^{\beta_1}.\cdots.q_\ell^{\beta_\ell}$, where $p_i \equiv -1 \; mod \; 4$ for $1 \leq i \leq r$ and $q_j \equiv 1 \; mod \; 4$ for $1 \leq j \leq \ell$. Then the index $|\Lambda_n(N) : \Gamma_{0,n}(N)|$ is*

$$\Psi_N(n) = \begin{cases} 2^{\ell}, & \alpha \leq 3, \\ 2^{\ell+1}, & \alpha > 3. \end{cases}$$

*Proof.* Since the function $\Psi_N$ is transitive, we can take $n$ as a prime power as follows.

i.) Let $n = 2^{\alpha}$ with $\alpha \leq 3$. Then, it is easy to see that

$$\Psi_N(2) = \Psi_N(2^2) = \Psi_N(2^3) = 1,$$

as expected.

ii.) Let $n = 2^{\alpha}$ with $\alpha > 3$. For the solution $x^4 \equiv 1 \, mod \, 2^{\alpha}$, we must check the numbers $1, 3, 5, \cdots, 2^{\alpha} - 1$. These numbers are not solutions of the congruence $x^2 + 1 \equiv 0 \, mod \, 2^{\alpha}$ by solutions of $x^2 + 1 \equiv 0 \, mod \, 2$. Therefore, the solutions of the congruence $x^4 \equiv 1 \, mod \, 2^{\alpha}$ comes from the congruence $x^2 - 1 \equiv 0 \, mod \, 2^{\alpha-1}$, since

$$x^4 - 1 \equiv (x^2 - 1)(x^2 + 1) \equiv 0 \, mod \, 2^{\alpha}.$$

$(x-1, x+1) = 2$ gives that $x - 1 \equiv 0 \, mod \, 2^{\alpha} - 2$ or $x + 1 \equiv 0 \, mod \, 2^{\alpha} - 2$. Then, there exist natural numbers $k$ and $\ell$ such that $x = 1 + k.2^{\alpha} - 2$ or $x = -1 + \ell.2^{\alpha} - 2$. Since $x < 2^{\alpha}$, we have $k = 1, 2, 3$ and $\ell = 1, 2, 3, 4$. Therefore, all these $x$ are as follows,

$$\begin{cases} x_1 = 1 + 2^{\alpha} - 2, & \text{for } k = 1, \\ x_2 = 1 + 2^{\alpha} - 1, & \text{for } k = 2, \\ x_3 = 1 + 3.2^{\alpha} - 2, & \text{for } k = 3, \end{cases}$$

$$\begin{cases} x_4 = -1 + 2^{\alpha} - 2, & \text{for } \ell = 1, \\ x_5 = -1 + 2^{\alpha} - 1, & \text{for } \ell = 2, \\ x_6 = -1 + 3.2^{\alpha} - 2, & \text{for } \ell = 3, \\ x_7 = -1 + 2^{\alpha}, & \text{for } \ell = 4, \end{cases}$$

and of course we have $x_8 = 1$. From the above solutions we have

$$\begin{cases} x_2^2 \equiv x_5^2 \equiv x_7^2 \equiv x_8^2 \equiv 1 & mod \, 2^{\alpha} \; and, \\ x_1^2 \equiv x_3^2 \equiv x_4^2 \equiv x_6^2 \not\equiv 1 & mod \, 2^{\alpha} \; and \; that, \\ x_1^4 \equiv x_3^4 \equiv x_4^4 \equiv x_6^4 \equiv 1 & mod \, 2^{\alpha}. \end{cases}$$

Therefore, we get that $[x_1]_{2^{\alpha}} \neq [x_8]_{2^{\alpha}}$. Consequently, we have conclude that $\Psi_N(n) = 2$, where $n = 2^{\alpha}$ and $\alpha > 3$.

iii.) Let $n = p^{\vartheta}$. In this case, there are two conditions:

(1.) Suppose that $p \equiv 1 \; mod \; 4$. Then, the congruence $x^2 \equiv -1 \; mod \; p^{\alpha}$ has a solution $x_1$. And, the only other solution is $x_2 = p^{\alpha} - x_1$. Also, the solutions of the congruence $x^2 \equiv 1 \; mod \; p^{\alpha}$ are $x_3 = 1$ and $x_4 = p^{\alpha} - 1$. Hence, the congruence $x^4 \equiv 1 \; mod \; p^{\alpha}$ has the solutions $x_1, x_2, x_3$ and $x_4$. Since $x_1^2 \equiv x_2^2 \equiv -1 \; mod \; p^{\alpha}$ we have $[x_1]_{p^{\vartheta}} = [x_2]_{p^{\vartheta}}$. Likewise, we have $[x_3]_{p^{\vartheta}} = [x_4]_{p^{\vartheta}}$. But it is easily seen that $[x_1]_{p^{\vartheta}} \neq [x_3]_{p^{\vartheta}}$. So, $\Psi_N(n) = 2$, as promised.

(2.) Now suppose that $p \equiv -1 \; mod \; 4$. In this case, the congruence $x^2 \equiv -1 \; mod \; p^{\vartheta}$ has no solution. Therefore, if the congruence $x^4 \equiv 1 \; mod \; p^{\vartheta}$ has a solution $x$, then $x^2 \equiv 1 \; mod \; p^{\vartheta}$. As in 1., the congruence $x^2 \equiv 1 \; mod \; p^{\vartheta}$ has the solutions $x_1 = 1$ and $x_2 = p^{\vartheta} - 1$. It is clear that $[x_1]_{p^{\vartheta}} = [x_2]_{p^{\vartheta}}$. That is, $\Psi_N(n) = 1$, as claimed.

Consequently, from the above and theorem 2.4, the proof of theorem 2.5 is completed. □

# References


[1] M. Akbaş,*The Normalizer of Modular Subgroup*, Ph. D. Thesis (1989), Faculty of Mathematical Studies, University of Southampton, Southampton, UK.
[2] J.S. Rose, *A Course on Group Theory*, Cambridge University Press (1978), Cambridge, UK.
[3] G.A. Jones, D. Singerman, K. Wicks, *The modular group and generalized Farey graphs*, London Math. Soc. Lecture Notes Series 160 (1991), Cambridge University Press, Cambridge, UK.
[4] N.L. Biggs, A.T. White, *Permutation Groups and Combinatorial Structures, 33rd edn.*, London Mathematical Society Lecture Note Series (1979), Cambridge University Press, Cambridge, UK.
[5] A. Büyükkaragöz, *Signatures and graph connections of some subgroups of extended modular group*, PhD Thesis (2019), Ordu University, Ordu, Turkey.
[6] G.H. Hardy, E.M. Wright,*An introduction to the theory of numbers, 5th edn*, Oxford University Press (1979), Oxford, UK.
[7] G.A. Jones, D. Singerman, *Complex Functions: An Algebraic and Geometric Viewpoint* Cambridge University Press (1997), UK.
[8] C.C. Sims, *Graphs and finite permutation groups*, Math. Zeitschr, 95(1967), 76–86.