Montes Taurus J. Pure Appl. Math. 7 (4), 64–73, 2025

Montes Taurus Journal of Pure and Applied Mathematics

https://www.mtjpamjournal.com

MTJPAM
ISSN: 2687-4814

# On the cusp number of a special congruence subgroup of the modular group

Seda Öztürk [a]

[a]*Department of Mathematics, Karadeniz Technical University, Trabzon, Türkiye*

**Abstract**

In this paper, we investigate the cusp structure of a special congruence subgroup of the modular group. Our motivation is to understand how arithmetic conditions on congruence subgroups influence the geometric and combinatorial properties of the associated Fuchsian groups. Using the action of the group on the extended rational numbers, we develop a systematic method to classify orbits corresponding to cusps. This approach allows us to distinguish cusps according to their denominators and to determine the number of inequivalent cusps in each case. As a result, we obtain an explicit formula for the cusp number of the group in terms of arithmetic data related to the level parameter. Our results provide a complete description of the cusp structure of the group and contribute to the study of signatures and invariants of congruence subgroups of the modular group.

*Keywords:* Fuchsian groups, congruence subgroups, cusp number, modular group, group action

*2020 MSC:* 20H05, 20H10, 30F35

## 1. Introduction

A discrete subgroup $\Lambda$ of $\mathrm{PSL}(2,\mathbb{R})$ acting properly discontinuously on the upper half-plane $\mathbb{U}$ is called a Fuchsian group and forms a central object in hyperbolic geometry. The quotient space $\mathbb{U}\backslash\Lambda$ obtained from such an action is a hyperbolic Riemann surface, whose global structure can be described by invariants such as genus, elliptic fixed points, and cusps. Among these, the cusp number is particularly important, as it captures the contribution of parabolic elements to the geometry of the quotient space. Algebraically, cusps correspond one-to-one with the conjugacy classes of parabolic elements in $\Lambda$, while geometrically they describe the asymptotic ends of the associated hyperbolic surface. This invariant plays a fundamental role in arithmetic contexts as well, influencing the structure of discrete groups and appearing naturally in the analysis of parabolic components in trace formulas and related spectral studies.

Within the framework of modular subgroups and Fuchsian groups, the cusp number emerges as a key invariant capturing essential geometric and arithmetic information. For a discrete subgroup of $\mathrm{PSL}(2,\mathbb{R})$, this invariant is defined as the cardinality of the set of inequivalent cusps, which is equivalent to counting conjugacy classes of parabolic elements. These cusps arise as fixed points of parabolic isometries on the boundary of the upper half-plane and represent the non-compact ends of the corresponding modular curve. In terms of arithmetic structure, cusp numbers govern the properties of congruence subgroups and influence both the geometry of modular curves and their compactifications. Consequently, cusp numbers play a decisive role in the theory of automorphic forms and contribute fundamentally to the parabolic components appearing in trace formulas and related spectral analyses.

†*Article ID:* MTJPAM-D-24-00182

*Email address:* seda.ozturk@ktu.edu.tr (Seda Öztürk)

Received:5 November 2024, Accepted:12 February 2026, Published:22 November 2026

⋆*Corresponding Author:* Seda Öztürk



This work is licensed under a Creative Commons Attribution 4.0 International License.

This viewpoint reveals a close parallel between parabolic subgroups of Fuchsian groups and translation subgroups occurring in Euclidean discrete group actions, underscoring a common structural theme in the geometry of quotient spaces. For a Fuchsian group $\Lambda$, the parabolic subgroups are precisely the maximal cyclic subgroups generated by parabolic elements together with the identity. The cusp number of $\Lambda$ is defined as the number of conjugacy classes of these subgroups. When $\Lambda$ is of the first kind, parabolic subgroups become indispensable for describing the geometry and topology of the associated quotient surface. In this setting, the cusp number serves as a bridge between the algebraic properties of $\Lambda$ and the geometric structure of a fundamental domain, and it provides a foundation for the study of signatures and other invariants of Fuchsian groups.

For Fuchsian groups $\Lambda$ of $\mathrm{PSL}(2,\mathbb{R})$ we recall the following facts. In [5, 12, 13], a limit point of $\Lambda$ is a point $\alpha \in \mathbb{C} \cup \{\infty\}$ if there exists a $z \in \mathbb{C} \cup \{\infty\}$ and a sequence of distinct $V_n \in \Lambda$ such that $V_n z \to \alpha$ (that is, the sequence $\{V_n(z)\}$ converges to $\alpha$).

A Fuchsian group $\Lambda$ is called the first kind if its limit set is $\mathbb{R} \cup \{\infty\}$; otherwise it is called the second kind (*cf.* [3, 13]).

To illustrate these concepts, we now present standard examples of Fuchsian groups of the first and second kind. As is well known, the modular group

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}$$

is a Fuchsian group of the first kind, whose limit set is the entire extended real line $\mathbb{R} \cup \{\infty\}$ in [5].

Another important family of Fuchsian groups of the first kind is given by the principal congruence subgroups

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : a \equiv d \equiv 1,\ b \equiv c \equiv 0 \pmod{N} \right\}.$$

Since $\Gamma(N)$ has finite index in $\Gamma$, its limit set is also $\mathbb{R} \cup \{\infty\}$ in [5].

On the other hand, the cyclic group $\Lambda_0$ generated by the transformation $z \mapsto 2z$, which is a subgroup of $\mathrm{PSL}(2,\mathbb{R})$, is also an example of a Fuchsian group of the second kind (*cf.* [5]).

As in [22] and [14], Fuchsian groups $\Lambda$ of the first kind have the following presentations:

Generators:

$$\begin{aligned} a_1, b_1, ..., a_g, b_g \quad & (hyperbolic), \\ e_1, ..., e_k \quad & (elliptic), \\ p_1, ..., p_t \quad & (parabolic), \end{aligned}$$

and relations:

$$e_1^{m_1} = ... = e_k^{m_k} = \prod_{i=1}^{g} [a_i, b_i] \prod_{l=1}^{k} e_l \prod_{j=1}^{t} p_j = 1.$$

Here, the generators of the Fuchsian group are given as follows (*cf.* [5]):

Hyperbolic generators $a_1, b_1, \ldots, a_g, b_g$ have traces whose absolute values are greater than 2 and they have two distinct fixed points in $\mathbb{R} \cup \{\infty\}$.

Elliptic generators $e_1, \ldots, e_k$ have traces whose absolute values are less than 2 and they have two complex conjugate fixed points in $\mathbb{C} \cup \{\infty\}$.

Parabolic generators $p_1, \ldots, p_t$ have traces whose absolute values are equal to 2 and they have exactly one fixed point in $\mathbb{R} \cup \{\infty\}$.

With this presentation, we say that $\Lambda$ has the signature $(g; m_1, \ldots, m_k; t)$, where $g$ denotes the genus of the underlying Riemann surface, $m_1, \ldots, m_k$ are the periods of the non-conjugate elliptic elements (that is, the generating elliptic elements of $\Lambda$), and $t$ is the cusp number, namely the number of non-conjugate maximal cyclic subgroups of $\Lambda$ generated by parabolic elements.

Several authors, such as (*cf.* [1, 2, 4], [7]-[11], [15]-[18], [21, 23]), have made significant contributions to this area. The signature $(g; m_1, \ldots, m_k; t)$ is both a geometric and a topological invariant of the group $\Lambda$. As shown in [5], the cusp number $t$ coincides with the number of non-equivalent rational points under $\Lambda$.

An important special congruence subgroup of the modular group $\Gamma$ is

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \,(\mathrm{mod}\ N) \right\}$$

(*cf.* [20]).

It is known in book of Schoeneberg [20] that the cusp number of $\Gamma_0(N)$, which is the number of $\Gamma_0(N)-$inequivalent rational cusps, is equal to

$$\sum_{a|N} \varphi\left(\left(a, \frac{N}{a}\right)\right),$$

where $\varphi$ is the Euler function. Here, $(x, y)$ is the greatest common divisor of $x$ and $y$.

Let $N$ be a positive integer. In this paper, we calculate the cusp number $\beta(N)$ of the special congruence subgroup

$$G = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma : a \equiv d \equiv \pm 1 \,(\mathrm{mod}\ N) \right\}$$

of the modular group $\Gamma$ by using its action on the extended rationals $\hat{\mathbb{Q}}$, which is very important for the signatures of the Fuchsian groups in general (*cf.* [5]). The group $G$ is finitely generated, and as shown in [13], it has the limit set $\mathbb{R} \cup \{\infty\}$; hence, $G$ is a Fuchsian group of the first kind and possesses a signature as described above.

## 2. Main results

In this section, we describe the methodology used to determine the cusp number of the special congruence subgroup $G$ of the modular group. Our approach combines arithmetic properties of the subgroup with its action on the extended rational numbers $\hat{\mathbb{Q}}$. By analyzing the orbits of rational points under the group action, we classify the inequivalent cusps and provide explicit formulas for their number. This technique leverages the interplay between the algebraic structure of $G$ and the geometric features of its fundamental domain, providing a systematic framework for calculating cusp numbers of finitely generated Fuchsian groups of the first kind.

To make this approach concrete, we first recall how the elements of $G$ act on $\hat{\mathbb{Q}}$.

The action of elements $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $G$ on $\hat{\mathbb{Q}}$ is that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} k \\ l \end{pmatrix} = \frac{ak + bl}{ck + dl},$$

and if $(k, l) = 1$, then $(ak + bl, ck + dl) = 1$ (*cf.* [5, 6]).

Throughout this section, we use the following notations.

We denote the orbit of $\frac{k}{l}$ under the action of $G$ by $\left[\frac{k}{l}\right]$ and the symbol $[|x|]$ denotes the greatest integer less than or equal to $x$.

**Lemma 2.1.** *If we denote the orbit of $\frac{k}{l}$ under $G$ by $\left[\frac{k}{l}\right]$, then $\left[\frac{k}{l}\right] = \left[\frac{k \mp l}{l}\right]$.*

*Proof.* $\begin{pmatrix} 1 & \mp 1 \\ 0 & 1 \end{pmatrix} \in G$ and $\begin{pmatrix} 1 & \mp 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} k \\ l \end{pmatrix} = \frac{k \mp l}{l}$. Hence, $\frac{k}{l}$ and $\frac{k \mp l}{l}$ belong to the same orbit under $G$, which proves the lemma. □

*Remark* 2.2. From Lemma 2.1, we assume that $k$ and $l$ are non-negative with $k \leq l$. Indeed, if $k > 0$, then $k + tl > 0$ for some integer $t$, and if $k > l$ then $k - ul \leq l$ for some integer $u$. Of course, if $l = 0$, then $\frac{k}{l} = \infty$.

**Theorem 2.3.** *Let $k, l$, and $N$ be positive integers and let $l \equiv l_0 \pmod N$ with $l_0 \neq 0$. Then there exists some $\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in G$ such that*

$$\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\begin{pmatrix} k \\ l \end{pmatrix} = \frac{ak+bl}{l_0}.$$

*Here, $l_o = N$ is allowed.*

*Proof.* Since $l \equiv l_o \pmod N$, we easily see that $(l, N) = (l_o, N)$. Let $N_o = (l_o, N)$. Then

$$\left(\frac{l}{N_o}, \frac{N}{N_o}\right) = \left(\frac{l_o}{N_o}, \frac{N}{N_o}\right) = 1.$$

In this case, there exist $c_1, d_1 \in \mathbb{Z}$ with $(c_1, d_1) = 1$ such that $\frac{Nk}{N_o}c_1 + d_1\frac{l}{N_o} = \frac{l_o}{N_o}$. That is, $\frac{Nk}{N_o}c_1 - \frac{l}{N_o}(-d_1) = \frac{l_o}{N_o}$. It is well-known for all $n \in \mathbb{Z}$,

$$\frac{Nk}{N_o}\left(c_1 + \frac{l}{N_o}n\right) - \frac{l}{N_o}\left(-d_1 + \frac{Nk}{N_o}n\right) = \frac{l_o}{N_o}. \tag{1.1}$$

Now, we find an integer $n \in \mathbb{Z}$ such that $-d_1 + \frac{Nk}{N_o}n \equiv -1 \pmod N$ and we obtain $\frac{Nk}{N_o}n \equiv d_1 - 1 \pmod N$. From the above, we obtain

$$d_1\frac{l}{N_o} \equiv \frac{l_o}{N_o} \pmod{\frac{N}{N_o}}$$

and $d_1\frac{l_o}{N_o} \equiv \frac{l_o}{N_o} \pmod{\frac{N}{N_o}}$. Since $\left(\frac{l_o}{N_o}, \frac{N}{N_o}\right) = 1$, we have

$$d_1 \equiv 1 \pmod{\frac{N}{N_o}} \quad \text{and} \quad \frac{N}{N_o} \mid (d_1 - 1).$$

Since $(k, N_o) = 1$, there exists $k^{-1} \in \mathbb{Z}$ such that $kk^{-1} \equiv 1 \pmod{N_o}$, that is, $kk^{-1} = 1 + N_o t_o$ with $t_o \in \mathbb{Z}$. Put

$$n_o := k^{-1}\frac{d_1 - 1}{\frac{N}{N_o}}.$$

Then

$$-d_1 + \frac{Nk}{N_o}n_o = -d_1 + \frac{Nk}{N_o}\left(k^{-1}\frac{d_1-1}{\frac{N}{N_o}}\right) = -d_1 + kk^{-1}(d_1 - 1) = -d_1 + (1 + N_o t_o)(d_1 - 1) \equiv -1 \pmod{N_o}.$$

Hence, let $c_2 := c_1 + \frac{l}{N_o}n_o$ and $d_2 := -d_1 + \frac{Nk}{N_o}n_o$. Then $d_2 \equiv -1 \pmod N$. From (1.1), we get $Nkc_2 + l(-d_2) = l_o$. Without loss of generality, we suppose that $(c_2, d_2) = 1$. Otherwise, using this pair $c_2, d_2$ in (1.1), we find solutions with desired property. In this case, we get $(Nc_2, d_2) = 1$. Therefore, there are integers $a, b$ such that $-ad_2 - bNc_2 = 1$. Consequently, $\begin{pmatrix} a & b \\ Nc_2 & -d_2 \end{pmatrix}$ is in $G$ and that $\begin{pmatrix} a & b \\ Nc_2 & -d_2 \end{pmatrix}\begin{pmatrix} k \\ l \end{pmatrix} = \frac{ak+bl}{l_o}$. This concludes the proof. □

Here we note that from Theorem 2.3, throughout the paper, we suppose $l \leq N$.

**Theorem 2.4.** *Let $N, l$ be positive integers with $1 \leq l < N$. Then, there exists some $T = \begin{pmatrix} a & b \\ cN & d \end{pmatrix}$ in $G$ such that*

$$\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\begin{pmatrix} k \\ l \end{pmatrix} = \frac{ak+bl}{N-l}.$$

*Proof.* Let $N_o = (l, N)$. Then $\left(\frac{l}{N_o}, \frac{N}{N_o}\right) = \left(\frac{Nk}{N_o}, \frac{l}{N_o}\right) = 1$. So, there exist $c_1, d_1 \in \mathbb{Z}$ with $(c_1, d_1) = 1$ and $c_1\frac{Nk}{N_o} - \left(\frac{l}{N_o}(-d_1)\right) = \frac{N-l}{N_o}$. Furthermore, for all $n \in \mathbb{Z}$,

$$\frac{Nk}{N_o}\left(c_1 + \frac{l}{N_o}n\right) - \frac{l}{N_o}\left(-d_1 + \frac{Nk}{N_o}n\right) = \frac{N-l}{N_o}.$$

We need to find an integer $n \in \mathbb{Z}$ such that $-d_1 + \frac{Nk}{N_o}n \equiv -1 \pmod{N}$. From the above, we get $\frac{l}{N_o}d_1 \equiv -\frac{l}{N_o} \pmod{\frac{N}{N_o}}$. $\left(\frac{l}{N_o}, \frac{N}{N_o}\right) = 1$ derives that $d_1 \equiv -1 \pmod{\frac{N}{N_o}}$ and $\frac{N}{N_o}|(d_1 + 1)$. Since $(k, N_o) = 1$, we have an integer $n \in \mathbb{Z}$ that $kn \equiv \frac{d_1+1}{\frac{N}{N_o}} \pmod{N_o}$. That is, $n \equiv k^{-1}\frac{d_1+1}{\frac{N}{N_o}} \pmod{N_o}$. So, take $n_o := k^{-1}\frac{d_1+1}{\frac{N}{N_o}}$, where $kk^{-1} = 1 + tN_o$ with $t \in \mathbb{Z}$.
Consequently,

$$-d_1 + \frac{Nk}{N_o}n_o = -d_1 + \frac{Nk}{N_o}\left(k^{-1}\frac{d_1+1}{\frac{N}{N_o}}\right) = -d_1 + kk^{-1}(d_1+1) \equiv 1 \pmod{N_o}.$$

Now let $d_o := -d_1 + \frac{Nk}{N_o}n_o$ and $c_o := c_1 + \frac{l}{N_o}n_o$. Then $Nkc_o - ld_o = N - l$. By Theorem 2.3, we have $(Nc_o, d_o) = 1$. Hence, there exist $a, b \in \mathbb{Z}$ such that $-ad_o - bN_oc_o = 1$.
Therefore,

$$\begin{pmatrix} a & b \\ Nc_o & -d_o \end{pmatrix} \in G \quad \text{and} \quad \begin{pmatrix} a & b \\ Nc_o & -d_o \end{pmatrix}\begin{pmatrix} k \\ l \end{pmatrix} = \frac{ak + bl}{N - l}.$$

This concludes the proof.

□

*Remark* 2.5. In Theorem 2.4, we take $l < N$. Otherwise, if $l = N$, the result, in general, is not true. For example, if $l = N = 5$, then $\begin{pmatrix} a & b \\ 5c & d \end{pmatrix}\begin{pmatrix} 3 \\ 5 \end{pmatrix} = \frac{3a+5b}{0}$ which is impossible, because $a \equiv 2 \pmod{5}$. In this case, $\begin{pmatrix} a & b \\ 5c & d \end{pmatrix}$ is not in $G$.

Note that from Theorem 2.4, if we are given a rational number $\frac{k}{l}$, then we may suppose $1 \le l \le [|\frac{N}{2}|]$.

**Theorem 2.6.** *Let $l, N$ be positive integers such that $1 \le l \le [|\frac{N}{2}|]$ and $(l, N) = 1$.*
*If $\frac{k_1}{l}, \frac{k_2}{l} \in \mathbb{Q}$ with $(k_1, l) = (k_2, l) = 1$, then there exists $T = \begin{pmatrix} a & b \\ cN & d \end{pmatrix}$ in $G$ satisfying $T\left(\frac{k_1}{l}\right) = \frac{k_2}{l}$. In this case, there is just one orbit (cusp) with denominator $l$. We denote the set of these $l$ by $P$.*

*Proof.* By Theorem 2.3, we get an element $T = \begin{pmatrix} a & b \\ cN & d \end{pmatrix}$ in $G$ such that $\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\begin{pmatrix} k_1 \\ l \end{pmatrix} = \frac{ak_1 + bl}{l}$. Then $cNk_1 + dl = l$ and $c \equiv 0 \pmod{l}$. Therefore, we take the element $\begin{pmatrix} a & b \\ cNl & d \end{pmatrix}$ instead of $\begin{pmatrix} a & b \\ cN & d \end{pmatrix}$. Hence, $d = 1 - cNk_1$. We now find an integer $c \in \mathbb{Z}$ such that $d = 1 - cNk_1 \equiv k_2^{-1}k_1 \pmod{l}$ with $k_2^{-1}k_2 \equiv 1 \pmod{l}$. Then $cNk_1 \equiv 1 - k_2^{-1}k_1 \pmod{l}$. Hence, $c \equiv (Nk_1)^{-1}(1 - k_2^{-1}k_1) \pmod{l}$.
Now let us take $c = (Nk_1)^{-1}(1 - k_2^{-1}k_1)$. In this case, $(d, cNl) = 1$. Since $ad \equiv 1 \pmod{l}$, $d \equiv k_2^{-1}k_1 \pmod{l}$, we have $ak_1 \equiv k_2 \pmod{l}$. From this, we get $ak_1 + bl = k_2 + tl$ for some $t \in \mathbb{Z}$. Therefore,

$$\begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ cNl & d \end{pmatrix}\begin{pmatrix} k_1 \\ l \end{pmatrix} = \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} k_2 + tl \\ l \end{pmatrix} = \frac{k_2}{l}.$$

This completes the proof of Theorem 2.6.

□

**Theorem 2.7.** *Let $l, N$ be positive integers with $2 \leq l \leq [|\frac{N}{2}|]$ and $l \mid N$. Then the following statements hold:*

**(a)** *If $N = 2l$, then there exists $T \in G$ such that $T\left(\frac{k}{l}\right) = \frac{l-k}{l}$.*

**(i)** *If $l = 2$, then there is one orbit $\left[\frac{1}{2}\right]$.*

**(ii)** *If $l > 2$, then there are $\frac{\varphi(l)}{2}$ orbits with representatives $\frac{k}{l}$.*

**(b)** *If $N \geq 3l$, then the number of orbits with representatives $\frac{k}{l}$ is just $\varphi(l)$.*

*Proof.* **(a)** Let $N = 2l$. By Theorem 2.3, there exists $\begin{pmatrix} a & b \\ cN & d \end{pmatrix}$ in $G$ such that $\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\begin{pmatrix} k \\ l \end{pmatrix} = \frac{ak+bl}{l}$. That is $c\frac{N}{l}k + d = 1$. Since $N = 2l$, then $(N, k) = 1$ or 2. In any case, there exists some integer $c$ such that $d = 1 - c\frac{N}{l}k \equiv -1 \pmod{N}$. It is clear that $(cN, d) = 1$ and $a \equiv -1 \pmod{N}$. Therefore, $ak + bl \equiv ak \equiv -k \pmod{l} \equiv l - k \pmod{l}$. As in Theorem 2.6, $\frac{k}{l}$ is sent to $\frac{l-k}{l}$ under the group $G$.

**(i)** Let $l = 2$. In this case, the result is clear.

**(ii)** Let $l > 2$. Then $\varphi(l)$ is even. Since $\frac{k}{l}$ goes only to $\frac{l-k}{l}$, the number of orbits $\left[\frac{k}{l}\right]$ is just $\frac{\varphi(l)}{2}$.

**(b)** As in (a) $c\frac{N}{l}k + d = 1$. Therefore, $d \equiv 1 \pmod{\frac{N}{l}}$. Since $N \geq 3l$, the case where $d \equiv -1 \pmod{N}$ does not occur. That is, we always get the congruence $d \equiv 1 \pmod{N}$. In this case, $\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\begin{pmatrix} k \\ l \end{pmatrix} = \frac{ak+bl}{l}$. $ak \equiv k \pmod{N}$ and Lemma 2.1, give that $\frac{ak+bl}{l}$ is sent to $\frac{k}{l}$ by $G$. Consequently, the number of orbits $\left[\frac{k}{l}\right]$ is just $\varphi(l)$. This completes the proof.

□

Let us denote by $D$ the set of all such $l$ as in Theorem 2.7.

**Definition 2.8.** Let $N$ be a positive integer. The function $\mu : D \to \mathbb{N}$ is defined by

$$\mu(l) := \begin{cases} 1, & l = 2, N = 4 \\ \frac{\varphi(l)}{2}, & l > 2, N = 2l \\ \varphi(l), & N \geq 3l. \end{cases}$$

**Theorem 2.9.** *Let $l, N, N_o$ be positive integers with $2 \leq l \leq [|\frac{N}{2}|]$, $(l, N) = N_o > 1$ and $l \nmid N$ and let $(k, l) = (k+mN_o, l) = 1$ for some $m \in \mathbb{N}$. Then, $T = \begin{pmatrix} a & b \\ cN & d \end{pmatrix}$ in $G$ such that $T\left(\frac{k}{l}\right) = \frac{k+mN_o}{l}$.*

*And the number of orbits $\left[\frac{k}{l}\right]$ is just $\varphi(N_o)$.*

*Proof.* By Theorem 2.3, there exists some element $\begin{pmatrix} a & b \\ cN & d \end{pmatrix}$ in $G$ such that $\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\begin{pmatrix} k \\ l \end{pmatrix} = \frac{ak+bl}{l}$. So, $cNk + dl = l$. From this, we get $c \equiv 0 \pmod{\frac{l}{N_o}}$. Without loss of generality, let us take $c \equiv 0 \pmod{l}$, otherwise take $N_oN$ in place of $N$ in Theorem 2.3. In this case, the result in Theorem 2.3 is not changed. So, take $U = \begin{pmatrix} a & b \\ cNl & d \end{pmatrix}$ instead of $\begin{pmatrix} a & b \\ cN & d \end{pmatrix}$. Now, we show that, for some $c$, $\begin{pmatrix} a & b \\ cNl & d \end{pmatrix}\begin{pmatrix} k \\ l \end{pmatrix} = \frac{k+mN_o}{l}$. $cNkl + dl = l$ or $cNk + d = 1$. Then $d = 1 - cNk$. Since, $(k + mN_o, l) = 1$, then $(k + mN_o)^{-1}$ exists in $\pmod{l}$.

Now let us find some integer $c$ such that $d = 1 - cNk \equiv (k + mN_o)^{-1}k \pmod{l}$ holds.

$$\text{If } 1 - cNk \equiv (k + mN_o)^{-1}k \pmod{l}, \text{then } cNk \equiv 1 - (k + mN_o)^{-1}k \pmod{l}. \tag{1.2}$$

On the other hand, there exists some integer $l_o$ such that

$$l_o l = -1 + (k + mN_o)^{-1}(k + mN_o) = -1 + k(k + mN_o)^{-1} + mN_o(k + mN_o)^{-1}.$$

Hence, $(N_o| - 1 + k(k + mN_o)^{-1})$. From (1.2), $c\dfrac{N}{N_o}k \equiv \dfrac{1 - (k + mN_o)^{-1}k}{N_o} \pmod{\dfrac{l}{N_o}}$. Since, $\left(\dfrac{Nk}{N_o}, \dfrac{l}{N_o}\right) = 1$, then

$$c \equiv \left(\frac{N}{N_o}k\right)^{-1} \frac{1 - (k + mN_o)^{-1}k}{N_o} \pmod{\frac{l}{N_o}}.$$

Therefore, $c = \left(\dfrac{N}{N_o}k\right)^{-1} \dfrac{1 - (k + mN_o)^{-1}k}{N_o}$ is one of the integer we looked for. Since $ad \equiv 1 \pmod{l}$, we have $ak \equiv k + mN_o \pmod{l}$. Hence there exists some integer $l_1$ such that $ak = k + mN_o + l_1 l$. Put $V := \begin{pmatrix} 1 & -b - l_1 \\ 0 & 1 \end{pmatrix}$. Then the element $T = V \circ U$ is in $G$ and sends $\dfrac{k}{l}$ to $\dfrac{k + mN_o}{l}$. We find the number of orbits as follows.

Let us define $A = \{a_1, a_2, \ldots, a_{\varphi(l)}\}$ to be the set of all positive integers less than $l$ that are coprime with $l$ and $a_1 < a_2 < \cdots < a_{\varphi(l)}$. Let $B = \{b_1, b_2, \ldots, b_{\varphi(N_o)}\}$ be the subset of $A$ such that $b_1 < b_2 < \cdots < b_{\varphi(N_o)}$ and the elements are chosen, starting $a_1$, in order so that if, for some $m$, $b_m > N_o$ then $b_m \in B$ if and only if $b_m - kN_o \notin A$ for all $k \in \mathbb{N}$. Suppose $b_1, b_2, \ldots, b_s < N_o$ and $b_{s+1}, \ldots, b_{\varphi(N_o)} > N_o$. In this case, for $1 \le i \le \varphi(N_o) - s, b_{s+i} \not\equiv b_1, b_2, \ldots, b_s \pmod{N_o}$. In fact, suppose that for some $1 \le i \le \varphi(N_o) - s$ there exists $b_v \in \{b_1, \ldots, b_s\}$ such that $b_{s+i_o} \equiv b_v \pmod{N_o}$. Hence, we have $k_o \in \mathbb{N}$ such that $b_{s+i_o} = b_v + k_o N_o$. In this case, $b_{s+i_o} - k_o N_o = b_v \in B$ which contradicts with the choice of $b_{s+i_o}$. Therefore the elements $b_{s+1}, \ldots, b_{\varphi(N_o)}$ are not congruent to any $b_1, b_2, \ldots, b_s \pmod{N_o}$. Now we show that any pair of the elements $b_{s+1}, \ldots, b_{\varphi(N_o)}$ are not congruent $\bmod N_o$.

Suppose that $b_g \equiv b_h \pmod{N_o}$ and $b_g > b_h$. In this case, for some $u \in \mathbb{N}, b_g - uN_o = b_h \in A$ again a contradiction. Now, finally, we show that for all $a_t \in A$ there exist $k_t \in \mathbb{N} \cup \{0\}$ and $b_t \in B$ such that $a_t = b_t + k_t N_o$. Let $a_t \equiv b_o \pmod{N_o}$. It is clear that $(b_o, N_o) = 1$. If $(b_o, l) = 1$, then we take $b_o$ as $b_t$. Let $(b_o, l) > 1$. Since $a_t \equiv b_o \pmod{N_o}$, there exists a positive integer $u \in \mathbb{N}$ such that $a_t = b_o + uN_o$. Suppose that the number $b_o + u_o N_o, u_o \in \mathbb{N}$, is the smallest one with $b_o + u_o N_o \in A$. It is clear that $b_o + u_o N_o \in B$. Taking $b_t := b_o + u_o N_o$ and $k_t = u - u_o$ we get that $a_t = b_o + uN_o = b_t + k_t N_o$. All these show that if $(N, l) = N_o > 1$, the number of elements of $B$ which is the number of orbits with representatives $\dfrac{a}{l}$ is just $\varphi(N_o)$ because if $\begin{pmatrix} a & b \\ cNl & d \end{pmatrix}\begin{pmatrix} k_1 \\ l \end{pmatrix} = \dfrac{k_2}{l}$ then $k_1 \equiv k_2 \pmod{N_o}$.

□

Let us denote by $R$ the set of all such $l$ as in Theorem 2.9.

**Example 2.10.** By using Theorem 2.9 for $N = 300, l = 140, N_o = (300, 140) = 20$, we obtain

$$A = \left\{\frac{1}{140}, \frac{3}{140}, \frac{9}{140}, \ldots, \frac{139}{140}\right\} \quad \text{and} \quad B = \left\{\frac{1}{140}, \frac{3}{140}, \frac{9}{140}, \frac{11}{140}, \frac{13}{140}, \frac{17}{140}, \frac{19}{140}, \frac{27}{140}\right\}.$$

We notice that $\dfrac{23}{140} \in A$ but $\dfrac{23}{140} \notin B$, since

$$\frac{23 - 1 \cdot N_o}{140} = \frac{23 - 1 \cdot 20}{140} = \frac{3}{140} \in B.$$

Furthermore, we have

$$\frac{1}{140}, \frac{41}{140}, \frac{61}{140}, \frac{81}{140}, \frac{101}{140}, \frac{121}{140} \in \left[\frac{1}{140}\right],$$

$$\frac{3}{140}, \frac{23}{140}, \frac{43}{140}, \frac{63}{140}, \frac{83}{140}, \frac{103}{140} \in \left[\frac{3}{140}\right],$$

$$\frac{9}{140}, \frac{29}{140}, \frac{69}{140}, \frac{89}{140}, \frac{109}{140}, \frac{129}{140} \in \left[\frac{9}{140}\right],$$

$$\frac{11}{140}, \frac{31}{140}, \frac{51}{140}, \frac{71}{140}, \frac{111}{140}, \frac{131}{140} \in \left[\frac{11}{140}\right],$$

$$\frac{13}{140}, \frac{33}{140}, \frac{53}{140}, \frac{73}{140}, \frac{93}{140}, \frac{113}{140} \in \left[\frac{13}{140}\right],$$

$$\frac{17}{140}, \frac{37}{140}, \frac{57}{140}, \frac{97}{140}, \frac{117}{140}, \frac{137}{140} \in \left[\frac{17}{140}\right],$$

$$\frac{19}{140}, \frac{39}{140}, \frac{59}{140}, \frac{79}{140}, \frac{99}{140}, \frac{119}{140} \in \left[\frac{19}{140}\right],$$

$$\frac{27}{140}, \frac{47}{140}, \frac{67}{140}, \frac{87}{140}, \frac{107}{140}, \frac{127}{140} \in \left[\frac{27}{140}\right].$$

Thus, we have $\varphi(20) = 8$ orbits.

**Lemma 2.11.** *Let $k, N$ be positive integers, and let $T, S$ be elements of $G$. Then, we have*

$$T\left(\frac{k}{N}\right) = \frac{k}{N} \quad \text{and} \quad S\left(\frac{k}{N}\right) = \frac{N-k}{N}.$$

*Proof.* By Theorem 2.3, we have an element $\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in G$ such that $\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\begin{pmatrix} k \\ N \end{pmatrix} = \frac{ak+bN}{N}$. So $ck + d = 1$. We find an integer $c$ such that $d = 1 - ck \equiv 1 \pmod{N}$. Let $c = N$. Hence, $d = 1 - Nk$ and $(cN, d) = (N^2, d) = 1$. Since $d \equiv 1 \pmod{N}$, then $a \equiv 1 \pmod{N}$. Therefore, $ak + bN \equiv ak \equiv k \pmod{N}$. So, for some $m$, $ak + bN = k + mN$. Let $T = \begin{pmatrix} 1 & -m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ cN & d \end{pmatrix}$. Then $T\left(\frac{k}{N}\right) = \begin{pmatrix} 1 & -m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} k+mN \\ N \end{pmatrix} = \frac{k}{N}$. Now, we find some integer $c$ such that $d = 1 - ck \equiv -1 \pmod{N}$. From this, $ck \equiv 2 \pmod{N}$. So, $c \equiv 2k^{-1} \pmod{N}$. Take $c = 2k^{-1}$, it is clear that $(cN, d) = 1$ and $d \equiv -1 \pmod{N}$ gives that $a \equiv -1 \pmod{N}$. Hence, $ak + bN \equiv -k \pmod{N}$. So, as the above, $\frac{k}{N}$ is sent to $\frac{-k}{N}$ or $\frac{N-k}{N}$. The number of such rationals is

$$\begin{cases} 1 & \text{if } N = 2 \\ \dfrac{\varphi(N)}{2} & \text{if } N > 2 \end{cases} \quad \text{which is} \quad \left[\left|\frac{\varphi(N)+1}{2}\right|\right].$$

□

**Corollary 2.12.** *Let $N$ be a positive integer. Then $\infty$, $\frac{1}{N}$, and $\frac{N-1}{N}$ belong to the same orbit $[\infty]$ of $G$.*

*Proof.* It is easily checked that $\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} \in G$ and $\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{N}$. From Lemma 2.11, the proof is completed.

□

We now arrive at the main result of the paper.

**Theorem 2.13.** *Let $N$ be a positive integer. Then, the cusp number $\beta(N)$ of the group*

$$G = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma : a \equiv d \equiv \pm 1 \pmod{N} \right\}$$

*is*

$$\beta(N) = |P| + \sum_{l \in D} \mu(l) + \sum_{l \in R} \varphi(l, N) + \left[ \left| \frac{\varphi(N) + 1}{2} \right| \right].$$

*Proof.* The numbers of cusps appearing in Theorem 2.6, Theorem 2.7, Theorem 2.9, and Lemma 2.11 are given respectively by

$$|P|, \quad \sum_{l \in D} \mu(l), \quad \sum_{l \in R} \varphi(l, N), \quad \left[ \left| \frac{\varphi(N) + 1}{2} \right| \right].$$

Since any two cusps are distinct, the sum of these quantities yields the main result. □

We conclude the paper by giving an example of Theorem 2.13.

**Example 2.14.** Let $N = 45$ with $\left[ \left| \frac{45}{2} \right| \right] = 22$. Using Theorem 2.13, we get $1 \leq l \leq 22$ and

$$P = \{1, 2, 4, 7, 8, 11, 13, 14, 16, 17, 19, 22\},$$

$$D = \{3, 5, 9, 15\} \qquad \text{and} \qquad R = \{6, 10, 12, 18, 20, 21\}.$$

Thus, we have $\beta(45) = 12 + 20 + 20 + 12 = 64$.

## 3. Conclusion

In this paper, we studied the cusp number of a special congruence subgroup of the modular group. By examining the structure of parabolic subgroups and employing arithmetic properties of the underlying group, we obtained an explicit formula for the number of inequivalent cusps. This result gives deeper insight into the distribution of cusps in such subgroups and emphasizes the close relationship between group theory and number theory in the context of modular groups. The techniques developed here may be extended in several directions. One natural problem is to apply similar arguments to other congruence subgroups of the modular group in order to determine their cusp numbers explicitly. Another promising direction is to investigate how the distribution of cusps influences the theory of modular forms, automorphic functions, and the spectral theory of Fuchsian groups. Furthermore, the connection with classical arithmetic functions such as Euler function suggests that deeper number-theoretic structures may underlie these results. We hope that the ideas presented in this work will provide a foundation for further research on cusp distributions, subgroup structures of modular groups, and their applications in number theory and geometry.

## Acknowledgments

This paper is dedicated to Professor Hari Mohan Srivastava on the occasion of his 85th anniversary.

The author sincerely thanks the editors and the referees for their careful reading of the manuscript and for their insightful and constructive comments, which have substantially contributed to improving the quality and clarity of this work.

***Author Contributions:*** This paper has only one author.

***Conflict of Interest:*** The author declares no conflict of interest.

***Funding (Financial Disclosure):*** There is no funding for this work.

## References


[1] M. Akbaş, *The normalizer of modular subgroups*, University of Southampton, Ph.D. Thesis, 1989.
[2] M. Akbaş and D. Singerman, *The signature of the normalizer of* $\Gamma_0(N)$, London Math. Soc. Lecture Note Ser. **165**, 77–86, 1992.
[3] A. F. Beardon, *The geometry of discrete groups*, Springer-Verlag, New York, 1983.
[4] T. Hsu, *Identifying congruence subgroups of the modular group*, Proc. Amer. Math. Soc. **124 (5)**, 1351–1359, 1996.
[5] G. A. Jones and D. Singerman, *Complex functions: An algebraic and geometric viewpoint*, Cambridge University Press, Cambridge, 1987.
[6] G. A. Jones, D. Singerman and K. Wicks, *The modular group and generalized Farey graphs*, London Math. Soc. Lecture Note Ser. **160**, 316–338, 1991.
[7] R. Keskin, *On the parabolic class number of some subgroups of Hecke groups*, Turkish J. Math. **22 (2)**, 199–206, 1998.
[8] R. Keskin, *On the parabolic class numbers of some Fuchsian groups*, Note Mat. **19**, 275–283, 1999.
[9] R. Keskin, *A note on some modular subgroups*, Rocky Mountain J. Math. **35 (2)**, 573–585, 2005.
[10] R. Keskin, *Parabolic class number of a subgroup of the normalizer of* $\Gamma_0(m)$, Miskolc Math. Notes **13**, 365–373, 2012.
[11] M. L. Lang, *The signature of* $\Gamma_0^+(n)$, J. Algebra **241**, 146–185, 2001.
[12] J. Lehner, *Discontinuous groups and automorphic functions*, Mathematical Surveys and Monographs (Number 8), Amer. Math. Soc., Providence, Rhode Island, 1964.
[13] J. Lehner, *A short course in automorphic functions*, Holt, Rinehart and Winston Inc., New York, 1966.
[14] C. Maclachlan, *Groups of units of zero ternary quadratic forms*, Proc. Roy. Soc. Edinburgh Sect. A **88**, 141–157, 1981.
[15] G. Muić, *On the cusp forms for the congruence subgroups of* $SL_2(\mathbb{R})$, Ramanujan J. **21**, 223–239, 2010.
[16] S. Öztürk, *Graphs of congruence subgroups*, Karadeniz Technical University, Institute of Science, Ph.D. Thesis, Trabzon, 2017.
[17] S. Öztürk, *A generalization of the suborbital graphs generating Fibonacci numbers for the subgroup* $\Gamma^3$, Filomat **34 (2)**, 631–638, 2020.
[18] S. Öztürk, *Fibonacci numbers sequence derived from suborbital graphs for the modular group* $\Gamma$, Bilecik Seyh Edebali Univ. J. Sci. **11 (2)**, 308–315, 2024.
[19] S. Öztürk, Y. Kesicioğlu and H. Şengül, *Solutions of congruence equations via an imprimitive action of some modular subgroups*, Adv. Stud. Euro-Tbil. Math. J. **16 (Suppl. 3)**, 139–143, 2023.
[20] B. Schoeneberg, *Elliptic modular functions*, Springer-Verlag, New York, 1974.
[21] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, 1971.
[22] D. Singerman, *Subgroups of Fuchsian groups and finite permutation groups*, Bull. Lond. Math. Soc. **2 (3)**, 319–323, 1970.
[23] H. C. Wilkie, *On non-Euclidean crystallographic groups*, Math. Z. **91**, 87–102, 1966.


**How to cite this article:** S. Öztürk, *On the cusp number of a special congruence subgroup of the modular group*, Montes Taurus J. Pure Appl. Math. **7 (4)**, 64–73, 2025; Article ID: MTJPAM-D-24-00182.