On Suborbital Graphs of the Congruence Subgroup \( \Gamma_0(N) \)

Bahadir O. Guler, Serkan Kader and Murat Besenk

**Abstract**—In this paper we examine some properties of suborbital graphs for the congruence subgroup \( \Gamma_0(N) \). Then we give necessary and sufficient conditions for graphs to have triangles.

**Keywords**—Congruence subgroup, Imprimitive action, Modular group, Suborbital graphs.

I. INTRODUCTION

Let \( \Gamma \) denote the inhomogeneous group \( \text{PSL}(2, \mathbb{Z}) \) acting on the upper half plane \( H := \{ z \in \mathbb{C} : \text{Im}(z) > 0 \} \) via:

\[
A(z) = \frac{az + b}{cz + d}, \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.
\]

Among the subgroups of \( \Gamma \) the congruence subgroups such as

\[
\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid a = d = 1 \mod N, b = c = 0 (\mod N) \right\}
\]

have been the objects of detailed studies due to their significance in the arithmetic of elliptic curves, integral quadratic forms, elliptic modular forms in [5], [6]. In this paper, we define \( \Gamma^*(N) \) as the group obtained by adding the stabilizer of \( \infty \) to the congruence subgroup \( \Gamma(N) \), that is,

\[
\Gamma^*(N) := \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \Gamma(N) \right\}
\]

which is easily seen that

\[
\Gamma^*(N) = \left\{ \begin{pmatrix} 1 + aN & b \\ cN & 1 + dN \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, \det = 1 \right\}.
\]

II. THE ACTION OF \( \Gamma_0(N) \) ON \( \hat{\mathbb{Q}} \)

Every element of \( \hat{\mathbb{Q}} := \mathbb{Q} \cup \{ \infty \} \) can be represented as a reduced fraction \( \frac{x}{y} \), with \( x, y \in \mathbb{Z} \) and \( (x, y) = 1 \). Since \( \frac{x}{y} = \frac{-x}{-y} \), this representation is not unique. We represent \( \infty \) as \( \frac{1}{0} \). The action of the matrix \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \) on \( \frac{x}{y} \) is

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{x}{y} = \frac{ax + by}{cx + dy}.
\]

It is easily seen that if \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \) and \( \frac{x}{y} \in \hat{\mathbb{Q}} \) is a reduced fraction then, since \( c(ax + by) - a(cx + dy) = -y \) and \( d(ax + by) - b(cx + dy) = x \),

\[
(ax + by, cx + dy) = 1.
\]

The action of a matrix on \( \frac{x}{y} \) and on \( \frac{-x}{-y} \) is identical.

**Theorem 2.1.** The action of \( \Gamma_0(N) \) on \( \hat{\mathbb{Q}} \) is not transitive.

**Proof.** From (1), for \( \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N) \)

\[
\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} a + bN \\ cN + dN \end{pmatrix},
\]

is a reduced fraction, so \( \frac{1}{N} \) is not sent to \( \frac{1}{N+1} \) under the action of \( \Gamma_0(N) \).

Without loss of generality, for making calculations easier, \( N \) will be a prime \( p \) throughout the paper.

**Theorem 2.2.** The orbits of \( \Gamma_0(p) \) are \( \left\{ \frac{1}{1} \right\} \) and \( \left\{ \frac{1}{p} \right\} \).

**Proof.** Using the corollaries from [2] we can write down the sets of orbits of \( \Gamma_0(N) \) in general

\[
\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid \frac{x}{y} \in \hat{\mathbb{Q}} : (p, y) = b, x = a \mod \left( b, \frac{N}{b} \right) \right\}.
\]

Bahadir O. Guler, is with the Rize University, Department of Mathematics, Faculty of Arts and Science, Rize-Turkey. email: bahadir@ktu.edu.tr.

Serkan Kader and Murat Besenk are with Karadeniz Technical University, Department of Mathematics, Faculty of Arts and Science, Trabzon-Turkey. emails: serkankader@mynet.com, besenk@ktu.edu.tr.
Then we have
\[
\left\{ \frac{1}{p} \right\} = \left\{ \frac{k}{yp} : k \in \mathbb{Z}, (k, yp) = 1 \right\}
\]
and
\[
\left\{ 1 \right\} = \left\{ \frac{k}{\ell} : k, \ell \in \mathbb{Z}, (k, \ell) = 1 \right\}.
\]

We now consider the imprimitivity of the action of \( \Gamma_s(p) \) on \( \mathbb{Q} \).

Let \( (G, \Omega) \) be transitive permutation group, consisting of a group \( G \) acting on a set \( \Omega \) transitively. An equivalence relation \( \equiv \) on \( \Omega \) is called \( G \)-invariant if whenever \( \alpha, \beta \in \Omega \) satisfy \( \alpha \equiv \beta \) then \( g(\alpha) \equiv g(\beta) \) for all \( g \in G \). The equivalence classes are called blocks.

We call \( (G, \Omega) \) imprimitive if \( \Omega \) admits some \( G \)-invariant equivalence relation different from

(i) the identity relation, \( \alpha \equiv \beta \) if and only if \( \alpha = \beta \)
(ii) the universal relation, \( \alpha \equiv \beta \) for all \( \alpha, \beta \in \Omega \).

Otherwise \( (G, \Omega) \) is called primitive. We now give a lemma from [3].

**Lemma 2.3.** Let \( (G, \Omega) \) be transitive. \( (G, \Omega) \) imprimitive if and only if \( G_\alpha \), the stabilizer of a point \( \alpha \in \Omega \), is a maximal subgroup of \( G \) for each \( \alpha \in \Omega \).

What the lemma is saying is whenever \( G_\alpha \leq H \leq G \), then \( \Omega \) admits some \( G \)-invariant equivalence relation other than trivial cases. In fact, since \( G \) acts transitively, every element of \( \Omega \) has the form \( g(\alpha) \) for some \( g \in G \). If we define the relation \( \equiv \) on \( \Omega \) as
\[
g(\alpha) \equiv g'(\alpha) \quad \text{if and only if} \quad g' \in gH,
\]
then it is easily seen that it is non-trivial \( G \)-invariant equivalence relation. That is \( (G, \Omega) \) imprimitive.

From the above we see that the number of blocks is equal to the index \(| G : H |\).

We now apply these ideas to the case where \( G \) is the \( \Gamma_s(p) \) and \( \Omega \) is \( \mathbb{Q} \). An obvious choice for \( H \) is \( \Gamma' \). Clearly \( \Gamma_s \leq \Gamma'(p) \leq \Gamma_s(p) \). Then we have \( \Gamma_s(p) \) acts transitively and imprimitively on the set \( \left\{ \frac{1}{p} \right\} \).

Let \( \approx \) denote the \( \Gamma_s(p) \)-invariant equivalence relation induced on \( \left\{ \frac{1}{p} \right\} \) by \( \Gamma_s(p) \) as:
\[
\text{If } \nu = \frac{a}{pc_1} \quad \text{and} \quad \omega = \frac{a}{pc_2} \quad \text{are elements of } \left\{ \frac{1}{p} \right\}, \text{ then} \nu = g(\alpha) \quad \text{and} \quad \omega = g'(\alpha) \quad \text{for elements} \quad g, g' \in \Gamma_s(p) \quad \text{of the form} \quad g = \left( \begin{array}{cc} a & b \\ pc_1 & d_1 \end{array} \right), \quad g' = \left( \begin{array}{cc} a & b' \\ pc_2 & d_1 \end{array} \right).
\]

Now \( \nu \approx \omega \) if and only if \( g^{-1}g' \in \Gamma'(p) \), that is,
\[
g^{-1}g' = \left( \begin{array}{cc} d_1a_1 - p(c_2b_1) & d_2b_1 - b_1d_1 \\ pc_1c_2 - c_1a_1 & a_1d_1 - p(c_1b_1) \end{array} \right) \in \Gamma'(p)
\]
if and only if \( d_1a_1 = 1 \pmod{p} \) and \( d_1a_1 = 1 \pmod{p} \). Then \( a_1d_1a_2 = a_1 \pmod{p} \) and so \( a_1 = a_2 \pmod{p} \).

Hence we see that
\[
\nu \approx \omega \quad \text{if and only if} \quad a_1 = a_2 \pmod{p}
\]

By our general discussion of imprimitivity, the number \( \psi(p) \) of equivalence class under \( \approx \) is given by
\[
\psi(p) = |\Gamma_s(p) : \Gamma'(p)|.
\]

Since \( \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \in \Gamma(p) \), then \( |\Gamma'(p) : \Gamma(p)| = p \). From [6], we know that
\[
|\Gamma : \Gamma(N)| = N \prod_{p \mid N} \left( 1 - \frac{1}{p^2} \right) \quad \text{and} \quad |\Gamma_s(p) : \Gamma(N)| = N \prod_{p \mid N} \left( 1 + \frac{1}{p} \right).
\]

Calculating for \( N = p \) and using the following equation
\[
|\Gamma : \Gamma(p)| = |\Gamma : \Gamma_s(p)| \cdot |\Gamma_s(p) : \Gamma'(p)| \cdot |\Gamma'(p) : \Gamma(p)|,
\]
we have that
\[
\left\{ \frac{1}{p} \right\} = \left\{ \frac{1}{p} \right\} \cup \left\{ \frac{2}{p} \right\} \cup \ldots \cup \left\{ \frac{p-1}{p} \right\}.
\]

From (1), it is clear that
\[
\left\{ \frac{1}{p} \right\} = \left\{ \frac{1 + xp}{yp} : x, y \in \mathbb{Z} \right\} \equiv [x] = \left\{ \frac{1}{p} \right\}.
\]
III. SUBORBITAL GRAPHS

In 1967 Sims introduced the idea of suborbital graphs of a permutation group $G$ acting on a set $\Omega$; these are graphs with vertex set $\Omega$, on which $G$ induces automorphism in [7]. Also in [8] the applications are used in finite groups.

Let $(G,\Omega)$ be transitive permutation group. Then $G$ acts on $\Omega \times \Omega$ by
$$g : (\alpha, \beta) \rightarrow (g(\alpha), g(\beta)),$$ $g \in G$ and $\alpha, \beta \in \Omega$.

The orbits of this action are called suborbital graphs of $G$. The $\gamma$-orbit of $\alpha$, that is, the set of all $g(\alpha)$ for $g \in G$, is denoted by $O(\gamma)$. If $O(\gamma)$ is a single element, we call that element $\gamma$. If $O(\gamma)$ contains two or more elements, we call $O(\gamma)$ a block of $G$.

Let $(G,\Omega)$ be transitive permutation group. Then $G$ acts on $\Omega \times \Omega$ by
$$g : (\alpha, \beta) \rightarrow (g(\alpha), g(\beta)),$$ $g \in G$ and $\alpha, \beta \in \Omega$.

The orbits of this action are called suborbital graphs of $G$, that containing $(\alpha, \beta)$ being denoted by $O(\alpha, \beta)$. From $O(\alpha, \beta)$ we can form a subgraph of $G(\alpha, \beta)$ : its vertices are the elements of $\Omega$, and there is a directed edge from $\gamma$ to $\delta$, denoted by $\gamma \rightarrow \delta$, if $O(\gamma, \delta) \in O(\alpha, \beta)$. We can draw this edge as a hyperbolic geodesic in the upper-half plane $H$.

In this final section, we determine the suborbital graphs for $\Gamma_o(p)$ on $\left[ \begin{array}{c} 1 \\ p \end{array} \right]$. Since $\Gamma_o(p)$ acts transitively on $\left[ \begin{array}{c} 1 \\ p \end{array} \right]$, each suborbital contains a pair $(\alpha, \beta)$ for some $\beta \in \left[ \begin{array}{c} 1 \\ p \end{array} \right]$. Therefore, it is sufficient to do the calculations only for the block $[\infty]$. Let $F_{p, \infty}$ denote the subgraph of $G_{p, \infty}$ whose vertices form the block $[\infty]$.

Theorem 3.2. $\Gamma_o(p)$ permutes the vertices and the edges of $F_{p, \infty}$ transitively.

Proof. Suppose that $u, v \in [\infty]$. As $\Gamma_o(p)$ acts on $\left[ \begin{array}{c} 1 \\ p \end{array} \right]$ transitively, $g(u) = v$ for some $g \in \Gamma_o(p)$. Since $u \equiv \infty \mod p$ and $v \equiv \infty \mod p$ is $\Gamma_o(p)$-invariant equivalence relation, then $g(u) \equiv g(\infty)$, that is, $v \equiv g(\infty)$. Thus, as $g(\infty) \in [\infty]$, $g \in \Gamma_o(p)$.

Assume that $v, w \in [\infty]$, $x, y \in [\infty]$ and $v \rightarrow w$, $x \rightarrow y \in F_{p, \infty}$. Then $v, w \in O_{p, \infty}$ and $(x, y) \in O(p, \infty)$. Therefore, for some $S, T \in \Gamma_o(p)$
$$S(\infty) = v, S\left[ \frac{u}{p} \right] = w; T(\infty) = x, T(\infty) = y.$$ As $S(\infty), T(\infty) \in [\infty]$, then $S, T \in \Gamma_o(p)$. So this proof is completed.
Theorem 3.3. $F_{u,p}$ contains a triangle if and only if $u^2 + u + 1 = 0 \pmod{p}$.

Proof. Since $\Gamma'(p)$ permutes the vertices transitively $F_{u,p}$ and $\infty \to \frac{u}{p}$, then we may suppose that triangle has the form

$$\infty \to \frac{u}{p} \to v \to \infty.$$ 

Assume that $v = \frac{x}{yp}$, $y > 0$. Since $\frac{x}{yp} \to 1 \frac{1}{0}$, then

$$0 \cdot x - yp = \pm p.$$ 

As $y > 0$, then $y = 1$. Therefore $v = \frac{x}{y}$. Since $\frac{u}{p} \to \frac{x}{y}$, then from Theorem 3.1 we obtain

$$u - x = 1 \quad \text{and} \quad x = u^2 \pmod{p} \quad (2)$$

$$u - x = -1 \quad \text{and} \quad x = -u^2 \pmod{p} \quad (3)$$

From (2) and (3), we have that

$$u^2 - u + 1 = 0 \pmod{p} \quad \text{and} \quad u^2 + u + 1 = 0 \pmod{p}$$

respectively.

Conversely, suppose that $u^2 + u + 1 = 0 \pmod{p}$. Clearly, we have the triangle

$$\infty \to \frac{u}{p} \to \frac{u + 1}{p} \to \infty$$

from Theorem 3.1.

ACKNOWLEDGMENT

We would like to express our sincere thanks to Professor Mehmet Akbas for his immense help during the preparation of this paper.

REFERENCES