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 triangels.

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

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

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

have been the objects of detailed studies due to their signifiance in the arithmetic of elliptic curves, integral quadratic forms, elliptic modular forms in [5], [6]. In this paper, we define $\Gamma_0(N)$ as the group obtained by adding the stabilizer of $\infty$ to the congruence subgroup $\Gamma(N)$, that is,

$$\Gamma_0(N) := \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \Gamma(N) \right\}$$

which is easily seen that

$$\Gamma_0(N) = \left\{ \begin{pmatrix} 1 + aN & b \\ cN & 1 + dN \end{pmatrix} : a, b, c, d \in \mathbb{Z}, \det = 1 \right\}.$$

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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \frac{x}{y} \rightarrow \frac{ax + by}{cx + dy}.$$ 

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 $\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$

$$\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \frac{1}{N} = \frac{a + bN}{cN + dN}$$

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

$$\begin{pmatrix} a \\ b \end{pmatrix} = \left\{ \frac{x}{y} \in \hat{\mathbb{Q}} : (p, y) = b, x \equiv a \pmod{b, \frac{N}{b}} \right\}.$$
Then we have
\[
\begin{cases}
1 & = \left\{ \frac{k}{yp} : k \in \mathbb{Z}, (k, yp) = 1 \right\}, \\
1 & = \left\{ \frac{k}{\ell} : k, \ell \in \mathbb{Z}, (k, \ell) = 1 \right\}.
\end{cases}
\]

and
\[
\begin{cases}
1 & = \left\{ \frac{k}{\ell} : k, \ell \in \mathbb{Z}, (k, \ell) = 1 \right\}.
\end{cases}
\]

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 \( \approx \) on \( \Omega \) is called \( G \)-invariant if whenever \( \alpha, \beta \in \Omega \) satisfy \( \alpha \approx \beta \) then \( g(\alpha) \approx g(\beta) \) for all \( g \in G \). The equivalence classes are called blocks.

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

(i) the identity relation, \( \alpha \approx \beta \) if and only if \( \alpha = \beta \)

(ii) the universal relation, \( \alpha \approx \beta \) 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. \((G, \Omega)\) is primitive 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 \( G \) 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 \( \approx \) on \( \Omega \) as
\[
g(\alpha) \approx g'(\alpha) \text{ if and only if } g' \in gH,
\]
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 \( \Gamma(p) \). Clearly \( \Gamma_s \leq \Gamma(p) \leq \Gamma_s(p) \). Then we have

Corollary 2.4. \( \left( \Gamma_s(p), \mathbb{Q} \right) \) is imprimitive permutation group.

\( \Gamma_s(p) \) acts transitively and imprimitively on the set \( \{1/p\} \).

Let \( \approx \) denote the \( \Gamma_s(p) \)-invariant equivalence relation induced on \( \{1/p\} \) by \( \Gamma_s(p) \) as:

If \( v = \frac{a_1}{pc_1} \) and \( w = \frac{a_2}{pc_2} \) are elements of \( \{1/p\} \), then
\[
v \approx w \Leftrightarrow v = g(\alpha) \text{ and } w = g'(\alpha) \text{ for elements } g, g' \in \Gamma_s(p) \text{ of the form}
\]
\[
g = \left( \begin{array}{cc} a & b \\ pc_1 & d \end{array} \right), \quad g' = \left( \begin{array}{cc} a' & b' \\ pc_2 & d' \end{array} \right).
\]

Now \( v \approx w \) if and only if \( g^{-1}g' \in \Gamma(p) \), that is,
\[
g^{-1}g' = \left( \begin{array}{cc} d & -p(c_bh) \\ pc(a_c - c_a) & d - p(c_b) \end{array} \right) \in \Gamma(p)
\]
if and only if \( d_{a_1} = 1 \mod p \) and \( d_{a_2} = 1 \mod p \). Then
\[
a_{d_1} = a_{d_2} \mod p \text{ and so } a_{d_1} = a_{d_2} \mod p.
\]

Hence we see that
\[
v \approx w \text{ if and only if } a_1 = a_2 \mod p (1)
\]

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 \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^p \in \Gamma(p) \), then \( |\Gamma(p) : \Gamma(p)| = p \). From [6], we know that
\[
|\Gamma : \Gamma(N)| = N \prod_{p^r \equiv 1 \mod p} \left( 1 - \frac{1}{p^r} \right) \text{ and } |\Gamma : \Gamma_s(N)| = N \prod_{p^r} \left( 1 + \frac{1}{p} \right).
\]

Calculating for \( N = p \) and using the following equation
\[
|\Gamma : \Gamma(p)| = \prod_{p^r \equiv 1 \mod p} \left( 1 + \frac{1}{p} \right) \cup \left( 1 + \frac{1}{p} \right) \cup \cdots \cup \left( 1 + \frac{1}{p} \right)
\]
we have that
\[
\begin{pmatrix} 1 \\ p \end{pmatrix} = \left[ \begin{array}{c} 1 \\ p \end{array} \right] \cup \left[ \begin{array}{c} 2 \\ p \end{array} \right] \cup \cdots \cup \left[ \begin{array}{c} p - 1 \\ p \end{array} \right].
\]

From (1), it is clear that
\[
\begin{pmatrix} 1 \\ p \end{pmatrix} = \left[ \begin{array}{c} 1 + xp \\ yp \end{array} : x, y \in \mathbb{Z} \right] \equiv [x] = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.
\]
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 

$$g: (\alpha, \beta) \rightarrow (g(\alpha), g(\beta)), \ g \in G \text{ and } \alpha, \beta \in \Omega.$$ 

The orbits of this action are called suborbitals of $G$, that containing $(\alpha, \beta)$ being denoted by $O(\alpha, \beta)$. From $O(\alpha, \beta)$ we can form a suborbital graph $G(\alpha, \beta)$; its vertices are the elements of $\Omega$, and there is a directed edge from $\gamma$ to $\delta$, denoted by $\gamma \rightarrow \delta$, if $(\gamma, \delta) \in O(\alpha, \beta)$. 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 $O_\alpha(p)$ on $[1 \ p]$. Since $O_\alpha(p)$ acts transitively on $[1 \ p]$, each suborbit contains a pair $(\alpha, \beta)$ for some $\beta \in [1 \ p]$; $\beta = u/p$, we denote this suborbital by $O_{u/p}$ and corresponding subgraph by $G_{u/p}$.

$G_{u/p}$ is a disjoint union of $\psi(\beta)$ subgraphs forming blocks with respect to $\approx = O_\alpha(p)$ -invariant equivalence relation. $O_\alpha(p)$ permutes these blocks transitively and these subgraphs are all isomorphic $[4]$.

Therefore, it is sufficient to do the calculations only for the block $[\infty]$. Let $F_{u/p}$ denote the subgraph of $G_{u/p}$ whose vertices form the block $[\infty]$.

**Theorem 3.1.** Let $r/s$ and $x/y$ be in the block $[\infty]$. Then there is an edge $r/s \rightarrow x/y$ in $F_{u/p}$ if and only if 

$$x = \pm ur \ (mod \ p) \text{ and } r = 1(mod \ p), \ ry - sx = \mp p$$

$$y = \pm su \ (mod \ p) \text{ and } s = 0(mod \ p), \ ry - sx = \pm p.$$  

**Proof.** Since $r/s \rightarrow x/y \in F_{u/p}$, then there exists some $T \in \Gamma(\alpha)$ such that $T$ sends the pair $\begin{pmatrix} u \\ p \end{pmatrix}$ to the pair $\begin{pmatrix} r \\ s \\ x \\ y \end{pmatrix}$, that is, for $T = \begin{pmatrix} 1 + ap \\ pc \ 1 + dp \end{pmatrix} \in \Gamma(\alpha)$, det $T = 1$,

$$T\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{r}{s} \text{ and } T\begin{pmatrix} u \\ p \end{pmatrix} = \frac{x}{y}.$$  

From these equations, it is clear that $x = ur \ (mod \ p)$ and $y = su \ (mod \ p)$.

Furthermore, 

$$\begin{pmatrix} 1 + ap \\ pc \ 1 + dp \end{pmatrix} \begin{pmatrix} u \\ p \end{pmatrix} = \begin{pmatrix} r \\ x \\ s \\ y \end{pmatrix},$$  

so that $ry - sx = p$.

Conversely, let be $x = ur \ (mod \ p)$ and $y = su \ (mod \ p)$ and also $r = 1(mod \ p)$ and $s = 0(mod \ p)$ Then there are $b, d \in \mathbb{Z}$ such that $x = ur + bp$ and $y = su + dp$. If we put these equivalences in $ry - sx = p$, we obtain

$$r(us + dp) - s(ur + bp) = p.$$  

Since

$$\begin{pmatrix} r \\ b \\ s \\ d \end{pmatrix} \begin{pmatrix} u \\ 0 \end{pmatrix} = \begin{pmatrix} r \\ ur + bp \\ s \\ us + dp \end{pmatrix},$$  

then $rd = bs = 1$. As $rd - bs = 1(mod \ p)$ and $s = 0(mod \ p)$, then $rd = 1(mod \ p)$. Since $r = 1(mod \ p)$, we obtain $d = 1(mod \ p)$.

Consequently,

$$A = \begin{pmatrix} r \\ b \\ s \\ d \end{pmatrix}, \ det A = 1 \text{ and } s = 0(mod \ p)$$

so $A \in \Gamma(p)$.

The proof for $(-)$ is similar.

**Theorem 3.2.** $\Gamma(p)$ permutes the vertices and the edges of $F_{u/p}$ transitively.

**Proof.** Suppose that $u,v \in [\infty]$. As $\Gamma(\alpha)$ acts on $[1 \ p]$ transitively, $g(u) = v$ for some $g \in \Gamma(\alpha)$. Since $u \approx \infty$ and $v \approx \infty$ is $\Gamma(\alpha)$ - invariant equivalence relation, then $g(u) \approx g(\infty)$, that is, $v \approx g(\infty)$. Thus, as $g(\infty) \in [\infty]$,

$g \in \Gamma(p)$.

Assume that $v,w \in [\infty]$; $x, y \in \infty$ and $v \rightarrow w, x \rightarrow y \in F_{u/p}.$

Then $(v,w) \in O_{u/p}$ and $(x,y) \in O_{u/p}$. Therefore, for some $S, T \in \Gamma(\alpha)$

$$S(\infty) = v, S\begin{pmatrix} u \\ p \end{pmatrix} = w; T(\infty) = x, T(\infty) = y.$$  

As $S(\infty), T(\infty) \in [\infty]$, then $S, T \in \Gamma(p)$. 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 \( \frac{x}{yp} \to \frac{1}{0} \), 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
\[ u \cdot x = 1 \quad \text{and} \quad x = u^2 \pmod{p} \quad (2) \]
\[ u \cdot x = -1 \quad \text{and} \quad x = -u^2 \pmod{p} \quad (3) \]

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