International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:2, No:7, 2008

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

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

Among the subgroups of Γ the congruence subgroups such as

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

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

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 $\Gamma^*(N)$ as the group obtained by adding the stabilizer of ∞ to the congruence subroup $\Gamma(N)$, that is,

$$\Gamma^*(N) := \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \Gamma(N) \right\rangle$$

which is easily seen that

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

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.

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 ∞ as $\frac{1}{0} = \frac{-1}{0}$. The action of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ on $\frac{x}{y}$ is

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

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

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

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 $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ p \end{pmatrix}$.

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

$$\begin{pmatrix} a \\ b \end{pmatrix} = \left\{ \frac{x}{y} \in \hat{\mathbb{Q}} : (p,y) = b,\ x \equiv a \ \bmod\left(b, \frac{N}{b}\right) \right\}.$$

Then we have

$$\binom{1}{p}=\left\{\frac{k}{yp}:k\in\mathbb{Z},(k,yp)=1\right\}$$

and

$$\binom{1}{1}=\left\{\frac{k}{\ell}:k,\ell\in\mathbb{Z},(k,\ell)=1\right\}.$$

We now consider the imprimitivity of the action of $\Gamma_0(p)$ on $\hat{\mathbb{Q}}$.

Let (G,Ω) be transitive permutation group, consisting of a group G acting on a set Ω transitively. An equivalence relation $\approx$ on Ω 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,Ω) imprimitive if Ω 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,Ω) is called primitive. We now give a lemma from [3].

Lemma 2.3. Let (G,Ω) be transitive. (G,Ω) imprimitive if and only if G_α, 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 $G_\alpha\lneq H\lneq G$, then Ω admits some G – invariant equivalence relation other than trivial cases. In fact, since G acts transitively, every element of Ω has the form $g(\alpha)$ for some $g\in G$. If we define the relation $\approx$ on Ω 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,Ω) 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 $\Gamma_0(p)$ and Ω is $\hat{\mathbb{Q}}$. An obvious choice for H is $\Gamma^*(p)$. Clearly $\Gamma_\infty\lneq\Gamma^*(p)\lneq\Gamma_0(p)$. Then we have

Corollary 2.4. ($\Gamma_0(p)$, $\hat{\mathbb{Q}}$) is imprimitive permutation group.

$\Gamma_0(p)$ acts transitively and imprimitively on the set $\binom{1}{p}$. Let $\approx$ denote the $\Gamma_0(p)$– invariant equivalence relation induced on $\binom{1}{p}$ by $\Gamma_0(p)$ as:

If $v=\frac{a_1}{pc_1}$ and $w=\frac{a_2}{pc_2}$ are elements of $\binom{1}{p}$, then $v=g(\infty)$ and $w=g'(\infty)$ for elements $g,g'\in\Gamma_0(p)$ of the form

$$g=\begin{pmatrix}a_1 & b_1\\ pc_1 & d_1\end{pmatrix}\quad,\quad g'=\begin{pmatrix}a_2 & b_2\\ pc_2 & d_2\end{pmatrix}.$$

Now $v\approx w$ if and only if $g^{-1}g'\in\Gamma^*(p)$, that is,

$$g^{-1}g'=\begin{pmatrix}d_1a_2-p(c_2b_1) & d_1b_2-b_1d_2\\ p(a_1c_2-c_1a_2) & a_1d_2-p(c_1b_2)\end{pmatrix}\in\Gamma^*(p)$$

if and only if $d_1a_2\equiv 1\ (\mathrm{mod}\ p)$ and $d_2a_1\equiv 1(\mathrm{mod}\ p)$. Then $a_1d_1a_2\equiv a_1\ (\mathrm{mod}\ p)$ and so $a_1\equiv a_2\ (\mathrm{mod}\ p)$.
Hence we see that

$$v\approx w\ \text{if and only if}\ a_1\equiv a_2\ (\mathrm{mod}\ p)\qquad (1)$$

By our general discussion of imprimitivity, the number $\psi(p)$ of equivalence class under $\approx$ is given by

$$\psi(p)=|\Gamma_0(p):\Gamma^*(p)|.$$

Since $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^p\in\Gamma(p)$, then $|\Gamma^*(p):\Gamma(p)|=p$. From [6], we know that

$$|\Gamma:\Gamma(N)|=N^3\prod_{p|N}\left(1-\frac{1}{p^2}\right)\ \text{and}\ |\Gamma:\Gamma_0(N)|=N\prod_{p|N}\left(1+\frac{1}{p}\right).$$

Calculating for $N=p$ and using the following equation

$$\underbrace{|\Gamma:\Gamma(p)|}_{p(p^2-1)}=\underbrace{|\Gamma:\Gamma_0(p)|}_{p+1}\cdot\underbrace{|\Gamma_0(p):\Gamma^*(p)|}_{p-1}\cdot\underbrace{|\Gamma^*(p):\Gamma(p)|}_{p},$$

we have that

$$\binom{1}{p}=\begin{bmatrix}1\\ p\end{bmatrix}\cup\begin{bmatrix}2\\ p\end{bmatrix}\cup\ldots\cup\begin{bmatrix}p-1\\ p\end{bmatrix}.$$

From (1), it is clear that

$$\begin{bmatrix}1\\ p\end{bmatrix}=\left\{\frac{1+xp}{yp}:x,y\in\mathbb{Z}\right\}\cong[\infty]=\begin{bmatrix}1\\ 0\end{bmatrix}.$$

International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:2, No:7, 2008

III. SUBORBITAL GRAPHS

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

Let (G,Ω) be transitive permutation group. Then G acts on $\Omega\times\Omega$ by

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

The orbits of this action are called suborbitals of G, that containing (α,β) 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 Ω, and there is a directed edge from γ to δ, denoted by $\gamma\to\delta$, 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 $\Gamma_0(p)$ on $\begin{pmatrix}1\\p\end{pmatrix}$. Since $\Gamma_0(p)$ acts transitively on $\begin{pmatrix}1\\p\end{pmatrix}$, each suborbital contains a pair (∞,v) for some $v\in\begin{pmatrix}1\\p\end{pmatrix}$; $v=\frac{u}{p}$, we denote this suborbital by $O_{u,p}$ and corresponding suborbital graph by $G_{u,p}$.

$G_{u,p}$ is a disjoint union of $\psi(p)$ subgraphs forming blocks with respect to $''\approx''$ $\Gamma_0(p)$–invariant equivalence relation. $\Gamma_0(p)$ 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 $\frac{r}{s}$ and $\frac{x}{y}$ be in the block $[\infty]$. Then there is an edge $\frac{r}{s}\to\frac{x}{y}$ in $F_{u,p}$ if and only if

$$x\equiv\pm ur \pmod p \text{ and } r\equiv 1 \pmod p,\ ry-sx=\pm p$$
$$y\equiv\pm su \pmod p \text{ and } s\equiv 0 \pmod p,\ ry-sx=\pm p.$$

Proof. Since $\frac{r}{s}\to\frac{x}{y}\in F_{u,p}$, then there exists some $T\in\Gamma^*(p)$ such that T sends the pair $\left(\frac{1}{0},\frac{u}{p}\right)$ to the pair $\left(\frac{r}{s},\frac{x}{y}\right)$, that is, for $T=\begin{pmatrix}1+ap & b\\ pc & 1+dp\end{pmatrix}\in\Gamma^*(p)$, det T = 1, $T\begin{pmatrix}1\\0\end{pmatrix}=\frac{r}{s}$ and $T\begin{pmatrix}u\\p\end{pmatrix}=\frac{x}{y}$. From these equations , it is clear that $x\equiv ur \pmod p$ and $y\equiv su \pmod p$.

Furthermore

$$\begin{pmatrix}1+ap & b\\ pc & 1+dp\end{pmatrix}\begin{pmatrix}1 & u\\ 0 & p\end{pmatrix}=\begin{pmatrix}r & x\\ s & y\end{pmatrix},$$

so that $ry-sx=p$.

Conversely, let be $x\equiv ur \pmod p$ and $y\equiv su \pmod p$ and also $r\equiv 1 \pmod p$ and $s\equiv 0 \pmod p$.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

$$\begin{pmatrix}r & b\\ s & d\end{pmatrix}\begin{pmatrix}1 & u\\ 0 & p\end{pmatrix}=\begin{pmatrix}r & ur+bp\\ s & us+dp\end{pmatrix},$$

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

Consequently,

$$A=\begin{pmatrix}r & b\\ s & d\end{pmatrix},\ \det A=1 \text{ and } \begin{matrix}r\equiv d\equiv 1 \pmod p\\ s\equiv 0 \pmod p\end{matrix},$$

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

The proof for (–) is similiar.

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

Proof. Suppose that $u,v\in[\infty]$. As $\Gamma_0(p)$ acts on $\begin{pmatrix}1\\p\end{pmatrix}$ transitively, $g(u)=v$ for some $g\in\Gamma_0(p)$. Since $u\approx\infty$ and $''\approx''$ is $\Gamma_0(p)-$ 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 $v\to w$, $x\to y\in F_{u,p}$. Then $(v,w)\in O_{u,p}$ and $(x,y)\in O_{u,p}$. Therefore, for some $S,T\in\Gamma_0(p)$

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

As $S(\infty), T(\infty)\in[\infty]$, then $S,T\in\Gamma^*(p)$. So this proof is completed.

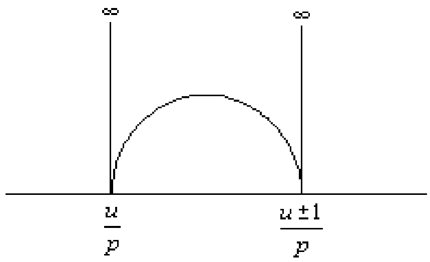

Fig. 1 $F_{u,p}$ – Suborbital Graph

Theorem 3.3. $F_{u,p}$ contains a triangle if and only if $u^2 \pm u + 1 \equiv 0 (\mathrm{mod}\, p)$.

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

$$u - x = 1 \quad \text{and} \quad x \equiv u^2 (\mathrm{mod}\, p) \qquad (2)$$
$$u - x = -1 \quad \text{and} \quad x \equiv -u^2 (\mathrm{mod}\, p) \qquad (3)$$

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

$$u^2 - u + 1 \equiv 0 (\mathrm{mod}\, p) \quad \text{and} \quad u^2 + u + 1 \equiv 0 (\mathrm{mod}\, p)$$

respectively.

Conversely, suppose that $u^2 \pm u + 1 \equiv 0 (\mathrm{mod}\, p)$. Clearly, we have the triangle

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

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

[1] M. Akbas, *On suborbital graphs for the modular group*, Bull. London Math. Soc. 33, no. 6, 2001, pp 647–652.
[2] M. Akbas and T. Başkan, *Suborbital graphs for the normalizer of* $\Gamma_0(N)$, Tr. J. of Mathematics 20, 1996, pp 379-387.
[3] N.L. Bigg and A.T. White, *Permutation groups and combinatorial structures*, London Mathematical Society Lecture Note Series 33, Cambridge Universty Press, Cambridge, 1979.
[4] G.A. Jones, D. Singerman, K. Wicks, *The Modular Group and Generalized Farey Graphs*, London Math. Soc. Lecture Note Series, Vol. 160, Cambridge Universty Press, 1991, pp 316-338.
[5] R. S. Kulkarni, *An Arithmetic-Geometric Method in The Study of The Subgroups of The Modular Group*, American Journal of Mathematics, 113 ,1991, pp 1053-1133.
[6] B. Schoeneberg, *Elliptic Modular Functions*, Springer Verlag, Berlin, 1974.
[7] C. C. Sims, *Graphs and Finite Permutation Groups*, Math. Z., 95, 1967, pp 76-86.
[8] T. Tsuzuku, *Finite Groups and Finite Geometries*, Cambridge University Pres, Cambridge,1982.