Note di Matematica ISSN 1123-2536, e-ISSN 1590-0932
Note Mat. **30** (2010) no. 2, 141–148. doi:10.1285/i15900932v30n2p141

On the Action of $\Gamma^0(N)$ on $\hat{\mathbb{Q}}$

Bahadır Özgür Güler
Department of Mathematics, University of Rize
bahadir.guler@rize.edu.tr

Serkan Kader
Department of Mathematics, University of Nigde
skader@nigde.edu.tr

Received: 31.7.2009; accepted: 29.10.2010.

Abstract. In this paper we examine $\Gamma^0(N)$-orbits on $\hat{\mathbb{Q}}$ and the suborbital graphs for $\Gamma^0(N)$. Each such suborbital graph is a disjoint union of subgraphs whose vertices form a block of imprimitivity for $\Gamma^0(N)$. Moreover, these subgraphs are shown to be vertex $\Gamma^0(N)$-transitive and edge $\Gamma^0(N)$-transitive. Finally, necessary and sufficient conditions for being self-paired edge are provided.

Keywords: Congruence groups, Transitive and Imprimitive action, Suborbital graphs.

MSC 2000 classification: primary 05C25, secondary 20H05

Introduction

Let PSL(2,$\mathbb{R}$) denote the group consisting of the Möbius transformations

$$T : z \to \frac{az+b}{cz+d}\text{ , where } a, b, c \text{ and } d \text{ are real and } ad - bc = 1.$$

This is the automorphism group of the upper half plane $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im(z)} > 0\}$. Γ will denote the modular group, a special subgroup of PSL(2,$\mathbb{R}$) with integral coefficients. Γ is a Fuchsian group whose fundamental domain has finite area, so it has a signature consisting of the geometric invariants

$$(g; m_1, \ldots, m_r, s) \tag{1}$$

where g is the genus of the compactified quotient space, $m_1, \ldots, m_r$ are the periods of the elliptic elements and s is the parabolic class number. The principal congruence subgroup of Γ, denoted by $\Gamma(N)$, is defined to be the subgroup

$$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : a \equiv d \equiv 1 mod N, b \equiv c \equiv 0 mod N\right\}. \tag{2}$$

A subgroup of Γ is called a congruence group provided it contains the principal congruence group $\Gamma(N)$. Congruence groups have been of great interest in many fields of mathematics, such as number theory, group theory, etc. This article is based on the idea of the suborbital graphs of a permutation group G acting on a set Δ introduced by Sims[9]. Some applications of this method can be found in papers [2],[3],[5],[6],[7]. Especially in [3],[6], authors give some results about a connection between the periods of elliptic elements of a chosen permutation group with the circuits in suborbital graphs of it. Our results for $\Gamma^0(N)$ may help to confirm the above idea. The congruence groups

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : b \equiv 0 mod N \right\} \tag{3}$$

are well known [8]. In this study, we define $\Gamma^*(N)$ as the group obtained by adding the stabilizer of 0 to $\Gamma(N)$; that is, $\Gamma^*(N) := \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \Gamma(N) \right\rangle$. It is easily seen that $\Gamma^*(N)$ is equal to

$$\left\{ \begin{pmatrix} 1+aN & bN \\ c & 1+dN \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\} \tag{4}$$

1 The Action of $\Gamma^0(N)$ on $\hat{\mathbb{Q}}$

Every element of $\hat{\mathbb{Q}}$ can be represented as a reduced fraction $\frac{x}{y}$, with $x, y \in \mathbb{Z}$ and $(x, y) = 1$. We represent 0 as $\frac{0}{1} = \frac{0}{-1}$. The action of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ on $\frac{x}{y}$ is

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

Theorem 1. *The action of* $\Gamma^0(N)$ *on* $\hat{\mathbb{Q}}$ *is not transitive.*

Proof. For $\begin{pmatrix} a & bN \\ c & d \end{pmatrix} \in \Gamma^0(N)$, $\begin{pmatrix} a & bN \\ c & d \end{pmatrix} \begin{pmatrix} N \\ 1 \end{pmatrix} = \frac{aN+bN}{cN+d}$ is a reduced fraction, so N is not sent to $N+1$ under the action of $\Gamma^0(N)$.

In this case, we will find a maximal subset of $\hat{\mathbb{Q}}$ on which $\Gamma^0(N)$ acts transitively. For this, we first prove one of our results in the following theorem:

Theorem 2. *Let k/s be an arbitrary rational number with $(k, s) = 1$. Then there exists some element $A \in \Gamma^0(N)$ such that $A(k, s) = (k_1, s_1)$ with $k_1 | N$.*

Proof. $\begin{pmatrix} a & bN \\ c & d \end{pmatrix}\begin{pmatrix} k \\ s \end{pmatrix} = \begin{pmatrix} ak+bsN \\ ck+ds \end{pmatrix}$. We find a pair $\{a, b\}$, for which the equation

$$ak + bsN = (N, k) \tag{5}$$

holds. Let $k_1 = (N, k)$. Since $(k/k_1, sN/k_1) = 1$, there exists a pair $\{a_0, b_0\}$ so that (5) is satisfied. Therefore, the general solution of (5) is

$$a = a_0 + sNn/k_1 \quad and \quad b = b_0 + kn/k_1, \quad where\ n \in \mathbb{Z} \tag{6}$$

Let $N = q_0^{\alpha_0} q_1^{\alpha_1} \cdots p_{s_0}^{\alpha_{s_0}}$ be the prime power decomposition of N. We must show that there exists a pair $\{a_*, b_*\}$ satisfying (6) such that $(a_*, Nb_*) = 1$. If $(N, a_0) = 1$, there is nothing to prove. If $(N, a_0) > 1$, then a_0 does have a common factor with N, say q_0. From (5) we get $(q_0, Ns/k_1) = 1$. Therefore, assuming n to be 1 in (6), we obtain an integer a_1, such that $q_0 | a_1$. If $(N, a_1) > 1$, then a_1 has a common factor with N, say q_1. Let $a_2 = a_1 - q_0Ns/k_1 = 1$. Then a_2 does not have q_1 as a factor. If $(N, a_2) > 1$, then a_2 has a common factor with N, say q_2. Therefore, we first obtain $a_3 = a_2 - q_0q_1Ns/k_1 = 1$ and by induction $a_{s_0+1} = a_{s_0} - q_0q_1 \cdots q_{s_0-1}Ns/k_1$ has no $q_0, q_1 \cdots, q_{s_0}$ as factors. Hence $(N, a_{s_0+1}) = 1$. Let $a_0 = a_{s_0+1}$ with the corresponding b, b_*. So $(a_*, Nb_*) = 1$. This shows that there exits an element (in fact, infinitely many) $A \in \Gamma^0(N)$ such that $A(k, s) = (k_1, s_1)$ with $k_1 | N$. ■

Theorem 3. *Let $a|N$ and $(a, e) = (a, f) = 1$. Then $\begin{pmatrix} a \\ e \end{pmatrix} \approx \begin{pmatrix} a \\ f \end{pmatrix}$ are conjugate under $\Gamma^0(N)$ if and only if $e \equiv f mod(a, N/a)$.*

Proof. The necessary part is obvious by Theorem 2. Let $A = \begin{pmatrix} \alpha & \beta N \\ \gamma & \delta \end{pmatrix} \in \Gamma^0(N)$. Then $A\begin{pmatrix} a \\ e \end{pmatrix} = \begin{pmatrix} \alpha a + \beta e N \\ \gamma a + \delta e \end{pmatrix} = \begin{pmatrix} a \\ f \end{pmatrix}$. Therefore $\gamma a + \delta e = f$, and so $\delta e - f \equiv 0 (mod a)$. Then

$$\alpha + \beta e N/a = 1 \quad and \quad \delta e - f \equiv 0 mod(a, N/a) \tag{7}$$

From $det A$, we have $\alpha\delta \equiv 1 mod(a, N/a)$, and from the above, $\alpha \equiv 1 mod(a, N/a)$. Consequently, $\delta \equiv 1 mod(a, N/a)$.

Theorem 4. *Let $a|N$. Then the orbit $\begin{pmatrix} a \\ e \end{pmatrix}$ of a/e under $\Gamma^0(N)$ is the set $\left\{x/y \in \hat{\mathbb{Q}} : (N, x) = a, e \equiv y\frac{x}{a} mod(a, N/a)\right\}$. Furthermore, the number of orbits $\begin{pmatrix} a \\ e \end{pmatrix}$ with $a|N$ under $\Gamma^0(N)$ is just $\varphi(a, N/a)$, where φ is Euler function.*

Proof. Theorems 2 and 3 complete the proof.

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

Corollary 1. *The orbits of* $\Gamma^0(p)$ *are* $\binom{1}{1}$ *and* $\binom{p}{1}$.

It is clear that $\Gamma_0 < \Gamma^*(p) < \Gamma^0(p)$, so Γ_0 is not maximal in $\Gamma^0(p)$ and hence the action of $\Gamma^0(p)$ on $\binom{p}{1}$ is imprimitive. Then we have

Corollary 2. $(\Gamma^0(p), \binom{p}{1})$ *is an imprimitive permutation group.*

$\Gamma^0(p)$ acts transitively and imprimitively on the set $\binom{p}{1}$. Let $\approx$ denote the $\Gamma^0(p)$-invariant equivalnce relation induced on $\binom{p}{1}$ by $\Gamma^0(p)$ as follows:

If $v = \frac{b_1 p}{d_1}$ and $w = \frac{b_2 p}{d_2}$ are elements of $\binom{p}{1}$, then $v = g(0)$ and $w = g'(0)$ for elements $g, g' \in \Gamma^0(p)$ of the form $\begin{pmatrix} a_1 & b_1 p \\ c_1 & d_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & b_2 p \\ c_2 & d_2 \end{pmatrix}$, respectively. Now $v \approx w$ iff $g^{-1}g' \in \Gamma^*(p)$; that is,

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

iff $d_1a_2 \equiv 1(modp)$ and $a_1d_2 \equiv 1(modp)$. Then $d_1a_1d_2 \equiv d_1(modp)$ and so $d_2 \equiv d_1(modp)$. Hence we see that

$$v \approx w \iff d_1 \equiv d_2(modp). \tag{8}$$

The number $\eta(p)$ of equivalence class under $\approx$ is given by $\eta(p) = |\Gamma^0(p) : \Gamma^*(p)|$. Since $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^p \in \Gamma(p)$, $|\Gamma^*(p) : \Gamma(p)| = p$. From [8], we know that $|\Gamma : \Gamma(N)| = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$ and $|\Gamma : \Gamma^0(N)| = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$. Calculating for $N = p$ and using the equation $|\Gamma : \Gamma(p)| = |\Gamma : \Gamma^0(p)| \cdot |\Gamma^0(p) : \Gamma^*(p)| \cdot |\Gamma^*(p) : \Gamma(p)|$, we have that

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

From (8), it is clear that $\begin{bmatrix} p \\ 1 \end{bmatrix} = \left\{ \frac{xp}{1+yp} : x, y \in \mathbb{Z} \right\} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = [0]$

2 Suborbital Graphs

Let (G, Ω) be a transitive permutation group. Then G acts on $\Omega \times \Omega$ by $g(\alpha, \beta) = (g(\alpha), g(\beta))(g \in G, \alpha, \beta \in \Omega)$.

The orbits of this action are called *suborbitals* of G. The orbit containing (α, β) is 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 if $(\gamma, \delta) \in O(\alpha, \beta)$. A directed edge from γ to δ is denoted by $(\gamma \to \delta)$. If $(\gamma, \delta) \in O(\alpha, \beta)$, then we will say that there exists an edge $(\gamma \to \delta)$ in $G(\alpha, \beta)$. These ideas were first introduced by Sims [9].

If $\alpha = \beta$, then the corresponding suborbital graph $G(\alpha, \alpha)$ is *self-paired*: it consists of a loop based at each vertex $\alpha \in \Omega$. By a *circuit*(or a closed edge path), we mean a sequence $\nu_1 \to \nu_2 \to \cdots \to \nu_m \to \nu_1$, where $m \geq 3$. If $m = 3$ or 4 then the circuit is called a triangle or a rectangle.

In this final section, we determine the suborbital graphs for $\Gamma^0(p)$ on $\binom{p}{1}$. Since $\Gamma^0(p)$ acts transitively on $\binom{p}{1}$, each suborbital contains a pair $(0, v)$ for some $v \in \binom{p}{1}$; i.e., $v = \dfrac{p}{u}$. We denote this suborbital by $O_{p,u}$ and corresponding suborbital graph by $G_{p,u}$ which is a disjoint union of $\eta(p)$ 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. Therefore, it is sufficient to do the calculations only for the block [0]. Let $F_{p,u}$ denote the subgraph of $G_{p,u}$ whose vertices form the block [0].

Theorem 5. *Let r/s and x/y be in block* [0]*. Then there is an edge $r/s \to x/y$ in $F_{p,u}$ iff $x \equiv \pm ur(modp) : r \equiv 0(modp), y \equiv \pm us(modp) : s \equiv 1(modp)$, and $ry - sx = \mp p$.*

(*Plus and minus signs correspond to $r/s > x/y$ and $r/s < x/y$, respectively.*)

Proof. Since $r/s \to x/y \in F_{p,u}$, then there exists some $T \in \Gamma^*(p)$ such that, T sends the pair $\left(\dfrac{0}{1}, \dfrac{p}{u}\right)$ to the pair $\left(\dfrac{r}{s}, \dfrac{x}{y}\right)$; that is,

$$T\left(\frac{0}{1}\right) = \frac{r}{s} \text{ and } T\left(\frac{p}{u}\right) = \frac{x}{y} \quad \text{for } \begin{pmatrix} 1+ap & bp \\ c & 1+dp \end{pmatrix} \in \Gamma^*(p),\ detT = 1.$$

From these equations, it is clear that $x \equiv\ ur(modp) : r \equiv 0(modp), y \equiv us(modp) : s \equiv 1(modp)$. Furthermore, $\begin{pmatrix} 1+ap & bp \\ c & 1+dp \end{pmatrix} \begin{pmatrix} 0 & p \\ 1 & u \end{pmatrix} = \begin{pmatrix} r & x \\ s & y \end{pmatrix}$, so that $ry - sx = -p$.

Conversely, let be $x \equiv\ ur(modp) : r \equiv 0(modp), y \equiv\ us(modp) : s \equiv$

$1(modp)$ and $ry - sx = -p$. Then there are $a, c \in \mathbb{Z}$ such that $x = ur + ap$ and $y = us + cp$. If we put these equivalences in $ry - sx = -p$, we obtain $r(us + cp) - s(ur + ap) = -p$. Since

$$\begin{pmatrix} a & r \\ c & s \end{pmatrix} \begin{pmatrix} 0 & p \\ 1 & u \end{pmatrix} = \begin{pmatrix} r & ur + ap \\ s & us + cp \end{pmatrix},$$

we have $as - rc = 1$. As $as - rc = 1(modp)$ and $r \equiv 0(modp)$, $as \equiv 1(modp)$. Since $s \equiv 1(modp)$, we obtain $a \equiv 1(modp)$. Consequently,

$$A = \begin{pmatrix} a & r \\ c & s \end{pmatrix}, detA = 1, a \equiv s \equiv 1(modp) \ \ and \ \ r \equiv 0(modp),$$

and so $A \in \Gamma^*(p)$. The proof for (-) is similar. ∎

Theorem 6. *$\Gamma^*(p)$ permutes the vertices and the edges of $F_{p,u}$ transitively.*

Proof. Suppose that $u, v \in [0]$. As $\Gamma^0(p)$ acts on $\begin{pmatrix} p \\ 1 \end{pmatrix}$ transitively, $g(u) = v$ for some $g \in \Gamma^0(p)$. Since $u \approx 0$ and $\approx$ is $\Gamma^0(p)$-invariant equivalence relation, $g(u) \approx g(0)$; that is, $v \approx g(0)$. Thus, as $g(0) \in [0]$, $g \in \Gamma^*(p)$.

Assume that $v, w \in [0]$; $x, y \in [0]$ and $v \to w$, $x \to y \in F_{p,u}$. Then $(v, w) \in O_{p,u}$ and $(x, y) \in O_{p,u}$. Therefore, for some $S, T \in \Gamma^0(p)$

$$S(0) = v \ \ and \ \ S(p/u) = w; \ T(0) = x \ \ and \ \ T(p/u) = y.$$

Hence, $S, T \in \Gamma^*(p)$, as $S(0), T(0) \in [0]$. Furthermore, $TS^{-1}(v) = x$ and $TS^{-1}(w) = y$; that is, $TS^{-1} \in \Gamma^*(p)$. ∎

Lemma 1. *Let r/s and x/y be rational numbers such that $r/s - x/y = -1$, where $s \geq 1$, $y \geq 1$. Then there exist no integers between r/s and x/y.*

Proof. Let k be an integer such that $r/s < k < x/y$. Then $r < sk$ and $x > ky$. Thus $1 = sx - ry > sx - sky = s(x - ky) \geq s$, which is a contradiction.

Theorem 7. *No edges of $F_{p,u}$ cross in $\mathbb{H}$.*

Proof. Without loss of generality, because of the transitive action, we can take the edges $0 \to \frac{p}{u}$, $\frac{x_1 p}{1 + y_1 p} \to \frac{x_2 p}{1 + y_2 p}$ and $\frac{x_1 p}{1 + y_1 p} < \frac{p}{u} < \frac{x_2 p}{1 + y_2 p}$, where all letters are positive integers. It is easily seen that $(1+y_1 p)/x_1 > u > (1+y_2 p)/x_2$. On the other hand, $x_1 - x_2 - p(x_1 y_2 - x_2 y_1) = -1$ by Theorem 5. Lemma 1 completes the proof. ∎

Theorem 8. *$F_{p,u}$ has a self-paired edge iff $u^2 \equiv -1(modp)$.*

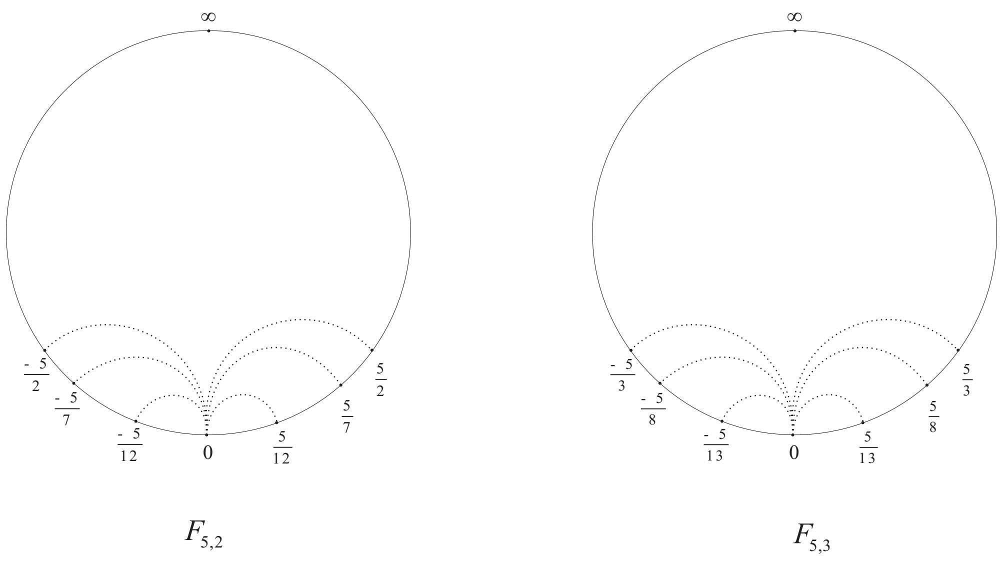

Figure 1. Examples of subgraph

Proof. Because of the transitive action, the form of a self-paired edge can be taken of $0/1 \rightarrow p/u \rightarrow 0/1$. The condition follows immediately from the second edge by Theorem 5.

Corollary 3. *$F_{p,u}$ has a self-paired edge iff $p \equiv 1(mod4)$ or $p = 2$.*

Example 1. Let $p = 5$. Since $|U_5| = \varphi(5) = 4$, $u = 1, 2, 3$ or 4. It is clear that $F_{p,u}$ has a self-paired edge only for $u = 2, 3$.(It is a well-known fact that there are at most two solution for all p such that $p \equiv 1(mod4)$). We can draw these graphs as in Figure 1. For $p < 100$, another subgraph which has a self paired edge is as following; $5, 13, 17, 29, 37, 41, 53, 61, 73, 79, 97$.

Theorem 9. *$F_{p,u}$ contains no triangles.*

Proof. Since $\Gamma^*(p)$ permutes the vertices transitively, we may suppose that the triangle has the form $0/1 \rightarrow p/u \rightarrow p/v \rightarrow 0/1$. From the second edge, we have that $v-u = \pm 1$. Then $v = u \pm 1$. From the second and third edges, we have that $u \equiv 1(modp)$ and $v \equiv 1(modp)$ respectively. It follows from the last equation that these congruences contradict each other. ∎

Acknowledgements. The authors are highly grateful to the referee for their valuable comments and suggestions for improving the paper.

References

[1] M. Akbas, D. Singerman: *The Signature of the normalizer of* $\Gamma_0(N)$, London Math. Soc. Lectures Note Series **165**, (1992),77-86.

[2] M. Akbas, T. Baskan: *Suborbital graphs for the normalizer of* $\Gamma_0(N)$, Tr. J. of Mathematics **20**,(1996), 379-387.

[3] M. Akbas: *On suborbital graphs for the modular group*, Bull. London Math. Soc. **33**, (2001), 647-652.

[4] N.L. Bigg, A.T. White: Permutation groups and combinatorial structures, London Mathematical Society Lecture Note Series **33**, CUP, Cambridge, 1979.

[5] G.A. Jones, D. Singerman, K.Wicks: *The modular group and generalized Farey graphs*, London Math. Soc. Lecture Note Series **160**, CUP, Cambridge, (1991), 316-338.

[6] R. Keskin: *On suborbitals graphs for some Hecke groups*, Discrete Math. **234**, no. 1-3, (2001), 53-64.

[7] R. Keskin: *Suborbital graphs for the normalizer of* $\Gamma_0(m)$, European J. Combin. **27** , no. 2, (2006), 193-206.

[8] B. Schoeneberg: Elliptic modular functions, Springer Verlag, Berlin, 1974.

[9] C.C. Sims: *Graphs and finite permutation groups*, Math. Z. **95**, (1967), 76-86.