Hacettepe Journal of Mathematics and Statistics
Volume 40 (2) (2011), 203 – 210

ELLIPTIC ELEMENTS AND CIRCUITS IN SUBORBITAL GRAPHS

B. Ö. Güler*†, M. Beşenk‡, A. H. Değer‡ and S. Kader§

Received 14 : 06 : 2010 : Accepted 03 : 02 : 2011

Abstract

We consider the action of a permutation group on a set in the spirit of the theory of permutation groups, and graph arising from this action in hyperbolic geometric terms. In this paper, we examine some relations between elliptic elements and circuits in graph for the normalizer of $\Gamma_0(N)$ in $PSL(2,\mathbb{R})$.

Keywords: Normalizer, Signature, Imprimitive action, Suborbital graph.

2010 AMS Classification: 05 C 05, 05 C 20, 11 F 06, 20 H 05.

Communicated by Yücel Tıraş

1. Introduction

Let $PSL(2,\mathbb{R})$ denote the group of all linear fractional transformations

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

In terms of the matrix representation, the elements of $PSL(2,\mathbb{R})$ correspond to the matrices

$$\pm\begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R} \text{ and } ad - bc = 1.$$

This is the automorphism group of the upper half plane $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. The modular group Γ is the subgroup of $PSL(2,\mathbb{R})$ such that a, b, c and d are integers. $\Gamma_0(N)$ is the subgroup of Γ with $N|c$.

*Rize University, Department of Mathematics, 53100 Rize, Turkey.
E-mail: `bahadir.guler@rize.edu.tr`
†Corresponding Author.
‡Karadeniz Technical University, Department of Mathematics, 61080 Trabzon, Turkey.
E-mail: (M. Beşenk) `mbesenk@ktu.edu.tr` (A. H. Değer) `ahdeger@ktu.edu.tr`
§Nigde University, Department of Mathematics, 51240 Nigde, Turkey.
E-mail: `skader@nigde.edu.tr`

In [6], the normalizer $\mathrm{Nor}(N)$ of $\Gamma_0(N)$ in $PSL(2,\mathbb{R})$ consists exactly of the matrices

$$\begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix},$$

where $e\|\frac{N}{h^2}$ and h is the largest divisor of 24 for which $h^2|N$ with the understanding that the determinant, e of the matrix is positive and that $r\|s$ means that $r|s$ and $(r,s/r)=1$ (r is called an exact divisor of s). The group $\mathrm{Nor}(N)$ is a Fuchsian group whose fundamental domain has finite area, so it has a signature consisting of the geometric invariants

$$(g; m_1, \ldots, m_r; s)$$

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.

2. The Action of Nor(N) on $\widehat{Q}$

Every element of the extended set of rationals $\widehat{\mathbb{Q}} = \mathbb{Q}\cup\{\infty\}$ can be represented as a reduced fraction $\frac{x}{y}$, with $x,y\in\mathbb{Z}$ and $(x,y)=1$. Here, ∞ is represented 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

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

2.1. Lemma. [2] *Let N have the prime power decomposition $2^{\alpha_1}\cdot 3^{\alpha_2}\cdot p_3^{\alpha_3}\cdots p_r^{\alpha_r}$. Then* $\mathrm{Nor}(N)$ *acts transitively on $\widehat{\mathbb{Q}}$ if and only if $\alpha_1\le 7$, $\alpha_2\le 3$ and $\alpha_i\le 1$ for $i=3,\ldots,r$.* □

In this study, N will be of the form 2^2p^2, where p is prime and $p>3$. All circuits in the suborbital graph for the normalizer of $\Gamma_0(N)$ in $PSL(2,\mathbb{R})$ were studied in [3,9] and [10], where N is a square-free positive integer and when N satisfies the condition of transitive action, respectively. Clearly, the general statement is an open problem and seems to be very difficult. In this study, we also investigate a case in which the normalizer does not satisfy the conditions in [3,9] and [10]. Therefore, we take $N=2^2p^2$, where p is an odd prime, as probably the simplest case where the conditions of Lemma 2.1 are not satisfied. We believe that we have succeeded in giving a method, finding a maximal subset that satisfies the transitive action, to extend the current situation to one step further.

In this case, as $h=2$, e must be 1 or p^2. So, $\mathrm{Nor}(N)$ consists of the following two types of element:

$$T_1=\begin{pmatrix} a & b/2 \\ 2p^2c & d \end{pmatrix} :\ ad-bp^2c=1 \text{ and } T_2=\begin{pmatrix} ap^2 & b/2 \\ 2p^2c & dp^2 \end{pmatrix} :\ adp^4-bp^2c=p^2.$$

Clearly, $\mathrm{Nor}(2^2p^2)$ is not transitive on $\widehat{\mathbb{Q}}$. Therefore, we will find a maximal subset of $\widehat{\mathbb{Q}}$ on which $\mathrm{Nor}(2^2p^2)$ acts transitively. For this, we give the following two results from [3].

2.2. Lemma. *Given an arbitrary rational number k/s with $(k,s)=1$, then there exists an element $A\in\Gamma_0(N)$ such that $A(k/s)=(k_1/s_1)$ with $s_1|N$.* □

2.3. Lemma. *Let $d|N$ and let $(a_1,d)=(a_2,d)=1$. Then $\begin{pmatrix} a_1 \\ d \end{pmatrix}$ and $\begin{pmatrix} a_2 \\ d \end{pmatrix}$ are conjugate under $\Gamma_0(N)$ iff $a_1=a_2 \bmod (d,N/d)$.* □

From Lemma 2.2 and Lemma 2.3, we get easily;

2.4. Corollary. *Let $d|N$. Then the orbit $\begin{pmatrix} a \\ d \end{pmatrix}$ of a/d with $(a,d)=1$ under $\Gamma_0(N)$ is the set $\{x/y \in \widehat{\mathbb{Q}} : (N,y)=d, a \equiv x\frac{y}{d} \bmod (d, N/d)\}$. Furthermore the number of orbits $\begin{pmatrix} a \\ d \end{pmatrix}$ with $d|N$ under $\Gamma_0(N)$ is just $\varphi(d,N/d)$, where $\varphi(n)$ is Euler's totient function, which is the number of positive integers less than or equal to n that are coprime to n.* □

So, the number of orbits of $\Gamma_0(2^2p^2)$ on $\widehat{\mathbb{Q}}$ is $\sum_{d|N}\varphi(d,N/d)$, which is $3p+3$. We give them explicitly in the following corollary (Here, for the sake of completeness, we give a simple proof);

2.5. Corollary. *The orbits of $\Gamma_0(2^2p^2)$ on $\widehat{\mathbb{Q}}$ are as follows:*

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix};\ \begin{pmatrix} 1 \\ 2 \end{pmatrix};\ \begin{pmatrix} 1 \\ 2^2 \end{pmatrix};\ \begin{pmatrix} 1 \\ p^2 \end{pmatrix};\ \begin{pmatrix} 1 \\ 2p^2 \end{pmatrix};\ \begin{pmatrix} 1 \\ 2^2p^2 \end{pmatrix};\ \begin{pmatrix} 1 \\ p \end{pmatrix},\ \begin{pmatrix} 2 \\ p \end{pmatrix}\cdots\begin{pmatrix} p-1 \\ p \end{pmatrix};$$
$$\begin{pmatrix} 1 \\ 2p \end{pmatrix},\ \begin{pmatrix} p+2 \\ 2p \end{pmatrix},\ \begin{pmatrix} 3 \\ 2p \end{pmatrix},\ \begin{pmatrix} p+4 \\ 2p \end{pmatrix}\cdots\begin{pmatrix} 2p-1 \\ 2p \end{pmatrix};$$
$$\begin{pmatrix} 1 \\ 2^2p \end{pmatrix},\ \begin{pmatrix} p+2 \\ 2^2p \end{pmatrix},\ \begin{pmatrix} 3 \\ 2^2p \end{pmatrix},\ \begin{pmatrix} p+4 \\ 2^2p \end{pmatrix}\cdots\begin{pmatrix} 2p-1 \\ 2^2p \end{pmatrix}.$$

Proof. Let us denote the representatives of the orbits by $\begin{pmatrix} a \\ d \end{pmatrix}$, as above. The possible values of d are $1, 2, 2^2, p, 2p, p^2, 2p^2, 2^2p$, and 2^2p^2 by Lemma 2.2. Hence, the number of non-conjugate classes of these orbits using Euler's formula are 1 and $p-1$ for $1, 2, 2^2, p^2, 2p^2, 2^2p^2$, and $p, 2p, 2^2p$ respectively. By Lemma 2.3, the result is obvious. □

If one just examines the action of the elements of $\mathrm{Nor}(2^2p^2)$ on the orbit $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, the following result is easily obtained:

2.6. Theorem. *The set $\widehat{\mathbb{Q}}(2^2p^2) := \begin{pmatrix} 1 \\ 1 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^2p^2 \end{pmatrix}$, is an orbit of $\mathrm{Nor}(2^2p^2)$ on $\widehat{\mathbb{Q}}$.*

Proof. Taking the element $T_1 = \begin{pmatrix} a & b/2 \\ 2p^2c & d \end{pmatrix}$, we see that $T_1\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2a+b \\ 2(2p^2c+d) \end{pmatrix}$.

(i) If b and d are odd; then $T_1\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \begin{pmatrix} 1 \\ 2 \end{pmatrix}$, and

(ii) If b is odd and d even; then $T_1\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \begin{pmatrix} 1 \\ 2^2 \end{pmatrix}$.

Taking the element $T_2 = \begin{pmatrix} ap^2 & b/2 \\ 2p^2c & dp^2 \end{pmatrix}$, we have that $T_2\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2ap^2+b \\ 2p^2(2c+d) \end{pmatrix}$.

(iii) If b and d are odd; then $T_2\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \begin{pmatrix} 1 \\ 2p^2 \end{pmatrix}$,

(iv) If b is even and d odd; then $T_2\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \begin{pmatrix} 1 \\ p^2 \end{pmatrix}$, and

(v) If b is odd and d even; then $T_2\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \begin{pmatrix} 1 \\ 2^2p^2 \end{pmatrix}$. □

Therefore the set $\widehat{\mathbb{Q}}(2^2p^2)$ is one on which $\mathrm{Nor}(2^2p^2)$ acts transitively. We now consider the imprimitivity of the action of $\mathrm{Nor}(2^2p^2)$ on $\widehat{\mathbb{Q}}(2^2p^2)$, beginning with a general discussion of primitivity of permutation groups. Let (G,Δ) be a transitive permutation group, consisting of a group G acting on a set Δ transitively. An equivalence relation $\approx$ on Δ is called *G-invariant* if, whenever $\alpha,\beta\in\Delta$ satisfy $\alpha\approx\beta$, then $g(\alpha)\approx g(\beta)$ for all $g\in G$. The equivalence classes are called blocks, and the block containing α is denoted by $[\alpha]$.

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

(i) The identity relation, $\alpha\approx\beta$ if and only if $\alpha=\beta$; and
(ii) The universal relation, $\alpha\approx\beta$ for all $\alpha,\beta\in\Delta$.

Otherwise, (G,Δ) is called *primitive*. The above two relations are regarded as trivial relations. Clearly, a primitive group must be transitive, for if not the orbits would form a system of blocks. The converse is false, but we have the following useful result.

2.7. Lemma. [5]. *Let (G,Δ) be a transitive permutation group. (G,Δ) is primitive if and only if G_α, the stabilizer of $\alpha\in\Delta$, is a maximal subgroup of G for each $\alpha\in\Delta$.* □

From the above lemma we see that whenever, for some α, $G_\alpha \lneq H \lneq G$, then Ω admits some G-invariant equivalence relation other than the trivial ones. Because of transitivity, every element of Ω has the form $g(\alpha)$ for some $g\in G$. Thus one of the non-trivial G-invariant equivalence relations on Ω is given as follows:

$$g(\alpha)\approx g'(\alpha) \text{ if and only if } g'\in gH.$$

The number of blocks (equivalence classes) is the index $|G:H|$, and the block containing α is just the orbit $H(\alpha)$.

We can apply these ideas to the case where G is $\mathrm{Nor}(2^2p^2)$ and Δ is $\widehat{\mathbb{Q}}(2^2p^2)$, which is the orbit in Theorem 2.6, G_α is the stabilizer of ∞ in $\widehat{\mathbb{Q}}(2^2p^2)$; that is, $G_\infty = \left\langle \begin{pmatrix}1 & 1/2\\ 0 & 1\end{pmatrix}\right\rangle$, and H is $N_0 := \langle \Gamma_0(2^2p^2), T_1, A_1\rangle$, where $T_1 = \begin{pmatrix} a & (2b+1)/2\\ 2p^2c & -a\pm 1\end{pmatrix}$ (as in Section 2) and $A_1 := \begin{pmatrix} ap^2 & b\\ 2^2p^2c & dp^2\end{pmatrix}\in\Gamma_0^+(2^2p^2)$ is an Atkin-Lehner involution (see [6] for the definition). Clearly $G_\infty < N_0 < \mathrm{Nor}(2^2p^2)$.

2.8. Lemma. [1] *The index $|\mathrm{Nor}(N):\Gamma_0(N)|$ is given by*

$$|\mathrm{Nor}(N):\Gamma_0(N)| = 2^\rho h^2\tau,$$

where ρ is the number of prime factors of N/h^2, $\tau = (\frac{3}{2})^{\varepsilon_1}(\frac{4}{3})^{\varepsilon_2}$,

$$\varepsilon_1 = \begin{cases}1 & \text{if } 2^2, 2^4, 2^6\| N,\\ 0 & \text{otherwise,}\end{cases}\qquad \varepsilon_2 = \begin{cases}1 & \text{if } 9\| N,\\ 0 & \text{otherwise.}\end{cases}$$ □

Using Lemma 2.8, we easily obtain the following.

2.9. Theorem. *There are only two blocks, which are $[\infty]$ and $[0]$. These are as follows:*

$$[0] := \begin{pmatrix}1\\1\end{pmatrix}\cup\begin{pmatrix}1\\2\end{pmatrix}\cup\begin{pmatrix}1\\2^2\end{pmatrix} \text{ and } [\infty] := \begin{pmatrix}1\\p^2\end{pmatrix}\cup\begin{pmatrix}1\\2p^2\end{pmatrix}\cup\begin{pmatrix}1\\2^2p^2\end{pmatrix}.$$

Proof. Here, $T_1^3 = I \implies \mathrm{trace}(T_1) = \pm 1$ and $A_1^2 = I$. So, we have that

$$|\mathrm{Nor}(2^2p^2):\Gamma_0(2^2p^2)| = 12 \text{ and } |N_0(2^2p^2):\Gamma_0(2^2p^2)| = 6.$$

Hence, it is clear that $|\mathrm{Nor}(2^2p^2):N_0(2^2p^2)| = 2$. □

3. Suborbital graphs of $\mathbf{Nor(2^2p^2)}$ on $\widehat{Q}(\mathbf{2^2p^2})$

In[14], Sims introduced the idea of the suborbital graphs of a permutation group G acting on a set Δ. These are graphs with vertex-set Δ, on which G induces automorphisms. We summarize Sims' theory as follows: Let (G, Δ) be a transitive permutation group. Then G acts on $\Delta \times \Delta$ by $g(\alpha, \beta) = (g(\alpha), g(\beta))$, $(g \in G, \alpha, \beta \in \Delta)$. 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 Δ, 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 $G(\alpha, \beta)$.

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

The above ideas are also described in a paper by Neumann[12], and in books by Tsuzuku[15] and by Biggs and White [5], the emphasis being on applications to finite groups.

In this study, G and Δ will be $\mathrm{Nor}(N)$ and $\widehat{\mathbb{Q}}$, respectively. All circuits in suborbital graph for $\mathrm{Nor}(N)$, where N is a square-free positive integer, were studied in [3,9,10]. We now investigate the suborbital graphs for the action $\mathrm{Nor}(2^2p^2)$ on $\widehat{\mathbb{Q}}(2^2p^2)$. Since the action $\mathrm{Nor}(2^2p^2)$ on $\widehat{\mathbb{Q}}(2^2p^2)$ is transitive, $\mathrm{Nor}(2^2p^2)$ permutes the blocks transitively; so the subgraphs are all isomorphic. Hence it is sufficient to study only one block. On the other hand, it is clear that each non-trivial suborbital graph contains a pair $(\infty, u/p^2)$ for some $u/p^2 \in \widehat{\mathbb{Q}}(2^2p^2)$ where $(u, p^2) = 1$. Therefore, we work on the following case: We denote by $F(\infty, u/p^2)$ the subgraph of $G(\infty, u/p^2)$ such that its vertices are in the block $[\infty]$.

3.1. Theorem. *Let r/s and x/y be in the block $[\infty]$. Then there is an edge $r/s \to x/y$ in $F(\infty, u/p^2)$ iff*

(i) *If $2^2p^2 \| s$, then $x \equiv \pm ur \pmod{p^2}, y \equiv \pm us \pmod{p^2}, ry - sx = \pm p^2$,*
(ii) *If $2p^2 \| s$, then $x \equiv \pm 2ur \pmod{2p^2}, y \equiv \pm 2us \pmod{p^2}, ry - sx = \pm 2p^2$,*
(iii) *If $p^2 \| s$, then $x \equiv \pm 4ur \pmod{p^2}, y \equiv \pm 4us \pmod{p^2}, ry - sx = \pm p^2$.*

(The plus and minus sign correspond to $r/s > x/y$ and $r/s < x/y$, respectively)

Proof. Assume first that $r/s \xrightarrow{>} x/y$ is an edge in $F(\infty, u/p^2)$, and $2^2p^2 \| s$. This means that there exists some T in the normalizer $\mathrm{Nor}(2^2p^2)$ such that T sends the pair $(\infty, u/p^2)$ to the pair $(r/s, x/y)$, that is $T(\infty) = r/s$ and $T(u/p^2) = x/y$. Since $2^2p^2 \| s$, T must be of the form T_1 where b and c are even. $T(\infty) = \dfrac{a}{2pc} = \dfrac{r}{s}$ gives that $r = a$ and $s = 2^2p^2c_0$. $T(u/p^2) = \dfrac{au + (b/2)p^2}{2p^2cu + dp^2} = \dfrac{r}{s}$ gives that $x \equiv ur \pmod{p^2}, y \equiv us \pmod{p^2}$. Furthermore, we get $ry - sx = p^2$ from the equation

$$\begin{pmatrix} a & b/2 \\ 2p^2c & d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & p^2 \end{pmatrix} = \begin{pmatrix} r & s \\ x & y \end{pmatrix}.$$

For the opposite direction, we assume that $2^2p^2 \| s$ and $x \equiv ur \pmod{p^2}, y \equiv us \pmod{p^2}, ry - sx = p^2$. In this case, there exist $b, d \in \mathbb{Z}$ such that $x = ur + bp^2$ and $y = us + dp^2$. If we put these equivalences in $ry - sx = p^2$, we obtain $rd - bs = 1$. So the element

$T_0 = \begin{pmatrix} r & b/2 \\ 2s & d \end{pmatrix}$ is clearly in N_0. Where there is a minus sign and another condition, similar calculations may be made. □

Now, let us represent the edges of $F(\infty, u/p^2)$ as hyperbolic geodesics in the upper half-plane $\mathbb{H}$, that is, as Euclidean semi-circles or half-lines perpendicular to the real line. Then we have:

3.2. Theorem. *$F(\infty, u/p^2)$ is self-paired iff $u^2 \equiv -1 \pmod{p^2}$, $4u^2 \equiv -1 \pmod{p^2}$ or $2u^2 \equiv -1 \pmod{2p^2}$.*

Proof. Because of the transitive action, the form of a self-paired edge can be taken as $1/0 \to x/y \to 1/0$. The conditions follows immediately from the first and second edge by Theorem 3.1. □

3.3. Theorem. *$F(\infty, u/p^2)$ contains a triangle if and only if $4u^2 \pm 2u + 1 \equiv 0 \pmod{p^2}$.*

Proof. We suppose that there is a triangle such as $k_0/l_0 \to m_0/n_0 \to x_0/y_0 \to k_0/l_0$ in $F(\infty, u/p^2)$. Since N_0 permutes the vertices transitively, we may suppose that the triangle has the form $1/0 \to m_0/p^2 \to x_0/y_0 \to 1/0$. Furthermore, without loss of generality, suppose $m_0/p^2 < x_0/y_0$. From theorem 3.1 (i), we have that $m_0 \equiv u \pmod{p^2}$ from the first edge and $y_0 = p^2$ or $y_0 = 2p^2$ from the third edge.

Case 1. If $y_0 = p^2$, then $up^2 - x_0p^2 = -p^2$ from the second edge by Theorem 3.1 (iii). This means that $x_0 = u + 1$. On the other hand $x_0 \equiv -4u^2 (\mathrm{mod}\, p^2)$, then we obtain that $4u^2 + u + 1 \equiv 0 (\mathrm{mod}\, p^2)$. But $4u^2 + u + 1 \equiv 0 \pmod{p^2}$, contradicts the congruence $4u^2 + 4u + 1 \equiv 0 \pmod{p^2}$, which is obtained from the third edge with the relation $1 \equiv -4u(u + 1) \pmod{p^2}$. If the minus sign is valid, which means that $m_0/p^2 > x_0/y_0$, we obtain similar a contradiction.

Case 2. If $y_0 = 2p^2$, then $2up^2 - x_0p^2 = -p^2$ from the second edge by Theorem 3.1 (iii). This means that $x_0 = 2u + 1$. Furthermore, $x_0 \equiv -4u^2 \pmod{p^2}$. Hence, we obtain that $4u^2 + 2u + 1 \equiv 0 \pmod{p^2}$. In addition, this congruence coincides with the relation $1 \equiv -2u(2u+1) \pmod{p^2}$ from the third edge. If $m_0/p^2 > x_0/y_0$, we obtain $4u^2 - 2u + 1 \equiv 0 \pmod{p^2}$. If we combine these, we have that $4u^2 \pm 2u + 1 \equiv 0 \pmod{p^2}$.

For the opposite direction, we assume that $4u^2 \pm 2u + 1 \equiv 0 \pmod{p^2}$. Using theorem 3.1, it is clear that $1/0 \to u/p^2 \to 2u \pm 1/2p^2 \to 1/0$ is a triangle in $F(\infty, u/p^2)$. □

3.4. Corollary. *If $F(\infty, u/p^2)$ contains a triangle for any prime p greater than 3, we have $p \equiv 1 \pmod 3$.*

Proof. Suppose that $F(\infty, u/p^2)$ contains a triangle. Then $4u^2 \pm 2u + 1 \equiv 0 \pmod{p^2}$. It follows that $x^2 \pm x + 1 \equiv 0 \pmod{p^2}$ for $x = 2u$. Hence, we have that $x^2 \pm x + 1 \equiv 0 \pmod{p}$. Taken with $(2x \pm 1)^2 + 3 \equiv 0 \pmod{p}$, it follows that $p \equiv 1 \pmod 3$. □

3.5. Examples. Using easy number-theoretical techniques, we can easily give some examples. For $p = 13$, let us calculate which suborbital graphs contains a self-paired edge.

(i) Since $u^2 \equiv -1 \pmod{13^2}$, then $u^2 \equiv -1 \pmod{13}$, giving $u = 5 + 13k_1$ such that $k_1 \in \mathbb{Z}$. Hence, we have $(5 + 13k_1)^2 \equiv -1 \pmod{13^2}$, then $26 + 130k_1 + 169(k_1)^2 \equiv 0 \pmod{13^2}$. As $2 + 10k_1 + 13(k_1)^2 \equiv 0 \pmod{13}$, we obtain $k_1 = 5$ and $u = 70$. Since $70^2 \equiv -1 \pmod{169}$, $F(\infty, 70/169)$ contains a self-paired edge.

(ii) In a similar way, for $p = 7$, let us find suborbital graphs which contains a triangle. Since $4u^2 + 2u + 1 \equiv 0 \pmod{7^2}$, then $4u^2 + 2u + 1 \equiv 0 \pmod 7$, giving $u = 1 + 7k_1$ such that $k_1 \in \mathbb{Z}$. Hence, we have $4(1 + 7k_1)^2 + 2(1 + 7k_1) + 1 \equiv 0 \pmod{7^2}$, then

$196(k_1)^2 + 70k_1 + 7 \equiv 0 \pmod{7^2}$. As $28(k_1)^2 + 10k_1 + 1 \equiv 0 \pmod 7$, we obtain $k_1 = 2$ and $u = 15$. Since $4(15)^2 + 2(15) + 1 \equiv 0 \pmod{49}$, $F(\infty, 15/49)$ contains a triangle.

3.6. Observation. *For the transformation* $\varphi := \begin{pmatrix} -2^2u & (4u^2+2u+1)/p^2, \\ -2^2p^2 & 2^2u+2, \end{pmatrix}$ *of order* 3, *where* $p \equiv 1 \pmod 3$ *is an elliptic element, it is easily seen that*

$$\varphi\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}u\\p^2\end{pmatrix},\ \varphi\begin{pmatrix}u\\p^2\end{pmatrix} = \begin{pmatrix}2u+1\\2p^2\end{pmatrix},\ \varphi\begin{pmatrix}2u+1\\2p^2\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}.$$

The only elements of finite order in $PSL(2,\mathbb{R})$ *are elliptic.* $\mathrm{Nor}(N)$ *can only have finite periods* $2, 3, 4, 6$.

In [2], the authors show that:

3.7. Lemma. [2]

(i) $\mathrm{Nor}(N)$ *has at most one period of order* 4. $\mathrm{Nor}(N)$ *has a period of order* 4 *iff* $2 \| N/h^2$, *and if* p *is an odd prime divisor of* N/h^2 *then* $p \equiv 1 \pmod 4$.
(ii) $\mathrm{Nor}(N)$ *has at most one period of order* 6. $\mathrm{Nor}(N)$ *has a period of order* 6 *iff* $3 \| N/h^2$, *and if* p *is an odd prime divisor of* N/h^2 *then* $p \equiv 1 \pmod 3$.
(iii) $\mathrm{Nor}(N)$ *has at most one period of order* 3. $\mathrm{Nor}(N)$ *has a period of order* 3 *iff for each prime divisor of* p *of* N/h^2, $p \equiv 1 \pmod 3$. □

3.8. Lemma. [2]

- $\mathrm{Nor}(N)$ *is a triangle group for precisely* 26 *values of* N.
- *If* $N = 1, 2^2, 2^4, 2^6, 3^2, 2^2 3^2, 2^4 3^2, 2^6 3^2$, *then* $\mathrm{Nor}(N)$ *has signature* $(2, 3, \infty)$.
- *If* $N = 2, 2^3, 2^5, 2^7, 23^2, 2^3 3^2, 2^5 3^2, 2^7 3^2$, *then* $\mathrm{Nor}(N)$ *has signature* $(2, 4, \infty)$.
- *If* $N = 3, 2^2 3, 2^4 3, 2^6 3, 3^3, 2^2 3^3, 2^4 3^3, 2^6 3^3$, *then* $\mathrm{Nor}(N)$ *has signature* $(2, 6, \infty)$.

All calculations for different N show that there is a very close relation between elliptic elements and circuits in the graph. According to our unpublished data and the above lemmas, it seems that

3.9. Conjecture. *Let* $N = 2^\alpha 3^\beta p^2$. *Then* $F(\infty, u/p^2)$ *has a circuit as follows:*

α	β	*Circuits*	*Conditions*
$0, 2, 4, 6$	$0, 2$	*triangle*	$p \equiv 1 \pmod 3$
$1, 3, 5, 7$	$0, 2$	*rectangle*	$p \equiv 1 \pmod 4$
$0, 2, 4, 6$	$1, 3$	*hexagon*	$p \equiv 1 \pmod 3$

Acknowledgement. First and foremost the authors offer their sincerest gratitude to their Ph.D. supervisor, Mehmet Akbaş who has continuously provided support for them throughout their studies and academic life. The authors also express their thanks to David Singerman for his very constructive comments and guidance.

References

[1] Akbaş, M. and Singerman, D. *The Normalizer of* $\Gamma_0(N)$ *in* $PSL(2,\mathbb{R})$, Glasgow Math. J. **32**, 317–327, 1990.
[2] Akbaş, M. and Singerman, D. *The Signature of the normalizer of* $\Gamma_0(N)$ (London Math. Soc. Lectures Note Series **165**, 1992), 77–86.
[3] Akbaş, M. and Başkan, T. *Suborbital graphs for the normalizer of* $\Gamma_0(N)$, Turkish J. Math. **20**, 379–387, 1996.
[4] Akbaş, M. *On suborbital graphs for the modular group*, Bull. London Math. Soc. **33**,647–652, 2001.

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

[6] Conway, J. H. and Norton, S. P. *Monstrous moonshine*, Bull. London Math. Soc. **11**, 308–339, 1977.

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

[8] Keskin, R. *On suborbitals graphs for some Hecke groups*, Discrete Math. **234** (1–3), 53–64, 2001.

[9] Keskin, R. *Suborbital graphs for the normalizer of* $\Gamma_0(m)$, European J. Combin. **27** (2), 193–206, 2006.

[10] Keskin, R. and Demirtürk, B. *On suborbital graphs for the normalizer of* $\Gamma_0(N)$, Electronic J. Combin. **27**, R116, 2009.

[11] Maclachlan, C. *Groups of units of zero ternary quadratic forms*, Proc. Roy. Soc., Edinburgh Sect. **A** **88**, 141–157, 1981.

[12] Neumann, P. M. *Finite Permutation Groups, Edge-Coloured Graphs and Matrices*, in *Topics in Group Theory and Computation*, Ed. M. P. J. Curran (Academic Press, London, New York, San Fransisco, 1977).

[13] Schoeneberg, B. *Elliptic Modular Functions* (Springer Verlag, Berlin, 1974).

[14] Sims, C. C. *Graphs and finite permutation groups*, Math. Z. **95**, 76–86, 1967.

[15] Tsuzuku, T. *Finite Groups and Finite Geometries* (Cambridge University Press, Cambridge, 1982).