




On congruence equations arising from suborbital graphs

Bahadır Özgür GÜLER^{1,*}, Murat BEŞENK², Serkan KADER³

¹Department of Mathematics, Faculty of Science, Karadeniz Technical University, Trabzon, Turkey

²Department of Mathematics, Faculty of Science and Letters, Pamukkale University, Denizli, Turkey

³Department of Mathematics, Faculty of Arts and Sciences, Ömer Halisdemir University, Niğde, Turkey

Received: 23.05.2019

Accepted/Published Online: 13.08.2019

Final Version: 28.09.2019

Abstract: In this paper we deal with congruence equations arising from suborbital graphs of the normalizer of $\Gamma_0(m)$ in $PSL(2, \mathbb{R})$. We also propose a conjecture concerning the suborbital graphs of the normalizer and the related congruence equations. In order to prove the existence of solution of an equation over prime finite field, this paper utilizes the Fuchsian group action on the upper half plane and Farey graphs properties.

Key words: Normalizer, imprimitive action, suborbital graphs

1. Introduction

1.1. Suborbital graphs

It is known that studying the idea of a group G acting on a set Ω , we can also establish some additional structure on Ω . One of these structures is a graph. The connection between transitive groups and graphs give us new insight into some known results. Here we also used this connection. The suborbital graph is a graph arisen from the transitive group action. The concept of this graph was introduced by Sims in [17]. When a group G acts on a set Ω , a typical point α is moved by the elements of G to various other points. The set of these images is called the orbit of α under G . We consider the usual action of G on the cartesian product $\Omega \times \Omega$. The orbits of G on this set are called the suborbitals of G on Ω . If O is a suborbital of G on $\Omega \times \Omega$, we can form a suborbital graph as follows. Vertices are the elements of Ω and the vertices may be thought as joined by directed or undirected line segments corresponding to the edges. In the directed case the edge (γ, δ) will be said to go from γ to δ and denoted by $\gamma \rightarrow \delta$. In the undirected case $\{\gamma, \delta\}$ will be said to go from γ to δ and from δ to γ . In either case we represent them as hyperbolic geodesics in the upper half-plane $\mathbb{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$ as in [9].

The least interesting suborbital graph is self-paired; it consists of a loop based at each vertex $\alpha \in \Omega$. A circuit of length m is a sequence $\nu_1 \rightarrow \nu_2 \rightarrow \cdots \rightarrow \nu_m \rightarrow \nu_1$ such that $\nu_i \neq \nu_j$ for $i \neq j$, where $m \geq 3$. The circuit is called a triangle or a quadrilateral if $m = 3$ or 4 , respectively.

In this study, G and Δ will be the normalizer of $\Gamma_0(N)$ in $PSL(2, \mathbb{R})$ and the extended rational $\hat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$, respectively.

*Correspondence: boguler@ktu.edu.tr

2010 AMS Mathematics Subject Classification: 11F06, 11F03, 05C25

1.2. Motivation

$\Gamma_0(N)$ is the best known congruence subgroup of the classical modular group $\Gamma = PSL(2, \mathbb{Z})$, the set of all 2 by 2 integer matrices with the unit determinant. Its normalizer in $PSL(2, \mathbb{R})$ has been studied by many authors because of the relation in the study of moonshine [4, 5, 14].

The modular group acts transitively on $\hat{\mathbb{Q}}$ and in [9], Jones et al. investigated and described many properties of suborbital graphs for Γ and showed that the most basic one turned out to be the well-known Farey graph.

In a series of papers, suborbital graphs of the normalizer were also studied under various restrictions by the same idea [3, 12, 13]. Then, nontransitive cases have been examined to reach the general statement [7, 10, 11]. An interesting contribution of these studies was that the action of normalizer offers solutions for some congruence equations dealing with the sizes of circuits in the suborbital graph [8]. In this paper, we continue to examine some new cases. Verification of these congruences would be interesting because one immediate result is that we come close to obtain the suborbital graphs of $Nor(N)$ for arbitrary- N .

1.3. Preliminaries

Let $\Gamma = PSL(2, \mathbb{Z})$ be the modular group acting on $\hat{\mathbb{Q}}$ as follows:

$$g = \begin{pmatrix} a & c \\ b & d \end{pmatrix} : z = \frac{x}{y} \rightarrow \frac{az + b}{cz + d} = \frac{ax + by}{cx + dy},$$

where $a, b, c,$ and d are rational integers and $ad - bc = 1$. The normalizer of $\Gamma_0(N) = \{g \in \Gamma : c \equiv 0 \pmod{N}\}$ in $PSL(2, \mathbb{R})$ consists exactly of the matrices

$$\begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix}, ade^2 - bcN/h^2 = e$$

where $e \parallel \frac{N}{h^2}$ and h is the largest divisor of 24 for which $h^2|N$ with understandings that the determinant e of the matrix is positive, and that $r \parallel s$ means that $r|s$ and $(r, s/r) = 1$ (r is called an exact divisor of s).

2. Main results

Throughout the paper, we suppose that N is equal to 2^3p^2 , where p is a prime and $p > 3$. In this case, since $h = 2^{\min\{3, [\alpha/2]\}} 3^{\min\{1, [\beta/2]\}}$, h is equal to 2 for $N = 2^\alpha 3^\beta p_3^{\alpha_3} \dots p_r^{\alpha_r}$. As $e \parallel \frac{N}{h^2}$, e must be $1, 2, p^2, 2p^2$. Hence, $Nor(2^3p^2)$ has the following four types of the element:

$$E_1 = \begin{pmatrix} a & b/2 \\ 2^2p^2c & d \end{pmatrix} : ad - 2bcp^2 = 1, \quad E_2 = \begin{pmatrix} 2a & b/2 \\ 2^2p^2c & 2d \end{pmatrix} : 4ad - 2bcp^2 = 2,$$

$$E_3 = \begin{pmatrix} ap^2 & b/2 \\ 2^2p^2c & dp^2 \end{pmatrix} : adp^4 - 2bcp^2 = p^2 \text{ and}$$

$$E_4 = \begin{pmatrix} 2ap^2 & b/2 \\ 2^2p^2c & 2dp^2 \end{pmatrix} : 4adp^4 - 2bcp^2 = 2p^2.$$

2.1. Transitive action

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

Hence, the following theorem holds.

Theorem 2.1 *$(Nor(2^3p^2), \hat{\mathbb{Q}})$ is not a transitive permutation group.*

Therefore, we try to find a maximal subset of $\hat{\mathbb{Q}}$ on which $Nor(2^3p^2)$ acts transitively. For this,

Lemma 2.2 [7, Corollary 2.4] *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 $\{x/y \in \hat{\mathbb{Q}} : (N, y) = d, a \equiv x \frac{y}{d} \pmod{(d, N/d)}\}$. 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 .*

By the above theorem, we can give the following

Theorem 2.2 *The orbits of $\Gamma_0(2^3p^2)$ on $\hat{\mathbb{Q}}$ are as follows;*

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

Proof Taking into account Lemma 2.2 that d are $1, 2, 2^2, 2^3, p, 2p, 2^2p, 2^3p, p^2, 2p^2, 2^2p^2, 2^3p^2$. Hence, the number of non-conjugate classes of these orbits with Euler formula are 1 and $p-1$ for $1, 2, 2^2, 2^3, p^2, 2p^2, 2^2p^2, 2^3p^2$ and $p, 2p, 2^2p, 2^3p$ respectively. Consequently, the number of orbits of $\Gamma_0(2^3p^2)$ on $\hat{\mathbb{Q}}$ is $4p+4$. □

Theorem 2.3 *The set $\hat{\mathbb{Q}}(2^3p^2) := \begin{pmatrix} 1 \\ 1 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^3 \end{pmatrix} \cup \begin{pmatrix} 1 \\ p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^2p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2^3p^2 \end{pmatrix}$, is a maximal orbit of $Nor(2^3p^2)$ on $\hat{\mathbb{Q}}$.*

Proof Let us consider the orbit $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ under the action of the elements of $Nor(2^3p^2)$. For the above element E_1 , it is clear that a and d must be odd by $\det(E_1)$. Hence,

$$(i) \ E_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2a+b \\ 2(2p^2c+d) \end{pmatrix} \cong \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

As for E_2 , we see that b must be odd by $\det(E_2)$.

(ii) $E_2 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2a + b \\ 2^2(2p^2c + d) \end{pmatrix} \cong \begin{pmatrix} 1 \\ 2^2 \end{pmatrix}$ for b -odd and d -odd.

(iii) $E_2 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2a + b \\ 2^3(p^2c + d_0) \end{pmatrix} \cong \begin{pmatrix} 1 \\ 2^3 \end{pmatrix}$ for b -odd and d -even.

For the element E_3 , it is clear that a and d must be odd by $\det(E_3)$. Hence,

(iv) $E_3 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2ap^2 + b \\ 2p^2(2^2c + d) \end{pmatrix} \cong \begin{pmatrix} 1 \\ 2p^2 \end{pmatrix}$ for d -odd and b -odd.

(v) $E_3 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} ap^2 + b_0 \\ p^2(2^2c + d) \end{pmatrix} \cong \begin{pmatrix} 1 \\ p^2 \end{pmatrix}$ for d -odd and b -even.

As for E_4 , we see that b must be odd by $\det(E_4)$.

(vi) $E_4 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2ap^2 + b \\ 2^2p^2(2c + d) \end{pmatrix} \cong \begin{pmatrix} 1 \\ 2^2p^2 \end{pmatrix}$ for b -odd and d -odd.

(vii) $E_4 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2ap^2 + b \\ 2^3p^2(c + d_0) \end{pmatrix} \cong \begin{pmatrix} 1 \\ 2^3p^2 \end{pmatrix}$ for b -odd and d -even.

□

Consequently, $(Nor(2^3p^2), \hat{\mathbb{Q}}(2^3p^2))$ is a transitive permutation group.

2.2. Imprimitve action

Lemma 2.3 [6, Theorem 1.5.A] *Let G be a group acting transitively on a set Δ . G is primitive if and only if each point stabilizer of G_α is a maximal subgroup of G .*

Hence, we find a subgroup H of G as follows: $G_\alpha \leq H \leq G$, then we can give some G -invariant equivalence relation other than the trivial cases. We know that every element of Δ has the form $g(\alpha)$ for some $g \in G$ by the transitivity. Thus, the desired nontrivial G -invariant equivalence relation on Δ can be given as follows:

$$g(\alpha) \approx g'(\alpha) \text{ if and only if } g^{-1}g' \in H.$$

The number of blocks (equivalence classes) is the index $|G : H|$.

Now, we consider the case where G is the $Nor(2^3p^2)$ and Δ is $\hat{\mathbb{Q}}(2^3p^2)$, G_α is the stabilizer of ∞ in $\hat{\mathbb{Q}}(2^3p^2)$; that is, $Nor(2^3p^2)_\infty = \left\langle \begin{pmatrix} 1 & 1/2 \\ 0 & 1 \end{pmatrix} \right\rangle$, and H is $H_0 := \langle \Gamma_0(2^3p^2), E_1, E_2 \rangle$ where

$$E_1 = \begin{pmatrix} a & b/2 \\ 2p^2c & d \end{pmatrix} \text{ and } E_2 := \begin{pmatrix} 2a & b/2 \\ 2^2p^2c & -2(a \pm 1) \end{pmatrix}.$$

Clearly, the relation $Nor(2^3p^2)_\infty < H_0 < Nor(2^3p^2)$ produce an imprimitive action as desired.

2.3. Block design

Lemma 2.4 [1, Proposition 2] *The index $|Nor(N) : \Gamma_0(N)| = 2^\rho h^2 \tau$,*

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

$$\varepsilon_1 = \begin{cases} 1 & \text{if } 2^2, 2^4, 2^6 \parallel N \\ 0 & \text{otherwise} \end{cases}, \quad \varepsilon_2 = \begin{cases} 1 & \text{if } 9 \parallel N \\ 0 & \text{otherwise} \end{cases}$$

By the Lemma 2.4, we obtain:

Theorem 2.4 *There are only two blocks which are $[\infty]$ and $[0]$. These are*

$$[0] := \binom{1}{1} \cup \binom{1}{2} \cup \binom{1}{2^2} \cup \binom{1}{2^3} \quad \text{and} \quad [\infty] := \binom{1}{p^2} \cup \binom{1}{2p^2} \cup \binom{1}{2^2 p^2} \cup \binom{1}{2^3 p^2}.$$

Proof First, let us calculate the index $|Nor(2^3 p^2) : \Gamma_0(2^3 p^2)|$ by using Lemma 2.4. Since $h = 2$, we have $\rho = 2$. As $2^2 \nmid 2^3 p^2$, then $\varepsilon_1 = \varepsilon_2 = 0$. Hence, $|Nor(2^3 p^2) : \Gamma_0(2^3 p^2)| = 2^2 \cdot 2^2 = 16$.

Second, we calculate the index $|H_0 : \Gamma_0(2^3 p^2)|$ by using [1]. For E_1 , a and d must be odd by $ad - 2bcp^2 = 1$. Since $a + d$ is even, then $(E_1)^2 = I$. It is also known that for any element $A = \begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix}$ of $Nor(N)$, $A^4 = I$ if $trace(A) = \pm 1$ and $det(A) = e = 2$. Clearly, E_2 holds them. Hence, we have that

$$\{I, E_1\} \times \{I, E_2, E_2^2, E_2^3\} = \{I, E_1, E_2, E_1 E_2^2, E_1 E_2^3, E_2^2, E_2^3\}$$

as cosets. Thus, we obtain that $|H_0 : \Gamma_0(2^3 p^2)| = 8$. Using the equation

$$|Nor(2^3 p^2) : \Gamma_0(2^3 p^2)| = |Nor(2^3 p^2) : H_0| \cdot |H_0 : \Gamma_0(2^3 p^2)|,$$

we have $|Nor(2^3 p^2) : H_0| = 2$. As in Theorem 2.3, the orbit $\hat{Q}(2^3 p^2)$ will be split into two blocks as the statement of the theorem taking into account the orbit $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ under the action of elements of H_0 . □

2.4. Edge condition

Since $Nor(2^3 p^2)$ acts transitively on $\hat{Q}(2^3 p^2)$, every suborbital $O(\alpha, \beta)$ contains a pair $(\infty, u/p^2)$ for $u/p^2 \in \hat{Q}(2^3 p^2)$. As $Nor(2^3 p^2)$ permutes the blocks transitively, all subgraphs corresponding to blocks are isomorphic. Therefore, we will only consider the subgraph $F(\infty, u/p^2)$ of $G(\infty, u/p^2)$ whose vertices form the block $[\infty]$.

Theorem 2.5 *Vertices r/s and x/y be in the block $[\infty]$. Then the edge $r/s \rightarrow x/y$ is in $F(\infty, u/p^2)$ iff*

- (i) $x \equiv \pm ur \pmod{p^2}, y \equiv \pm us \pmod{p^2}, ry - sx = \pm p^2$ for $2^3 p^2 \parallel s$,
- (ii) $x \equiv \pm 2ur \pmod{p^2}, y \equiv \pm 2us \pmod{2p^2}, ry - sx = \pm 2p^2$ for $2^2 p^2 \parallel s$,
- (iii) $x \equiv \pm 4ur \pmod{p^2}, y \equiv \pm 4us \pmod{4p^2}, ry - sx = \pm 2p^2$ for $2p^2 \parallel s$,
- (iv) $x \equiv \pm 8ur \pmod{p^2}, y \equiv \pm 8us \pmod{4p^2}, ry - sx = \pm p^2$ for $p^2 \parallel s$.

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

Proof We suppose that $r/s \xrightarrow{>} x/y$ is an edge in $F(\infty, u/p^2)$. It means that there exists some T in the normalizer $Nor(2^3p^2)$ such that T sends the pair $(\infty, u/p^2)$ to the pair $(r/s, x/y)$, that is $T(\infty) = r/s$ and $T(u/p^2) = x/y$.

Case 1. If $T = \begin{pmatrix} a & b \\ 2^3p^2c & d \end{pmatrix}$, a must be odd by the equation $ad - bc(2^3p^2) = 1$. Since $T(\infty) = \frac{a}{2^3p^2c} = \frac{r}{s}$, then $r = a$ and $s = 2^3p^2c$. Since $T(u/p^2) = \frac{au + bp^2}{2^3p^2cu + dp^2} = \frac{x}{y}$, then $x \equiv ur \pmod{p^2}, y \equiv us \pmod{p^2}$. In addition, we obtain $ry - sx = p^2$ from the equation

$$\begin{pmatrix} a & b \\ 2^3p^2c & d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & p^2 \end{pmatrix} = \begin{pmatrix} r & s \\ x & y \end{pmatrix} .$$

Case 2. If $T = \begin{pmatrix} a & b/2 \\ 2^2p^2c & d \end{pmatrix}$, a must be odd by the equation $ad - bc(2p^2) = 1$. Since $T(\infty) = \frac{a}{2^2p^2c} = \frac{r}{s}$, then $r = a$ and $s = 2^2p^2c$. Since $T(u/p^2) = \frac{au + bp^2/2}{2^2p^2cu + dp^2} = \frac{2au + bp^2}{2^3p^2cu + 2dp^2} = \frac{x}{y}$, then $x \equiv 2ur \pmod{p^2}, y \equiv 2us \pmod{2p^2}$. In addition, we obtain $ry - sx = 2p^2$ from the equation

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

If $T = \begin{pmatrix} 2a & b/2 \\ 2^2p^2c & 2d \end{pmatrix}$, a could be odd or even by the equation $2ad - bc(p^2) = 1$.

Case 3. Suppose that $T = \begin{pmatrix} 2a & b/2 \\ 2^2p^2c & 2d \end{pmatrix}$ and a is odd. Since $T(\infty) = \frac{2a}{2^2p^2c} = \frac{a}{2p^2c} = \frac{r}{s}$, then $r = a$ and $s = 2p^2c$. Since $T(u/p^2) = \frac{2au + bp^2/2}{2^2p^2cu + dp^2} = \frac{4au + bp^2}{2^3p^2cu + 4dp^2} = \frac{x}{y}$ then $x \equiv 4ur \pmod{p^2}, y \equiv 4us \pmod{4p^2}$. In addition, we obtain $ry - sx = 2p^2$ from the equation

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

Case 4. Suppose that $T = \begin{pmatrix} 2a & b/2 \\ 2^2p^2c & 2d \end{pmatrix}$ and a is even. Since $T(\infty) = \frac{2a}{2^2p^2c} = \frac{a}{2p^2c} = \frac{a_0}{p^2c} = \frac{r}{s}$, then $r = a_0$ and $s = 2p^2c$. Since $T(u/p^2) = \frac{2au + bp^2/2}{2^2p^2cu + dp^2} = \frac{4au + bp^2}{2^3p^2cu + 4dp^2} = \frac{8a_0u + bp^2}{2^3p^2cu + 4dp^2} = \frac{x}{y}$ then $x \equiv 8ur \pmod{p^2}, y \equiv 8us \pmod{4p^2}$. In addition, we obtain $ry - sx = p^2$ from the equation

$$\begin{pmatrix} 4a & b \\ 2^3p^2c & 4d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & p^2 \end{pmatrix} = \begin{pmatrix} 8r & x \\ 8s & y \end{pmatrix} .$$

To prove opposite direction, we assume that $2^3p^2 \parallel s$ 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 write these equivalences

in $ry - sx = p^2$, we get $rd - bs = 1$. Thus, the element $T_0 = \begin{pmatrix} r & b \\ s & d \end{pmatrix}$ is clearly in H_0 . For minus sign and another conditions, similar calculations are done. □

2.5. Circuit condition

In the introduction part, we mentioned that the trivial suborbital graphs are self-paired ones. In this section, we will be mainly interested in the remaining nontrivial suborbital graphs.

Theorem 2.6 $F(\infty, u/p^2)$ contains a quadrilateral iff $8u^2 \pm 4u + 1 \equiv 0 \pmod{p^2}$.

Proof We suppose that there is a quadrilateral such as $\frac{m}{n} \rightarrow \frac{r}{s} \rightarrow \frac{x}{y} \rightarrow \frac{k}{l} \rightarrow \frac{m}{n}$ in $F(\infty, u/p^2)$. Since H_0 permutes the vertices transitively, we may suppose that the quadrilateral has the form $\frac{1}{0} \rightarrow \frac{r_0}{s_0p^2} \rightarrow \frac{x_0}{y_0p^2} \rightarrow \frac{k_0}{l_0p^2} \rightarrow \frac{1}{0}$. Furthermore, without loss of generality, suppose $\frac{r_0}{s_0p^2} < \frac{x_0}{y_0p^2} < \frac{k_0}{l_0p^2}$. From Theorem 2.5(i), we have that $r_0 \equiv u \pmod{p^2}$ and $s_0 = 1$ from the first edge. Hence, we get the second vertex as $\frac{u}{p^2}$. Applying to Theorem 2.5(iv) to second edge, we obtain that $x_0 \equiv -8u^2 \pmod{p^2}$, $y_0 = 4$ and $uy_0 - x_0 = -1$. Using these values, we get that $x_0 = 4u + 1$ and the third vertex as $\frac{4u + 1}{4p^2}$. Hence, we have $8u^2 + 4u + 1 \equiv 0 \pmod{p^2}$ by $x \equiv -8u^2 \pmod{p^2}$. By third condition in Theorem 2.5(ii), there are two possibilities for the rest of configuration as follows:

Case 1. If $\frac{4u + 1}{4p^2} \rightarrow \frac{k_0}{p^2} \rightarrow \frac{1}{0}$, we have that $4up^2 + p^2 - 4p^2k_0 = -2p^2$ from third edge. Simplifying $4u + 1 - 4k = -2$, then $4(u - k_0) = -3$ gives a contradiction for $u, k_0 \in \mathbb{Z}$.

Case 2. If $\frac{4u + 1}{4p^2} \rightarrow \frac{k_0}{2p^2} \rightarrow \frac{1}{0}$, we have that $8up^2 + 2p^2 - 4p^2k_0 = -2p^2$ from third edge. Simplifying $4(2u - k_0) = -4$, then $2u - k_0 = -1$ gives $k_0 = 2u + 1$.

If the inequalities $\frac{r_0}{s_0p^2} > \frac{x_0}{y_0p^2} > \frac{k_0}{l_0p^2}$ hold then we conclude that $8u^2 - 4u + 1 \equiv 0 \pmod{p^2}$.

To prove opposite direction, we assume that $8u^2 \pm 4u + 1 \equiv 0 \pmod{p^2}$. Using Theorem 2.5, it is clear that $\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{4u \pm 1}{4p^2} \rightarrow \frac{2u \pm 1}{2p^2} \rightarrow \frac{1}{0}$ is a quadrilateral in $F(\infty, u/p^2)$. □

Example 2.1 As a simple example, suppose that p is equal to 5 which is a first prime greater than 3. We calculate which suborbital graphs contains a quadrilateral. Since $8u^2 + 4u + 1 \equiv 0 \pmod{5^2}$, then $8u^2 + 4u + 1 \equiv 0 \pmod{5}$, giving $u = 3 + 5k$ such that $k \in \mathbb{Z}$. Hence, we have $8(3 + 5k)^2 + 4(3 + 5k) + 1 \equiv 0 \pmod{5^2}$, then $200k^2 + 260k + 85 \equiv 0 \pmod{5^2}$. As $40k^2 + 52k + 17 \equiv 0 \pmod{5}$, we obtain $k = 4$ and $u = 23$. Since $8(23)^2 + 4(23) + 1 \equiv 0 \pmod{25}$, $F(\infty, 23/25)$ contains a quadrilateral.

3. Conclusion

Theorem 3.1 The prime divisors p of $8u^2 \pm 4u + 1$, for any $u \in \mathbb{Z}$, are of the form $p \equiv 1 \pmod{4}$.

Proof Let u be any integer and p a prime divisor of $8u^2 \pm 4u + 1$. Then, without any difficulty, it can be easily seen that the normalizer $Nor(2^3p)$, like $Nor(2^3p^2)$, has the elliptic element

$$\varphi := \begin{pmatrix} -2^3u & (8u^2 \pm 4u + 1)/p \\ -2^3p & 2^3u + 4 \end{pmatrix}$$

of order 4. From [2, Theorem 2], we get that $p \equiv 1 \pmod{4}$. \square

Remark 3.1 Following the sketch of this paper, similar solutions can be given for other congruences in the following conjecture. We note that the technique we used relies on the choice of group for imprimitive action. By carefully choosing these groups, the proofs of the main results can be obtained by similar algebraic considerations. We also think that our attempts on suborbitals might help to find unknown invariants of the signature of $Nor(N)$ for arbitrary- N taking into account the fact that the graph of a group provides a method by which a group can be visualized (see also [15]). In suggestion of a next step to advance the literature, we also give a conjecture below.

Conjecture 3.1 For $\alpha \leq 7$ and $\beta \leq 3$, solutions to possible congruence equations arising from the circuit conditions in suborbital graphs of $Nor(2^\alpha 3^\beta p_3^{\alpha_3} \cdots p_r^{\alpha_r})$ are as follows:

- (i) The prime divisors p of $2^\alpha 3^\beta u^2 \pm 2^{\frac{\alpha}{2}} 3^{\frac{\beta}{2}} u + 1 \pmod{p}$ in which α -even, β -even, and any $u \in \mathbb{Z}$ are of the form $p \equiv 1 \pmod{3}$.
- (ii) The prime divisors p of $2^\alpha 3^\beta u^2 \pm 2^{\frac{\alpha+1}{2}} 3^{\frac{\beta}{2}} u + 1 \pmod{p}$ in which α -odd, β -even, and any $u \in \mathbb{Z}$ are of the form $p \equiv 1 \pmod{4}$.
- (iii) The prime divisors p of $2^\alpha 3^\beta u^2 \pm 2^{\frac{\alpha}{2}} 3^{\frac{\beta+1}{2}} u + 1 \pmod{p}$ in which α -even, β -odd, and any $u \in \mathbb{Z}$ are of the form $p \equiv 1 \pmod{3}$.

Acknowledgment

This work is supported by the Scientific and Technical Research Council of Turkey (TÜBİTAK) under Grant No. 118F018.

References

- [1] Akbas M, Singerman, D. The normalizer of $\Gamma_0(N)$ in $PSL(2, R)$. Glasgow Mathematical Journal 1990; 32: 317-327.
- [2] Akbas M, Singerman, D. The signature of the normalizer of $\Gamma_0(N)$ in $PSL(2, R)$. London Mathematical Society Lecture Note Series 1992; 165: 77-86.
- [3] Akbaş M, Başkan T. Suborbital graphs for the normalizer of $\Gamma_0(N)$. Turkish Journal of Mathematics 1996; 20(3): 379-387.
- [4] Chua KS, Lang ML. Congruence subgroups associated to the monster. Experimental Mathematics 2004; 13(3): 343-360. doi: 10.1080/10586458.2004.10504546
- [5] Conway JH, Norton SP. Monstrous Moonshine. Bulletin of the London Mathematical Society 1977; 11: 308-339.
- [6] Dixon JD, Mortimer B. Permutation Groups. Graduate Texts in Mathematics, 163. New York, NY, USA: Springer-Verlag, 1996.

- [7] Güler BÖ, Beşenk M, Değer AH, Kader S. Elliptic elements and circuits in suborbital graphs. Hacettepe Journal of Mathematics and Statistics 2011; 40(2): 203-210.
- [8] Güler BÖ, Kör T, Şanlı Z. Solution to some congruence equations via suborbital graphs. Springerplus 2016; 2016(5): 1327. doi: 10.1186/s40064-016-3016-5
- [9] Jones GA, Singerman D, Wicks K. The modular group and generalized Farey graphs. London Mathematical Society Lecture Note Series 1991; 160: 316-338.
- [10] Kader S, Guler BO, Deger AH. Suborbital graphs for a special subgroup of the normalizer. Iranian Journal of Science and Technology. Transaction A. Science 2010; 34(A4): 305-312.
- [11] Kader S. Circuits in suborbital graphs for the normalizer. Graphs and Combinatorics 2017; 33(6): 1531-1542. doi: 10.1007/s00373-017-1852-x
- [12] Keskin R. Suborbital graphs for the normalizer of $\Gamma_0(m)$. European Journal of Combinatorics 2006; 27(2): 193-206. doi: 10.1016/j.ejc.2004.09.004
- [13] Keskin R, Demirtürk B. On suborbital graphs for the normalizer of $\Gamma_0(N)$. Electronic Journal of Combinatorics 2009; 27: R116.
- [14] Maclachlan C. Groups of units of zero ternary quadratic forms. Proceedings of the Royal Society of Edinburgh. Section A. Mathematics 1981; 88(A): 141-157.
- [15] Magnus W, Karrass A, Solitar D. Combinatorial Group Theory. New York, NY, USA: Wiley, 1966.
- [16] Rose HE. A course in Number Theory. Oxford University Press, 1982.
- [17] Sims CC. Graphs and finite permutation groups. Mathematische Zeitschrift 1967; 95: 76-86.