Güler *et al. SpringerPlus (2016) 5:1327*
DOI 10.1186/s40064-016-3016-5

SpringerPlus

RESEARCH Open Access

Solutions to some congruence equations via suborbital graphs

Bahadır Özgür Güler*, Tuncay Kör and Zeynep Şanlı

*Correspondence:
boguler@yahoo.com.tr
Department of Mathematics, Faculty of Science, Karadeniz Technical University, Trabzon, Turkey

Abstract

We relate the connection between the sizes of circuits in suborbital graph for the normalizer of $\Gamma_0(m)$ in PSL(2,$\mathbb{R}$) and the congruence equations arising from related group action. We give a number theoretic result which says that all prime divisors of $3u^2 \mp 3u + 1$for any integer u must be congruent to $1 \pmod{3}$.

Keywords: Normalizer, Imprimitive action, Suborbital graphs

Mathematics Subject Classification: 11F06, 20H10, 05C25

Background

It is known that the graph of a group provides a method by which a group can be visualized; in many cases it suggests an economical algebraic proof for a result and it gives same information but in a much more efficient way (Magnus et al. 1966). In this view, the idea of suborbital graph has been used mainly by finite group theorists.

After it was shown that this idea is also useful in the study of the modular group which is a finitely generated Fuchsian group (Jones et al. 1991), some other finitely generated groups have been studied by suborbital graphs (see Akbaş and Başkan 1996; Akbaş 2001; Akbaş et al. 2013; Beşenk et al. 2013; Deger et al. 2011; Güler et al. 2011, 2015; Kader et al. 2010; Kader and Güler 2013; Kesicioğlu et al. 2013; Keskin 2006; Kör et al. 2016). In most of them, it has been emphasized the connection between elliptic elements in group and circuits of the same order in graph closely related with the signature problem.

On the other hand, interesting number theoretic results arise from suborbital graphs as follows:

- A shortest path in subgraphs can be expressed as a continued fraction (Jones et al. 1991);
- A shortest path in trees of suborbital graphs is a special case of Pringsheim continued fraction (Deger et al. 2011);
- The subgraph $F_{1,2}$ can be defined as a new kind of continued fraction and any irrational numbers has a unique $F_{1,2}$ expansion (Sarma et al. 2015);
- The set of vertices of some suborbital graphs is strongly connected to the Fibonacci sequence (Akbaş et al. 2013).

Springer Open

In this light, we conclude that these graphs might be worth examining when just viewed from number theory aspect. In fact, it is well-known that modular groups have been studied much in number theory.

The aim of this paper is to examine the action of the normalizer of $\Gamma_0(m)$ which produce some congruence equations with solutions. Actually, the suborbital graphs of the normalizer were studied for some special cases (see Güler et al. 2011; Kader et al. 2010; Keskin 2006). In here, we take a different case that m will be of the form $3p^2$ where p is prime number greater than or equal to 5.

Preliminaries

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

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

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

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

This is the automorphism group of the upper half plane $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im(z)} > 0\}$. Γ, the modular group which is also denoted by $PSL(2, \mathbb{Z})$, is the subgroup of $PSL(2, \mathbb{R})$ such that a, b, c and d are integers. It is one of the most well-known and important discrete groups.

Arithmetic subgroups are finite index subgroups of the modular group. An arithmetic subgroup is said to be congruence if it contains the kernel of a modulo m homomorphism from $PSL(2, \mathbb{Z})$ to $PSL(2, \mathbb{Z}/m\mathbb{Z})$ for some positive integer m. $\Gamma_0(m)$ is the congruence subgroup of Γ with $m|c$.

$$\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \pm\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{m} \right\} \tag{2}$$

We refer the interested reader to a number of sources (Kulkarni 1991; Miyake 1989; Schoeneberg 1974; Shimura 1971) which are also useful to follow the proofs in next section.

Conway and Norton (1977), the normalizer $Nor(m)$ of $\Gamma_0(m)$ in $PSL(2, \mathbb{R})$ consists exactly of matrices

$$\begin{pmatrix} ae & b/h \\ cm/h & de \end{pmatrix}, \tag{3}$$

where $e \parallel \frac{m}{h^2}$ and h is the largest divisor of 24 for which $h^2|m$ 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). $Nor(m)$ is a Fuchsian group whose fundamental domain has finite area, so it has a signature consisting of the geometric invariants

$$(g; m_1, \ldots, m_r; s) \tag{4}$$

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 action of *Nor*(m) on $\hat{\mathbb{Q}}$

Every element of the extended set of rationals $\hat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ can be represented as a reduced fraction $\frac{x}{y}$, with $x, y \in \mathbb{Z}$ and $(x, y) = 1$; since $x/y = -x/-y$, this presentation is not unique. We represented ∞ as $\frac{1}{0} = \frac{-1}{0}$. The action of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on x / y is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \frac{x}{y} \to \frac{ax+by}{cx+dy}. \tag{5}$$

Lemma 1 (Akbaş and Singerman 1992, Corollary 2) *Let m has prime power decomposition $2^{\alpha_1} \cdot 3^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_r^{\alpha_r}$. Then Nor(m) acts transitively on $\hat{\mathbb{Q}}$ if and only if $\alpha_1 \leq 7$, $\alpha_2 \leq 3$ and $\alpha_i \leq 1$ for $i = 3, \ldots, r$.*

Corollary 2 *The action of the normalizer $Nor(3p^2)$ is not transitive on $\hat{\mathbb{Q}}$.*

Proof Since m is taken as the aforementioned case, the result is obvious by Lemma 1.

In this case, we will find a maximal subset of $\hat{\mathbb{Q}}$ on which the normalizer acts transitively. Since $\Gamma_0(m) \subset Nor(m)$, we give more special case before our desired result to understand the situation better. We now give a Lemma as follows.

Lemma 3 (Akbaş and Başkan 1996, Theorem 4.1) *Given an arbitrary rational number k / s with $(k, s) = 1$, then there exists an element $A \in \Gamma_0(m)$ such that $A(k/s) = (k_1/s_1)$ with $s_1|m$.*

The following known Theorem is also proved in the same paper. We will present a different proof for the sake of completeness.

Lemma 4 (Akbaş and Başkan 1996, Theorem 4.3) *Let $b|m$ and let $(a_1, b) = (a_2, b) = 1$. Then $\begin{pmatrix} a_1 \\ b \end{pmatrix}$ and $\begin{pmatrix} a_2 \\ b \end{pmatrix}$ are conjugate under the action of $\Gamma_0(m)$ if and only if $a_1 \equiv a_2 \pmod{t}$, where $t = \left(b, \frac{m}{b}\right)$.*

Proof The necessary part is obvious by Lemma 3. We must prove the converse. Suppose that $a_2 = a_1 + t(b, m/b)$ for some $t \in \mathbb{Z}$. We need an element $T = \begin{pmatrix} k & \ell \\ rm & s \end{pmatrix}$ of $\Gamma_0(m)$ such that $T\begin{pmatrix} a_1 \\ b \end{pmatrix} = \begin{pmatrix} a_2 \\ b \end{pmatrix}$. Performing the multiplication of matrix T and $\begin{pmatrix} a_1 \\ b \end{pmatrix}$ we have three equations in four variables k, ℓ, r and s as follows.

$$\begin{aligned} &ka_1 + \ell b = a_1 + t(b, m/b) \\ &ra_1\frac{m}{b} + s = 1 \\ &ks - rm\ell = 1. \end{aligned}$$

Put $b_0 = (b, m/b)$. Since $(a, b) = 1$, the first equation has solutions (k, ℓ). So $k = \frac{a_1 + tb_0 - \ell b}{a_1}$ and from the second equation $s = 1 - ra\frac{m}{b}$. Putting these k and s into the third equation we get $r(a_1^2 + atb_0)\frac{m}{bb_0} + \ell\frac{b}{b_0} = t$. The coefficient of r and $\frac{b}{b_0}$ are coprime. Therefore the equation has solutions r and ℓ. Consequently, we have obtained an element T (in fact, infinitely many) in $\Gamma_0(m)$ such that $T\begin{pmatrix} a_1 \\ b \end{pmatrix} = \begin{pmatrix} a_2 \\ b \end{pmatrix}$.

Lemma 5 (Güler et al. 2011, Corollary 2.4) *Let* $b|m$*. Then the orbit* $\begin{pmatrix} a \\ b \end{pmatrix}$ *of* a/b *under the action of* $\Gamma_0(m)$*is the set* $\left\{x/y \in \hat{\mathbb{Q}} : (m,y) = b, a \equiv x\frac{y}{b} \pmod{\left(b, \frac{m}{b}\right)}\right\}$*. Furthermore the number of orbits is* $\varphi\left(b, \frac{m}{b}\right)$ *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.*

Proof Lemma 3 and 4 complete the proof.

From the above we come to the following conclusion.

Corollary 6 *The orbits of the action of* $\Gamma_0(3p^2)$ *on* $\hat{\mathbb{Q}}$ *are*

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

Proof Let us denote the representatives of the orbits by $\begin{pmatrix} a \\ b \end{pmatrix}$ as above. The possible values of b are $1, 3, p, 3p, p^2, 3p^2$ by Lemma 3. Hence, the number of non-conjugate classes of these orbits with Euler formula are 1 and $p-1$ for $1, 3, p^2, 3p^2$ and p, $3p$ respectively. By Lemma 5, the result is obvious □

Theorem 7 *The orbits of the action of* $Nor(3p^2)$ *on* $\hat{\mathbb{Q}}$ *are as follows. Let* $l \in \{1, 2, \ldots, p-1\}$*. Then*

(1) (a) If $3 \not| l$ *and* $l \not\equiv p \pmod 3$,

$$\begin{pmatrix} l \\ p \end{pmatrix} \cup \begin{pmatrix} p-l \\ p \end{pmatrix} \cup \begin{pmatrix} l \\ 3p \end{pmatrix} \cup \begin{pmatrix} p-l \\ 3p \end{pmatrix}$$

(b) *If* $3 \not| l$ *and* $l \equiv p \pmod 3$,

$$\begin{pmatrix} l \\ p \end{pmatrix} \cup \begin{pmatrix} p-l \\ p \end{pmatrix} \cup \begin{pmatrix} l \\ 3p \end{pmatrix} \cup \begin{pmatrix} 2p-l \\ 3p \end{pmatrix}$$

(2) If $3 \mid l$, *then*

$$\begin{pmatrix} l \\ p \end{pmatrix} \cup \begin{pmatrix} p-l \\ p \end{pmatrix} \cup \begin{pmatrix} p+l \\ 3p \end{pmatrix} \cup \begin{pmatrix} p-l \\ 3p \end{pmatrix}$$

(3)

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3 \end{pmatrix} \cup \begin{pmatrix} 1 \\ p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3p^2 \end{pmatrix}$$

Proof We prove only (1)-(a). The rest are done similarly. If $T = \begin{pmatrix} ae & b \\ 3p^2c & de \end{pmatrix} \in Nor(3p^2)$, then $e = 1, 3, p^2$ or $3p^2$.

(i) If $e = 1$, then $T\begin{pmatrix} l \\ p \end{pmatrix} = \begin{pmatrix} l \\ p \end{pmatrix}$.

(ii) If $e = 3$, then $T\begin{pmatrix} l \\ p \end{pmatrix} = \begin{pmatrix} 3a & b \\ 3p^2c & 3d \end{pmatrix}\begin{pmatrix} l \\ p \end{pmatrix} = \frac{3al+bp}{3p^2cl+3dp}$. Since $det\begin{pmatrix} 3a & b \\ p^2c & d \end{pmatrix} = 1$, then $(3al + bp, p^2cl + 3d) = 1$. So $\frac{3al+bp}{3p(pcl+d)} \in \begin{pmatrix} x \\ 3p \end{pmatrix}$ and $x \equiv (3al + bp)$ $(pcl + d) \pmod{p}$. As $detT = 3$, then $x \equiv l \pmod{p}$. Consequently $\begin{pmatrix} l \\ p \end{pmatrix} \cup \begin{pmatrix} l \\ 3p \end{pmatrix}$.

(iii) If $e = p^2$, then $T\begin{pmatrix} l \\ p \end{pmatrix} = \frac{apl+b}{p(3cl+dp)} \in \begin{pmatrix} x \\ p \end{pmatrix}$. As $detT = p^2$, then $x \equiv p - l \pmod{p}$. Consequently $\begin{pmatrix} l \\ p \end{pmatrix} \cup \begin{pmatrix} p-l \\ p \end{pmatrix}$.

(iv) If $e = 3p^2$, then $T\begin{pmatrix} l \\ p \end{pmatrix} = \frac{3apl+b}{3p(cl+3dp)} \in \begin{pmatrix} x \\ 3p \end{pmatrix}$. So $x \equiv -l \equiv p - l \pmod{p}$. (i), (ii), (iii) and (iv) complete the proof

□

Corollary 8 *$\hat{\mathbb{Q}}(3p^2) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3 \end{pmatrix} \cup \begin{pmatrix} 1 \\ p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3p^2 \end{pmatrix}$ is the maximal subset of $\hat{\mathbb{Q}}$ on which the normalizer $Nor(3p^2)$ acts transitively.*

Lemma 9 *The stabilizer of a point in $\hat{\mathbb{Q}}(3p^2)$ is an infinite cyclic group.*

Proof Because of the transitive action, stabilizers of any two points are conjugate. So it is enough to look at just $\infty = \frac{1}{0} \in \begin{pmatrix} 1 \\ 3p^2 \end{pmatrix}$. As $T\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} ae & b \\ 3p^2c & de \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{ae}{3p^2c} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, then $c = 0$ and $e = 1$. From the determinant equality, $T = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Consequently $(Nor(3p^2))_\infty = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$.

Now we consider the imprimitivity of the action of $Nor(3p^2)$ on $\hat{\mathbb{Q}}(3p^2)$, beginning with a general discussion of primitivity of permutation groups.

Let (G, Ω) be a 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*. These two relations are supposed to be trivial relations.

Lemma 10 (Biggs and White 1979, Theorem 1.6.5) *Let (G, Ω) be a transitive permutation group. Then (G, Ω) is primitive if and only if G_α, the stabilizer of $\alpha \in \Omega$, is a maximal subgroup of G for each $\alpha \in \Omega$.*

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 cases. Because of the transitivity, every element of Ω has the form $g(\alpha)$ for some $g \in G$. Thus one of the non-trivial G-invariant equivalence relation 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 $H(\alpha)$.

For applying the above to the case; let's take that $Nor(3p^2)$, $\hat{\mathbb{Q}}(3p^2)$, $H_0(3p^2) := \left\langle \Gamma_0(3p^2), \begin{pmatrix} 3a & b \\ 3p^2c & 3d \end{pmatrix} \right\rangle$ and the stabilizer $(Nor(3p^2))_\infty$ instead of G, Ω, H and G_x. Clearly

$$G_\infty < H_0(3p^2) < Nor(3p^2). \tag{6}$$

Lemma 11 (Akbaş and Singerman 1990, 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, $\tau = (\frac{3}{2})^{\varepsilon_1}(\frac{4}{3})^{\varepsilon_2}$,

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

Theorem 12 *The blocks arising from the imprimitive action of the normalizer by above relation (3.2) have the form:*

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

Proof First, we calculate the index $|Nor(3p^2) : \Gamma_0(3p^2)|$ using Lemma 11. It is clear that $h = 1$ for $N = 3p^2$. Furthermore, we have $\rho = 2$ and $\varepsilon_1 = \varepsilon_2 = 0$ in this case. Hence, it can be concluded that $|Nor(3p^2) : \Gamma_0(3p^2)| = 4$. Taking into account the definition of $H_0(3p^2)$, it is clear that $H_0(3p^2) = \Gamma_0(3p^2) \cup g\Gamma_0(3p^2)$ for the element g of the form $\begin{pmatrix} 3a & b \\ 3p^2c & 3d \end{pmatrix}$. So, we have that $|H_0(3p^2) : \Gamma_0(3p^2)| = 2$. Using the equation

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

we have $|Nor(3p^2) : H_0(3p^2)| = 2$. So, the number of blocks is 2 by earlier comments. As we observed in Theorem 7, the orbit $\hat{\mathbb{Q}}(3p^2)$ is divided into two blocks as

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 \\ p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3p^2 \end{pmatrix}$$

taking into account orbit $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ under the action of g.

The suborbital graph of $Nor(3p^2)$ and $\hat{\mathbb{Q}}(3p^2)$

Sims (1967) 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 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 $v_1 \to v_2 \to \cdots \to v_m \to v_1$ such that $v_i \neq v_j$ for $i \neq j$, where $m \geq 3$. If $m = 3, 4$ and 6, then the circuit is called a triangle, a quadrilateral and a hexagon, respectively.

We now investigate the suborbital graphs for the action of $Nor(3p^2)$ on $\hat{\mathbb{Q}}(3p^2)$. Since the action of $Nor(3p^2)$ on $\hat{\mathbb{Q}}(3p^2)$ is transitive, $Nor(3p^2)$ permutes the blocks transitively; so the subgraphs are all isomorphic. Hence it is sufficent to study with 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 $u/p^2 \in \hat{\mathbb{Q}}(3p^2)$. We let $F(\infty, u/p^2)$ be the subgraph of $G(\infty, u/p^2)$ whose vertices form the block $[\infty] = \begin{pmatrix} 1 \\ p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 3p^2 \end{pmatrix}$, so that $G(\infty, u/p^2)$ consists of two disjoint copies of $F(\infty, u/p^2)$.

Theorem 13 (Edge condition) *Let* r/s and x/y *be in the block* $[\infty]$. *Then there is an edge* $r/s \to x/y$ *in* $F(\infty, u/p^2)$ *if and only if*

(i) If $p^2|s$ but $3p^2 \not| s$, then $x \equiv \mp 3ur \pmod{p^2}, y \equiv \mp 3us \pmod{3p^2}, ry - sx = \mp p^2$
(ii) If $3p^2|s$ then $x \equiv \mp ur \pmod{p^2}, y \equiv \mp us \pmod{p^2}, ry - sx = \mp p^2$

Proof Assume first $\frac{r}{s} \to \frac{x}{y}$ is an edge in $F(\infty, u/p^2)$ and $p^2|s$ but $3p^2 \not| s$. Therefore there exists some T in the normalizer $Nor(3p^2)$ such that T sends the pair $(\infty, u/p^2)$ to the pair $(r\ /\ s, x\ /\ y)$, that is $T(\infty) = r/s$ and $T(u/p^2) = x/y$. Since $3p^2 \not| s$, T must be of the form $\begin{pmatrix} 3a & b \\ 3p^2c & 3d \end{pmatrix}$. $T(\infty) = 3a/3p^2c = \begin{pmatrix} (-1)^i r \\ (-1)^i s \end{pmatrix}$ gives that $r = (-1)^i a$ and $s = (-1)^i p^2 c$, for $i = 0, 1$. $T(u/p^2) = \begin{pmatrix} 3a & b \\ 3p^2c & 3d \end{pmatrix} \begin{pmatrix} u \\ p^2 \end{pmatrix} =$

$$= \begin{pmatrix} 3au + bp^2 \\ 3p^2cu + 3dp^2 \end{pmatrix} = \begin{pmatrix} (-1)^j x \\ (-1)^j y \end{pmatrix} \quad \text{for } j = 0, 1.$$

Since the matrix $\begin{pmatrix} 3a & b \\ p^2c & d \end{pmatrix}$ has determinant 1 and $(u, p^2) = 1$, then $(3au + bp^2, p^2cu + dp^2) = 1$. Therefore $(3au + bp^2, 3p^2cu + 3dp^2) = 1$. So

$$x = (-1)^j (3au + bp^2),\ y = (-1)^j (3p^2cu + 3dp^2).$$

That is, $x = (-1)^{i+j} 3au \pmod{p^2}$, $y = (-1)^{i+j} 3su \pmod{3p^2}$. Finally, since

$$\begin{pmatrix} 3a & b \\ 3p^2c & 3d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & p^2 \end{pmatrix} = \begin{pmatrix} (-1)^i 3r & (-1)^j x \\ (-1)^i 3s & (-1)^j y \end{pmatrix} \quad \text{for } i, j = 0, 1,$$

we get $ry - sx = \mp p^2$. This proves (i).

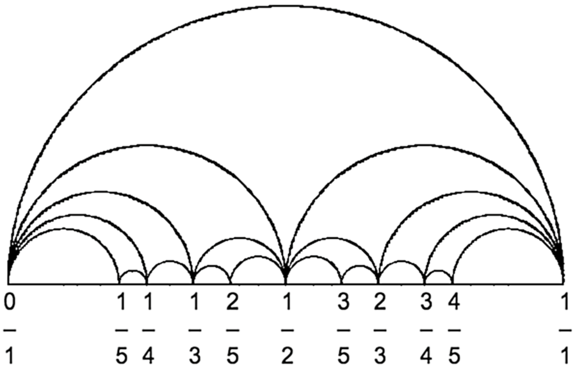

Fig. 1 Farey graph

Secondly let $\frac{r}{s} \to \frac{x}{y}$ be an edge in $F(\infty, u/p^2)$ and $3p^2|s$. In this case T must be of the form $\begin{pmatrix} a & b \\ 3p^2c & d \end{pmatrix}$, det $T = 1$. Therefore, since $T(\infty) = \begin{pmatrix} a \\ 3p^2c \end{pmatrix} = \begin{pmatrix} (-1)^i r \\ (-1)^i s \end{pmatrix}$ we get $a = r$ and $s = 3p^2c$, by taking i to be 0. Likewise, since

$$\begin{pmatrix} a & b \\ 3p^2c & d \end{pmatrix} \begin{pmatrix} u \\ p^2 \end{pmatrix} = \begin{pmatrix} au + bp^2 \\ 3p^2cu + dp^2 \end{pmatrix} = \begin{pmatrix} (-1)^j x \\ (-1)^j y \end{pmatrix},$$

we have $x \equiv ur(\text{mod } p^2)$ and $y \equiv us(\text{mod } p^2)$ and that $ry - sx = p^2$ with $j = 0$. The case where $i = 0$ and $j = 1$ gives (b).

In the opposite direction we do calculations only for (i)(a). The others are likewise done. So suppose $x \equiv 3ur \pmod{p^2}$, $y \equiv 3us \pmod{3p^2}$, $ry - sx = p^2$, $p^2|s$ and $3p^2 \not| s$. Therefore there exist b, d in $\mathbb{Z}$ such that $x = 3ur + p^2b$ and $y = 3su + 3p^2d$. Since $ry - sx = p^2$, we get $3rd - bs = 1$, or $9rd - 3bs = 3$. Hence the element $T := \begin{pmatrix} 3r & b \\ 3s & 3d \end{pmatrix}$ is not only in the normalizer $Nor(3p^2)$, but also in H. It is obvious that $T(\infty) = \begin{pmatrix} r \\ s \end{pmatrix}$ and $T\begin{pmatrix} u \\ p^2 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$. □

Farey graph and subgraph $F(\infty, u/p^2)$

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 real line as in Jones and Singerman (1987). To understand the situation better, we give the Farey graph and some its properties as follows:

Definition 14 The Farey graph, denoted by F, is defined as : the vertex ∞ is joined to the integers, while two rational numbers *r/s* and *x/y* (in reduced form) are adjacent in F if and only if $r/s - x/y = \mp 1$, or equivalently if they are consecutive terms in some Farey sequence F_m (consisting of the rationals x/y *with* $|y| \leq m$, arranged in increasing order). See also Fig. 1.

Lemma 15 (Jones et al. 1991, Corollary 4.2) *No edges of F cross in* $\mathbb{H}$.

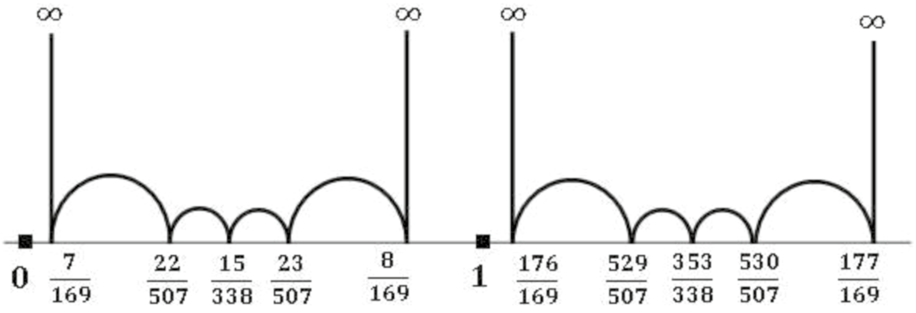

Fig. 2 Subgraph $F(\infty, 7/169)$

Similar result can be given by both of following useful Lemma and Theorem 13 as in (Jones et al. 1991);

Lemma 16 *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 17 *No edges of the subgraph $F(\infty, u/p^2)$ of $Nor(3p^2)$ cross in $\mathbb{H}$.*

Proof Without loss of generality, because of the transitive action, we can take the edges $\infty \rightarrow \frac{u}{p^2}$, $\frac{x_1}{y_1 p^2} \rightarrow \frac{x_2}{y_2 p^2}$ and $\frac{x_1}{y_1 p^2} < \frac{u}{p^2} < \frac{x_2}{y_2 p^2}$, where all letters are positive integers. It is easily seen that $x_1 y_2 p^2 - x_2 y_1 p^2 = -p^2$ by Theorem 13. $\frac{x_1}{y_1} < u < \frac{x_2}{y_2}$ and Lemma 16 complete the proof.

Results

Theorem 18 *$F(\infty, u/p^2)$ has a self-paired edge iff $3u^2 \equiv -1 \pmod{p^2}$.*

Proof Because of the transitive action, the form of self-paired edge can be taken of $1/0 \rightarrow u/p^2 \rightarrow 1/0$. The condition follows immediately from the second edge by Theorem 13.

Theorem 19 *$F(\infty, u/p^2)$ has no triangle or quadrilateral.*

Proof We suppose that it has a triangle. Because of the transitive action, it must be of the form $1/0 \rightarrow u/p^2 \rightarrow x/3p^2 y \rightarrow 1/0$. But this contradicts Theorem 13 which says that both denominators of vertices of an edge having the form $\frac{r}{s} \rightarrow \frac{x}{y}$ are not divisible by 3 at the same time. We now suppose that it has a quadrilateral. It must be of the form $1/0 \rightarrow u/p^2 \rightarrow x/3p^2 y \rightarrow k/p^2 \rightarrow 1/0$ by same reason. From second, third and fourth edges by Theorem 13, we have the equations; $3uy - x = -1$, $x - 3ky = -1$ and $1 \equiv -3uk \pmod{p^2}$. Therefore we obtain a contradiction $3|2$.

Theorem 20 *If* $3u^2 \mp 3u + 1 \equiv 0 \pmod{p^2}$, $F(\infty, u/p^2)$ *has a hexagon.*

Proof By Theorem 13, we obtain easily that

$$\infty \to \frac{u}{p^2} \to \frac{3u \mp 1}{3p^2} \to \frac{2u \mp 1}{2p^2} \to \frac{3u \mp 2}{3p^2} \to \frac{u \mp 1}{p^2} \to \infty$$

As an example, we can verify easily $\frac{1}{0} \to \frac{7}{169} \to \frac{22}{507} \to \frac{15}{338} \to \frac{23}{507} \to \frac{8}{169} \to \frac{1}{0}$ is a hexagon in $F(\infty, 7/169)$. See also Fig. 2.

Theorem 21 $H_0(3p^2)$ *contains an elliptic element* φ *of order 6 if and only if* $F(\infty, u/p^2)$ *contains a hexagon.*

Proof Taking into account (3), we suppose that $\varphi = \begin{pmatrix} 3a & b \\ 3p^2c & 3d \end{pmatrix}$ is an elliptic element of order 6. It is known that $a + d = \pm 1$ for order 3, 4, 6. Since $det = 3$, we have $3a(\pm 1 - a) \equiv 1(\mathrm{mod}p^2)$, that is $3a^2 \mp 3a + 1 \equiv 1(\mathrm{mod}p^2)$. As $(a, n) = 1$, $F(\infty, u/p^2)$ contains a hexagon by above Theorem.

Conversely, we suppose that $F(\infty, u/p^2)$ contains a hexagon. Because of the transitive action, we have

$$\infty \to \frac{u}{p^2} \to \frac{3u \mp 1}{3p^2} \to \frac{2u \mp 1}{2p^2} \to \frac{3u \mp 2}{3p^2} \to \frac{u \mp 1}{p^2} \to \infty$$

Hence we get the element $\varphi := \begin{pmatrix} -3u & (3u^2 \mp 3u + 1)/p^2 \\ -3p^2 & 3u + 3 \end{pmatrix}$.

Lemma 22 (Akbaş and Singerman 1990, Theorem 2) *The periods of elliptic elements of Nor(m) may be 2, 3, 4, 6. Nor(m) has at most one period of order 6. It has a period of order 6 iff* $3 \| m/h^2$ *and if p is an odd prime divisor of* m/h^2 *then* $p \equiv 1 \pmod 3$.

Corollary 23 *The prime divisors p of* $3u^2 \mp 3u + 1$, *for any* $u \in \mathbb{Z}$, *are of the form* $p \equiv 1 \pmod 3$.

Proof Let p a prime number and a divisor of $3u^2 \mp 3u + 1$ for any integer u. In this case, it is clear that $Nor(3p)$ has the elliptic element $\begin{pmatrix} -3u & (3u^2 \mp 3u + 1)/p \\ -3p & 3u + 3 \end{pmatrix}$ of order 6 as in $Nor(3p^2)$. We get $p \equiv 1 \pmod 3$ by above Lemma.

Conclusions

Because this work combine different fields of mathematics such as algebra, geometry, group theory and number theory, it can be seen as an example of multidisciplinary approach which offer a new understanding of some situations. We show that we can produce solutions for some number theoretic problems using finite group theory once again. Taking into account the conjecture (Güler et al. 2011) which is also confirmed for the simplest hexagonal case within non-transitive cases by this paper, the normalizer has a potential to suggest solutions for other congruence equations such as $8u^2 \mp 4u + 1 \equiv 0 \pmod p$, $9u^2 \mp 3u + 1 \equiv 0 \pmod p$, $27u^2 \mp 9u + 1 \equiv 0 \pmod p$ etc.

Authors' contributions

BÖG, TK, ZŞ completed the paper together. All authors read and approved the final manuscript.

Acknowledgements

We would like to express our sincere gratitude to Professor M. Akbaş for his immense help during the preparation of this paper. The authors are also thankful to the anonymous referees for the valuable suggestions towards the improvement of this manuscript.

Competing interests

The authors declare that they have no competing interests.

Received: 9 April 2016 Accepted: 5 August 2016
Published online: 11 August 2016

References

Akbaş M, Singerman D (1990) The normalizer of $\Gamma_0(N)$ in $PSL(2, R)$. Glasgow Math 32:317–327
Akbaş M, Singerman D (1992) The signature of the normalizer of $\Gamma_0(N)$ in $PSL(2, R)$. Lond Math Soc 165:77–86
Akbaş M, Başkan T (1996) Suborbital graphs for the normalizer of $\Gamma_0(N)$. Turk J Math 20:379–387
Akbaş M (2001) On suborbital graphs for the modular group. Bull Lond Math Soc 33:647–652
Akbaş M, Kör T, Kesicioglu Y (2013) Disconnectedness of the subgraph F^3 for the group Γ^3. J Inequal Appl 283:7
Beşenk M et al (2013) Circuit lengths of graphs for the Picard group. J Inequal Appl 106:8
Bigg NL, White AT (1979) Permutation groups and combinatorial structures. London mathematical society lecture note series, 33, CUP, Cambridge
Conway JH, Norton SP (1977) Monstrous moonshine. Bull Lond Math Soc 11:308–339
Deger AH, Beşenk M, Güler BO (2011) On suborbital graphs and related continued fractions. Appl Math Comput 218(3):746–750
Güler BO et al (2011) Elliptic elements and circuits in suborbital graphs. Hacet J Math Stat 40(2):203–210
Güler BO et al (2015) Suborbital graphs for the group Γ^2. Hacet J Math Stat 44(5):1033–1044
Jones GA, Singerman D (1987) Complex functions: an algebraic and geometric viewpoint. Cambridge University Press, Cambridge
Jones GA, Singerman D, Wicks K (1991) The modular group and generalized Farey graphs. Lond Math Soc Lect Note Ser 160:316–338
Kader S, Güler BO, Değer AH (2010) Suborbital graphs for a special subgroup of the normalizer. Iran J Sci Technol A 34(A4):305–312
Kader S, Güler BO (2013) On suborbital graphs for the extended modular group $\hat{\Gamma}$. Gr Comb 29(6):1813–1825
Kesicioğlu Y, Akbaş M, Beşenk M (2013) Connectedness of a suborbital graph for congruence subgroups. J Inequal Appl 117:7
Keskin R (2006) Suborbital graphs for the normalizer of $\Gamma_0(m)$. Eur J Comb 27(2):193–206
Kör T, Güler BO, Şanlı Z (2016) Suborbital graphs for Atkin–Lehner group. Turk J Math. doi:10.3906/mat-1602-10
Kulkarni RS (1991) An arithmetic–geometric method in the study of the subgroups of the modular group. Am J Math 113(6):1053–1133
Magnus M, Karrass A, Solitar D (1966) Combinatorial group theory. Wiley, New York
Miyake T (1989) Modular forms. Springer, Berlin
Sarma R, Kushwaha S, Krishnan R (2015) Continued fractions arising from $F_{1,2}$. J Number Theory 154:179–200
Schoeneberg B (1974) Elliptic modular functions. Springer, Berlin
Shimura G (1971) Introduction to the arithmetic theory of automorphic functions. Princeton University Press, Princeton
Sims CC (1967) Graphs and finite permutation groups. Math Z 95:76–86