

SUBORBITAL GRAPHS FOR A SPECIAL SUBGROUP OF THE NORMALIZER OF $\Gamma_0(m)^*$

S. KADER¹, B. O. GULER^{2**} AND A. H. DEGER³

¹Department of Mathematics, Nigde University, Nigde, Turkey
Email: skader@nigde.edu.tr

²Department of Mathematics, Rize University, Rize, Turkey
Email: bahadir.guler@rize.edu.tr

³Department of Mathematics, Karadeniz Technical University, Trabzon, Turkey
Email: ahikmetd@ktu.edu.tr

Abstract – In this paper, we find the number of sides of circuits in suborbital graph for the normalizer of $\Gamma_0(m)$ in $\text{PSL}(2, \mathbb{R})$, where m will be of the form $2p^2$, p is a prime and $p \equiv 1 \pmod{4}$. In addition, we give a number theoretical result which says that the prime divisors p of $2u^2 \pm 2u + 1$ are of the form $p \equiv 1 \pmod{4}$.

Keywords – Normalizer, imprimitive action, suborbital graph, circuits

1. INTRODUCTION

Let $\text{PSL}(2, \mathbb{R})$ denote the group of all linear fractional $T: z \rightarrow \frac{az+b}{cz+d}$, where a, b, c, d are real and $ad - bc = 1$. The modular group Γ is the subgroup of $\text{PSL}(2, \mathbb{R})$ such that a, b, c and d are integers. For any natural number m , $\Gamma_0(m)$ is the subgroup of Γ with $m | c$. The elements of $\text{PSL}(2, \mathbb{R})$ are represented as

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

We will omit the symbol \pm and identify each matrix with its negative.

$\Gamma_1(m)$ will denote the normalizer of $\Gamma_0(m)$ in $\text{PSL}(2, \mathbb{R})$. The elements of $\Gamma_1(m)$ are of the form by [1]

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

where all letters are integers, $e \parallel m/h^2$ and h is the largest divisor of 24 for which $h^2 | m$ with the understanding that the determinant is $e > 0$, and that $r \parallel s$ means that $r | s$ and $\left(r, \frac{s}{r}\right) = 1$.

Here, m will be $2p^2$, where p is a prime such that $p \equiv 1 \pmod{4}$. All circuits in suborbital graph for the normalizer of $\Gamma_0(m)$ in $\text{PSL}(2, \mathbb{R})$ where m is a square-free positive integer was studied in [2, 3].

*Received by the editor February 21, 2009 and in final revised form December 18, 2010

**Corresponding author

Our main idea is that we investigate a case in which m is not square-free. Similar studies were done for the modular group and some Hecke groups [4-6]. In this case, h will be 1 and e is 1, 2, p^2 or $2p^2$.

2. THE ACTION OF $\Gamma_1(2p^2)$ ON $\hat{\mathbb{Q}}$

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

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

Therefore, the action of a matrix on $\frac{x}{y}$ and on $\frac{-x}{-y}$ is identical. If the determinant of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is 1 and $(x, y) = 1$, then $(ax+by, cx+dy) = 1$. A necessary and sufficient condition for $\Gamma_1(m)$ to act transitively on $\hat{\mathbb{Q}}$ is given in [7].

Lemma 2.1. Let m be any integer and $m = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot p_3^{\alpha_3} \dots p_r^{\alpha_r}$, the prime power decomposition of m . Then $\Gamma_1(m)$ is transitive on $\hat{\mathbb{Q}}$ if and only if $\alpha_1 \leq 7, \alpha_2 \leq 3$ and $\alpha_i \leq 1$ for $i = 3, \dots, r$.

Corollary 2.2. The action of the normalizer $\Gamma_1(2p^2)$ is not transitive on $\hat{\mathbb{Q}}$.

Since the action is not transitive on $\hat{\mathbb{Q}}$ we now find a maximal subset of $\hat{\mathbb{Q}}$ on which the normalizer acts transitively. First we start with

Lemma 2.3. The orbits of the action of $\Gamma_0(2p^2)$ on $\hat{\mathbb{Q}}$ are $\begin{pmatrix} 1 \\ 1 \end{pmatrix}; \begin{pmatrix} 1 \\ 2 \end{pmatrix}; \begin{pmatrix} 1 \\ p \end{pmatrix}; \begin{pmatrix} 2 \\ p \end{pmatrix}, \dots, \begin{pmatrix} p-1 \\ p \end{pmatrix};$
 $\begin{pmatrix} 1 \\ 2p \end{pmatrix}; \begin{pmatrix} 3 \\ 2p \end{pmatrix}, \dots, \begin{pmatrix} p-2 \\ 2p \end{pmatrix}; \begin{pmatrix} p+2 \\ 2p \end{pmatrix}; \begin{pmatrix} p+4 \\ 2p \end{pmatrix}, \dots, \begin{pmatrix} 2p-1 \\ 2p \end{pmatrix}; \begin{pmatrix} 1 \\ p^2 \end{pmatrix}; \begin{pmatrix} 1 \\ 2p^2 \end{pmatrix}$, where
 $\begin{pmatrix} x \\ y \end{pmatrix} := \left\{ \frac{k}{l} \in \hat{\mathbb{Q}} \mid (2p^2, l) = y, x \equiv k \frac{l}{y} \pmod{y, \frac{2p^2}{y}} \right\}.$

Proof: It is well known that if $\frac{k}{s} \in \hat{\mathbb{Q}}$ is given, then there exists some $T \in \Gamma_0(2p^2)$ such that $T \begin{pmatrix} k \\ s \end{pmatrix} = \begin{pmatrix} k_1 \\ s_1 \end{pmatrix}$ with $s_1 \mid 2p^2$. And furthermore, for $d \mid 2p^2$, $\begin{pmatrix} a_1 \\ d \end{pmatrix} = \begin{pmatrix} a_2 \\ d \end{pmatrix}$ if and only if $a_1 \equiv a_2 \pmod{d, \frac{2p^2}{d}}$. So the result follows.

Lemma 2.4. The orbits of the action of $\Gamma_1(2p^2)$ are as follows. Let $l \in \{1, 2, \dots, p-1\}$. Then

(a) If l is odd then

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

(b) If l is even then

$$\begin{pmatrix} l \\ p \end{pmatrix} \cup \begin{pmatrix} p-l \\ p \end{pmatrix} \cup \begin{pmatrix} p+l \\ 2p \end{pmatrix} \cup \begin{pmatrix} 2p-l+1 \\ 2p \end{pmatrix}$$

$$(c) \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2p^2 \end{pmatrix}$$

Proof: We prove only (a). The rest are similar.

Let $T = \begin{pmatrix} ae & b \\ 2p^2c & de \end{pmatrix}$ be an arbitrary element in $\Gamma_1(2p^2)$. Then e must be $1, 2, p^2$ or $2p^2$.

Case 1. Let $e = 1$. Then $T \in \Gamma_0(2p^2)$. Therefore T fixes $\begin{pmatrix} l \\ p \end{pmatrix}$.

Case 2. Let $e = 2$. Then $\begin{pmatrix} 2a & b \\ 2p^2c & 2d \end{pmatrix} \begin{pmatrix} l \\ p \end{pmatrix} = \begin{pmatrix} 2al + bp \\ 2p^2cl + 2dp \end{pmatrix}$.

Since $\begin{pmatrix} 2a & b \\ p^2c & d \end{pmatrix} \begin{pmatrix} l \\ p \end{pmatrix} = \begin{pmatrix} 2al + bp \\ p^2cl + dp \end{pmatrix}$ and $2ad - p^2bc = 1$, we conclude that $(2al + bp, 2p^2cl + 2dp) = 1$.

Therefore,

$$\begin{pmatrix} 2al + bp \\ 2p(pcl + d) \end{pmatrix} = \begin{pmatrix} x \\ 2p \end{pmatrix}, \text{ where } x \equiv (2al + bp)(pcl + d) \pmod{p}.$$

This shows that $\begin{pmatrix} l \\ p \end{pmatrix}$ and $\begin{pmatrix} \ell \\ 2p \end{pmatrix}$ must be in a single orbit of $\Gamma_1(2p^2)$.

Case 3. Let $e = p^2$. Then $T = \begin{pmatrix} ap^2 & b \\ 2p^2c & dp^2 \end{pmatrix}$, $adp^4 - 2p^2bc = p^2$.

$$T \begin{pmatrix} l \\ p \end{pmatrix} = \begin{pmatrix} ap^2l + bp \\ 2p^2cl + dp^3 \end{pmatrix} = \begin{pmatrix} apl + b \\ 2pcl + dp^2 \end{pmatrix}$$

and as in Case 2, $(apl + b, 2pcl + dp^2) = 1$. Therefore,

$$T \begin{pmatrix} l \\ p \end{pmatrix} = \begin{pmatrix} x \\ p \end{pmatrix}, \text{ where } x \equiv (apl + b)(2cl + dp) \pmod{p} \text{ or } x \equiv 2bcl \pmod{p}.$$

Since $2bc \equiv -1 \pmod{p}$, $x \equiv p - l \pmod{p}$. Therefore $\begin{pmatrix} l \\ p \end{pmatrix}$ and $\begin{pmatrix} p-l \\ p \end{pmatrix}$ must be in a single orbit of $\Gamma_1(2p^2)$.

Case 4. Let $e = 2p^2$. Then we easily find that T sends $\begin{pmatrix} l \\ p \end{pmatrix}$ to $\begin{pmatrix} 2p-l \\ 2p \end{pmatrix}$. So we consequently have the orbit $\begin{pmatrix} l \\ p \end{pmatrix} \cup \begin{pmatrix} p-l \\ p \end{pmatrix} \cup \begin{pmatrix} l \\ 2p \end{pmatrix} \cup \begin{pmatrix} 2p-l \\ 2p \end{pmatrix}$.

Corollary 2.6. The action of $\Gamma_1(2p^2)$ on $\widehat{\mathbb{Q}}(2p^2) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ p^2 \end{pmatrix} \cup \begin{pmatrix} 1 \\ 2p^2 \end{pmatrix}$ is transitive.

Lemma 2.7. The stabilizer of a point in $\widehat{\mathbb{Q}}(2p^2)$ is an infinite cyclic group.

Proof: Since the action is transitive, stabilizers of any two points are conjugate. Therefore, we can only look at the stabilizer of ∞ in $\Gamma_1(2p^2)$.

$$T \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} ae & b \\ 2p^2c & de \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} ae \\ 2p^2c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

then $c = 0$. In this case $e = 1$ and since $ad = 1$, $T = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. This shows that stabilizer $(\Gamma_1(2p^2))_\infty$ of ∞ is $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$.

We know from [7] (see also [8]) that the orders of the elliptic elements of $\Gamma_1(2p^2)$ may be 2, 3, 4, or

6. Therefore, we give the following:

Lemma 2.8. Let p be a prime and $p \equiv 1 \pmod{4}$. Then the normalizer $\Gamma_1(2p^2)$ contains an elliptic element E of order 4 and that E is of the form $\begin{pmatrix} 2a & b \\ 2p^2c & 2(1-a) \end{pmatrix}$, $\det E = 2$.

Let (G, X) be transitive permutation group, and suppose that R is an equivalence relation on X . R is said to be G -invariant if $(x, y) \in R$ implies $(g(x), g(y)) \in R$ for all $g \in G$. The equivalence classes of a G -invariant relation are called *blocks*. We give the following from [9].

Lemma 2.9. Suppose that (G, X) is a transitive permutation group, and H is a subgroup of G such that, for some $x \in X$, $G_x \subset H$. Then $R = \{(g(x), gh(x)) : g \in G, h \in H\}$ is an equivalence relation.

Lemma 2.10. Let (G, X) be a transitive permutation group, and \approx the G -invariant equivalence relation defined in Lemma 2.9; then $g_1(\alpha) = g_2(\alpha)$ if and only if $g_1 \in g_2H$. Furthermore, the number of blocks is $|G:H|$.

To apply the ideas, we take $(\Gamma_1(2p^2), \widehat{\mathbb{Q}}(2p^2))$, $\left\langle \Gamma_0(2p^2), \begin{pmatrix} 2a & b \\ 2p^2c & 2(1-a) \end{pmatrix} \right\rangle$ and the stabilizer $(\Gamma_1(2p^2))_\infty$ of ∞ in $\Gamma_1(2p^2)$ instead of (G, X) , H and G_x . In this case the number of blocks is 2 and these blocks are

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

3. SUBORBITAL GRAPHS OF $\Gamma_1(2p^2)$ ON $\widehat{\mathbb{Q}}(2p^2)$

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

$$g(\alpha, \beta) = (g(\alpha), g(\beta)), \quad (g \in G; \alpha, \beta \in X).$$

The orbits of this action are called suborbitals of the normalizer 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 X , 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 $\gamma \rightarrow \delta$. If $(\gamma, \delta) \in O(\alpha, \beta)$, then we will say that there exists an edge $\gamma \rightarrow \delta$ 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 $x \in X$. We will mainly be interested in the remaining non-trivial suborbital graphs. These ideas were first introduced by Sims [10].

We now investigate the suborbital graphs for the action of $\Gamma_1(2p^2)$ on $\widehat{\mathbb{Q}}(2p^2)$. Since the action of $\Gamma_1(2p^2)$ on $\widehat{\mathbb{Q}}(2p^2)$ is transitive, $\Gamma_1(2p^2)$ permutes the blocks transitively; so the subgraphs are all isomorphic. Hence, it is sufficient 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 $u/p^2 \in \mathbb{Q}(2p^2)$. 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 $[\infty]$.

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

- (i) If $p^2 \mid s$ but $2p^2 \nmid s$, then $x \equiv \pm 2ur \pmod{p^2}$, $y \equiv \pm 2us \pmod{2p^2}$, $ry - sx = \pm p^2$
- (ii) If $2p^2 \mid s$, then $x \equiv \pm ur \pmod{p^2}$, $y \equiv \pm us \pmod{p^2}$, $ry - sx = \pm p^2$.

Proof: Assume first that $r/s \rightarrow x/y$ is an edge in $F(\infty, u/p^2)$ and that $p^2 \mid s$ but $2p^2 \nmid s$. Therefore, there exists some T in the normalizer $\Gamma_1(2p^2)$ 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 $2p^2 \nmid s$, T must be of the form $\begin{pmatrix} 2a & b \\ 2p^2c & 2d \end{pmatrix}$. $T(\infty) = \frac{2a}{2p^2c} = \frac{(-1)^i r}{(-1)^i s}$ gives that $r = (-1)^i a$ and $s = (-1)^i p^2 c$, for $i = 0, 1$.

$$T(u/p^2) = \begin{pmatrix} 2a & b \\ 2p^2c & 2d \end{pmatrix} \begin{pmatrix} u \\ p^2 \end{pmatrix} = \begin{pmatrix} 2au + bp^2 \\ 2p^2cu + 2dp^2 \end{pmatrix} = \begin{pmatrix} (-1)^j x \\ (-1)^j y \end{pmatrix} \text{ for } j = 0, 1.$$

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

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

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

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

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

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

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

we have $x \equiv ur \pmod{p^2}$ and $y \equiv us \pmod{p^2}$ and that $ry - sx = p^2$. In the case where $i = 0$ and $j = 1$, the minus sign holds.

In the opposite direction we do calculations only for (i) and the plus sign. The other are likewise done. So suppose $x \equiv 2ur \pmod{p^2}$, $y \equiv 2us \pmod{2p^2}$, $ry - sx = p^2$, $p^2 \mid s$ and $2p^2 \nmid s$.

Therefore there exists b, d in \mathbb{Z} such that $x = 2ur + p^2b$ and $y = 2us + 2p^2d$. Since $ry - sx = p^2$, we

get $2rd - bs = 1$, or $4rd - bs = 2$. Hence the element $T := \begin{pmatrix} 2r & b \\ 2s & 2d \end{pmatrix}$ is not only in the normalizer $\Gamma_1(2p^2)$, but also H . It is obvious that $T(\infty) = \begin{pmatrix} r \\ s \end{pmatrix}$ and $T\begin{pmatrix} u \\ p^2 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$.

Theorem 3.2. If we present edges of $F(\infty, u/p^2)$ as hyperbolic geodesics in the upper half-plane \mathbb{H} , no edges of the subgraph $F(\infty, u/p^2)$ of $\Gamma_1(2p^2)$ cross in \mathbb{H} .

Proof: Without loss of generality, since the action on $\widehat{\mathbb{Q}}(2p^2)$ is transitive, suppose that $\infty \rightarrow u/p^2$, $x_1/y_1p^2 \rightarrow x_2/y_2p^2$ and $x_1/y_1p^2 < u/p^2 < x_2/y_2p^2$, where all letters are positive integers. Since $x_1/y_1p^2 \rightarrow x_2/y_2p^2$ and $x_1/y_1p^2 < u/p^2 < x_2/y_2p^2$, then $x_1y_2 - x_2y_1 = -1$ and $x_1/y_1 < u < x_2/y_2$, respectively. Therefore

$$(x_1/y_1) - (x_2/y_2) < u - (x_2/y_2) < 0.$$

Then $(x_1y_2 - x_2y_1)/y_1y_2 < (uy_2 - x_2)/y_2 < 0$. So $-1/y_2 < uy_2 - x_2 < 0$, a contradiction [11].

4. THE NUMBER OF SIDES OF CIRCUITS

Let (G, X) be a transitive permutation group and $G(\alpha, \beta)$ be a suborbital graph. By a directed circuit in $G(\alpha, \beta)$, we mean a sequence $v_1 \rightarrow v_2 \rightarrow \dots \rightarrow v_m \rightarrow v_1$, where $m \geq 3$; an anti-directed circuit will denote a configuration like the above with at least one arrow (not all) reversed. If $m = 2, 3$ or 4 then the circuit, directed or not, is called a self-paired, a triangle or a rectangle, respectively.

Theorem 4.1. $F(\infty, u/p^2)$ has a self-paired edge if and only if $2u^2 \equiv -1 \pmod{p^2}$.

Proof: Without loss of generality, from transitivity, we can suppose that the self-paired edge be $\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{1}{0}$. Applying Theorem 3.1, the proof then follows.

Theorem 4.2. $F(\infty, u/p^2)$ contains no triangles.

Proof: Suppose contrary $F(\infty, u/p^2)$ contains a triangle. From transitivity and Theorem 3.1 the form of such a triangle $\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{x}{2p^2} \rightarrow \frac{1}{0}$. But, to be $\frac{x}{2p^2} \rightarrow \frac{1}{0}$ gives a contradiction to Theorem 3.1(ii).

Theorem 4.3. The normalizer $\Gamma_1(2p^2)$ does not contain period 3.

Proof: Suppose the converse that $\Gamma_1(2p^2)$ does have a period 3. Then it has an elliptic element T of order 3. T must be of the form $\begin{pmatrix} a & b \\ 2p^2c & d \end{pmatrix}$, $\det T = 1$ and $a + d = \pm 1$. Take $a + d = 1$. Then $a + d = 1 \pmod{2p^2}$, and since $a + d = 1$, then $a(1 - a) = 1 \pmod{2p^2}$, or $a^2 - a + 1 = 0 \pmod{2p^2}$, which is a contradiction.

Theorem 4.4. The subgraph $F(\infty, u/p^2)$ contains a rectangle if and only if $2u^2 \pm 2u + 1 \equiv 0 \pmod{p^2}$.

Proof: Assume first that $F(\infty, u/p^2)$ has a rectangle $\frac{k_0}{l_0} \rightarrow \frac{m_0}{n_0} \rightarrow \frac{s}{t} \rightarrow \frac{x_0}{y_0} \rightarrow \frac{k_0}{l_0}$. It can be easily shown that H permutes the vertices and edges of $F(\infty, u/p^2)$ transitively. Therefore we suppose that the above rectangle is transformed under H to the rectangle $\frac{1}{0} \rightarrow \frac{m}{p^2} \rightarrow \frac{x}{y} \rightarrow \frac{k}{l} \rightarrow \frac{1}{0}$.

Furthermore, without loss of generality, suppose $\frac{m}{p^2} < \frac{x}{y} < \frac{k}{l}$. From the first edge and Theorem 3.1 we get $m \equiv u \pmod{p^2}$. The second edge gives $x \equiv -2um \pmod{p^2}$ and $2ym - x = -1$; and that from the third edge we have $k \equiv -ux \pmod{p^2}$ and $x - 2ky = -1$. If we combine these we obtain

$$2u^2 + 2ym + 1 \equiv 0 \pmod{p^2} \text{ or } 2u^2 + 2uy + 1 \equiv 0 \pmod{p^2}.$$

Since $x = 2ym + 1 = 2ky - 1$, then $y(m - k) = -1$. This gives that $y=1$. Therefore $2u^2 + 2u + 1 \equiv 0 \pmod{p^2}$.

If $\frac{m}{p^2} > \frac{x}{y} > \frac{k}{l}$ holds then we conclude that $2u^2 - 2u + 1 \equiv 0 \pmod{p^2}$, and furthermore, if $2u^2 - 2u + 1 \equiv 0 \pmod{p^2}$ then we get the rectangle

$$\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{2u-1}{2p^2} \rightarrow \frac{u-1}{p^2} \rightarrow \frac{1}{0}.$$

Secondly suppose that $2u^2 \pm 2u + 1 \equiv 0 \pmod{p^2}$. Then, using Theorem 3.1, we see that $\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{2u \pm 1}{2p^2} \rightarrow \frac{u \pm 1}{p^2} \rightarrow \frac{1}{0}$ is a rectangle.

As an example, $\infty \rightarrow 3/25 \rightarrow 7/50 \rightarrow 4/25 \rightarrow \infty$ is a rectangle in $G(\infty, 3/25)$.

Corollary 4.5. For some u in \mathbb{Z} , $F(\infty, u/p^2)$ contains a rectangle if and only if the group H has a period 4.

Proof: Firstly suppose $F(\infty, u/p^2)$ contains a rectangle. Then, Theorem 4.4 shows that

$2u^2 \pm 2u + 1 \equiv 0 \pmod{p^2}$. So we have the elliptic element $\begin{pmatrix} -2u & \frac{2u^2 \pm 2u + 1}{p^2} \\ -2p^2 & 2u \pm 2 \end{pmatrix}$ of order 4 in H .

Since the index of H is 2 in $\Gamma_1(2p^2)$, the elements of this form must be in H .

Conversely, suppose that H has a period for order 4, so H contains an elliptic element of order 4. Let this element be $\begin{pmatrix} 2a & b \\ 2p^2 & -2a \pm 2 \end{pmatrix}$, $\det = 2$. From this we get $p^2 \mid (2u^2 \pm 2u + 1)$. Therefore $F(\infty, u/p^2)$ contains a rectangle.

We predict from the above lemmas that the elliptic elements of $\Gamma_1(2p^2)$ correspond to the circuit in $F(\infty, u/p^2)$. To support this idea we have

Theorem 4.6. The set $H \setminus \Gamma_0(2p^2)$ has a period for order 2 if and only if there exists some $u \in \mathbb{Z}$, $(u, p) = 1$ such that $F(\infty, u/p^2)$ has a self-paired edge.

Proof: First suppose that the set has such an elliptic element T . Then T must be of the form $\begin{pmatrix} 2a & -b \\ 2p^2 & -2a \end{pmatrix}$, $\det T = 2$. Therefore we have $2a^2 + 1 \equiv 0 \pmod{p^2}$. So, Theorem 3.1 shows that $\frac{1}{0} \rightarrow \frac{a}{p^2} \rightarrow \frac{1}{0}$ is a self-paired edge in $F(\infty, u/p^2)$.

Secondly, let $F(\infty, u/p^2)$ have a self-paired edge. Without loss of generality, from transitivity, we can suppose that the self-paired edge be $\frac{1}{0} \rightarrow \frac{u}{p^2} \rightarrow \frac{1}{0}$. So we have, by Theorem 3.1, $2u^2 \equiv -1 \pmod{p^2}$. This shows that there exists some $b \in \mathbb{Z}$ such that $b = \frac{-(2u^2 + 1)}{p^2}$. Therefore $\begin{pmatrix} 2a & -b \\ 2p^2 & -2a \end{pmatrix}$ is an elliptic element of order 2 in the set $H \setminus \Gamma_0(2p^2)$.

Notice that $H \setminus \Gamma_0(2 \cdot 5^2)$ has no period for order 2, and therefore $F(\infty, u/25)$ does not have a self-paired edge.

Finally, as a finishing point, we give a number theoretical result as follows:

Theorem 4.7. The prime divisors p of $2u^2 + 2u + 1$, 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 $2u^2 + 2u + 1$. Then, without any difficulty, it can be easily seen that the normalizer $\Gamma_1(2p)$, like $\Gamma_1(2p^2)$, has the elliptic element $\begin{pmatrix} -2u & \frac{2u^2 + 2u + 1}{p} \\ -2p & 2u + 2 \end{pmatrix}$ of order 4. From Lemma 2.8 we get that $p \equiv 1 \pmod{4}$.

REFERENCES

1. Conway, J. H. & Norton, S. P. (1977). Monstrous Moonshine. *Bull. London Math. Soc.* 11, 308-339.
2. Akbas, M. & Baskan, T. (1996). Suborbital graphs for the normalizer of $\Gamma_0(\mathbb{N})$. *Tr. J. of Mathematics* 20, 379-387.
3. Keskin, R. (2006). Suborbital graphs for the normalizer $\Gamma_0(m)$. *European J. Combin.* 27 (2), 193-206.
4. Akbas, M. (2001). On suborbital graphs for the modular group. *Bull. London Math. Soc.* 33(6), 647-652.
5. Jones, G. A., Singerman, D. & Wicks, K. (1991). The Modular Group and Generalized Farey Graphs. *London Math. Soc. Lecture Note Series*, 160, 316-338.
6. Keskin, R. (2001). On suborbital graphs for some Hecke groups. *Discrete Math.* 234(1-3), 53-64.
7. Akbas, M. & Singerman, D. (1992). The Signature of the normalizer of $\Gamma_0(\mathbb{N})$. *London Math. Soc. Lecture Note Series* 165, 77-86.
8. Machlaclan, C. (1981). Groups of units of zero ternary quadratic forms. *Proceeding of the Royal Society of Edinburgh*, 88 A, 141-157.
9. Bigg, N. L. & White, A. T. (1979). Permutation groups and combinatorial structures. *London Mathematical Society Lecture Note Series* 33, CUP.
10. Sims, C. C. (1967). Graphs and Finite Permutation Groups. *Math. Z.*, 95, 76-86.
11. Rose, H. E. (1988). *A Course in Number Theory*. Oxford University Press.