Suborbital graphs for the normalizer of $\Gamma_0(m)$

Refik Keskin

Department of Mathematics, Faculty of Science and Arts, Sakarya University, Sakarya, Turkey

Received 12 August 2003; accepted 30 September 2004
Available online 4 January 2005

Abstract

In this study, we characterize all circuits in the suborbital graph for the normalizer of $\Gamma_0(m)$ when $m$ is a square-free positive integer. We propose a conjecture concerning the suborbital graphs.

MSC: 46A40; 05C05; 20H10

1. Introduction

Let $m$ be a positive integer and let $\Gamma_1(m)$ be the normalizer of the congruence subgroup $\Gamma_0(m)$ of the modular group in $PSL(2, \mathbb{R})$. The normalizer $\Gamma_1(m)$ was studied by various authors (see [6,7] and the references there). A necessary and sufficient condition for $\Gamma_1(m)$ to act transitively on $\hat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ is given in [6]. In [1], the authors investigated the suborbital graph for the modular group on $\hat{\mathbb{Q}}$ and so conjectured that the suborbital graph $G(\infty, u/n)$ is a forest if and only if $G(\infty, u/n)$ contains no triangles where $n > 1$. Then, in [3], the author proved that the conjecture is true. In [4], we investigated the suborbital graph for the Hecke group $H(\sqrt{m})$ on the set of cusps of $H(\sqrt{m})$ where $H(\sqrt{m})$ is the Hecke group generated by the mappings

$$z \rightarrow z + \sqrt{m}, \quad z \rightarrow -1/z,$$

$m = 1, 2, 3$. 

E-mail address: rkeskin@sakarya.edu.tr.

0195-6698/$-$ see front matter © 2004 Elsevier Ltd. All rights reserved.
2. The action of \( \Gamma_1(m) \) on \( \hat{\mathbb{Q}} \)

A complete description of the elements of \( \Gamma_1(m) \) is given in [10]. If we represent the elements of \( \Gamma_1(m) \) by the associated matrices, then the normalizer consists exactly of the matrices

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

where \( e | (m/h^2) \) and \( h \) is the largest divisor of 24 for which \( h^2 | m \) with the understanding that the determinant of the matrix is \( e > 0 \), and that \( (e, m/h^2e) = 1 \). The following theorem is proved in [6].

**Theorem 2.1.** Let \( m \) have prime power decomposition \( 2^{a_1}3^{a_2}p_3^{a_3} \cdots p_r^{a_r} \). Then \( \Gamma_1(m) \) acts transitively on \( \hat{\mathbb{Q}} \) if and only if \( a_1 \leq 7, a_2 \leq 3, a_i \leq 1, i = 3, 4, \ldots, r \).

If \( m \) is a square-free positive integer, then \( h = 1 \). Therefore we give the following (see also [7]).

**Theorem 2.2.** Let \( m \) be a square-free positive integer. Then we have

\[
\Gamma_1(m) = \left\{ \left( \frac{a\sqrt{q}}{cm/\sqrt{q}}, \frac{b/\sqrt{q}}{d\sqrt{q}} \right) : 1 \leq q, q | m; a, b, c, d \in \mathbb{Z}; adq - bcm/q = 1 \right\}.
\]

Let \( m \) be a square-free positive integer. Then, in view of the above theorem, the following theorem holds. (Here, for the sake of completeness, we give a simple proof.)

**Theorem 2.3.** Let \( m \) be a square-free positive integer. Then \( \Gamma_1(m) \) acts transitively on the set \( \hat{\mathbb{Q}} = \mathbb{Q} \cup \{ \infty \} \) of the cusps of \( \Gamma_1(m) \) where we represent \( \infty \) as \( \frac{1}{0} = \frac{-1}{0} \).

**Proof.** Let \( k/s \in \hat{\mathbb{Q}} \) with \( (k, s) = 1 \). Let \( q_1 = (s, m) \). Then \( s = s^*q_1 \) for some integer \( s^* \). Since \( m \) is square-free, \( (s, m/q_1) = 1 \). Thus we have \( (s, km/q_1) = 1 \). Therefore there exist two integers \( x \) and \( y \) such that \( (m/q_1)ky - sx = 1 \). Let \( q_2 = m/q_1 \) and let

\[
T(z) = \frac{k\sqrt{q_2}z + x/\sqrt{q_2}}{s\sqrt{q_2}z + y\sqrt{q_2}}.
\]

Then it is easily seen that \( T \in \Gamma_1(m) \) and \( T(\infty) = k/s \). Thus the proof follows. \( \square \)
Let \((m, n) = 1\) and let \(\Gamma_0^*(n)\) be defined by
\[
\Gamma_0^*(n) = \left\{ \left( \frac{a\sqrt{q}}{cm/\sqrt{q}}, \frac{b\sqrt{q}}{dm/\sqrt{q}} \right) : c \equiv 0 \pmod{n} \right\}.
\]

Then \(\Gamma_0^*(n)\) is a subgroup of \(\Gamma_1(m)\) and \(\Gamma_0(mn) \subset \Gamma_0^*(n) \subset \Gamma_1(m)\).

Let \((G, X)\) be a 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 now give a lemma from [2].

**Lemma 1.** 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. Furthermore, \(R = \Delta\), the diagonal of \(X \times X \iff H = G_x\), and \(R = X \times X \iff H = G\).

**Lemma 2.** Let \((G, X)\) be a transitive permutation group, and \(\approx\) the \(G\)-invariant equivalence relation defined in Lemma 1; then \(g_1(\alpha) \approx g_2(\alpha)\) if and only if \(g_1 \in g_2H\). Furthermore, the number of blocks is \(|G : H|\).

Let \(G = \Gamma_1(m)\) and \(X = \hat{\mathbb{Q}}\). In this case \(G_\infty = \langle T \rangle\) where \(T(z) = z + 1\). It is clear that \(G_\infty \subset \Gamma_0^*(n) \subset G\). Let \(\approx\) be the relation defined in Lemma 1, and assume that \(r/s, x/y \in \hat{\mathbb{Q}}\). Then according to Theorem 2.3, there exist \(T, S \in \Gamma_1(m)\) such that \(T(\infty) = r/s\), \(S(\infty) = x/y\) where
\[
T(z) = \frac{r\sqrt{q_1z} + *}{(s\sqrt{q_1})z + *}, \quad S(z) = \frac{x\sqrt{q_2z} + *}{(y\sqrt{q_2})z + *}
\]
for some divisors \(q_1\) and \(q_2\) of \(m\). Therefore, \(r/s \approx x/y\) if and only if \(T(\infty) \approx S(\infty)\) if and only if \(T^{-1}s \in \Gamma_0^*(n)\). We then see that \(T^{-1}s \in \Gamma_0^*(n)\) if and only if \(r/s \approx x/y\) if and only if \(ry - sx \equiv 0 \pmod{n}\). The number of equivalence classes under \(\approx\) is \(|\Gamma_1(m) : \Gamma_0^*(n)|\). We give the following from [11].

**Theorem 2.4.** Let \((m, n) = 1\). Then the index \(|\Gamma_1(m) : \Gamma_0^*(n)|\) of \(\Gamma_0^*(n)\) in \(\Gamma_1(m)\) is
\[
|\Gamma : \Gamma_0(n)| = n \prod_{p | n} \left( 1 + \frac{1}{p} \right).
\]

3. The suborbital graph for \(\Gamma_1(m)\) on \(\hat{\mathbb{Q}}\)

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 \(G\). The orbit containing \((\alpha, \beta)\) 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 \(\gamma\) to \(\delta\) if \((\gamma, \delta) \in O(\alpha, \beta)\).
A directed edge from $y$ to $\delta$ is denoted by $y \rightarrow \delta$ or $\delta \leftarrow y$. If $(y, \delta) \in O(\alpha, \beta)$, then we will say that there exists an edge $y \rightarrow \delta$ in $G(\alpha, \beta)$.

Clearly $O(\beta, \alpha)$ is also a suborbital, and it is either equal to or disjoint from $O(\alpha, \beta)$. In the former case, $G(\alpha, \beta) = G(\beta, \alpha)$ and the graph consists of pairs of oppositely directed edges. It is convenient to replace each such pair by a single undirected edge, so that we have an undirected graph which we call self-paired. In the latter case, $G(\beta, \alpha)$ is just $G(\alpha, \beta)$ with the arrows reversed, and we call $G(\alpha, \beta)$ and $G(\beta, \alpha)$ paired suborbital graphs.

The above ideas were first introduced by Sims [8], and are also described in a paper by Neuman [5] and in the books by Tsuzuku [9] and by Bigg and White [2], the emphasis being on applications to finite groups.

If $\alpha = \beta$, then $O(\alpha, \alpha)$ is the diagonal of $X \times X$. 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 be mainly interested in the remaining non-trivial suborbital graphs.

We now investigate the suborbital graphs for the action of $\Gamma_1(m)$ on $\hat{Q}$. Since $\Gamma_1(m)$ acts transitively on $\hat{Q}$, each non-trivial suborbital graph contains a pair $(\infty, u/n)$ for some $u/n \in \hat{Q}$. Furthermore, it can be easily shown that $O(\infty, u/n) = O(\infty, v/n)$ if and only if $u \equiv v \pmod{n}$. Therefore, we may suppose that $u \leq n$ where $(u, n) = 1$.

**Theorem 3.1.** There is an isomorphism $G(\infty, u/n) \rightarrow G(\infty, (n - u)/n)$ given by $v \rightarrow 1 - v$.

**Proof.** It is clear that $v \rightarrow 1 - v$ is one-to-one and onto. Suppose that there exists an edge $r/s \rightarrow x/y$ in $G(\infty, u/n)$. Then $(r/s, x/y) \in O(\infty, u/n)$ and therefore there exists an element $S$ in $\Gamma_1(m)$ such that $S(\infty) = r/s$ and $S(u/n) = x/y$. Let $\Psi(z) = 1 - z$. Then $\Psi S \Psi \in \Gamma_1(m)$. Moreover, we get

$$\Psi S \Psi(\infty) = \Psi S(\infty) = \Psi(r/s) = 1 - r/s$$

and

$$\Psi S \Psi((n - u)/n) = \Psi S(u/n) = \Psi(x/y) = 1 - x/y.$$  

Then $(1 - r/s, 1 - x/y) \in O(\infty, (n - u)/n)$. This shows that there exists an edge $1 - r/s \rightarrow 1 - x/y$ in $G(\infty, (n - u)/n)$. \(\square\)

**Theorem 3.2.** Suppose $(m, n) = 1$. Then there exists an edge $r/s \rightarrow x/y$ in $G(\infty, u/n)$ if and only if

$$\frac{m}{q}|s, q|y, ry - sx = \mp n,$$

and $x \equiv \mp qu\pmod{n}$, $y \equiv \mp qu\pmod{n}$

for some divisor $q$ of $m$.

**Proof.** Suppose that there exists an edge $r/s \rightarrow x/y$ in $G(\infty, u/n)$. Then $(r/s, x/y) \in O(\infty, u/n)$, and therefore, there exists $T \in \Gamma_1(m)$ such that $T(\infty) = r/s$ and $T(u/n) = x/y$. Suppose that

$$T(z) = \frac{a\sqrt{q}z + b/\sqrt{q}}{(cm/\sqrt{q})z + d/\sqrt{q}}, adq - bcm/q = 1$$

for some $q|m$. Then we have $a/(cm/q) = r/s$ and $(auq + bn)/(cmu + dqn) = x/y$. Since $(a, cm/q) = 1$, there exists $i \in \{0, 1\}$ such that $a = (-1)^i r$, $cm/q = (-1)^i s$. On the other
hand, since \((m, n) = 1\), we see that \((q, auq + bn) = 1\). Moreover, since
\[
d(auq + bn) - b(ucm/q + dn) = u,
\]
and
\[
aq(uqm/q + dn) - cm/q(auq + bn) = n,
\]
it follows that \((auq + bn, cmu + dqn) = 1\). Thus there exists \(j \in \{0, 1\}\) such that
\((-1)^j x = auq + bn, (-1)^j y = cmu + dqn\). Hence we obtain the matrix equation
\[
\begin{pmatrix}
a & b \\
(cm/q dq) & (1 uq) \\
0 & n
\end{pmatrix}
= \begin{pmatrix}
(-1)^j r & (-1)^j x \\
(-1)^j s & (-1)^j y
\end{pmatrix}.
\]
Taking determinants in (3.1) we see that \(n = (-1)^{i+j}(ry - sx)\). Furthermore, we have
\(x \equiv (-1)^{i+j} qur \mod n\) and \(y \equiv (-1)^{i+j} qus \mod n\). So, \(ry - sx = \mp n\), and \(x \equiv \mp qur \mod n\), \(y \equiv \mp qus \mod n\). In addition, since \(cm/q = (-1)^j s\) and
\((-1)^j y = q (ucm/q + dn)\), we have \(m/q\) is and \(q|y\).

Now suppose that for some divisors \(q\) of \(m\), \(q|y, \frac{m}{q}|s, \varepsilon(ry - sx) = n\), and \(x \equiv \varepsilon qur \mod n\), \(y \equiv \varepsilon qus \mod n\) where \(\varepsilon = \mp 1\). Then, we have \(\varepsilon x = qur + bn\), \(\varepsilon y = qus + kn\) for some integers \(k\) and \(b\). Since \(m|sq, sq = cm\) for some integer \(c\). On the other hand, since \(q|y\) and \((q, n) = 1\), we see that \(q|k\). This shows that \(\varepsilon y = qus + qdn\) for some integer \(d\). Thus we obtain the matrix equation
\[
\begin{pmatrix}
r & b \\
s & dq
\end{pmatrix}
\begin{pmatrix}
1 & uq \\
0 & n
\end{pmatrix}
= \begin{pmatrix}
r \varepsilon x \\
\varepsilon y
\end{pmatrix}.
\]
Taking determinants in (3.2) we get \((rdq - sb)n = \varepsilon(ry - sx) = n\). Thus \(rdq - sb = 1\). By using \(s = cm/q\), we obtain \(rdq - bcm/q = 1\). If we take
\[
T(z) = \frac{r\sqrt{d} + b}{(cm/q + dq)^r/dq},
\]
then we have \(T(\infty) = r/s\) and \(T(u/n) = (ruq + bn)/(mcu + dqn) = x/y\). So, we see that \((r/s, x/y) \in O(\infty, u/n)\). Therefore there is an edge \(r/s \to x/y\) in \(G(\infty, u/n)\). □

From now on, unless otherwise stated, we will assume that \((m, n) = 1\).

**Corollary 1.** There exists an edge \(r/s \to x/y\) in \(G(\infty, 1)\) if and only if \(ry - sx = \mp 1\), and \(q|s, \frac{m}{q}|y\) for some \(q|m\). In particular, if \(k\) is an integer, then there is an edge \(r/s \to \infty = \frac{1}{0}\) in \(G(\infty, 1)\).

Now let us represent the edges of \(G(\infty, u/n)\) as hyperbolic geodesics in the upper half-plane \(U = \{z \in \mathbb{C} : \text{Im} z > 0\}\), that is, as Euclidean semi-circles or half-lines perpendicular to the real line. Then we have

**Lemma 3.** No edges of \(G(\infty, 1)\) cross in \(U\).

**Proof.** Let \(r_1/s_1 \to x_1/y_1\) be an edge in \(G(\infty, 1)\). Then \(T(\infty) = r_1/s_1\) and \(T(1) = x_1/y_1\) for some \(T \in \Gamma_1(m)\). Let \(S(z) = z + 1\). Then \(TS(\infty) = r_1/s_1\) and \(TS(0) = x_1/y_1\). Since any element of \(\Gamma_1(m)\) preserves the geodesics, we may suppose that the edges \(0 \to \infty\) and \(r/s \to x/y\) cross in \(U\). But this is impossible, since \(ry - sx = \pm 1\). □
In Section 2, we introduced for each integer $n$, an $\Gamma_1(m)$-invariant equivalence relation $\sim$ on $\hat{\mathcal{Q}}$ with $r/s \sim x/y$ if and only if $r y - s x \equiv 0 \pmod{n}$. If there is an edge $r/s \to x/y$ in $G(\infty, u/n)$, then this implies that $r y - s x = \mp n$. So, $r/s \approx x/y$. Thus each connected component of $G(\infty, u/n)$ lies in a single block for $\sim$.

Let $F(\infty, u/n)$ denote the subgraph of $G(\infty, u/n)$ whose vertices form the block $[\infty] = \{x/y : y \equiv 0 \pmod{n}\}$.

Since $\Gamma_1(m)$ acts transitively on $\hat{\mathcal{Q}}$, it permutes the blocks transitively. It can be easily seen that the subgraphs whose vertices form the blocks are all isomorphic.

**Theorem 3.3.** There is an edge $r/s \to x/y$ in $F(\infty, u/n)$ if and only if

$$\frac{m}{q} \mid s, q \mid y, r y - s x = \mp n \text{ and } x \equiv \mp qur \pmod{n}$$

for some divisor $q$ of $m$.

**Lemma 4.** There is an isomorphism $F(\infty, u/n) \to F(\infty, (n-u)/n)$ given by $v \to 1-v$.

**Proof.** Let $\psi$ be as in Theorem 3.1. If $r/s \in [\infty]$, then $1 - r/s = (s-r)/s \in [\infty]$. The proof then follows. \(\square\)

Let us represent the edges of $F(\infty, u/n)$ as hyperbolic geodesics in the upper half-plane $\mathcal{U} = \{z \in \mathbb{C} : \Im z > 0\}$. Then we have

**Lemma 5.** No edges of $F(\infty, u/n)$ cross in $\mathcal{U}$.

**Proof.** Suppose that the edges $r/sn \to x/yn$ and $r'/s'n \to x'/y'n$ cross in $\mathcal{U}$. Then $r y - s x = \mp 1$, and $\frac{m}{q} \mid s, q \mid y$, for some $q \mid m$. Also, $r'y' - s'x' = \mp 1$, and $\frac{m}{q} \mid s', q \mid y'$. Therefore, the edges $r/s \to x/y$ and $r'/s' \to x'/y'$ in $G(\infty, 1)$ cross in $\mathcal{U}$. This is impossible by Lemma 3. \(\square\)

**Lemma 6.** There does not exist any integer between two adjacent vertices in $F(\infty, u/n)$.

**Proof.** Suppose that there exists an edge $r/sn \to x/yn$ in $F(\infty, u/n)$ and assume that $k$ lies between the vertices. Then $kn$ lies between the adjacent vertices $r/s$ and $x/y$ in $G(\infty, 1)$. There is also an edge $kn \to \infty$ in $G(\infty, 1)$. But, this is impossible by Lemma 3. \(\square\)

**Theorem 3.4.** Let $(m, n) > 1$. Then there exists an edge $r/s \to x/y$ in $G(\infty, u/n)$ if and only if

$$r y - s x = \mp \frac{n}{q_1}, \frac{q_1}{q_1} \mid y, m \mid s q_1,$$

and

$$x \equiv \mp \frac{q}{q_1} ru \left(\mod \frac{n}{q_1}\right), \quad y \equiv \mp \frac{q}{q_1} su \left(\mod \frac{n q}{q_1}\right)$$

for some divisor $q$ of $m$ with $q_1 = (q, n)$.

**Proof.** The proof is similar. \(\square\)
4. Circuits in $G(\infty, u/n)$

Let $(G, X)$ be a transitive permutation group and let $G(\alpha, \beta)$ be a suborbital graph. If $v \to w$ or $w \to v$ in $G(\alpha, \beta)$ we represent this as $v \equiv w$. By a circuit of length $n$ we will mean $n$ vertices $v_1, v_2, \ldots, v_n$ such that $v_i \neq v_j$ for $i \neq j$, and $v_1 \to v_2 \equiv \cdots \equiv v_n \equiv v_1$ where $n \geq 3$. A circuit of length 3 is called a triangle. A graph which contains no circuit is called a forest. If $G$ has an element of finite order $n$, then it is easy to construct a circuit of length $n$. Assume that $T$ is of finite order $n$ and $\alpha \in X$ for which $T(\alpha) \neq \alpha$. Then $G(\alpha, \beta)$ is a non-trivial suborbital graph where $\beta = T(\alpha)$. We can construct a circuit of length $n$ as follows. It is obvious that there exists an edge $\alpha \to \beta$ in $G(\alpha, \beta)$. On the other hand, it is easy to see that if $w \to v$ is an edge in $G(\alpha, \beta)$, then $T(w) \to T(v)$ is an edge in $G(\alpha, \beta)$. Thus we obtain the circuit $\alpha \to T(\alpha) \to T^2(\alpha) \to \cdots \to T^{n-1}(\alpha) \to \alpha$ in $G(\alpha, \beta)$.

It is easy to see that $G(\infty, 1)$ contains many circuits. For instance, if $n$ is odd, then $\infty \to 1 \to 1/2 \to 1/3 \to \cdots \to 1/(n - 1) \to 0 \to \infty$ is a circuit of length $n$ in $G(\infty, 1)$ where $G(\infty, 1)$ is the suborbital graph for the action of $I_1(2)$ on $\hat{Q}$. Moreover, $\infty \to 1 \to 2/3 \to 1/2 \to 1/3 \to 0 \to \infty$ is a circuit of length 6 in $G(\infty, 1)$ where $G(\infty, 1)$ is the suborbital graph for the action of $I_1(3)$ on $\hat{Q}$.

We describe some circuits in $G(\infty, u/n)$ when $n > 1$. We know that any element of finite order of $PSL(2, \mathbb{C})$ is an elliptic element and that any elliptic element of any discrete subgroup of $PSL(2, \mathbb{R})$ is of finite order. To construct a circuit in $G(\infty, u/n)$ for some $u/n$, we may consider elliptic elements of $I_1(m)$. Moreover, we know from [6] (see also [7]) that the orders of the elliptic elements of $I_1(m)$ may be 2, 3, 4, or 6. Let

$$T(z) = \frac{2z - 1}{3z - 1}, \quad S(z) = \frac{-3\sqrt{2}z + 5/\sqrt{2}}{-5\sqrt{2}z + 4\sqrt{2}}, \quad U(z) = \frac{-2\sqrt{3}z + 1/\sqrt{3}}{-7\sqrt{3}z + \sqrt{3}}.$$  

Then $T \in I_1(3)$, $S \in I_1(2)$, $U \in I_1(3)$, and $T^3 = S^4 = U^6 = I$. Therefore

$$\infty \to T(\infty) \to T^2(\infty) \to \infty$$

is a triangle in $G(\infty, T(\infty))$,  

$$\infty \to S(\infty) \to S^2(\infty) \to S^3(\infty) \to \infty$$

is a circuit of length 4 in $G(\infty, S(\infty))$, and

$$\infty \to U(\infty) \to U^2(\infty) \to U^3(\infty) \to U^4(\infty) \to U^5(\infty) \to \infty$$

is a circuit of length 6 in $G(\infty, U(\infty))$. That is,  

$$\infty \to 2/3 \to 1/3 \to \infty$$

is a triangle in $G(\infty, 2/3)$,  

$$\infty \to 3/5 \to 7/10 \to 4/5 \to \infty$$

is a circuit of length 4 in $G(\infty, 3/5)$, and

$$\infty \to 2/7 \to 5/21 \to 13/14 \to 4/21 \to 1/7 \to \infty$$

is a circuit of length 6 in $G(\infty, 2/7)$. In the following we prove our main theorems.
Theorem 4.1. Suppose that \((m, n) = 1 \text{ and } n > 1\). Then any circuit in \(G(\infty, u/n)\) is in the form
\[
v \to T(v) \to T^2(v) \to T^3(v) \to \cdots \to T^{k-1}(v) \to v
\]
for a unique elliptic mapping \(T\) of order \(k\) and for some \(v \in \hat{Q}\).

Proof. Assume that \(G(\infty, u/n)\) contains a circuit. Let this circuit be in the form \(v_1 \to v_2 \subseteq v_3 \subseteq \cdots \subseteq v_k \subseteq v_1\) where each \(v_j\) is different from the others. Since \((v_1, v_2) \in \hat{O}(\infty, u/n)\), there exists some \(S \in \Gamma_1(m)\) such that \(S(\infty) = v_1\), and \(S(u/n) = v_2\). By applying \(S^{-1}\) to the above circuit and taking \(w_i = S^{-1}(v_i)\), we obtain a circuit \(C\) in the form
\[
\infty \to u/n \subseteq w_3 \subseteq \cdots \subseteq w_{k-1} \subseteq w_k \subseteq \infty
\]
where \(w_1 = \infty, w_2 = u/n\). Since \(\infty \in [\infty]\), we see that the edges of the above circuit lie in \([\infty]\). Since no edges of \(F(\infty, u/n)\) cross in \(\mathcal{U}\), either \(u/n < w_3 < \cdots < w_{k-1} < w_k\) or \(u/n > w_3 > \cdots > w_{k-1} > w_k\).

Suppose that \(u/n < w_3 < \cdots < w_{k-1} < w_k\). Let \(w_k = x/yn > u/n\) and suppose that \(\infty \to x/yn\) in \(F(\infty, u/n)\). Then \(1/0 \to x/yn\), so \(yn - 0r = n\). That is, \(y = 1\). Since \(1/0 \to x/n\), we see that \((m/q)|0\) and \(q|n\) for some \(q|m\). Thus \(q = 1\) and therefore \(x = u + bn\) for some integer \(b > 0\). This shows that \(x/n = u/n + b\), which implies that there exists an integer \(a\) in the interval \((u/n, x/n)\). Therefore, \(a\) must lie between two adjacent vertices of the above circuit \(C\). But this is impossible by Lemma 6. Therefore, \(w_k \to \infty\) is impossible and thus we have \(w_k \to \infty\). Let \(r/sn \to \infty\) be an edge in \(F(\infty, u/n)\), then it is seen that \(s = 1\). Since \(r/n \to 1/0\), \((m/q)|n\) and \(q|0\) for some \(q|m\). Thus we see that \(q = m\). Therefore \(1 \equiv -rmu\,(\text{mod } n)\). Since \(w_k = x/yn \to \infty\), we have \(y = 1\) and \(1 + xmu \equiv 0\,(\text{mod } n)\). Let \(w_k = x/n = (u + k_0)/n, k_0 \geq 1\). Then, we have \(1 + mu(u + k_0) \equiv 0\,(\text{mod } n)\). Thus the mapping
\[
\varphi(z) = \frac{-u\sqrt{mz} + (mu(u + k_0) + 1)/n\sqrt{m}}{-n\sqrt{mz} + (u + k_0)\sqrt{m}}
\]
is in \(F^*_0(n)\) and \(\varphi(\infty) = u/n, \varphi((u + k_0)/n) = \varphi(w_k) = \infty\). Moreover, it can be seen that
\[
\varphi\left(\frac{u + \frac{x}{n}}{y}\right) = \frac{u + \frac{y}{m(k_0)y - x}}{n}.
\]
Since \(\varphi\) is increasing and \(u/n < \varphi(u/n)\), we see that
\[
u/n < \varphi(w_3) < \cdots < \varphi(w_{k-1}).
\]
By applying the mapping \(\varphi\) to the circuit \(C\),
\[
\infty \to u/n \subseteq w_3 \subseteq \cdots \subseteq w_{k-1} \subseteq w_k \to \infty,
\]
we obtain another circuit \(C^*\) in the form
\[
\infty \to u/n \to \varphi(u/n) \subseteq \varphi(w_3) \subseteq \cdots \subseteq \varphi(w_{k-1}) \to \infty
\]
of the same length. Let \(\varphi(w_{k-1}) = r/n\). Then since \(r/n \to \infty\), we have \(1 \equiv -rmu\,(\text{mod } n)\). Since \(1 \equiv -xmu\,(\text{mod } n)\), we get \(mxu \equiv mr\,(\text{mod } n)\). Since \((mu, n) = 1\),
we obtain \( x \equiv r \pmod{n} \). Thus \( x/n = r/n + b \) for some integer \( b \). If \( r/n \) is different from \( x/n \), then \( b \neq 0 \), so there exists an integer \( a \) between \( r/n \) and \( x/n \). Firstly, assume that \( r/n < x/n \). Then either \( r/n \) is a vertex in the circuit \( C \) or there exist two adjacent vertices \( w_j \) and \( w_{j+1} \) in \( C \) such that \( w_j < r/n < w_{j+1} \). Assume that \( w_j < r/n < w_{j+1} \). Then the edges \( r/n \rightarrow \infty \) and \( w_j \equiv w_{j+1} \) cross in \( U \), which is impossible by Lemma 5. If \( r/n \) is a vertex in the circuit \( C \), then the integer \( a \) must lie between two adjacent vertices of the circuit \( C \). But this is impossible by Lemma 6. Now assume that \( x/n < r/n \). Then either \( x/n \) is an vertex in the circuit \( C^* \), or there exist two adjacent vertices \( w_j \) and \( w_{j+1} \) in \( C \) such that \( \varphi(w_j) < x/n < \varphi(w_{j+1}) \). The same argument gives a contradiction. Therefore \( r/n = x/n \), i.e., \( \varphi(w_{k-1}) = w_k \). Now assume that \( \varphi^i(w_{k-i}) = w_k \) for \( 1 \leq i \leq s \), and then we show that \( \varphi^{s+1}(w_{k-s-1}) = w_k \). Since \( w_{k-s-1} \equiv w_{k-s} \) and \( \varphi^s(w_{k-s}) = w_k \), we have \( \varphi^{s+1}(w_{k-s}) = \varphi(w_k) = \infty \). By applying \( \varphi \) to the circuit \( C \), \( s + 1 \) times, we get the circuit

\[
\infty \rightarrow u/n \rightarrow \varphi(u/n) \rightarrow \varphi^2(u/n) \rightarrow \cdots \rightarrow \varphi^{s+1}(w_{k-s-1}) \equiv \infty.
\]

A similar argument shows that \( \varphi^{s+1}(w_{k-s-1}) \rightarrow \infty \) and \( \varphi^{s+1}(w_{k-s-1}) = w_k \). Now we show that

\[
\varphi^k(\infty) = \infty, \varphi^k(u/n) = u/n, \text{ and } \varphi^k(w_k) = w_k.
\]

Taking \( i = k - 1 \), we obtain \( w_k = \varphi^{k-1}(w_1) = \varphi^{k-1}(\infty) \). Thus \( \varphi^k(\infty) = \varphi(w_k) = \infty \). Moreover, \( \varphi^k(u/n) = \varphi^k(\varphi(\infty)) = \varphi(\varphi^k(\infty)) = \varphi(\infty) = u/n \) and \( \varphi^k(w_k) = \varphi^k(\varphi(w_k)) = \varphi^{k-1}(\infty) = \varphi^{-1}(\infty) = w_k \). Therefore \( \varphi_k \) has three different fixed points and this implies that \( \varphi_k \) is the identity mapping. So \( \varphi \) is an elliptic element of the order \( k \). Since \( \varphi \) is elliptic, \( k_0 = 1 \) and \( m \leq 3 \). On the other hand, since \( \varphi \) is injective and \( \varphi^i(w_{k-i}) = w_k = \varphi^{i+1}(w_{k-i-1}) \), we see that \( \varphi(w_{k-i-1}) = w_{k-i} \). Thus it can be seen that \( w_i = \varphi^{i-1}(\infty) \). Moreover, we see that our circuit is in the form

\[
\infty \rightarrow u/n \rightarrow w_3 \rightarrow \cdots \rightarrow w_{k-1} \rightarrow w_k \rightarrow \infty.
\]

Therefore the circuit \( C \) is of the form

\[
\infty \rightarrow \varphi(\infty) \rightarrow \varphi^2(\infty) \rightarrow \varphi^3(\infty) \rightarrow \cdots \rightarrow \varphi^{k-1}(\infty) \rightarrow \infty
\]

for the elliptic mapping \( \varphi \) of order \( k \) where

\[
\varphi(z) = \frac{-u\sqrt{mz} + (mu(u + 1) + 1)/n\sqrt{m}}{-n\sqrt{mz} + (u + 1)\sqrt{m}}.
\]

Then it follows that the first circuit

\[
v_1 \rightarrow v_2 \equiv v_3 \equiv \cdots \equiv v_k \equiv v_1
\]

is equal to the circuit

\[
v_1 \rightarrow T(v_1) \rightarrow T^2(v_1) \rightarrow \cdots \rightarrow T^{k-1}(v_1) \rightarrow v_1
\]

where \( T = S_0S^{-1} \) and \( T \) is an elliptic mapping in \( \Gamma_1(m) \) of order \( k \).

Now suppose that \( u/n > w_3 > \cdots > w_{k-1} > w_k \). Then there exists a circuit in \( F(\infty, (n - u)/n) \) in the form

\[
\infty \rightarrow (n - u)/n \equiv 1 - w_3 \equiv \cdots \equiv 1 - w_{k-1} \equiv 1 - w_k \equiv \infty.
\]
But the above circuit must be of the form
\[ \infty \rightarrow \varphi(\infty) \rightarrow \varphi^2(\infty) \rightarrow \varphi^3(\infty) \rightarrow \cdots \rightarrow \varphi^{k-1}(\infty) \rightarrow \infty \]
for some elliptic element \( \varphi \) of order \( k \) and
\[ \varphi(z) = \frac{-(n-u)\sqrt{m}z + (m(n-u)(n-u+1) + 1)/n}{-n\sqrt{m}z + (n-u+1)\sqrt{m}}. \]

Then, one can easily see that our circuit in \( F(\infty, u/n) \) must be in the form
\[ \infty \rightarrow \Psi \varphi \Psi(\infty) \rightarrow \Psi \varphi^2 \Psi(\infty) \rightarrow \Psi \varphi^3 \Psi(\infty) \rightarrow \cdots \rightarrow \Psi \varphi^{k-1} \Psi(\infty) \rightarrow \infty \]
where \( \Psi(z) = 1 - z \). Moreover, it can be seen that
\[ \Psi \varphi \Psi(z) = \frac{-u\sqrt{m}z + (mu(u-1) + 1)/n\sqrt{m}}{-n\sqrt{m}z + (u-1)\sqrt{m}} \]
and that \( \Psi \varphi \Psi \) is an elliptic element of order \( k \). Thus it follows that the first circuit
\[ v_1 \rightarrow v_2 \equiv v_3 \equiv \cdots \equiv v_k \equiv v_1 \]
is equal to the circuit
\[ v_1 \rightarrow T(v_1) \rightarrow T^2(v_1) \rightarrow \cdots \rightarrow T^{k-1}(v_1) \rightarrow v_1 \]
where \( T = S \Psi \varphi \Psi S^{-1} \) and \( T \) is an elliptic mapping of order \( k \).

**Corollary 2.** \( G(\infty, u/n) \) contains a circuit if and only if \( mu^2 \equiv mu + 1 \equiv 0(\text{mod } n) \) and \( m \leq 3 \).

**Proof.** The first part of the theorem is obvious. Let \( mu^2 \equiv mu + 1 \equiv 0(\text{mod } n) \) and \( m \leq 3 \). Then the mapping
\[ \varphi(z) = \frac{-u\sqrt{m}z + (mu(u \equiv 1) + 1)/n\sqrt{m}}{-n\sqrt{m}z + (u \equiv 1)\sqrt{m}} \]
is in \( \Gamma_0^*(n) \) and \( \varphi(\infty) = u/n \). Moreover, \( \varphi \) is of finite order and the order of \( \varphi \) is equal to 4 if \( m \) is 2 and 6 if \( m = 3 \). The proof then follows.

**Corollary 3.** Let \( m \leq 3 \). If \( G(\infty, u/n) \) contains a circuit of length \( k \), then \( \Gamma_0^*(n) \) contains an elliptic element of order \( k \) where \( k \geq 3 \).

We give some lemmas which will be useful in the proof of the next theorem. In what follows, we will assume that \( (m, n) > 1 \).

**Lemma 7.** Let \( r/s \) and \( x/y \) be rational numbers such that \( ry - sx = -1 \), 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.

**Lemma 8.** Suppose that there is an edge \( r/sn \equiv x/y \) in \( G(\infty, u/n) \). Then we have \( n\mid y \) and \( ry - snx = \mp n \). In particular, if \( \infty \equiv x/y \), then \( y = n \).
**Proof.** Let \( r/sn \to x/y \) be an edge in \( G(\infty, u/n) \). Then by Theorem 3.4, there exists some divisor \( q \) of \( m \) such that \( y \equiv \mp \frac{a}{q_1} \text{sn}u \pmod{n/q_1} \) and \( ry - sn = \mp \frac{n}{q_1} \) where \( q_1 = (q, n) \). Then it follows that \( n|y \) and therefore \( q_1 = 1 \). This shows that \( ry - sn = \mp n \).

Now suppose that \( x/y \to r/sn \) is an edge in \( G(\infty, u/n) \). Then by Theorem 3.4, there exists some divisor \( q \) of \( m \) such that \( snx - ry = \mp \frac{n}{q_1} \) and \( sn \equiv \mp yu \frac{a}{q_1} \pmod{n/q_1} \) where \( q_1 = (q, n) \). Thus we see that \( n|\frac{a}{q_1}yu \) and therefore \( n|\frac{a}{q_1}y \), since \( (u, n) = 1 \). Then

\[
\frac{q}{q_1}snx - ry \frac{q}{q_1} = \mp \frac{n}{q_1}.
\]

Thus it follows that \( n|(nq/q_1^2) \), which implies that \( q_1^2|q \). Since \( m \) is a square-free integer and \( q|m \), we see that \( q_1 = 1 \). Therefore, \( snx - ry = \mp n \), which implies that \( n|ry \). Thus, \( n|y \), since \((n, r) = 1 \). If \( \infty \subseteq x/y \), then the proof is similar. \( \square \)

**Corollary 4.** Let \( C \) be a circuit in \( G(\infty, u/n) \) in the form

\[
\infty \to u/n \subseteq w_3 \subseteq \cdots \subseteq w_{k-1} \subseteq w_k \subseteq \infty.
\]

Then there exist no integers between adjacent vertices of \( C \) in \( \mathbb{Q} \) and any rational number of the form \( a/n \) does not lie between adjacent vertices of \( C \) in \( \mathbb{Q} \).

**Proof.** By Lemma 8, any edge of \( C \) whose vertices in \( \mathbb{Q} \) is of the form \( x/yn \equal{} r/sn \) with \( snx - ryn = \mp n \). Suppose that the integer \( k \) lies between \( x/yn \) and \( r/sn \). Then \( kn \) must lie between \( x/y \) and \( r/s \), which is impossible by Lemma 7. Now suppose that \( x/yn \) and \( r/sn \) are adjacent vertices of \( C \) with \( x/yn < a/n < r/sn \). Then \( x/yn < a < r/s \) and \( sx - ry = -1 \), which contradicts Lemma 7. \( \square \)

Now let us represent the edges of \( G(\infty, u/n) \) as hyperbolic geodesics in the upper half-plane \( \mathcal{U} = \{ z \in \mathbb{C} : \text{Im} z > 0 \} \). Then we have

**Corollary 5.** Let \( C \) be any circuit in \( G(\infty, u/n) \) in the form

\[
\infty \to u/n \subseteq w_3 \subseteq \cdots \subseteq w_{k-1} \subseteq w_k \subseteq \infty.
\]

Then no edges of \( C \) cross in \( \mathcal{U} \).

**Proof.** First of all, we note that the edge \( \infty \equiv x/n \) and any other different edge in the form \( x/yn \equiv r/sn \) with \( snx - ryn = \mp n \) do not cross in \( \mathcal{U} \) by Corollary 4. Now suppose that the edges \( w_i \to w_{i+1} \) and \( w_j \to w_{j+1} \) cross in \( \mathcal{U} \). Since \( w_i \to w_{i+1} \), there exists \( T \in \Gamma_1(m) \) such that \( T(\infty) = w_i \) and \( T(u/n) = w_{i+1} \). Applying the mapping \( T \) to the vertices of the above edges, we see that the edges \( \infty \to u/n \) and \( T^{-1}(w_j) \to T^{-1}(w_{j+1}) \) cross in \( \mathcal{U} \). Since the edges \( \infty \to u/n \) and \( T^{-1}(w_j) \to T^{-1}(w_{j+1}) \) are in the circuit

\[
T^{-1}(\infty) \to T^{-1}(u/n) \subseteq \cdots \to u/n \subseteq \cdots \subseteq T^{-1}(w_j),
\]

we have \( x/yn = T^{-1}(w_j) \) and \( r/sn = T^{-1}(w_{j+1}) \) with \( ryn - snx = \mp n \). Then the edges \( \infty \to u/n \) and \( x/yn \equiv r/sn \) cross in \( \mathcal{U} \), which is impossible. \( \square \)

**Theorem 4.2.** Let \((m, n) > 1\). Then any circuit in \( G(\infty, u/n) \) is in the form

\[
v \to T(v) \to T^2(v) \to T^3(v) \to \cdots \to T^{k-1}(v) \to v
\]
for a unique elliptic mapping $T$ of order $k$ and for some $v \in \hat{Q}$.

**Proof.** Let $G(\infty, u/n)$ contain a circuit in the form

$$v_1 \rightarrow v_2 \Leftarrow v_3 \Rightarrow \cdots \Rightarrow v_k \Leftarrow v_1$$

where each $v_j$ is different from the others. Then since $(v_1, v_2) \in O(\infty, u/n)$, there exists some $S \in \Gamma_1(m)$ such that $S(\infty) = v_1, S(u/n) = v_2$. Then $S^{-1}(v_1) = \infty, S^{-1}(v_2) = u/n$. By applying $S^{-1}$ to the circuit and taking $w_i = S^{-1}(v_i)$, we obtain the circuit $C$

$$\infty \rightarrow u/n \Leftarrow w_3 \Rightarrow \cdots \Rightarrow w_{k-1} \Leftarrow w_k \Leftarrow \infty$$

where $w_1 = \infty, w_2 = u/n$. Since no edges of $C$ cross in $U$, either $u/n < w_3 < \cdots < w_{k-1} < w_k$ or $u/n > w_3 > \cdots > w_{k-1} > w_k$. Suppose that $u/n < w_3 < \cdots < w_{k-1} < w_k$. Let $w_k = x/n$ and suppose that $w_k = x/n \leftarrow \infty$. Then $(\infty, w_k) \in O(\infty, u/n)$. Thus there exists $T_1 \in \Gamma_1(m)$ such that $T_1(\infty) = \infty$ and $T_1(u/n) = w_k = x/n$. Then it is seen that $T_1(z) = z + b$ for some integer $b$ and so $x/n = (u/n) + b$. Therefore, there exists an integer $a$ between $u/n$ and $x/n$. Since $a$ is not any vertex of the above circuit $C$, there exist two vertices $w_j$ and $w_{j+1}$ such that $w_j < a < w_{j+1}$. But this is impossible by Corollary 4. Therefore $w_k \rightarrow \infty$. Thus a simple calculation shows that there exists a divisor $q$ of $m$ such that $m|qn$ and $1 + xuq \equiv 0(\mod n)$. Let $w_k = (u + k_0)/n$. Then since $m|qn$ and $qu(u + k_0) + 1 \equiv 0(\mod n)$, the mapping

$$\varphi(z) = \frac{-u\sqrt{q}z + (qu(u + k_0) + 1)/n\sqrt{q}}{(-nq/\sqrt{q})z + (u + k_0)\sqrt{q}}$$

is in $\Gamma_1(m)$ and $\varphi(\infty) = u/n, \varphi(w_k) = \varphi((u + k_0)/n) = \infty$. Moreover, it is easy to see that

$$\varphi\left(\frac{u + x}{n}\right) = \frac{u + y}{q(k_0) - y}$$

for $0 \leq x/y \neq k_0$.

By applying $\varphi$ to the above circuit $C$, we obtain another circuit $C^*$

$$\infty \rightarrow u/n \rightarrow \varphi(u/n) \Leftarrow \varphi(w_3) \Rightarrow \cdots \Rightarrow \varphi(w_{k-1}) \rightarrow \infty,$$

which is of the same length. Since $\varphi$ is increasing and $u/n < \varphi(u/n)$, we see that $u/n < \varphi(w_3) < \cdots < \varphi(w_{k-1})$. Let $\varphi(w_{k-1}) = r/n$. Since $r/n \rightarrow \infty$ and $w_k = x/n \rightarrow \infty$, there exist two mappings $T_1$ and $T_2$ such that $T_1(\infty) = x/n, T_1(u/n) = \infty, T_2(\infty) = r/n, and T_2(u/n) = \infty$. Thus we get $T_2T_1^{-1}(\infty) = T_2(u/n) = \infty$ and $T_2T_1^{-1}(x/n) = T_2(\infty) = r/n$. Thus we see that $T_2T_1^{-1}(z) = z + b$ for some integer $b$. This implies that $b + x/n = r/n$. Assume that $x/n \neq r/n$. Then there exists an integer $a$ between $x/n$ and $r/n$. Firstly, assume that $r/n < x/n$. Then either $r/n$ is a vertex in the circuit $C$ or there exist two adjacent vertices $w_j$ and $w_{j+1}$ in $C$ such that $w_j < r/n < w_{j+1}$. The case $w_j < r/n < w_{j+1}$ is impossible by Corollary 4. If $r/n$ is a vertex in the circuit $C$, then the integer $a$ must lie between two adjacent vertices of $C$, which is impossible by Corollary 4. Now assume that $x/n < r/n$. Then either $x/n$ is a vertex in the circuit $C^*$ or there exist two adjacent vertices $w_j$ and $w_{j+1}$ in $C$ such that $\varphi(w_j) < x/n < \varphi(w_{j+1})$. By Corollary 4, we get another contradiction.
\( r/n = x/n, \) i.e., \( \varphi(w_{k-1}) = w_k \). Now assume that \( \varphi^i(w_{k-i}) = w_k \) for \( 1 \leq i \leq s \), and then we show that \( \varphi^{s+1}(w_{k-s-1}) = w_k \). Since \( w_{k-s-1} \subseteq w_{k-s} \) and \( \varphi^s(w_{k-s}) = w_k \), we have \( \varphi^{s+1}(w_{k-s}) = \varphi(w_k) = \infty \). By applying \( \varphi \) to the circuit \( C, s + 1 \) times, we get the circuit

\[
\infty \rightarrow u/n \rightarrow \varphi(u/n) \rightarrow \varphi^2(u/n) \equiv \cdots \equiv \varphi^{s+1}(w_{k-s-1}) \equiv \infty.
\]

A similar argument shows that \( \varphi^{s+1}(w_{k-s-1}) = w_k \). Thus we get \( \varphi^k(\infty) = \infty, \varphi^k(u/n) = u/n, \) and \( \varphi^k(w_k) = w_k \). Therefore, \( \varphi^k \) is the identity mapping and thus \( \varphi \) is an elliptic mapping of order \( k \). Since \( \varphi \) is an elliptic mapping, \( k_0 = 1 \) and \( q \leq 3 \). Moreover, it can be seen that \( \varphi(w_{k-i-1}) = w_{k-i} \) and \( w_i = \varphi^{i-1}(\infty) \). Therefore, we see that our circuit \( C \) is in the form

\[
\infty \rightarrow u/n \rightarrow w_3 \rightarrow \cdots \rightarrow w_{k-1} \rightarrow w_k \rightarrow \infty.
\]

Thus the circuit \( C \) is of the form

\[
\infty \rightarrow \varphi(\infty) \rightarrow \varphi^2(\infty) \rightarrow \varphi^3(\infty) \rightarrow \cdots \rightarrow \varphi^{k-1}(\infty) \rightarrow \infty
\]

for the elliptic mapping \( \varphi \) of order \( k \) where

\[
\varphi(z) = \frac{-u\sqrt{q}z + (qu(u + 1) + 1)/n\sqrt{q}}{(-nq/\sqrt{q})z + (u + 1)\sqrt{q}}.
\]

\( q|m, q \leq 3, \) and \( m|qn \). Then it follows that the first circuit

\[
v_1 \rightarrow v_2 \equiv v_3 \equiv \cdots \equiv v_k \equiv v_1
\]

is equal to the circuit

\[
v_1 \rightarrow T(v_1) \rightarrow T^2(v_1) \rightarrow \cdots \rightarrow T^{k-1}(v_1) \rightarrow v_1
\]

where \( T = S\varphi S^{-1} \) and \( T \) is an elliptic mapping in \( G_1(m) \) of order \( k \).

Now assume that \( u/n > w_3 > \cdots > w_{k-1} > w_k \). Then there exists a circuit

\[
\infty \rightarrow (n-u)/n \equiv 1 - w_3 \equiv \cdots \equiv 1 - w_{k-1} \equiv 1 - w_k \equiv \infty
\]

in \( G(\infty, (n-u)/n) \) with \( (n-u)/n < 1 - w_3 < \cdots < 1 - w_{k-1} < 1 - w_k \). But this circuit must be of the form

\[
\infty \rightarrow \varphi(\infty) \rightarrow \varphi^2(\infty) \rightarrow \varphi^3(\infty) \rightarrow \cdots \rightarrow \varphi^{k-1}(\infty) \rightarrow \infty
\]

for the elliptic mapping \( \varphi \) of order \( k \) where

\[
\varphi(z) = \frac{(n-u)\sqrt{q}z + (q(n-u)(n-u + 1) + 1)/n\sqrt{q}}{(-(n-u)q/\sqrt{q})z + (n-u + 1)\sqrt{q}}.
\]

\( q|m, q \leq 3, \) and \( m|qn \). Then our circuit must be in the form

\[
\infty \rightarrow \Psi \varphi (\infty) \rightarrow \Psi \varphi^2 (\infty) \rightarrow \Psi \varphi^3 (\infty) \rightarrow \cdots \rightarrow \Psi \varphi^{k-1} (\infty) \rightarrow \infty
\]

where \( \Psi (z) = 1 - z \). Moreover, it can be seen that

\[
\Psi \varphi (z) = \frac{-u\sqrt{q}z + (qu(u - 1) + 1)/n\sqrt{q}}{(-nq/\sqrt{q})z + (u - 1)\sqrt{q}}
\]

and that \( \Psi \varphi \) is an elliptic element of order \( k \). Then it follows that our first circuit

\[
v_1 \rightarrow v_2 \equiv v_3 \equiv \cdots \equiv v_k \equiv v_1
\]
is equal to the circuit
\[ v_1 \rightarrow T(v_1) \rightarrow T^2(v_1) \rightarrow \cdots \rightarrow T^{k-1}(v_1) \rightarrow v_1 \]
where \( T = S\Psi\varphi\Psi S^{-1} \) and \( T \) is an elliptic mapping in \( \Gamma_1(m) \) of order \( k \). □

**Corollary 6.** Let \((m, n) > 1\). Then \( G(\infty, u/n) \) contains a circuit if and only if \( qu^2 \equiv qu + 1 \equiv 0\,(\text{mod} \, n) \) for some divisor \( q \) of \( m \) with \( m|qn, q \leq 3 \).

**Proof.** The first part of the theorem is obvious. Let \( qu^2 \equiv qu + 1 \equiv 0\,(\text{mod} \, n) \) for some divisor \( q \) of \( m \) with \( m|qn, q \leq 3 \). Then the mapping
\[
\varphi(z) = \frac{-u\sqrt{q}z + (qu \mp 1) + 1/n\sqrt{q}}{(-nq/\sqrt{q})z + (u \mp 1)\sqrt{q}}
\]
is in \( \Gamma_1(m) \) and \( \varphi(\infty) = u/n \). Moreover, it can be seen easily that \( \varphi \) is of finite order and that the order of \( \varphi \) is equal to 3, 4, and 6 when \( q \) is 1, 2, and 3 respectively. The proof then follows. □

**Corollary 7.** Let \((m, n) > 1\). If \( G(\infty, u/n) \) contains a circuit of the length \( k \), then \( \Gamma_1(m) \) contains an elliptic element of order \( k \).

At this point, it is reasonable to conjecture that

**Conjecture 1.** Let \( n > 1 \) and let \( \Gamma_1(m) \) act transitively on \( \mathbb{Q} \cup \{\infty\} \). Then any circuit of the length \( k \) in the suborbital graph \( G(\infty, u/n) \) is of the form
\[ v \rightarrow T(v) \rightarrow T^2(v) \rightarrow T^3(v) \rightarrow \cdots \rightarrow T^{k-1}(v) \rightarrow v \]
for a unique elliptic element \( T \) in \( \Gamma_1(m) \) of order \( k \) and for some \( v \in \mathbb{Q} \cup \{\infty\} \).

**References**


[11] R. Keskin, Some subgroups of the normalizer of \( \Gamma_0(m) \) (submitted for publication).