

## CHAPTER 3

### Main Results

In this chapter, we present the characterizations of left regular elements, right regular elements, intra-regular elements, completely regular elements and unit regular elements on  $Fix(X, Y)$ . Moreover, we count the numbers of left regular, right regular and intra-regular elements and determine the maximal congruence on  $Fix(X, Y)$  when  $X$  is a finite set.

#### 3.1 The action of $\mathcal{H}(\sqrt{m})$ on $\sqrt{m}\widehat{\mathbb{Q}}$

$\mathcal{H}(\sqrt{m})$  acts on  $\sqrt{m}\widehat{\mathbb{Q}}$  naturally by  $T.x = T(x) \forall T \in \mathcal{H}(\sqrt{m}) \forall x \in \sqrt{m}\widehat{\mathbb{Q}}$ . Then we have the following lemma:

**Lemma 3.1.1.**  $\mathcal{H}(\sqrt{m})$  acts on  $\sqrt{m}\widehat{\mathbb{Q}}$  transitively if and only if  $m$  is prime or  $m = 1$ .

*Proof.* Let  $m$  be prime or  $m = 1$  and  $(x/y)\sqrt{m} \in \sqrt{m}\widehat{\mathbb{Q}} \setminus \{\infty\}$  with  $(x, y) = 1$ . We will show that we can find  $T \in \mathcal{H}(\sqrt{m})$  such that  $T(\infty) = (x/y)\sqrt{m}$ . Since  $(x, y) = 1$ , there are  $a, b \in \mathbb{Z}$  such that  $ax - by = 1$ . If  $m \mid y$ , we may take

$$T(z) = \frac{xz + b\sqrt{m}}{(y/m)\sqrt{m}z + a}$$

as the element desired.

If  $m \nmid y$ , since  $m$  is prime or 1, we have  $(mx, y) = 1$ . Thus, there exist  $a, b \in \mathbb{Z}$  such that  $mxa - yb = 1$ . Now we take

$$T(z) = \frac{x\sqrt{m}z + b}{yz + \sqrt{m}a},$$

and we have  $T(\infty) = (x/y)\sqrt{m}$ . Since the orbit of  $\infty$  on  $\mathcal{H}(\sqrt{m})$  is  $\sqrt{m}\widehat{\mathbb{Q}}$ , the action is transitive.

Conversely, let  $m$  be a composite number. Then there are different primes  $p, q$  such that  $p \mid m$  and  $q \mid m$ . We will show that there is no such  $T \in \mathcal{H}(\sqrt{m})$  that  $T(\infty) = (p/q)\sqrt{m}$ , and so the action is not transitive. Suppose that such  $T \in \mathcal{H}(\sqrt{m})$  exists. Then either

$$T(z) = \frac{az + b\sqrt{m}}{c\sqrt{m}z + d}, a, b, c, d \in \mathbb{Z}, ad - bcm = 1$$

or

$$T(z) = \frac{a\sqrt{m}z + b}{cz + d\sqrt{m}}, a, b, c, d \in \mathbb{Z}, adm - bc = 1.$$

In the former case,  $a = (cpm)/q$ . Since  $q \mid m$ , we have  $p \mid a$  and so  $p \mid (ad - bcm) = 1$  which is impossible. As for the latter case,  $c = (aq)/p$ . Since  $(p, q) = 1$ ,  $p \mid a$  and  $q \mid c$ . Thus,  $q \mid (adm - bc) = 1$  which is also impossible. Hence, such  $T$  doesn't exist. The action is not transitive.  $\square$

From here on we only consider the case where  $m$  is a prime.

**Definition 3.1.1.** Let  $(G, X)$  be a transitive permutation group and  $R$  an equivalence relation on  $X$ . If, for each  $(x, y) \in R$ , we have  $(g(x), g(y)) \in R \forall g \in G$ , then  $R$  is  $G$ -invariant. Equivalence classes of a  $G$ -invariant relation are called blocks.

In [2], a  $G$ -invariant relation  $R$  was defined on  $X$ . Let  $H$  be a subgroup of  $G$  containing  $G_x$ , the stabilizer of  $x$  in  $G$ , for some  $x \in X$ . Then

$$R = \{(g(x), gh(x)) : g \in G, h \in H\}$$

is a  $G$ -invariant relation. In our case when  $G = \mathcal{H}(\sqrt{m})$  and  $X = \sqrt{m}\hat{\mathbb{Q}}$ , we have that  $((r/s)\sqrt{m}, (x/y)\sqrt{m}) \in R$  if and only if  $n \mid (ry - sx)/m$ .

**Lemma 3.1.2.** In  $(\mathcal{H}(\sqrt{m}), \sqrt{m}\hat{\mathbb{Q}})$ , if  $(m, n) = 1$ , then  $((r/s)\sqrt{m}, (x/y)\sqrt{m}) \in R$  if and only if  $n \mid (ry - sx)$ . There are a total of  $|\mathcal{H}(\sqrt{m}) : \mathcal{H}_0^m(n)|$  blocks induced by  $R$  where  $\mathcal{H}_0^m(n) = \{T \in \mathcal{H}(\sqrt{m}) : c \equiv 0 \pmod{n}\}$ .

### 3.2 Suborbital graph for $\mathcal{H}(\sqrt{m})$ on $\sqrt{m}\hat{\mathbb{Q}}$

$\mathcal{H}(\sqrt{m})$  acts on  $\sqrt{m}\hat{\mathbb{Q}} \times \sqrt{m}\hat{\mathbb{Q}}$  by

$$T(\alpha, \beta) = (T(\alpha), T(\beta)), T \in \mathcal{H}(\sqrt{m}), \alpha, \beta \in \sqrt{m}\hat{\mathbb{Q}}$$

Recall that the orbits of this action are called suborbitals of  $\mathcal{H}(\sqrt{m})$ . We denote the orbit containing  $(\alpha, \beta)$  by  $O(\alpha, \beta)$ . A suborbital graph  $\mathcal{G}(\alpha, \beta)$  is a graph with the elements of  $\sqrt{m}\hat{\mathbb{Q}}$  as its vertices and there is a directed edge from  $\gamma$  to  $\delta$  if  $(\gamma, \delta) \in O(\alpha, \beta)$ . We denote the directed edge from  $\gamma$  to  $\delta$  by  $\gamma \rightarrow \delta$  or  $\delta \leftarrow \gamma$ . That is, the vertices are the points on  $\partial\mathbb{H}^2$  and we represent the edges as hyperbolic geodesics in  $\mathbb{H}^2$ .

From now on, we will work on the non-trivial suborbital graphs  $\mathcal{G}(\alpha, \beta)$  with  $\alpha \neq \beta$ .

Since  $\mathcal{H}(\sqrt{m})$  acts on  $\sqrt{m}\widehat{\mathbb{Q}}$  transitively, each suborbital graph contains a pair  $(\infty, (u/n)\sqrt{m})$  for some  $(u/n)\sqrt{m} \in \sqrt{m}\widehat{\mathbb{Q}} \setminus \{\infty\}$ . We can see that

$$O(\infty, (u/n)\sqrt{m}) = O(\infty, (v/n)\sqrt{m}) \text{ if and only if } n \mid (u - v).$$

Therefore, we may assume that each suborbital graph is in the form  $O(\infty, (u/n)\sqrt{m})$  with  $u \leq n$  where  $(u, n) = 1$ .

Now we give a necessary and sufficient condition for the connection of two vertices in  $\mathcal{G}(\infty, (u/n)\sqrt{m})$ .

**Theorem 3.2.1.** *If  $(m, n) = 1$ , then there exists an edge  $(r/s)\sqrt{m} \rightarrow (x/y)\sqrt{m}$  in  $\mathcal{G}(\infty, (u/n)\sqrt{m})$  if and only if  $ry - sx = \pm n$  and either*

- (i)  $m \mid s$  and  $x \equiv \pm ur \pmod{n}$ ,  $y \equiv \pm us \pmod{n}$  or
- (ii)  $m \mid y$  and  $x \equiv \pm mur \pmod{n}$ ,  $y \equiv \pm mus \pmod{n}$ .

*Proof.* Suppose that there exists an edge  $(r/s)\sqrt{m} \rightarrow (x/y)\sqrt{m}$  in  $\mathcal{G}(\infty, (u/n)\sqrt{m})$ . Then there exists  $T \in \mathcal{H}(\sqrt{m})$  such that  $T(\infty) = (r/s)\sqrt{m}$  and  $T((u/n)\sqrt{m}) = (x/y)\sqrt{m}$ . If

$$T(z) = \frac{az + b\sqrt{m}}{c\sqrt{m} + d}, a, b, c, d \in \mathbb{Z}, ad - bcm = 1.$$

Then we have  $a/mc = r/s$  and  $(au + bn)/(mcu + dn) = x/y$ . Since  $ad - bcm = 1$ ,  $(a, mc) = 1$ . Thus,  $a = ir, mc = is$  where  $i = \pm 1$ . So we have  $m \mid s$ . On the other hand, since

$$a(muc + dn) - mc(au + bn) = n$$

and

$$d(au + bn) - b(muc + dn) = u,$$

we have  $(au + bn, muc + dn) = (n, u) = 1$ . Thus,  $jx = au + bn$  and  $jy = muc + dn$  where  $j = \pm 1$ . Hence,

$$\begin{aligned} x &\equiv j(au + bn) \pmod{n} \\ &\equiv ja u \pmod{n} \\ &\equiv i j u r \pmod{n} \end{aligned}$$

So  $x \equiv \pm ur \pmod{n}$ . Similarly,

$$\begin{aligned} y &\equiv j(muc + dn) \pmod{n} \\ &\equiv jmuc \pmod{n} \\ &\equiv i j u s \pmod{n} \end{aligned}$$

That is  $y \equiv \pm us \pmod{n}$ . Also,  $ry - sx = (ij)[a(muc + dn) - mc(au + bn)] = (ij)(ad - bcm)n = \pm n$ .

In the case that

$$T(z) = \frac{a\sqrt{m}z + b}{c + d\sqrt{m}}, a, b, c, d \in \mathbb{Z}, mad - bc = 1.$$

Then we have  $a/c = r/s$  and  $(mau + bn)/m(cu + dn) = x/y$ . Since  $(a, c) = (r, s) = 1$ ,  $a = ir, c = is$  where  $i = \pm 1$ . On the other hand, since  $(m, n) = 1$  and  $mad - bc = 1$ , we have  $(m, mau + bn) = 1$ . We also have

$$ma(cu + dn) - c(mau + bn) = n$$

and

$$d(mau + bn) - b(cu + dn) = u,$$

we have  $(mau + bn, cu + dn) = (n, u) = 1$ . Thus,  $(m(cu + dn), mau + bn) = 1$ . Then,  $jx = mau + bn$  and  $jy = m(cu + dn)$  where  $j = \pm 1$ . Hence,

$$\begin{aligned} x &\equiv j(mau + bn) \pmod{n} \\ &\equiv jmau \pmod{n} \\ &\equiv ijmur \pmod{n}. \end{aligned}$$

So  $x \equiv \pm mur \pmod{n}$ . Similarly,

$$\begin{aligned} y &\equiv jm(cu + dn) \pmod{n} \\ &\equiv jmcu \pmod{n} \\ &\equiv ijmus \pmod{n}. \end{aligned}$$

That is  $y \equiv \pm mus \pmod{n}$ . Also,  $ry - sx = (ij)[am(cu + dn) - c(mau + bn)] = (ij)(mad - bc)n = \pm n$ .

Now, suppose that  $m \mid y, ry - sx = kn$  and  $x \equiv kmur \pmod{n}, y \equiv kmus \pmod{n}$  where  $k = \pm 1$ . Since  $m \mid y$  and  $(m, n) = 1$ , there are integers  $b, d$  such that  $kx = mur + bn, ky = mus + mdn$ . Taking  $a = r, c = s$  we have that  $mad - bc = (kry - mrus)/n - s(kx - mur)/n = k(ry - sx)/n = k^2 = 1$ . We may take

$$T(z) = \frac{a\sqrt{m}z + b}{cz + d\sqrt{m}}$$

so that  $T(\infty) = (r/s)\sqrt{m}$  and  $T((u/n)\sqrt{m}) = (mau + bn)/(cu + dn)\sqrt{m} = (x/y)\sqrt{m}$ . So,  $((r/s)\sqrt{m}, (x/y)\sqrt{m}) \in O(\infty, (u/n)\sqrt{m})$ . That is, there exists an edge  $(r/s)\sqrt{m} \rightarrow (x/y)\sqrt{m}$  in  $\mathcal{G}(\infty, (u/n)\sqrt{m})$ .

If  $m \mid s, ry - sx = kn$  and  $x \equiv kur(\text{mod } n), y \equiv kus(\text{mod } n)$  where  $k = \pm 1$ . Then there are integers  $b, d$  such that  $kx = ur + bn, ky = us + dn$ . Taking  $a = r$  and  $c = s/m$ , we have  $ad - bcm = 1$ . So, with

$$T(z) = \frac{az + b\sqrt{m}}{c\sqrt{m}z + d}$$

we can reach the same conclusion as the earlier case.  $\square$

We can also prove the following theorem in the same way.

**Theorem 3.2.2.** *Suppose  $(m, n) = m$ , then there exists an edge  $(r/s)\sqrt{m} \rightarrow (x/y)\sqrt{m}$  in  $\mathcal{G}(\infty, (u/n)\sqrt{m})$  if and only if either*

- (i)  $m \mid s, ry - sx = \pm n$  and  $x \equiv \pm ur(\text{mod } n), y \equiv \pm us(\text{mod } n)$  or
- (ii)  $ry - sx = \pm n/m$  and  $x \equiv \pm ur(\text{mod } n), y \equiv \pm us(\text{mod } n)$ .

From now on we only consider the case where  $(m, n) = 1$ .

Consider the suborbital graph  $\mathcal{G}(\infty, \sqrt{m})$ . With hyperbolic geodesics as its edges, we have

**Lemma 3.2.3.** *No edges of  $\mathcal{G}(\infty, \sqrt{m})$  cross in  $\mathbb{H}^2$ .*

*Proof.* Let  $(r_1/s_1)\sqrt{m} \rightarrow (r_2/s_2)\sqrt{m}$  be an edge in  $\mathcal{G}(\infty, \sqrt{m})$ . Let  $T(z) = z + \sqrt{m}$ , then  $T \in \mathcal{H}(\sqrt{m})$  and  $T(\infty) = \infty, T(0) = \sqrt{m}$ . So  $O(\infty, 0) = O(\infty, \sqrt{m}) = O((r_1/s_1)\sqrt{m}, (r_2/s_2)\sqrt{m})$ . Therefore, there is an element of  $\mathcal{H}(\sqrt{m})$  sending the edge  $(r_1/s_1)\sqrt{m} \rightarrow (r_2/s_2)\sqrt{m}$  to  $0 \rightarrow \infty$ . Since the element preserves the geodesics, we may assume that an edge  $(r/s)\sqrt{m} \rightarrow (x/y)\sqrt{m}$  cross with  $0 \rightarrow \infty$  instead of assuming that two random edges cross in  $\mathbb{H}^2$ . But it is impossible since  $ry - sx = \pm 1$  which contradicts to the fact that either  $r/s < 0$  or  $x/y < 0$ .  $\square$

For each integer  $n$  we have an  $\mathcal{H}(\sqrt{m})$ -invariant relation  $R$  defined earlier. Recall that  $((r/s)\sqrt{m}, (x/y)\sqrt{m}) \in R$  if and only if  $ry - sx \equiv 0(\text{mod } n)$ . If there is an edge  $(r/s)\sqrt{m} \rightarrow (x/y)\sqrt{m}$  in  $\mathcal{G}(\infty, (u/n)\sqrt{m})$ , then  $ry - sx = \pm n$ . That is  $((r/s)\sqrt{m}, (x/y)\sqrt{m}) \in R$ . Thus, each connected component of  $\mathcal{G}(\infty, (u/n)\sqrt{m})$  is in the same block for  $R$ .

Let  $\mathcal{F}(\infty, (u/n)\sqrt{m})$  be a subgraph of  $\mathcal{G}(\infty, (u/n)\sqrt{m})$  with the set of vertices  $[\infty] = \{(x/y)\sqrt{m} : y \equiv 0(\text{mod } n)\}$ . Each block is permuted transitively by  $\mathcal{H}(\sqrt{m})$  on  $\sqrt{m}\widehat{\mathbb{Q}}$  and the subgraph corresponding to each block is all isomorphic. We can apply the same techniques used on  $\mathcal{G}(\infty, (u/n)\sqrt{m})$  to  $\mathcal{F}(\infty, (u/n)\sqrt{m})$  and give this theorem:

**Theorem 3.2.4.** *There is an edge  $(r/s)\sqrt{m} \rightarrow (x/y)\sqrt{m}$  in  $\mathcal{F}(\infty, (u/n)\sqrt{m})$  if and only if  $ry - sx = \pm n$  and either*

- (i)  $m \mid s$  and  $x \equiv \pm ur \pmod{n}$  or
- (ii)  $m \mid y$  and  $x \equiv \pm mur \pmod{n}$ .

**Lemma 3.2.5.**  *$T : \mathcal{F}(\infty, (u/n)\sqrt{m}) \rightarrow \mathcal{F}(\infty, ((n-u)/n)\sqrt{m})$  given by  $T(v) = \sqrt{m} - v$  is an isomorphism.*

*Proof.* We see that  $T$  is bijective. Suppose that there is an edge  $(r/s)\sqrt{m} \rightarrow (x/y)\sqrt{m}$  in  $\mathcal{F}(\infty, (u/n)\sqrt{m})$ . We will show that the edge  $T((r/s)\sqrt{m}) \rightarrow T((x/y)\sqrt{m}) = ((s-r)/s)\sqrt{m} \rightarrow ((y-x)/y)\sqrt{m}$  is in  $\mathcal{F}(\infty, ((n-u)/n)\sqrt{m})$ . Since  $m \mid s, ry - sx = \pm n$ , and  $x \equiv \pm ur \pmod{n}$  or  $m \mid y, ry - sx = \pm n$ , and  $x \equiv \pm mur \pmod{n}$ , we have  $y(s-r) - s(y-x) = -ry + sx = \pm n$ . Since  $(r/s)\sqrt{m}, (x/y)\sqrt{m} \in \mathcal{F}(\infty, (u/n)\sqrt{m})$ , then if  $m \mid s, y-x \equiv \pm(n-u)(s-r) \pmod{n}$ , and if  $m \mid y$ , then  $y-x \equiv \pm m(n-u)(s-r) \pmod{n}$ . By Theorem 3.2.4, there is an edge  $((s-r)/s)\sqrt{m} \rightarrow ((y-x)/y)\sqrt{m}$  in  $\mathcal{F}(\infty, ((n-u)/n)\sqrt{m})$ .  $\square$

Again, we represent the edges of  $\mathcal{F}(\infty, (u/n)\sqrt{m})$  as hyperbolic geodesics in  $\mathbb{H}^2$ . We have

**Lemma 3.2.6.** *No edges of  $\mathcal{F}(\infty, (u/n)\sqrt{m})$  cross in  $\mathbb{H}^2$ .*

*Proof.* Suppose that the edges  $(r/sn)\sqrt{m} \rightarrow (x/yn)\sqrt{m}$  and  $(r'/s'n)\sqrt{m} \rightarrow (x'/y'n)\sqrt{m}$  cross in  $\mathbb{H}^2$ . Then  $ry - sx = \pm 1$  and  $m \mid yn$  or  $m \mid y'$ . Also,  $r'y' - s'x' = \pm 1$ , and  $m \mid y'n$  or  $m \mid s'n$ . Since  $(m, n) = 1$  and  $m$  is a prime,  $m \mid s$  or  $m \mid y$  and  $m \mid s'$  or  $m \mid y'$ . Therefore, the edges  $(r/s)\sqrt{m} \rightarrow (x/y)\sqrt{m}$  and  $(r'/s')\sqrt{m} \rightarrow (x'/y')\sqrt{m}$  in  $\mathcal{G}(\infty, \sqrt{m})$  cross in  $\mathbb{H}^2$ . A contradiction.  $\square$

**Lemma 3.2.7.** *There is no element of  $\sqrt{m}\mathbb{Z} = \{k\sqrt{m} : k \in \mathbb{Z}\}$  between two adjacent vertices in  $\mathcal{F}(\infty, (u/n)\sqrt{m})$  except when one of the two vertices is  $\infty$ .*

*Proof.* Suppose that there exists an edge  $(r/sn)\sqrt{m} \rightarrow (x/yn)\sqrt{m}$  in  $\mathcal{F}(\infty, (u/n)\sqrt{m})$  and assume that  $(r/sn)\sqrt{m} < k\sqrt{m} < (x/yn)\sqrt{m}$ . Then  $(r/s)\sqrt{m} < kn\sqrt{m} < (x/y)\sqrt{m}$ . Since there are edges  $kn\sqrt{m} \rightarrow \infty$  and  $(r/s)\sqrt{m} \rightarrow (x/y)\sqrt{m}$  in  $\mathcal{G}(\infty, \sqrt{m})$ , they cross in  $\mathcal{G}(\infty, \sqrt{m})$  which is impossible by Lemma 3.2.3.  $\square$

### 3.3 Circuits in $\mathcal{G}(\infty, (u/n)\sqrt{m})$

In  $\mathcal{G}(\infty, (u/n)\sqrt{m})$ , every edge is a directed edge. For  $v, w \in \sqrt{m}\widehat{\mathbb{Q}}$ , we say that  $v \leftrightharpoons w$  if there is the edge  $v \rightarrow w$  or  $w \rightarrow v$  in  $\mathcal{G}(\infty, (u/n)\sqrt{m})$ . We call a sequence of  $n$  different vertices  $v_1, v_2, \dots, v_n$  with  $v_1 \rightarrow v_2 \leftrightharpoons \dots \leftrightharpoons v_n \leftrightharpoons v_1$  where  $n \geq 3$  a circuit of length  $n$ . A forest is a graph containing no circuit.

**Lemma 3.3.1.** *If  $n > 1$ , then  $\mathcal{G}(\infty, (u/n)\sqrt{m})$  contains a circuit if and only if  $n \mid mu^2 \pm mu + 1$ .*

*Proof.* It's sufficient to assume that  $\mathcal{F}(\infty, (u/n)\sqrt{m})$  contains a circuit  $v_1 \rightarrow v_2 \leftrightharpoons \dots \leftrightharpoons v_n \leftrightharpoons v_1$  where every  $v_j$  is different from one another. Since  $(v_1, v_2) \in O(\infty, (u/n)\sqrt{m})$ , there exist some  $T \in \mathcal{H}(\sqrt{m})$  such that  $T(\infty, (u/n)\sqrt{m}) = (v_1, v_2)$ . We have  $T \in H_0^m(n), T^{-1} \in H_0^m(n)$ . Also, if  $v \in [\infty]$ , then  $T^{-1}(v) \in [\infty]$ . So, we may assume that  $\infty \rightarrow \frac{u}{n}\sqrt{m} \leftrightharpoons w_3 \leftrightharpoons \dots \leftrightharpoons w_{k-1} \leftrightharpoons w_k \leftrightharpoons \infty = T^{-1}(v_1) \rightarrow T^{-1}(v_2) \leftrightharpoons \dots \leftrightharpoons T^{-1}(v_n) \leftrightharpoons T^{-1}(v_1)$  is a circuit in  $\mathcal{F}(\infty, (u/n)\sqrt{m})$ .

Since no edges of  $\mathcal{F}(\infty, (u/n)\sqrt{m})$  cross in  $\mathbb{H}^2$ , we have

$$\frac{u}{n}\sqrt{m} < w_3 < \dots < w_{k-1} < w_k$$

or

$$\frac{u}{n}\sqrt{m} > w_3 > \dots > w_{k-1} > w_k.$$

If  $(u/n)\sqrt{m} < w_3 < \dots < w_{k-1} < w_k$ , then we will show that  $w_k \rightarrow \infty$ . Suppose that  $\infty \rightarrow w_k = (r/sn)\sqrt{m}$ . Then, we have  $sn1 - 0r = n$ , so  $s = 1$ . Since  $m \mid 0$ , we have from Theorem 3.2.4 that  $r \equiv u \pmod{n}$ . Since  $n > 1, w_k = (r/n)\sqrt{m}$  and  $r \neq u$ , there is an element of  $\sqrt{m}\mathbb{Z}$  between  $(u/n)\sqrt{m}$  and  $(r/n)\sqrt{m}$ . Because all the vertices in the circuit lie in  $\mathcal{F}(\infty, (u/n)\sqrt{m})$ , they don't belong to  $\sqrt{m}\mathbb{Z}$ . That means there is an element of  $\sqrt{m}\mathbb{Z}$  between two adjacent vertices in  $\mathcal{F}(\infty, (u/n)\sqrt{m})$  which is impossible by Lemma 3.2.6. So  $w_k \rightarrow \infty$ . In a similar way, we can prove that  $w_k = (c/n)\sqrt{m}$  and  $1 + muc \equiv 0 \pmod{n}$ .

Let  $c = u + t, t \geq 1$ . Then  $n \mid (mu(u + t) + 1)$ . We will show that  $t = 1$ . Suppose not, then  $c/n < 1$  since otherwise there would be an integer between  $u/n$  and  $c/n$ . Let

$$\varphi(z) = \frac{-u\sqrt{m}z + (mu(u + t) + 1)/n}{-nz + (u + t)\sqrt{m}}.$$

Then,  $\varphi \in H_0^m(n)$ . Moreover,  $\varphi(\infty) = (u/n)\sqrt{m}$ , and  $\varphi((u+t)/n\sqrt{m}) = \infty$ . We can show the vertices adjacent to  $(u/n)\sqrt{m}$  are not greater than  $\varphi((u/n)\sqrt{m}) = [(u+1/tm)/n]\sqrt{m}$ . From then, we can show using mathematical induction that the vertices adjacent to the vertex  $\varphi^i((u/n)\sqrt{m})$  are less than or equal to  $\varphi^{i+1}((u/n)\sqrt{m})$  for all positive integer  $i$ . We can see that  $w_j \leq \varphi^{j-1}((u/n)\sqrt{m})$  for all  $3 \leq j \leq k$ . Again, we can show by using mathematical induction that  $\varphi^i((u/n)\sqrt{m}) < \frac{u+\frac{1}{t-1}}{n}\sqrt{m} < \frac{u+1}{n}\sqrt{m}$  for  $i \geq 1$ . Since  $w_k = (c/n)\sqrt{m} = [(u+t)/n]\sqrt{m} \geq [(u+2)/n]\sqrt{m}$ , we have  $[(u+2)/n]\sqrt{m} \leq w_k \leq \varphi^{k-1}((u/n)\sqrt{m}) < [(u+1)/n]\sqrt{m}$ , a contradiction. Thus  $t = 1$ . That is,  $mu^2 + mu + 1 = mu(u+1) + 1 = muc + 1$ . Thus,  $n \mid mu^2 + mu + 1$ .

If  $(u/n)\sqrt{m} > w_3 > \dots > w_{k-1} > w_k$ , then

$$\infty \rightarrow \frac{n-u}{n}\sqrt{m} \leftrightarrows \sqrt{m} - w_3 \leftrightarrows \dots \leftrightarrows \sqrt{m} - w_k \rightarrow \infty$$

with  $[(n-u)/n]\sqrt{m} < \sqrt{m} - w_3 < \dots < \sqrt{m} - w_k$  is a circuit in  $\mathcal{F}(\infty, [(n-u)/n]\sqrt{m})$ .

With the same method we reach the conclusion that

$$mu^2 - mu + 1 \equiv m(n-u)^2 + m(n-u) + 1 \equiv 0 \pmod{n}.$$

Hence, if the exists a circuit in  $\mathcal{G}(\infty, (u/n)\sqrt{m})$ , then  $mu^2 \pm mu + 1 \equiv 0 \pmod{n}$ .

Now let  $n \mid mu^2 \pm mu + 1$ . Taking

$$T(z) = \frac{-u\sqrt{m}z + (mu^2 \pm mu + 1)/n}{-nz + (u \pm 1)\sqrt{m}},$$

then  $T \in H_0^m(n)$  and  $T(\infty) = (u/n)\sqrt{m}$ . Since  $T$  is elliptic,  $T$  is of finite order. We can construct the circuit

$$\infty \rightarrow T(\infty) \rightarrow T^2(\infty) \rightarrow \dots \rightarrow T^{k-1}(\infty) \rightarrow \infty$$

in  $\mathcal{G}(\infty, (u/n)\sqrt{m})$  where  $k$  is the order of  $T$ .  $\square$

**Theorem 3.3.2.** *If  $(m, n) = 1$  and  $n > 1$ , Then  $\mathcal{G}(\infty, (u/n)\sqrt{m})$  is a forest if and only if  $n \nmid (mu^2 \pm mu + 1)$ .*