Open Journal of Discrete Mathematics, 2011, 1, 103-107
doi:10.4236/ojdm.2011.13013 Published Online October 2011 (http://www.SciRP.org/journal/ojdm)

Symmetric Digraphs from Powers Modulo *n*

Guixin Deng[1*], Pingzhi Yuan[2]
[1]*School of Mathematics, Guangxi Teachers Education University, Nanning, China*
[2]*School of Mathematics, South China Normal University, Guangzhou, China*
E-mail: *oldlao@163.com, mcsypz@mail.sysu.edu.cn
Received June 21, 2011; *revised July* 25, 2011; *accepted August* 5, 2011

Abstract

For each pair of positive integers n and k, let $G(n,k)$ denote the digraph whose set of vertices is $H = \{0,1,2,\cdots, n-1\}$ and there is a directed edge from $a \in H$ to $b \in H$ if $a^k \equiv b \pmod n$. The digraph $G(n,k)$ is symmetric if its connected components can be partitioned into isomorphic pairs. In this paper we obtain all symmetric $G(n,k)$.

Keywords: Congruence, Digraph, Component, Height, Cycle

1. Introduction

In [12], L. Szalay showed that $G(n,2)$ is symmetric if $n \equiv 2(\bmod 4)$ or $n \equiv 4(\bmod 8)$. In [1], the authors proved that if p is a Fermat prime, then $G(2^r p,2)$ is not symmetric when $r=3$ or $r=5$, but it is symmetric when $k=4$. And the following theorem is part of Theorem 5.1 in [13].

Theorem 1.1 ([13] Theorem 5.1) *Let* $n = n_1 n_2$, *where* $n_1 > 1,\ n_2 > 1$ *and* $\gcd(n_1 n_2) = 1$. *Suppose that* $n_1 = 2^m$, *where* $m \ge 1$. *Then* $G(n,k)$ *is symmetric if one of the following conditions holds:*

i) $m \le 2,\ k \ge 2,$ and $2^{m-1} \mid k$;

ii) $m \ge 3,\ k > 2,$ and $2^{m-2} \mid k$;

iii) $m = 4$ and $k = 2$

In this paper we prove that if $G(n,k)$ is symmetric, where $k \ge 2$ and $2^m \| n$, then $m = 5,\ k = 4$ or $m,\ k$ satisfy one of the conditions of the above theorem.

The outline of this paper is as follows. In Section 3 we obtain all symmetric $G(2^m,k)$ by direct computation. In Section 4 we prove some properties about digraph products which will be useful in the proof of our main theorem. In Section 5 we state and prove the main theorem of the present paper.

2. The Carmichael Lambda-Function

Before proceeding further, we need to review some properties of the Carmichael lambda-function $\lambda(n)$.

Definition 2.1 *Let* n *be a positive integer. Then the Carmichael-lambda-function* $\lambda(n)$ *is defined as follows:*

$$\lambda(1)=1,$$
$$\lambda(2)=1,$$
$$\lambda(4)=2,$$
$$\lambda(2^k)=2^{k-2} \text{ if } k \ge 3,$$
$$\lambda(p^k)=(p-1)p^{k-1} \text{ if } p \text{ is an odd prime},$$
$$\lambda\left(\prod_{i=1}^r p_i^{e_i}\right) = \operatorname{lcm}\left[\lambda(p_1^{e_1}),\lambda(p_2^{e_2}),\cdots,\lambda(p_r^{e_r})\right]$$

where p_i *are distinc primes.*

The following theorem generalizes the well-known Euler's theorem which says that $a^{\phi(n)} \equiv 1(\bmod\ n)$ if and only if $\gcd(a,n)=1$.

Theorem 2.1 (*Camichael*). *Let* $a,n \in \mathbb{N}$. *Then* $a^{\lambda(n)} \equiv 1(\bmod\ n)$ *if and only if* $\gcd(a,n)=1$. *Moreover, there exists an integer* g *such that* $ord_n g = \lambda(n)$, *where* $ord_n g$ *denotes the multiplicative order of g modulo n.*

For the proof see [5, p. 21]

3. The Case $n = 2^m$

Let G be a digraph and a be a vertex in G. The indegree of a, denoted by ind(a) is the number of directed edges coming to a, and the outdegree of a is the number of edges leaving a. Particularly, let $\operatorname{ind}_n^k(a)$ denote the indegree of a vertex a contained in $G(n,k)$.

There are two particular subdigraphs of $G(n,k)$. Let $G_1(n,k)$ be the induced subdigraph of $G(n,k)$ on the set of vertices which are coprime to n and $G_2(n,k)$ be the induced subdigraph of $G(n,k)$ on the set of vertices which are not coprime with n. We observe that $G_1(n,k)$

and $G_2(n,k)$ are disjoint and that $G(n,k) = G_1(n,k) \bigcup G_2(n,k)$, that is, no edges goes between $G_2(n,k)$ and $G_2(n,k)$.

It is clear that each component of $G(n,k)$ contains a unique cycle, since the component has only a finite number of vertices and each vertex has outdegree 1. The following lemma tells us that every component contained in $G_1(n,k)$ is determined by its cycle length.

Lemma 3.1 ([13] Corollary 6.4) *Let $t \geq 1$ be a fixed integer. Then any two components in $G_1(n,k)$ containing t-cycle are isomorphic.*

Definition 3.1 *We define a height function on the vertices and components of $G(n,k)$. Let c be a vertex of $G(n,k)$, we define $h(c)$ to be the minimal nonnegative integer i such that c^{k^i} is congruent modulo n to a cycle vertex in $G(n,k)$. And if C is a component of $G(n,k)$, we define $h(C) = \sup_{c \in C} h(c)$.*

The indegree and the height function play an important role in the structure of $G(n,k)$. We need the following results concerning the indegrees and heights.

Lemma 3.2 ([14]) *Let $n = \prod_{i=1}^{r} p_i^{e_i}$ be the prime factorization of n. Let a be a vertex of positive indegree in $G_1(n,k)$. Then*

$$\mathrm{ind}_n^k(a) = \prod_{i=1}^{r} \mathrm{ind}_{p_i^{e_i}}^k(a) = \prod_{i=1}^{r} \delta_i \gcd\left(\lambda\left(p_i^{e_i}\right), k\right),$$

where $\delta_i = 2$ if $2 \mid k$ and $8 \mid p_i^{e_i}$, and $\delta_i = 1$ otherwise.

Lemma 3.3 ([11] Theorem 3.2) *Let p be a prime. Let a be a vertex of positive indegree in $G_2(p^e,k)$, and assume that $p^l \| k$ and $a \neq 0$. Then $l = kt$ for some positive integer t and*

$$\mathrm{ind}_{p^e}^k(a) = \delta p^{(k-1)t} \gcd\left(\lambda\left(p^{e-l}\right), k\right)$$

where $\delta = 2$ if $p = 2, 2 \mid k$ and $e - l \geq 3$, and $\delta = 1$ otherwise.

Lemma 3.4 ([13] Lemma 3.2) *Let p be a prime and e, k be two positive integers. Then*

$$\mathrm{ind}_{p^e}^k(0) = p^{e - \left\lceil \frac{e}{k} \right\rceil}.$$

Lemma 3.5 *Let p be a prime and $e \geq 2$, $k \geq 2$ be two positive integers. Let h be the positive integer such that $k^{h-1} < e \leq k^h$. Then $h = h\left(G_2\left(p^e,k\right)\right)$.*

Proof. It is clear that $p \in G_2(p^e,k)$ and $h(p) = h\left(G_2\left(p^e,k\right)\right)$. And $p^{k^i} \equiv 0 \left(\mathrm{mod}\ p^e\right)$ if and only if $k^i \geq e$. This proves the Lemma. □

Lemma 3.6 *Let p be a prime and $e,k \geq 2$ be two positive integers. Let $\lambda(p^e) = uv$ where u is the maximal divisor of $\lambda(p^e)$ relatively prime to k. If G is the component of $G(p^e,k)$ containing 1, then*

$$h(C) = \min\left\{i : v \mid k^i\right\}$$

Proof. Let $h = \min\left\{i : v \mid k^i\right\}$. Then there exists a divisor d of v such that d is not a divisor of k^{h-1}. By Theorem 2.1 there exists a vertex $g \in G(p^e,k)$ such that $ord_{p^e} g = uv$. Let $a \equiv g^{\frac{uv}{d}} \left(\mathrm{mod}\ p^e\right)$. Then $ord_{p^e} a = d$ and $a^{k^{h-1}}$ is not congruent modulo p^e to 1, but $a^{k^h} \equiv 1 \left(\mathrm{mod}\ p^e\right)$. We have $h(C) \geq h(a) = h$ by the definition of height function.

Conversely if $a \in C$, then there exists $j \geq 1$ such that $a^{k^j} \equiv 1 \left(\mathrm{mod}\ p^e\right)$, then $ord_{p^e} a \mid k$. But $ord_{p^e} a \mid uv$, hence $ord_{p^e} a \mid v$. And $a^{k^h} \equiv 1 \left(\mathrm{mod}\ p^e\right)$. That is $h(C) \leq h.$ Lemma 3.6 is proved. □

Now we can prove our first result.

Theorem 3.1 *Let $k \geq 2, m \geq 1$ be two positive integers. Then $G(2^m,k)$ is symmetric if and only if one of the following conditions holds.*

i) $m = 1$;
ii) $m = 2, 2 \mid k$;
iii) $m = 4, k = 2$;
iv) $m = 5, k = 4$;
v) $m \geq 3, 2^{m-2} \mid k, k \geq m.$

Proof. The case $m < 3$ follows directly by simple computations, so we may assume that $m \geq 3$, thus $\lambda(2) = 2^{m-2}$. We first suppose that $G(2^m,k)$ is symmetric. Let C_0 and C_1 be the components of $G(2^m,k)$ containing the vertex 0 and 1, respectively. Then it is easy to see that C_0 is just $G_2(2^m,k)$. Since the cycle lengths of C_0 and C_1 are 1, by the assumptions and Lemma 3.1 we must have $C_0 \simeq C_1$, thus $h = h(C_0) = h(C_1)$.

If $h = 1$, then $k \geq m$ and $\in \gcd\left(2^{m-2}, k\right) = ind(1) = ind(0) = 2^{m-1}$, where $\in = 1$ if k is odd, and $\in = 2$ if $2 \mid k$. We must have $2^{m-2} \mid k$.

If $2 \nmid k$, then C_1 is a cycle, however C_0 is not a cycle. Hence we may assume that $2^r \| k$, $r \geq 1$ and $h \geq 2$. We have $h = h(C_1) = \min\left\{i : 2^{m-2} \mid k^i\right\}$ by Lemma 3.6. It implies that

$$r(h-1) < m - 2 \leq rh. \tag{3.1}$$

Since $h = h(C_0)$, by Lemma 3.5 we have

$$k^{h-1} < m \leq k^h. \tag{3.2}$$

Combining (3.1) and (3.2), we obtain

$$2^{r(h-1)} \leq k^{h-1} \leq m - 1 \leq rh + 1,$$

so $h \leq 3$ and $r \leq 2$. By an easy computation, we have $(m,k,h,r) = (5,4,2,2), (6,4,2,2), (5,2,3,1)$ or $(4,2,2,1)$.

By computations we know that both $G(16,2)$ and $G(32,4)$ are symmetric. For $G(32,2)$ and $G(64,4)$, by Lemmas 3.2 and 3.3, we have $\mathrm{ind}_{32}^{2}(4)=8$, and for any vertex a in C_1 which has positive indegree, $\mathrm{ind}_{32}^{2}(a)=4$. Similarly $\mathrm{ind}_{64}^{4}(16)=16$, $\mathrm{ind}_{64}^{4}(\mathrm{a})=8$. Thus neither of them are symmetric.

Finally, from Theorem 1.1 it is clear that if *m*, *k* satisfy one of *i*) - *v*), then $G(2^m,k)$ is symmetric. Theorem 3.1 is proved. □

4. Properties of Digraphs Product

Given two digraphs G_1 and G_2. Let $G_1\times G_2$ be the digraph whose vertices are the ordered pairs (a_1,a_2), where $a_i\in G_i$ and there is a directed edge from (a_1,a_2) to (b_1,b_2) if there is a directed edge from a_i to b_i for $i=1,2$. In [13] L. Somer and M. Krizek proved the following fact: Let $n=n_1n_2$ where $\gcd(n_1,n_2)=1$, then $G(n,k)\cong G(n_1,k)\times G(n_2,k)$. And the canonical isomorphism is given by $a\mapsto(a_1,a_2)$ where $a\equiv a_i(\mathrm{mod}\, n_i)$, $i=1,2$. In general we have

$$G(n,k)\cong G\left(p_1^{e_1},k\right)\times G\left(p_2^{e_2},k\right)\times\cdots\times G\left(p_r^{e_r},k\right),$$

if $n=\prod_{i=1}^{r}p_i^{e_i}$ is the prime factorization of *n*. We need this fact and the following lemma.

Lemma 4.1 ([4] Lemma 3.1) *Let* $n=n_1n_2$ *where* $\gcd(n_1,n_2)=1$. *Let* C_i *be a component of* $G(n_i,k)$. *And the cycle length of* C_i *is* t_i. *Then* $C_1\times C_2$ *is a subdigraph of* $G(n,k)$ *consisting of* $\gcd(t_1,t_2)$ *components, each having cycles of length* $\mathrm{lcm}(t_1,t_2)$.

Lemma 4.2 *Let* $n=n_1n_2$ *where* $\gcd(n_1,n_2)=1$. *If* $G(n_1,k)$ *is symmetric, then* $G(n,k)$ *is symmetric*.

Proof. It follows immediately from Lemma 4.1 and the fact $G(n,k)\simeq G(n_1,k)\times G(n_2,k)$. □

Lemma 4.3 *If* $G(n,k)$ *is symmetric, then* $G(n,k^r)$ *is also symmetric for any* $r\geq 1$.

Proof. Assume that $G(n,k)$ has 2*m* components, say, $C_1,C_2,\cdots,C_{2m}$, and for each $i=1,2,\cdots,m$ there exists an isomorphism φ_i of digraphs:

$$\varphi_i: C_i\to C_{i+m}.$$

If two vertices *x*, *y* are in the same component of $G(n,k^r)$, then there exists a vertex *z* and positive integers *u*, *v* and $x^{k^u}\equiv z(\mathrm{mod}\ n)$, $y^{k^v}\equiv z(\mathrm{mod}\ n)$ which implies that *x*, *y* are in the same component of $G(n,k)$. It follows that if *D* is a component of $G(n,k^r)$, then there exists a $j\in\{1,2,\cdots,2m\}$ such that $D\subseteq C_j$.

Let $C_1=\bigcup_{i=1}^{s_1}D_j$ and $C_{m+1}=\bigcup_{i=1}^{s_2}E_j$ where D_j, $j=1,2,\cdots,s_1$ and E_l, $l=1,2,\cdots,s_2$ are components of $G(n,k^r)$. If $x,y\in C_1$ and $x^{k^r}\equiv y(\mathrm{mod}\ n)$, then there exist $y_1,y_2,\cdots,y_r=y$ such that $x^k\equiv y_1(\mathrm{mod}\ n)$, and $y_i^k\equiv y_{i+1}(\mathrm{mod}\ n)$. So $\varphi_1(x)^k\equiv\varphi_1(y)(\mathrm{mod}\ n)$ and $\varphi_1(y_i)^k\equiv\varphi_1(y_{i+1})(\mathrm{mod}\ n)$, we get $\varphi_1(x)^{k^r}\equiv\varphi_1(y)(\mathrm{mod}\ n)$ and φ_1 still preserves arrows if we consider C_1 and C_{m+1} as subdigraphs of $G(n,k^r)$

It follows that $s_1=s_2$ and φ_1 is still an isomorphism if we consider C_1 and C_{m+1} as subdigraphs of $G(n,k^r)$. Hence $G(n,k^r)$ is also symmetric. Lemma 4.3 is proved. □

Let *G* be a digragh. Let $|G|$ denote the number of vertices in *G*, and let $M(G)=\max_{c\in G}\{ind(c)\}$.

Lemma 4.4 *Let G and H be two digraphs, and* $a\in G$, $b\in H$. *Then* $\mathrm{ind}((a,b))=\mathrm{ind}(a)\mathrm{ind}(b)$, $M(G\times H)=M(G)M(H)$, *and* $|G\times H|=|G||H|$.

Proof. It follows immediately from the definitions. □

The following lemma is the key lemma for the proof of the main result of this paper.

Lemma 4.5 *Let* O_m *denote the digraph whose set of vertices is* $\{a=a_0,a_1,\cdots,a_{m-1}\}$ *and there is a directed edge from* a_i *to* a_j *if and only if* $a_j=a_0=a$. *Let G and H be two digraphs such that all vertices in G and H have outdegree* 1. *Then* $O_m\times G\simeq O_m\times H$ *if and only if* $G\simeq H$.

Proof. Assume that $\varphi: O_m\times G\to O_m\times H$ is an isomorphism of digraphs. Let

$$G_0=\{x\in G\,|\,\mathrm{ind}(x)=0\},\ G_1=\{x\in G\,|\,\mathrm{ind}(x)>0\},$$
$$H_0=\{x\in H\,|\,ind(x)=0\},\ H_1=\{x\in H\,|\,ind(x)>0\}.$$

If $x\in G_1$ and $\mathrm{ind}((a,x))=\mathrm{ind}(a)ind(x)>0$, then $\mathrm{ind}(\varphi(a,x))>0$. Let $\varphi((a,x))=(a_j,x')$, then we have $x'\in H_1$ and $a_j=a$. Now we define a map $\varphi_1: G_1\to H_1$ by $\varphi_1(x)=x'$, $x\in G_1$. Obviously, φ_1 is injective.

If $y'\in H_1$, then there exists a vertex (a,y) of positive indegree in $O_m\times G$ such that $\varphi((a,y))=(a,y')$. Hence $\varphi_1(y)=y'$ and φ_1 is also surjective.

Now we assume that $x,y\in G_1$, and there is a directed edge from *x* to y. Let $\varphi_1(x)=x',\varphi_1(y)=y'$, by definition we have $\varphi((a,x))=(a,x')$ and $\varphi((a,y))=(a,y')$. We know that there is a directed edge from (a,x) to (a,y), then there is also a directed edge from (a,x') to (a,y') since φ preserves arrows. So there is also a directed edge from x' and y'. We showed that φ_1 preserves arrows.

For any $y\in G_1$, let

$$E_0(y)=\{x\in G_0\,|\,\text{there is a directed edge from } x \text{ to } y\},$$
$$E_1(y)=\{x\in G_0\,|\,\text{there is a directed edge from } x \text{ to } y\},$$

then

$$G_0=\bigcup_{y\in G_1}E_0(y)$$

And the above union is a disjoint union since each vertex has outdegree 1. If $\varphi_1(y)=y'$, by Lemma 4.4 we have

$$\mathrm{indeg}((a,y))=m(|E_0(y)|+|E_1(y)|)$$
$$=\mathrm{ind}((a,y'))=m(|E_0(y')|+|E_1(y')|)$$

and $|E_1(y)| = |E_1(y')|$ since φ_1 maps $E_1(y)$ into $E_1(y')$. Then we also have $|E_0(y)| = |E_0(y')|$. Now we can define a map φ_0 from G_0 to H_0 such that for any $x \in E_0(y)$, $\varphi_0(x) \in E_0(\varphi_1(y))$.

Finally we can define $\phi : G \to H$

$$\phi(a) = \varphi_i(a) \text{ if } a \in G_i,$$

for $i = 0,1$. It is easy to show that ϕ is bijective.

Now we prove that ϕ preserve arrows. Suppose $x, y \in G$ and there is a directed edge from *x* to *y*. We only need to treat the case when $x \in G_0$ and $y \in G_1$. Let $\phi(y) = \varphi_1(y) = y'$. By the construction of φ_0 we see that $\phi(x) = \varphi_0(x) \in E_0(y')$, so there is also a arrow from $\phi(x)$ to $\phi(y)$. It is easy to show that the number of directed edges of *G* is equal to the number of directed edges of *H*. Thus ϕ is an isomorphism. Lemma 4.5 is proved. □

5. The Main Theorem

To begin with, we prove the following lemma.

Lemma 5.1 *Let E be the component of* $G(64q,4)$ *containing the vertex* 0 *where q is odd and F be another component of* $G(64q,4)$. *Then E is not isomorphic to F. And the similar result for* $G(32q,2)$ *is also valid.*

Proof. We only prove the case for $G(64q,4)$, the proof for $G(32q,2)$ is similar and we omit the details. Assume that $q = \prod_{i=1}^{r} p_i^{e_i}$ where each p_i is an odd prime, and $e_i \ge 2$ if $i \le s$, $e_i = 1$ if $s < i \le r$. Let $\in = 0$ or 1, and let $C_\in$ and $C_\in^i$ the components of $G(64,4)$ and $G(p_i^{e_i},4)$, containing the vertex $\in$ and $i = 1,2,\cdots,r$ respectively. Then

$$E \cong C_0 \times C_0^1 \times \cdots \times C_0^r.$$

If the cycle length of F > 1, then *F* is not isomorphic to *E*. Suppose that the cycle length of *F* is 1, by Lemma 4.1

$$F \simeq C_\in \times F_1 \times F_2 \times \cdots \times F_r,$$

where F_i is a component of cycle length 1 contained in $G(p_i^{e_i},4)$. By Lemma 3.1 we can write

$$F \cong C_{\in_0} \times C_{\in_1}^1 \times \cdots \times C_{\in_r}^r,$$

where $\in_i = 0$ or 1. By computations we know that $M(C_0) = 16$, $M(C_1) = 8$. By Lemma 3.3 there exists $u_i \ge 1$ such that $M(C_0^i) = p_i^{u_i}$ or $2p_i^{u_i}$, or $4p_i^{u_i}$ if $1 \le i \le s$, $M(C_0^i) = 1$ if $s < i \le r$. And by Lemma 3.2 $M(C_1^i) = \gcd((p_i - 1)p_i^{e_i - 1}, 4) = 2$ or 4. for any $1 \le i \le r$. Thus

$$M(E) = 16\prod_{i=1}^{r} M(C_0^i) = 16\prod_{i=1}^{s} M(C_0^i),$$

$$M(F) = M(C_\in) \cdot \prod_{i=1}^{r} M(C_{\in_i}^i).$$

Now if $M(E) = M(F)$, we have $\in_1 = \in_2 = \cdots = \in_s = 0$, and if $\in_0 = 0$ then all $\in_i = 0$, $E = F$. If $\in_0 = 1$, then $s = r - 1$ and $\gcd(p_r - 1, k) = 2$. But in this case

$$|E| = |C_0| \cdot \prod_{i=1}^{r} C_0^i = 32\prod_{i=1}^{r-1} p_i^{e_i - 1},$$

$$|F| = |C_1| \cdot |C_1^r| \cdot \left(\prod_{i=1}^{r-1} C_0^i\right).$$

Therefore we have $M(E) \ne M(F)$ or $|E| \ne |F|$, *E* is not isomorphic to *F*. Lemma 5.1 is proved. □

Theorem 5.1 (Main Theorem) *Let* $k \ge 2$ *and* $n = 2^m q$, *where* $m \ge 1$ *and q is odd. Then* $G(n,k)$ *is symmetric if and only if* $G(2^m,k)$ *is symmetric.*

Proof. By Lemma 4.2 we only need to prove the necessity. The case $m = 1$ is trivial, so we may assume that $m \ge 2$. Let C_0 be the component of $G(2^m,k)$ containing the vertex 0, and C_1 be the component of $G(2^m,k)$ containing the vertex 1. Let $h_0 = h(C_0)$ and $h_1 = h(C_1)$. We claim that $2|k$ and $h_0 = h_1$. Otherwise we assume firstly that *k* is odd or $h_0 < h_1$. In both cases we have $G_2(2^m,k^{h_0}) \simeq O_{2^{m-1}}$, and if $x \in G(2^m,k^{h_0})$ and $x \ne 0$, then $\text{ind}_{2^m}^{k^{h_0}}(x) < 2^{m-1}$.

By Lemma 4.3 $G(n,k^{h_0})$ is also symmetric and $G(n,k^{h_0}) \simeq G(2^m,k^{h_0}) \times G(q,k^{h_0})$. Let

$$G(q,k^{h_0}) \simeq \bigcup_{i=1}^{s} m_i H_i,$$

where each H_i is a connect component such that $H_i \simeq H_j$ if and only if $i = j$, and $M(H_i) \le M(H_j)$ for $i < j$. We can choose an *l* such that m_l is odd and $2|m_j$ if $j > l$, since $G(q,k^{h_0})$ is not symmetric. Then $G(2^m,k^{h_0}) \times \left(\bigcup_{i=1}^{l} m_i H_i\right)$ is also symmetric. Let $E = G_2(2^m,k^{h_0}) \times H_l$, by Lemma 4.1 *E* is a connected component of $G(2^m,k^{h_0}) \times \left(\bigcup_{i=1}^{l} m_i H_i\right)$ since $G_2(2^m,k^{h_0})$ is a component of cycle length 1. Let *F* be another component of $G(2^m,k^{h_0}) \times \left(\bigcup_{i=1}^{l} m_i H_i\right)$. Suppose that

$$E \simeq F,$$

by Lemma 4.1 again *F* is a component of $K \times H_i$, where *K* is a component of $G(2^m,k^{h_0})$ and $1 \le i \le l$. But we have

$$\begin{aligned} M(E) &= M(O_{2^{m-1}} \times H_l) \\ &= 2^{m-1} M(H_l) \\ &\ge M(K) M(H_i) \\ &\ge M(F) \end{aligned}$$

where the equality holds if and only if $M(K)=2^{m-1}$ and $M(H_i)=M(H_l)$, which implies $K=G_2(2^m,k^{h_0})$. But now we have $F=G_2(2^m,k^{h_0})\times H_i$ and

$$O_{2^{m-1}}\times H_l \simeq O_{2^{m-1}}\times H_i.$$

Hence $H_l \simeq H_i$ by Lemma 4.5, $i=l$ .We show that there are exactly m_l components contained in $G(2^m,k^{h_0})\times\left(\bigcup_{i=1}^{l} m_i H_i\right)$ which are isomorphic to E.

It is contrary to the fact that $G(2^m,k^{h_0})\times\left(\bigcup_{i=1}^{l} m_i H_i\right)$ is symmetric.

Now we have $2|k$, if $h_0>h_1$, consider

$$G(2^m,k^{h_1})=G_1(2^m,k^{h_1})\bigcup G_2(2^m,k^{h_1}).$$

We have $G_1(2^m,k^{h_1})\simeq O_{2^{m-1}}$ and

$$M\left(G_2\left(2^m,k^{h_1}\right)\right)<M\left(G_1\left(2^m,k^{h_1}\right)\right).$$

Using the same arguments we can show that $G(n,k^{h_1})$ is not symmetric. Hence $h_0=h_1=h.$

If $h=1$, , then for any vertex $a\in G(2^m,k)$, we have $a^k\equiv 0(\bmod 2^m)$ if a is even and $a^k\equiv 1(\bmod 2^m)$ if a is odd. It implies that $G(2^m,k)\simeq 2O_{2^{m-1}}$. $G(2^m,k)$ is symmetric in this case.

If $h>1$, then $m\geq 3$. Assume that $2^r\|k$, then we have (3.1) and (3.2), by the proof of Theorem 3.1 we have (m, k) = (5, 4), (6, 4), (5, 2) or (4, 2). Then the proof is completed by Lemma 5.1 and Theorem 3.1.□

Corollary 5.1 *Let n, k be two positive integers and* $2^m \| n, m\geq 1$. *Then* $G(n,k)$ *is symmetric if and only if* k = 1 *or k, m satisfy one of* (*i*) **-** (*v*) *in Theorem* 3.1.

6. References

[1] W. Carlip and M. Mincheva, "Symmetry of Iteration Digraphs," *Czechoslovak Mathematic Journal*, Vol. 58, No. 1, 2008, pp. 131-145. doi:10.1007/s10587-008-0009-8

[2] G. Chartrand and L. Lesnidk, "Graphs and Digraphs (3rd Edition)," Chapman Hall, London, 1996.

[3] Wun-Seng Chou and Igor E. Shparlinski, "On the Cycle Structure of Repeated Exponentiation Modulo a Prime," *Journal of Number Theory*, Vol.107, No. 2, 2004, pp. 345-356. doi:10.1016/j.jnt.2004.04.005

[4] Joe Kramer-Miller, "Structural Properties of Power Digraphs Mudulo *n*," Manuscript.

[5] M. Krizek, F. Lucas and L. Somer, "17 Lectures on the Femat Numbers, from Number Theory to Geometry," Springer, New York, 2001.

[6] C. Lucheta, E. Miller and C. Reiter, "Digraphs from Powers Modulo *p*," *Fibonacci Quart*, Vol. 34, 1996, pp. 226-239.

[7] I. Niven, H. S. Zuckerman and H. L. Montgomery, "An Introduction to the Theory of Numbers," 5th Edition, John Wiley & Sons, New York, 1991.

[8] T. D. Rogers, "The Graph of the Square Mapping on the Prime Fields," *Discrete Mathematics*, Vol. 148, No. 1-23, 1996, pp. 317-324. doi:10.1016/0012-365X(94)00250-M

[9] L. Somer and M. Krizek, "On a Connection of Number Theory with Graph Theory," *Czechoslovak Mathematic Journal*, Vol. 54, No. 2, 2004, pp. 465-485. doi:10.1023/B:CMAJ.0000042385.93571.58

[10] L. Somer and M. Krizek, "Structure of Digrphs Associated with Quadratic Congruences with Composite Moduli," *Discrete Mathematics*, Vol. 306, No. 18, 2006, pp. 2174-2185. doi:10.1016/j.disc.2005.12.026

[11] L. Somer and M. Krizek, "On Semiregular Digraphs of the Congruence $x^k \equiv y$(mod n)," *Commentationes Mathematicae Universitatis Carolinae*, Vol. 48, No. 1, 2007, pp. 41-58.

[12] L. Szalay, "A Discrete Iteration in Number Theory," *BDTF Tud. KÄozl*, Vol. 8, 1992, pp. 71-91.

[13] L. Somer and M. Krizek, "On Symmetric Digrphs of the Congruence $x^k \equiv y$ (mod n)," *Discrete Mathematics*, Vol. 309, No. 8, 2009, pp. 1999-2009. doi:10.1016/j.disc.2008.04.009

[14] B. Wilson, "Power Digraphs Modulo *n*," *Fibonacci Quart*, Vol. 36, 1998, pp. 229-239.

