POWER DIGRAPHS MODULO n ARE SYMMETRIC OF ORDER M IF AND ONLY IF M IS SQUARE FREE

LAWRENCE SOMER AND MICHAL KŘÍŽEK

ABSTRACT. We assign to each pair of positive integers $k \geq 2$ and n a digraph $G(n,k)$ whose set of vertices is $H = \{0, 1, \ldots, n-1\}$ and for which 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 of order M if its set of components can be partitioned into disjoint subsets, each containing exactly M isomorphic components. Deng and Yuan completely characterized all symmetric digraphs of order M when $M = 2$ or M is divisible by an odd prime. We demonstrate that their classification is complete by showing that there are no symmetric digraphs $G(n,k)$ of order 2^s for $s \geq 2$.

1. INTRODUCTION

For $n \geq 1$ set

$$H = \{0, 1, \ldots, n-1\}.$$

For a fixed integer $k \geq 2$ and for each $a \in H$, let $b \in H$ be the remainder of a^k modulo n, i.e.,

$$b \in H \quad \text{and} \quad a^k \equiv b \pmod{n}. \tag{1.1}$$

In this paper, we construct an iteration directed graph $G(n,k)$ (called *digraph*) associated with the congruence (1.1) such that there exists exactly one directed edge from a to b for all $a \in H$. Each pair of natural numbers $k \geq 2$ and n thus has a specific iteration digraph corresponding to it.

In [2] and [3], Deng and Yuan gave necessary and sufficient conditions for a large set of digraphs $G(n,k)$ to be symmetric. We demonstrate that their classification of symmetric digraphs is in fact complete by showing that symmetric digraphs $G(n,k)$ of a certain type cannot exist.

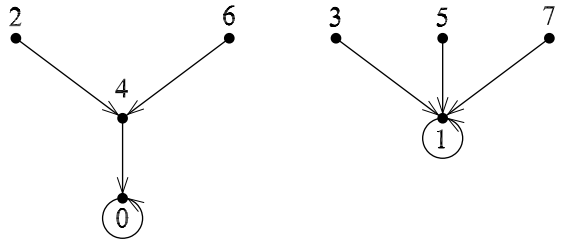

FIGURE 1. The iteration digraph $G(8,2)$.

For brevity we will make statements such as $\gcd(a,n) = 1$, treating the vertex a as a number. Moreover, when we refer, for instance, to the vertex a^k, we identify it with the remainder from H given by (1.1), see Figure 1.

This paper was supported by Grant no. IAA 100190803 of the Grant Agency of the Academy of Sciences of the Czech Republic and RVO 67985840.

Let $\omega(n)$ denote the number of distinct primes dividing $n \geq 2$ and let the prime power factorization of n be given by

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}, \tag{1.2}$$

where $p_1 < p_2 < \cdots < p_r$ are primes and $\alpha_i > 0$, i.e., $r = \omega(n)$. For $n = 1$, we set $\omega(1) = 0$.

A *component* of the iteration digraph is a subdigraph which is a maximal connected subgraph of the associated nondirected graph.

The *indegree* of a vertex $a \in H$ of $G(n,k)$, denoted by $\text{indeg}_n^k(a)$, is the number of directed edges coming into a, and the *outdegree* of a is the number of directed edges leaving the vertex a. Frequently we will simply write $\text{indeg}(a)$ when it is understood that a is a vertex in $G(n,k)$. Obviously, the outdegree of each vertex of $G(n,k)$ is equal to 1. Therefore, $G(n,k)$ with n vertices also has exactly n directed edges. Thus, if b_i, $i = 1, 2, \ldots, q$, denote the indegrees of all the vertices of $G(n,k)$ having positive indegree, then

$$\sum_{i=1}^{q} b_i = n. \tag{1.3}$$

It is clear that each component has a unique cycle, since each vertex of the component has outdegree 1 and the component has only a finite number of vertices. It is also evident that cycle vertices have positive indegree. Cycles of length 1 are called fixed points (cf. Figure 2).

Note that 0 and 1 are always fixed points of $G(n,k)$. Cycles of length t are called t-cycles. Let $A_t(G(n,k))$ denote the number of t-cycles in $G(n,k)$. Let $J(n,k)$ be a component in $G(n,k)$ and let c be a cycle vertex in $J(n,k)$. It is evident that b is a vertex in $J(n,k)$ if and only if $b^{k^h} \equiv c \pmod{n}$ for some positive integer h.

Definition 1.1. *Let $M \geq 2$ be an integer. The digraph $G(n,k)$ is said to be symmetric of order M if its set of components can be partitioned into disjoint subsets, each containing exactly M isomorphic components.*

We have the following proposition.

Proposition 1.2. *If the digraph $G(n,k)$ is symmetric of order M then $M \mid n$.*

Proof. Suppose that $G(n,k)$ has ℓ disjoint subsets of components, each containing exactly M isomorphic components. Let each component in the ith subset, $1 \leq i \leq \ell$, have n_i vertices. Then the ith subset has Mn_i vertices. Hence,

$$n = \sum_{i=1}^{\ell} Mn_i = M \sum_{i=1}^{\ell} n_i,$$

and $M \mid n$. □

Notice that for a given symmetric digraph $G(n,k)$ the order M is not necessarily uniquely defined.

Figure 2 shows a symmetric digraph $G(39,3)$ of order 3, while Figure 3 exhibits a symmetric digraph of order 5. The digraph in Figure 1 is not symmetric of order M for any $M \geq 2$ while the digraphs in Figures 4, 5, and 6 are each symmetric of order 2.

In Szalay [12], it was shown that $G(n,2)$ is symmetric of order 2 if $n \equiv 2 \pmod{4}$ or $n \equiv 4 \pmod{8}$. In [1], it was proved that $G(2^r q, 2)$ is symmetric of order 2 if and only if $r = 1, 2$, or 4, where q is a Fermat prime, that is, a prime $q = 2^{2^m} + 1$ for some nonnegative integer m (see [7] for properties of Fermat primes).

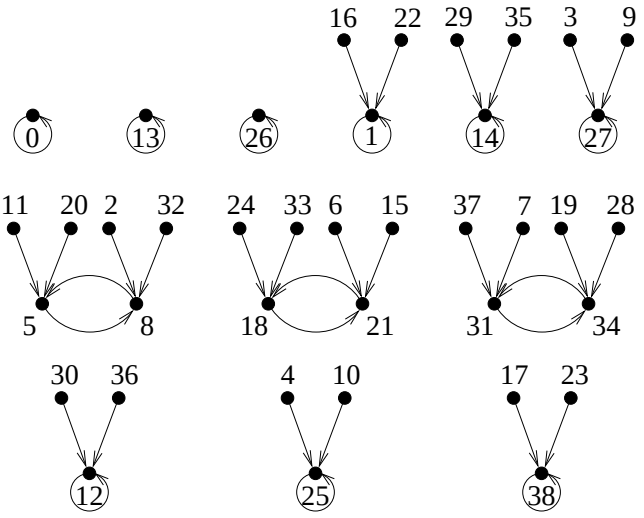

FIGURE 2. The symmetric iteration digraph $G(39, 3)$ of order 3.

In [10], we found sufficient conditions for $G(n, k)$ to be symmetric of order M, where $M \geq 2$ is an arbitrary square-free number. Kramer-Miller [6] gave necessary and sufficient conditions for $G(n, k)$ to be symmetric of order p when p is an odd prime, $p \mid n$, and n is square free. This result was extended in [5], where necessary and sufficient conditions were given for $G(p^{\alpha}n_1, k)$ to be symmetric of order p, where p is an odd prime, $\alpha \geq 1$, $n_1 \geq 1$ is square free and odd, and $p \nmid n_1$.

2. Classification of All Symmetric Iteration Digraphs

By the combined results of Theorem 2.1 proved in [3] and Theorem 2.4 which was proved in [2], Deng and Yuan determined all symmetric digraphs $G(n, k)$ of order M when M is divisible by an odd prime or $M = 2$. The following theorem which extends results given in [10] and [6] can be extracted from the results in [3]. For $\gcd(n, a) = 1$ let $\mathrm{ord}_n a$ denote the multiplicative order of a modulo n.

Theorem 2.1. *Let $k \geq 2$ and let $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ as given in (1.2). If p_i is odd and $p_i \mid n$, let $T(p_i)$ be the set of all odd primes $p_j \neq p_i$ such that $p_j \mid n$ and $\gcd((p_j - 1)p_j^{\alpha_j - 1}, k) = p_j^{\alpha_j - 1}$. Suppose that M is divisible by an odd prime. Then $G(n, k)$ is symmetric of order M if and only if condition (i) holds and one of conditions (ii)–(iv) also holds:*

(i) *M is square free, $M \mid n$, and k is odd,*
(ii) *$\omega(n) = 1$, p_1 is an odd prime such that $M = p_1$, $\gcd((p_1 - 1)p_1^{\alpha_1 - 1}, k) = p_1^{\alpha_1 - 1}$, and $k \equiv 1 \pmod{p_1 - 1}$,*
(iii) *$2 \mid M$, $\omega(n) \geq 2$, $2 \| n$, and $G(n/2, k)$ is symmetric of order $M/2$,*
(iv) *M is odd, n is divisible by at least two distinct odd primes, and for each prime p_i such that $p_i \mid M$, $\gcd((p_i - 1)p_i^{\alpha_i - 1}, k) = p_i^{\alpha_i - 1}$ and one of the following two subconditions hold:*

(a) $G(p_i, k)$ is symmetric of order p_i, or

(b) $G(p_i, k)$ is not symmetric of order p_i, $T(p_i)$ is nonempty, and either

$$p_i \mid A_t(G(\prod_{j \in T(p_i)} p_j, k))$$

or $\mathrm{ord}_{p_i-1} k \mid t$ *for all* $t \in \mathbb{N}$.

Remark 2.2. We observe that the digraph $G(25, 5)$ appearing in Figure 3 is an example to part (ii) of Theorem 2.1 for $M = k = 5$ and $n = 5^2$.

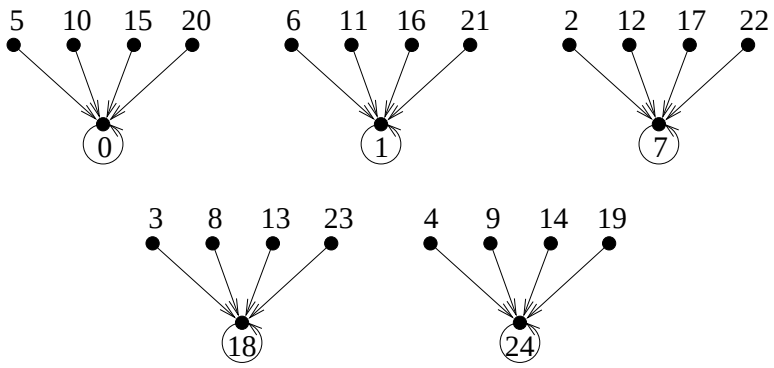

FIGURE 3. The symmetric and semiregular iteration digraph $G(25, 5)$ of order 5.

Let us denote the *radical* of n by

$$\mathrm{rad}(n) = \prod_{i=1}^{r} p_i$$

and let the factorization of n be as given in (1.2). We have the following corollary to Theorem 2.1.

Corollary 2.3. *Let k, M, and n be defined as in Theorem* 2.1. *Let T be the set of primes p_i such that $p_i \mid n$ and* $\gcd((p_i - 1)p_i^{\alpha_i - 1}, k) = p_i^{\alpha_i - 1}$. *If T is nonempty, let $n_T = \prod_{p_i \in T} p_i$ and let m be a positive integer such that* $\mathrm{rad}(m) = n_T$ *and $m \mid n$. Then $G(n, k)$ is symmetric of order M if and only if $G(m, k)$ is symmetric of order M.*

Theorem 2.4 given below follows from Theorems 3.1 and 5.1 of [2] and generalizes Theorem 5.1 (ii) in [10].

Theorem 2.4. *Let $k \geq 2$ and $n = 2^\alpha n_1$, where $\alpha \geq 0$ and $n_1 \geq 1$ is odd. Then $G(n, k)$ is symmetric of order* 2 *if and only if condition (i) holds and one of conditions (ii)–(vi) holds:*

(i) $\alpha \geq 1$,
(ii) $\alpha = 1$, $k \geq 2$,
(iii) $\alpha = 2$, $2 \mid k$,
(iv) $\alpha \geq 3$, $2^{\alpha-2} \mid k$, $k > 2$,
(v) $\alpha = 4$, $k = 2$,
(vi) $\alpha = 5$, $k = 4$.

Moreover, $G(2^\alpha n_1, k)$ is symmetric of order 2 *if and only if $G(2^\alpha, k)$ is symmetric of order* 2.

Remark 2.5. We note that the digraph $G(14,2)$ in Figure 4 is an example to Theorem 2.4 (ii), the digraph $G(12,2)$ in Figure 6 is an example to Theorem 2.4 (iii), and the digraph $G(16,2)$ in Figure 5 is an example to Theorem 2.4 (v).

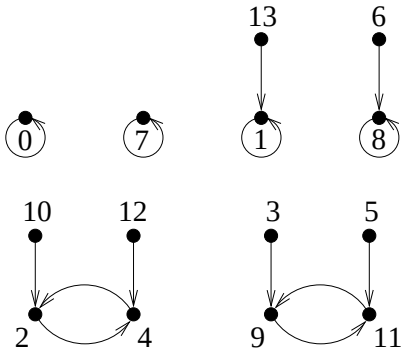

FIGURE 4. The symmetric iteration digraph $G(14,2)$ of order 2.

Definition 2.6. The digraph $G(n,k)$ is *semiregular* if there exists a positive integer d such that $\text{indeg}_n^k(a) = 0$ or d for all vertices $a \in G(n,k)$.

Semiregular digraphs are given in Figures 3 and 5. The digraphs in the remaining figures are not semiregular. We note that the definition of a semiregular graph includes the case in which the digraph $G(n,k)$ is regular, that is, all the vertices in the digraph have the same indegree.

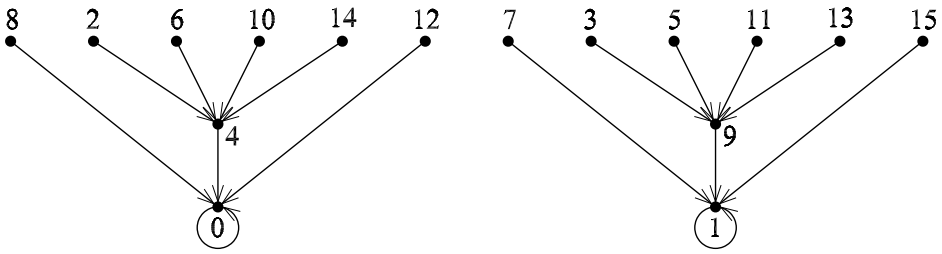

FIGURE 5. The symmetric and semiregular iteration digraph $G(16,2)$ of order 2.

In [3], Deng and Yuan show that there is a close link between symmetric and semiregular digraphs. The following theorem is a special case of results given in Theorem 2.4 of [8] and Theorem 4.4 of [9].

Theorem 2.7. *Suppose that p is an odd prime and $\alpha \geq 1$.*

(i) *$G(p^\alpha, k)$ is semiregular if and only if* $\gcd((p-1)p^{\alpha-1}, k) = p^{\alpha-1}$.
(ii) *$G(2^\alpha, k)$ is semiregular if and only if one of the conditions (ii)–(vi) in Theorem* 2.4 *holds.*

We have the following corollaries to Theorem 2.1 and 2.4, respectively, which relate symmetric digraphs to semiregular digraphs.

Corollary 2.8. *Consider the digraph $G(n,k)$, where n has the factorization given in (1.2). Suppose that M is square free and has an odd prime divisor and $M \mid n$. Then $G(n,k)$ is symmetric of order M only if $G(p_i^{\alpha_i},k)$ is semiregular for each prime p_i such that $p_i \mid M$.*

Corollary 2.9. *Let $n = 2^\alpha n_1$, where $\alpha \geq 1$ and $n_1 \geq 1$ is odd. Then $G(2^\alpha n_1,k)$ is symmetric of order 2 if and only if $G(2^\alpha,k)$ is semiregular if and only if $G(2^\alpha,k)$ is symmetric of order 2.*

The following examples show that the condition given in Corollary 2.8 for $G(n,k)$ to be symmetric is necessary, but not sufficient. We see by Theorem 2.7 (i) and Theorem 2.1 (ii) that $G(5,3)$ is regular but not symmetric of order M for any $M \geq 2$. Similarly, we find that $G(25,15)$ is semiregular, but not regular and not symmetric of order M for any $M \geq 2$.

The next theorem demonstrates that the classification of symmetric digraphs $G(n,k)$ of order M given by Deng and Yuan in Theorems 2.1 and 2.4 is in fact complete.

Theorem 2.10. *There are no symmetric digraphs $G(n,k)$ of order 2^s for $s \geq 2$.*

A proof of Theorem 2.10 will be given in Section 9.

Corollary 2.11 below follows from Theorems 2.1, 2.4, and 2.10.

Corollary 2.11. *There exists a symmetric digraph $G(n,k)$ of order $M \geq 2$ if and only if M is square free.*

3. Two Special Subdigraphs of $G(n,k)$

We specify 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 on the remaining vertices not coprime with n. We observe that $G_1(n,k)$ and $G_2(n,k)$ are disjoint and that $G(n,k) = G_1(n,k) \cup G_2(n,k)$, that is, no edge goes between $G_1(n,k)$ and $G_2(n,k)$. Since $\gcd(a,n) = 1$ if and only if $\gcd(a^k,n) = 1$, it follows that both $G_1(n,k)$ and $G_2(n,k)$ are unions of components of $G(n,k)$. For example, the second component of Figure 6 is $G_1(12,2)$ whereas the remaining three components make up $G_2(12,2)$. It is clear that 0 is always a fixed point of $G_2(n,k)$. If $n > 1$, then 1 and $n-1$ are always vertices of $G_1(n,k)$.

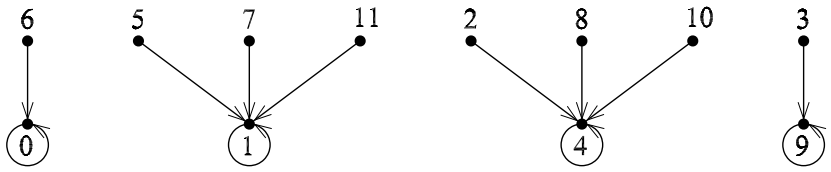

Figure 6. The symmetric iteration digraph $G(12,2)$ of order 2.

We also specify two components in $G_1(n,k)$ and $G_2(n,k)$, which will be used in Section 9. These are C_1 containing the fixed point 1 and C_0 containing the fixed point 0, respectively. It is clear that if p is a prime and $\alpha \geq 1$, then $G_2(p^\alpha,k) = C_0$.

4. Properties of the Carmichael Lambda-Function

Before proceeding further, we need to review some properties of the Carmichael lambda-function $\lambda(n)$. Its definition is a modification of the definition of the Euler totient function $\phi(n)$.

Definition 4.1. Let n be a positive integer. Then the *Carmichael lambda-function* $\lambda(n)$ is defined as follows:

$$\begin{aligned}
\lambda(1) &= 1 = \phi(1),\\
\lambda(2) &= 1 = \phi(2),\\
\lambda(4) &= 2 = \phi(4),\\
\lambda(2^k) &= 2^{k-2} = \frac{1}{2}\phi(2^k) \text{ for } k \geq 3,\\
\lambda(p^k) &= (p-1)p^{k-1} = \phi(p^k) \text{ for any odd prime } p \text{ and } k \geq 1,\\
\lambda(p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}) &= \operatorname{lcm}[\lambda(p_1^{k_1}),\ \lambda(p_2^{k_2}),\ldots,\ \lambda(p_r^{k_r})],
\end{aligned}$$

where $p_1,\ p_2,\ldots,\ p_r$ are distinct primes and $k_i \geq 1$ for all $i \in \{1,\ldots,r\}$.

It immediately follows from Definition 4.1 that

$$\lambda(n) \mid \phi(n)$$

for all n and that $\lambda(n) = \phi(n)$ if and only if $n \in \{1,\ 2,\ 4,\ q^k,\ 2q^k\}$, where q is an odd prime and $k \geq 1$.

The following theorem generalizes the well-known Euler's Theorem which says (see [7, p. 20]) that $a^{\phi(n)} \equiv 1 \pmod{n}$ if and only if $\gcd(a,n) = 1$. It shows that $\lambda(n)$ is the smallest possible universal order modulo n.

Theorem 4.2. (Carmichael) *Let $a, n \in \mathbb{N}$. Then*

$$a^{\lambda(n)} \equiv 1 \pmod{n}$$

if and only if $\gcd(a,n) = 1$. *Moreover, there exists an integer g such that*

$$\operatorname{ord}_n g = \lambda(n).$$

For the proof, see [7, p. 21].

5. Results on Cycles

Consider a digraph $G(n,k)$ and factorize $\lambda(n)$ as

$$\lambda(n) = uv, \tag{5.1}$$

where u is the largest divisor of $\lambda(n)$ relatively prime to k. We will need the following theorems to prove our main results.

Theorem 5.1. *There exists a t-cycle in $G_1(n,k)$ if and only if*

$$t = \operatorname{ord}_d k$$

for some factor d of u. Moreover, the longest cycle in $G_1(n,k)$ has length equal to $\operatorname{ord}_u k$.

This was proved in [13, pp. 232–233].

Theorem 5.2. ([11, Theorem 7.1]) *If there exists a t-cycle in $G_2(n,k)$, then there exists a t-cycle in $G_1(n,k)$.*

Theorem 5.3. ([10, Theorem 6.6]) *Let n have the factorization given in* (1.2) *and let t be a positive integer. Then*

$$A_t(G(n,k)) = \frac{1}{t}\left[\prod_{i=1}^{r}(\delta_i \gcd(\lambda(p_i^{\alpha_i}), k^t - 1) + 1) - \sum_{d|t,\, d\neq t} dA_d(G(n,k))\right], \tag{5.2}$$

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

6. An Example to Theorem 2.1

Looking at Figure 2, we see that $G(39,3) = G(3 \cdot 13, 3)$ is symmetric of order 3. Making use of part (ii) of Theorem 2.1, we find that the digraph $G(39,3)$ satisfies condition (iv)(a) of Theorem 2.1. However, it is not immediately clear that there exists a digraph $G(n,k)$ which actually satisfies the hypotheses of part (iv)(b) of Theorem 2.1. Example 6.1 given below shows that this can indeed occur. This is a slightly changed version of Example 38 in [5].

Example 6.1. Let $n = p_1^{\alpha_1} p_2$, where $p_1 = 7$, $\alpha_1 = 2$ and $p_2 = 103$, and let $k = 35$. Consider the digraph

$$G(n,k) = G(7^2 \cdot 103, 35) = G(5047, 35).$$

We shall demonstrate that condition (iv)(b) of Theorem 2.1 is satisfied, and thus, $G(7^2 \cdot 103, 35)$ is symmetric of order 7.

We first note that $p_1 = 7 \mid M = 7$, while $p_2 = 103 \nmid M = 7$,

$$\gcd((p_1 - 1)p_1^{\alpha_1 - 1}, k) = \gcd(42, 35) = 7 = p_1^{\alpha_1 - 1},$$

and

$$\gcd(p_2 - 1, k) = \gcd(102, 35) = p_2^0 = 1.$$

We next observe that $G(7,35)$ is not symmetric of order 7 by Theorem 2.1 (ii), since $k = 35 \not\equiv 1 \pmod 7$. We further note that

$$\operatorname{ord}_{p_1 - 1} k = \operatorname{ord}_6 35 = 2 \tag{6.1}$$

and

$$\operatorname{ord}_{p_2 - 1} k = \operatorname{ord}_{102} 35 = 2. \tag{6.2}$$

Thus, it follows from (6.2) and Theorems 5.1 and 5.2 that the longest cycle in $G(103,35)$ has length 2. Thus, $G(103,35)$ only has t-cycles for $t = 1$ or $t = 2$. By Theorem 5.3,

$$A_1(G(103,35)) = \gcd(102, 34) + 1 = 35.$$

Hence,

$$p_1 = 7 \mid A_1(G(p_2, k)) = 35.$$

We also note that when $t = 2$, then

$$\operatorname{ord}_{p_1 - 1} k = 2 \mid t = 2.$$

Moreover, $A_t(G(103,35)) = 0$ when $t > 2$. We now see that $G(7^2 \cdot 103, 35)$ indeed satisfies condition (iv)(b) of Theorem 2.1.

7. Digraph Products

Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$, $n_1 > 1$, and $n_2 \geq 1$. We show that we can represent $G(n,k)$ as a product of the two digraphs $G(n_1,k)$ and $G(n_2,k)$. By the Chinese Remainder Theorem, we can uniquely represent each vertex $a \in G(n,k)$ as the ordered pair (a_1, a_2), where $0 \leq a_1 \leq n_1 - 1$, $0 \leq a_2 \leq n_2 - 1$, $a \equiv a_1 \pmod{n_1}$, and $a \equiv a_2 \pmod{n_2}$. For $a = (a_1, a_2)$ define

$$a^k = (a_1, a_2)^k = (a_1^k, a_2^k), \tag{7.1}$$

where we assume that a^k, a_1^k, and a_2^k are all reduced modulo n, n_1, and n_2, respectively.

Let $G(n_1,k) \times G(n_2,k)$ denote the digraph whose vertices are the ordered pairs (a_1, a_2), where $0 \leq a_1 \leq n_1 - 1$ and $0 \leq a_2 \leq n_2 - 1$. In addition, $\langle (a_1, b_1), (a_2, b_2) \rangle$ is a directed edge of $G(n_1,k) \times G(n_2,k)$ if and only if $a_2 \equiv a_1^k \pmod{n_1}$ and $b_2 \equiv b_1^k \pmod{n_2}$ (see [4]).

From (7.1), it follows that

$$G(n,k) \cong G(n_1,k) \times G(n_2,k)$$

and for simplicity we write

$$G(n,k) = G(n_1,k) \times G(n_2,k). \tag{7.2}$$

If n has the factorization given in (1.2), it follows from (7.2) that

$$G(n,k) = G(p_1^{\alpha_1}, k) \times G(p_2^{\alpha_2}, k) \times \cdots \times G(p_r^{\alpha_r}, k).$$

8. Further Results

We will need the following results in order to prove our main results on symmetric digraphs.

Theorem 8.1. *Let p be a prime and $\alpha \geq 1$. Let a be a vertex of positive indegree in $G_1(p^\alpha, k)$. Then*

$$\operatorname{indeg}_{p^\alpha}^k(a) = \varepsilon \gcd(\lambda(p^\alpha), k),$$

where $\varepsilon = 2$ if $2 \mid k$ and $8 \mid p^\alpha$, and $\varepsilon = 1$ otherwise.

This is proved in [13, pp. 231–232].

Lemma 8.2. ([10, Lemma 3.2]) *Let p be a prime and let $\alpha \geq 1$ and $k \geq 2$ be integers. Then*

$$\operatorname{indeg}_{p^\alpha}^k(0) = p^{\alpha - \lceil \alpha/k \rceil}.$$

Lemma 8.3. ([6, Lemma 5]) *Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$. Let $a = (a_1, a_2)$ be a vertex in $G(n,k) = G(n_1,k) \times G(n_2,k)$. Then*

$$\operatorname{indeg}_n^k(a) = \operatorname{indeg}_{n_1}^k(a_1) \operatorname{indeg}_{n_2}^k(a_2).$$

Theorem 8.4. ([10, Theorem 6.7]) *Let $c = (c_1, c_2)$ be a vertex in $G(n,k) = G(n_1,k) \times G(n_2,k)$. Then c is a cycle vertex in $G(n,k)$ if and only if c_i is a cycle vertex in $G(n_i,k)$ for $i = 1, 2$.*

Theorem 8.5. ([10, Theorem 6.8]) *Assume that $n = n_1 n_2$ and $\gcd(n_1, n_2) = 1$. Let $J(n_1,k)$ be a union of components of $G(n_1,k)$ and let $L(n_2,k)$ be a union of components of $G(n_2,k)$. Then $J(n_1,k) \times L(n_2,k)$ is a union of components of $G(n,k) = G(n_1,k) \times G(n_2,k)$. Moreover, if*

$$J(n_1,k) = \bigcup_{i=1}^{m_1} E_i(n_1,k)$$

and

$$L(n_2,k)=\bigcup_{j=1}^{m_2}F_j(n_2,k),$$

where $E_i(n_1,k)$ *and* $F_j(n_2,k)$ *are distinct components of* $G(n_1,k)$ *and* $G(n_2,k)$*, respectively, then*

$$J(n_1,k)\times L(n_2,k)=\bigcup_{i,j}E_i(n_1,k)\times F_j(n_2,k), \tag{8.1}$$

where the union in (8.1) *is a disjoint union.*

Lemma 8.6. ([6, Lemma 1]) *Let* $n=n_1n_2$*, where* $\gcd(n_1,n_2)=1$*. Let* $E(n_1,k)$ *be a component of* $G(n_1,k)$ *and let* $J(n_2,k)$ *be a component of* $G(n_2,k)$*. Let* s *be the length of* $E(n_1,k)$*'s cycle and let* t *be the length of* $J(n_2,k)$*'s cycle. Then* $D(n,k)=E(n_1,k)\times J(n_2,k)$ *is a subdigraph of* $G(n,k)$ *consisting of* $\gcd(s,t)$ *components each having cycles of length* $\operatorname{lcm}(s,t)$*.*

9. Proof of the Main Theorem 2.10

Proof. We note that if $G(n,k)$ is symmetric of order 2^s, $s\geq 1$, then it is symmetric of order 2. We now define an equivalence relation on the set of components of $G(n,k)$. We say that two components in $G(n,k)$ are in the same equivalence class if and only if they are isomorphic. Given any digraph $G(n,k)$ that is symmetric of order 2, we will find an equivalence class containing exactly two members of components of $G(n,k)$. It will then follow that no digraph $G(n,k)$ can be symmetric of order 2^s for $s\geq 2$.

Suppose that $G(n,k)$ is symmetric of order 2. Let $n=2^\alpha n_1$, where $n_1\geq 1$ is odd. By Proposition 1.2, $\alpha\geq 1$. If $\alpha=1$, then $G(n,k)$ cannot be symmetric of order 2^s for $s>1$ by Proposition 1.2.

From here on, we suppose that $\alpha\geq 2$. Then by Theorem 2.4, $2\mid k$. Since $\lambda(2^\alpha)\mid 2^{\alpha-1}$, it follows from Theorem 4.2 that if $a\in G_1(2^\alpha,k)$, then $a^{k^i}\equiv 1 \pmod{2^\alpha}$ when $i\geq \alpha-1$. Hence, $G(2^\alpha,k)$ consists of exactly the two components $C_1=G_1(2^\alpha,k)$ and $C_0=G_2(2^\alpha,k)$, where C_1 and C_0 are the components in $G(2^\alpha,k)$ containing the fixed points 1 and 0, respectively. Moreover, it follows from Theorem 2.4 that $G(2^\alpha,k)$ is symmetric of order 2, which implies that $C_1\cong C_0$. In particular, if $n_1=1$, then $G(n,k)=G(2^\alpha,k)$ is symmetric of order 2, but is not symmetric of order 2^s for $s>1$.

We assume from now on that $n_1>1$. Let

$$n_1=\prod_{i=1}^{m}p_i^{\beta_i}.$$

Consider the subdigraph of $G(n_1,k)$ given by the digraph product

$$A=\prod_{i=1}^{m}G_2(p_i^{\beta_i},k).$$

Noting that $G_2(p_i^{\beta_i},k)$ consists of a single component containing the fixed point 0 for $i=1,2,\ldots,m$, we see by Theorem 8.4 that A consists of a unique component having the fixed point $a=(0,0,\ldots,0)$. It follows from Lemmas 8.2 and 8.3 that the indegree of a is odd, since

$$\operatorname{indeg}_{n_1}^k(a)=\prod_{i=1}^{m}p_i^{\beta_i-\lceil\frac{\beta_i}{k}\rceil}.$$

Let B be the union of all components in $G(n_1, k)$ that are distinct from A, that is, $G(n_1, k) = A \cup B$. Let $b = (b_1, b_2, \ldots, b_m)$ be a cycle vertex in B. Then there exists j, $1 \le j \le m$, such that $b_j \in G_1(p_j^{\beta_j}, k)$. Let $q_j = p_j^{\beta_j}$. Noting that p_j is odd and k is even, it follows from Theorem 8.1 that $\operatorname{indeg}_{q_j}^k(b_j)$ is even. Hence, by Lemma 8.3, we have $2 \mid \operatorname{indeg}_{n_1}^k(b)$.

Let $e = \alpha - \lceil \frac{\alpha}{k} \rceil$. Then

$$\operatorname{indeg}_{2^\alpha}^k(0) = 2^e = \operatorname{indeg}_{2^\alpha}^k(1).$$

By Theorem 8.5,

$$G(n, k) = G(2^\alpha, k) \times G(n_1, k) = (C_0 \times A) \cup (C_0 \times B) \cup (C_1 \times A) \cup (C_1 \times B).$$

It follows from Lemma 8.6 that $C_0 \times A$ and $C_1 \times A$ each consists of a single component containing the fixed points $a_0 = (0, 0, \ldots, 0)$ and $a_1 = (1, 0, \ldots, 0)$, respectively. Since $C_0 \cong C_1$, we find that $C_0 \times A \cong C_1 \times A$. Let b^* be any cycle vertex in $(C_0 \times B) \cup (C_1 \times B)$. We see by Lemma 8.3 that

$$2^e \| \operatorname{indeg}_n^k(a_0), \quad 2^e \| \operatorname{indeg}_n^k(a_1), \quad \text{and} \quad 2^{e+1} \mid \operatorname{indeg}_n^k(b^*).$$

Hence, the equivalence class of the component $C_0 \times A$ in $G(n, k)$ contains exactly two members, namely $C_0 \times A$ and $C_1 \times A$. Therefore, $G(n, k)$ is not symmetric of order 2^s for $s > 1$. □

References

[1] W. Carlip and M. Mincheva, *Symmetry of iteration digraphs*, Czechoslovak Math. J., **58** (2008), 131–145.

[2] G. Deng and P. Yuan, *Symmetric digraphs from powers modulo n*, Open J. Discrete Math., **1** (2011), 103–107.

[3] G. Deng and P. Yuan, *On the symmetric digraphs from powers modulo n*, Discrete Math., **312** (2012), 720–728.

[4] B. Hartnell and D. Rall, *Domination in Cartesian products: Vizing's conjecture*, In Domination in Graphs – Advanced Topics (Ed. T. W. Haynes, S. T. Hedetniemi, and P. J. Slater), Dekker, New York, 1998, 163–189.

[5] S. M. Husnine, U. Ahmad, and L. Somer, *On symmetries of power digraphs*, Util. Math., **85** (2011), 257–271.

[6] J. Kramer-Miller, *Structural properties of power digraphs modulo n*, Proc. of the 2009 Midstates Conference on Undergraduate Research in Computer Science and Mathematics, Oberlin, 2009, 40–49.

[7] M. Křížek, F. Luca, and L. Somer, *17 Lectures on Fermat Numbers: From Number Theory to Geometry*, CMS Books in Mathematics, Vol. 9, Springer-Verlag, New York, 2001.

[8] L. Somer and M. Křížek, *On a connection of number theory with graph theory*, Czechoslovak Math. J., **54** (2004), 465–485.

[9] L. Somer and M. Křížek, *On semiregular digraphs of the congruence* $x^k \equiv y \pmod n$, Comment. Math. Univ. Carolin., **48** (2007), 41–58.

[10] L. Somer and M. Křížek, *On symmetric digraphs of the congruence* $x^k \equiv y \pmod n$, Discrete Math., **309** (2009), 1999–2009.

[11] L. Somer and M. Křížek, *The structure of digraphs associated with the congruence* $x^k \equiv y \pmod n$, Czechoslovak Math. J., **61** (2011), 337–358.

[12] L. Szalay, *A discrete iteration in number theory (in Hungarian)*, BDTF Tud. Közl. VIII. Természettudományok 3., Szombathely, 1992, 71–91.

[13] B. Wilson, *Power digraphs modulo n*, The Fibonacci Quarterly, **36.3** (1998), 229–239.

MSC2010: 11A07, 11A15, 05C20

Department of Mathematics, Catholic University of America, Washington, D.C. 20064
E-mail address: somer@cua.edu

Institute of Mathematics, Academy of Sciences, Žitná 25, CZ – 115 67 Prague 1, Czech Republic
E-mail address: krizek@math.cas.cz