Characterization of power digraphs modulo n

Uzma Ahmad, Syed Husnine

Abstract. A power digraph modulo n, denoted by $G(n,k)$, is a directed graph with $Z_n = \{0,1,\dots,n-1\}$ as the set of vertices and $E = \{(a,b) : a^k \equiv b \pmod{n}\}$ as the edge set, where n and k are any positive integers. In this paper we find necessary and sufficient conditions on n and k such that the digraph $G(n,k)$ has at least one isolated fixed point. We also establish necessary and sufficient conditions on n and k such that the digraph $G(n,k)$ contains exactly two components. The primality of Fermat number is also discussed.

Keywords: iteration digraph, isolated fixed points, Charmichael lambda function, Fermat numbers, Regular digraphs

Classification: 11A07, 11A15, 20K01, 05C20, 11A51

1. Introduction

Power digraphs provide a link between graph theory and number theory. By using graph theoretic properties of Power digraphs, we can infer many number theoretic properties of the congruence $a^k \equiv b \pmod{n}$. Some characteristics of power digraph $G(n,k)$, where n and k are arbitrary positive integers, have been investigated by C. Lucheta et al. [2], Wilson [1], Somer and Křížek [7], [8], [9], [10], Kramer-Miller [5], S.M. Husnine, Uzma and Somer [15]. We continue their work by generalizing previous results. The existence of isolated fixed point for $k = 2$ is studied in [7] and for $k = 3$ in [16]. In this paper we study the existence of isolated fixed points in $G(n,k)$ for any positive integers n and k. We obtain necessary and sufficient conditions on n and k such that the digraph $G(n,k)$ has at least one isolated fixed point. We also establish necessary and sufficient conditions on n and k such that the digraph $G(n,k)$ contains exactly two components.

Let $g : Z_n \to Z_n$ be any function, where $Z_n = \{0,1,\dots n-1\}$ and $n \geq 1$. An iteration digraph defined by g is a directed graph whose vertices are the elements from Z_n, such that there exists exactly one edge from x to y if and only if $g(x) \equiv y \pmod{n}$. In this paper, we consider $g(x) \equiv x^k \pmod{n}$. For the fixed values of n and k the iteration digraph is represented by $G(n,k)$, where $k \geq 2$ and is called power digraph modulo n. Each $x \in G(n,k)$ corresponds uniquely to a residue modulo n.

The research of the first author is partially supported by the Higher Education Commission, Pakistan.

A component of $G(n,k)$ is a subdigraph which is the largest connected subgraph of the associated nondirected graph. The indegree of x, denoted by $\mathrm{indeg}_n(x)$ is the number of directed edges coming into a vertex x, and the number of edges coming out of x is referred to as the outdegree of x denoted by $\mathrm{outdeg}_n(x)$.

A digraph $G(n,k)$ is said to be regular if every vertex of $G(n,k)$ has same indegree. We note that a regular digraph does not contain any vertex of indegree 0. We can see that a digraph $G(n,k)$ is regular if and only if each component of $G(n,k)$ is a cycle and for each vertex x, $\mathrm{indeg}_n(x) = \mathrm{outdeg}_n(x) = 1$. A digraph $G(n,k)$ is said to be semi-regular of degree j if every vertex of $G(n,k)$ has indegree j or 0.

A cycle is a directed path from a vertex a to a, and a cycle is a z-cycle if it contains precisely z vertices. A cycle of length one is called a fixed point. It is clear that 0 and 1 are fixed points of $G(n,k)$. Since each vertex has outdegree one, it follows that each component contains a unique cycle. A vertex a is said to be an isolated fixed point if it is a fixed point and there does not exist a non cycle vertex b such that $b^k \equiv a \pmod{n}$. In other words a has indegree 1.

The Carmichael lambda-function $\lambda(n)$ is defined as the smallest positive integer such that $x^{\lambda(n)} \equiv 1 \pmod{n}$ for all x relatively prime to n. The values of the Carmichael lambda-function $\lambda(n)$ are

$$\begin{aligned}
\lambda(1) &= 1, \\
\lambda(2) &= 1, \\
\lambda(4) &= 2, \\
\lambda(2^k) &= 2^{k-2} \quad \text{for } k \geq 3, \\
\lambda(p^k) &= (p-1)p^{k-1},
\end{aligned}$$

for any odd prime p and $k \geq 1$ and

$$\lambda(p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}) = \mathrm{lcm}(\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \ldots, \lambda(p_r^{e_r})),$$

where $p_1, p_2, \ldots, p_r$ are distinct primes and $e_i \geq 1$ for all i.

The subdigraph of $G(n,k)$, containing all vertices relatively prime to n, is denoted by $G_1(n,k)$ and the subdigraph containing all vertices not relatively prime to n is denoted by $G_2(n,k)$. It is obvious that $G_1(n,k)$ and $G_2(n,k)$ are disjoint and there is no edge between $G_1(n,k)$ and $G_2(n,k)$ and $G(n,k) = G_1(n,k) \cup G_2(n,k)$.

Let $n = ml$, where $\gcd(m,l) = 1$. We can easily see with the help of the Chinese Remainder Theorem that corresponding to each vertex $x \in G(n,k)$, there is an ordered pair (x_1, x_2), where $0 \leq x_1 < m$ and $0 \leq x_2 < l$ and x^k corresponds to (x_1^k, x_2^k). The product of digraphs, $G(m,k)$ and $G(l,k)$ is defined as follows: a vertex $x \in G(m,k) \times G(l,k)$ is an ordered pair (x_1, x_2) such that $x_1 \in G(m,k)$ and $x_2 \in G(l,k)$. Also there is an edge from (x_1, x_2) to (y_1, y_2) if and only if there is an edge from x_1 to y_1 in $G(m,k)$ and there is an edge from x_2 to y_2 in $G(l,k)$. This implies that (x_1, x_2) has an edge leading to (x_1^k, x_2^k). We then see that $G(n,k) \cong G(m,k) \times G(l,k)$. We can further assert that if $\omega(n)$ denotes the number of distinct prime divisors of n and

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \tag{1.1}$$

where $p_1 < p_2 < \cdots < p_r$ and $e_i > 0$, i.e. $r = \omega(n)$, then

$$G(n,k) \cong G(p_1^{e_1},k) \times G(p_2^{e_2},k) \times \cdots \times G(p_r^{e_r},k). \tag{1.2}$$

Let $N(n,k,b)$ denote the number of incongruent solutions of the congruence $x^k \equiv b \pmod{n}$. Then $N(n,k,b) = \operatorname{indeg}_n(b)$ and by the Chinese Remainder Theorem, we have

$$N(n,k,b) = \operatorname{indeg}_n(b) = \prod_{i=1}^{r} N(p_i^{e_i},k,b). \tag{1.3}$$

2. Some previous results

Theorem 2.1 (Carmichael [14]). *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*

$$\operatorname{ord}_n a = \lambda(n),$$

where $\operatorname{ord}_n g$ *denotes the multiplicative order of g modulo n.*

Lemma 2.2 ([1]). *Let $n = n_1 n_2$, where $\gcd(n_1,n_2) = 1$ and $a = (a_1,a_2)$ be a vertex in $G(n,k) \cong G(n_1,k) \times G(n_2,k)$. Then $N(n,k,a) = N(n_1,k,a_1) \cdot N(n_2,k,a_2)$.*

Theorem 2.3 ([1]). *Let n be an integer having factorization as given in* (1.1) *and a be a vertex of $G_1(n,k)$. Then*

$$\operatorname{indeg}_n(a) = N(n,k,a) = \prod_{i=1}^{r} N(p_i^{e_i},k,a) = \prod_{i=1}^{r} \varepsilon_i \gcd(\lambda(p_i^{e_i}),k),$$
$$\text{or} \quad N(n,k,a) = 0,$$

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

Theorem 2.4 ([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, where $\lambda(n) = uv$ and u is the highest factor of $\lambda(n)$ relatively prime to k.*

Theorem 2.5 ([9]). *Let $n \geq 1$ and $k \geq 2$ be integers. Then*

1. *$G_1(n,k)$ is regular if and only if* $\gcd(\lambda(n),k) = 1$;
2. *$G_2(n,k)$ is regular if and only if either n is square free and* $\gcd(\lambda(n),k) = 1$ *or $n = p$, where p is prime;*
3. *$G(n,k)$ is regular if and only if n is square free and* $\gcd(\lambda(n),k) = 1$.

Lemma 2.6 ([10]). *Let p be a prime and $\alpha \geq 1$, $k \geq 2$ be integers. Then* $N(p^\alpha, k, 0) = p^{\alpha - \lceil \frac{\alpha}{k} \rceil}$.

Theorem 2.7 ([10]). *Let n be an integer having factorization as given in* (1.1). *Then*

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

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

Theorem 2.8 ([10]). *Let $n = n_1 n_2$, where* $\gcd(n_1, n_2) = 1$ *and $a = (a_1, a_2)$ be a vertex in $G(n,k) \cong G(n_1,k) \times G(n_2,k)$. Then a is a cycle vertex if and only if a_1 is a cycle vertex in $G(n_1,k)$ and a_2 is a cycle vertex in $G(n_2,k)$.*

Lemma 2.9 ([5]). *Let $n = n_1 n_2$, where* $\gcd(n_1, n_2) = 1$ *and $J(n_1,k)$ be a component of $G(n_1,k)$ and $L(n_2,k)$ be a component of $G(n_2,k)$. Suppose s is the length of $L(n_2,k)$'s cycle and let t be the length of $J(n_1,k)$'s cycle. Then $C(n,k) \cong J(n_1,k) \times L(n_2,k)$ is a subdigraph of $G(n,k)$ consisting of* $\gcd(s,t)$ *components, each having cycles of length* $\operatorname{lcm}(s,t)$.

3. Existence of isolated fixed points

We know that if n is square free then 0 is an isolated fixed point of $G(n,k)$. Now if $G_1(n,k)$ is regular then 1 is an isolated fixed point of $G(n,k)$. We also know that for $k = 1$, the digraph $G(n,k)$ consists of isolated fixed points only. However, the criteria for the existence of isolated point for other cases are yet not studied by any other author. In the following section we attempt to sort out this problem for the case when $G_1(n,k)$ is not regular and n is not square free.

Lemma 3.1. *Let $n = ml$, where* $\gcd(m,l) = 1$ *and $x = (x_1, x_2)$ be a vertex in $G(n,k) \cong G(m,k) \times G(l,k)$. Then x is an isolated fixed point of $G(n,k)$ if and only if x_1 and x_2 are isolated fixed points of $G(m,k)$ and $G(l,k)$, respectively.*

Proof: Let x be an isolated fixed point. Then x is cycle of length one and $N(n,k,x) = 1$. From Theorems 2.8 and 2.9, x_1 and x_2 are fixed points of $G(m,k)$ and $G(l,k)$, respectively. Also by Theorem 2.2, $N(m,k,x_1) = 1 = N(l,k,x_2)$. Hence, x_1 and x_2 are isolated fixed points in $G(m,k)$ and $G(l,k)$, respectively. Converse is similar. □

Theorem 3.2. *The power digraph $G(n,k)$, where n is defined as in* (1.1) *and $k \geq 2$, has at least one isolated fixed point if and only if either $e_i = 1$ or* $\gcd(\lambda(p_i^{e_i}), k) = 1$ *for all $1 \leq i \leq r$ in prime factorization of n.*

Proof: Suppose $G(n,k)$ has an isolated fixed point a. For all $p_i^{e_i} \parallel n$, where $1 \leq i \leq r$, either $e_i = 1$ or $e_i > 1$. Suppose to the contrary that there exists $1 \leq j \leq r$ such that $\gcd(\lambda(p_j^{e_j}), k) \neq 1$ and $e_j > 1$. Since a is a fixed point, by Theorems 2.8, Theorem 2.9 and equation (1.2) there exist fixed points $a_i \in G(p_i^{e_i}, k)$ for all $1 \le i \le r$ such that $a = (a_1, \dots, a_j, \dots, a_r)$. Now from Theorem 2.2, we can write

$$N(n,k,a) = \prod_{i=1}^{r} N(n,k,a_i). \tag{3.1}$$

If $a_j \in G_1(p_j^{e_j}, k)$ then $N(p_j^{e_j}, k, a_j) = \gcd(\lambda(p_j^{e_j}), k) \neq 1$. Thus in this case from equation (3.1), $N(n,k,a) \neq 1$, which contradicts the fact that a is an isolated fixed point. Hence, we may suppose $a_j \in G_2(p_j^{e_j}, k)$. Now we know that $G_2(p_j^{e_j}, k)$ consists of one component containing fixed point 0. Thus $a_j \equiv 0 \pmod{p_j^{e_j}}$. From Lemma 2.6, $N(p_j^{e_j}, k, a_j) = N(p_j^{e_j}, k, 0) = p_j^{e_j - \lceil \frac{e_j}{k} \rceil}$. Since $e_j > 1$ and $k \geq 2$, $N(p_j^{e_j}, k, a_j) \neq 1$. Now from equation (3.1) it follows that $N(n,k,a) \neq 1$ which again is a contradiction.

Conversely, suppose for all $p_i^{e_i} \parallel n$, where $1 \le i \le r$, either $e_i = 1$ or $\gcd(\lambda(p_i^{e_i}), k) = 1$. If $e_i = 1$, 0 is an isolated fixed point in $G(p_i, k)$. If $e_i > 1$ and $\gcd(\lambda(p_i^{e_i}), k) = 1$, 1 is an isolated point in $G(p_i^{e_i}, k)$. Now consider $a = (a_1, a_2, \dots, a_r)$, where

$$\begin{aligned} a_i &= 0 \quad \text{if } e_i = 1, \\ &= 1 \quad \text{if } e_i > 1. \end{aligned}$$

From Lemma 3.1, a is an isolated fixed point of $G(n,k)$. □

Corollary 3.3. *Suppose k is even and $n > 2$ is defined as in* (1.1). *The power digraph $G(n,k)$ has at least one isolated fixed point if and only if n is square free.*

PROOF: We know that $2 \mid \lambda(p_i^{e_i})$ for all $1 \le i \le r$. Since k is even, $\gcd(\lambda(p_i^{e_i}), k) \neq 1$ for any $1 \le i \le r$. Hence, from Theorem 3.2, $e_i = 1$ for all $1 \le i \le r$ which implies n is square free.

Conversely, if n is square free, 0 is an isolated fixed point of $G(n,k)$. □

Corollary 3.4. *Suppose $G_1(n,k)$ is not regular and n is not square free. The power digraph $G(n,k)$, where n is defined as in* (1.1) *and $k \geq 2$, has an isolated fixed point if and only if the following statements are satisfied.*

(1) *k must be odd.*
(2) *The sets $l = \{p_i^{e_i} \mid e_i > 1 \text{ and } \gcd(\lambda(p_i^{e_i}, k) = 1)\}$ and $m = \{p_j^{e_j} \mid e_j = 1\}$ are non empty. Also $G(n,k) \cong G(l,k) \times G(m,k)$.*
(3) *The digraph $G_1(m,k)$ is not regular.*

PROOF: Suppose $G(n,k)$ has an isolated fixed point a. If k is even then from Corollary 3.3, n is square free which is a contradiction. Now from Theorem 3.2, either $e_i = 1$ or $\gcd(\lambda(p_i^{e_i}), k) = 1$ for all $1 \le i \le r$ in the prime factorization of n. Since $G_1(n,k)$ is not regular and n is not square free, there must exist $1 \le s < r$ such that $e_i = 1$ for all $1 \le i \le s$ and $\gcd(\lambda(p_i^{e_i}), k) = 1$ for all $i > s$. Hence, the sets l and m are non empty. Since l and m are disjoint, from equation (1.2), we get $G(n,k) \cong G(l,k) \times G(m,k)$.

Now if $G_1(m,k)$ is regular then from equation (1.2) and Theorem 2.5, $G_1(n,k) = G_1(l,k) \times G_1(m,k)$ is also regular which is a contradiction.

Conversely, suppose all three conditions are true. Since l is non empty and $G_1(l,k)$ is regular, 1 is an isolated fixed point in $G(l,k)$. Again since m is nonempty, 0 is an isolated fixed point of $G_2(m,k)$. Thus from Lemma 3.1, $a = (1,0)$ is an isolated fixed point of $G(n,k) \cong G(l,k) \times G(m,k)$. □

Example 3.5. Let $n = 28 = 2^2 \cdot 7$ and $k = 15$. Here we can see that the sets $l = \{2^2\}$ and $m = \{7\}$ are non empty. Since $\gcd(\lambda(4), 15) = 1$ and $\gcd(\lambda(7), 15) = 3 \neq 1$, from Theorem 2.5, $G_1(l,k)$ is regular and $G_1(m,k)$ is not regular. Thus $G(28,15)$ satisfies conditions 1, 2 and 3 of Theorem 3.2. Hence, $G(28,15)$ contains an isolated fixed point. It is shown in Figure 1.

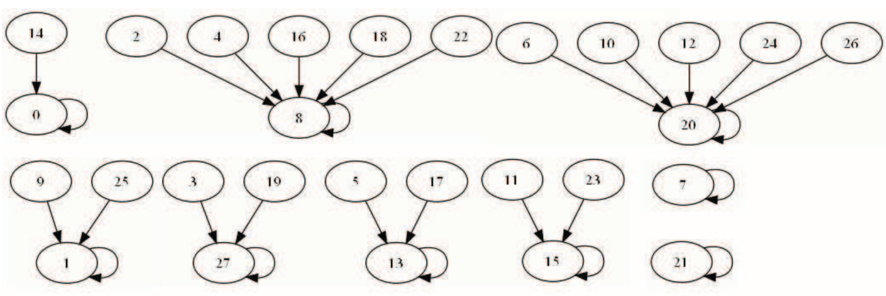

FIGURE 1. The isolated fixed points of G(28,15) are 7 and 21

4. Power digraphs of Fermat numbers

Theorem 4.1. *The power digraph $G(n,k)$, where $n > 2$ and $k \geq 2$ are positive integers exhibits the following properties:*

(1) *$G(n,k)$ consists of exactly two components containing fixed points 0 and 1,*
(2) *$G_1(n,k)$ is semi-regular of degree 2^d for some $d \geq 1$*

if and only if k is even and $n = 2^l$ or $n = F_m$, where $l \geq 2$, $m \geq 1$ are integers and $F_m = 2^{2^m} + 1$ is Fermat prime.

PROOF: Suppose that a power digraph $G(n,k)$ exhibits the above properties (1) and (2). Since 0 and 1 are fixed points of $G(n,k)$, $G_2(n,k)$ and $G_1(n,k)$ both consist of one component containing fixed points 0 and 1, respectively.

First suppose k is odd; then $2 \mid k-1$. Since $n > 2$, 2 divides $\lambda(p_i^{e_i})$ for all $1 \leq i \leq r$. Thus from Theorem 2.6, $A_1(G(n,k)) \geq 3$. This along with the fact that each component of $G(n,k)$ contains a unique cycle implies that the number of components of $G(n,k)$ is greater than or equal to 3 which contradicts (1).

We know that the Euler function $\phi(n)$ is a power of 2 if and only $n = 2^l F_{m_1} F_{m_2} \ldots F_{m_s}$. Also it is easy to show that $\phi(n) = 2^i$ if and only if $\lambda(n) = 2^j$, where

$j \leq i$. Now we claim that n must be of the form $2^l F_{m_1} F_{m_2} \dots F_{m_s}$, where $l \geq 0$ and F_{m_i} are Fermat primes for all i. For if $n \neq 2^l F_{m_1} F_{m_2} \dots F_{m_s}$ then $\lambda(n)$ is not a power of 2. Therefore, there exists an odd prime divisor p of $\lambda(n)$. Then by definition of $\lambda(n)$ there exists i, where $1 \leq i \leq r$ such that p is a prime divisor of $\lambda(p_i^{e_i})$. If $p \mid k$, by Theorem 2.3, either $N(n,k,a) = 0$ or $p \mid N(n,k,a)$ for all $a \in G_1(n,k)$ which contradicts (2). Thus we may suppose $p \nmid k$. Now p is a factor of $\lambda(n)$ which is relatively prime to k. Thus from Theorem 2.4 there exists a cycle of length t in $G_1(n,k)$ such that

$$k^t \equiv 1 \pmod{p}.$$

If $t = 1$ then $p \mid k - 1$. Now from Theorem 2.6, $A_1(G(n,k)) \geq p + 1$ which contradicts (1). Hence, we may suppose $t > 1$. But then there exists a component containing a cycle of length $t > 1$ which again contradict (1). Thus in any case, we get a contradiction. Hence, $n = 2^l F_{m_1} F_{m_2} \dots F_{m_s}$, where $l \geq 0$ and F_{m_i} are Fermat primes for all i.

Now since $G_2(n,k)$ consists of only one component containing the fixed point 0, n must be of the form p^α, where p is any prime and $\alpha \geq 1$. Thus $n = 2^l$ or $n = F_m$, where $l \geq 2$, $m \geq 1$ are integers and $F_m = 2^{2^m} + 1$ is Fermat prime.

Conversely, suppose k is even and $n = 2^l$ or $n = F_m$, where $l \geq 2$, $m \geq 1$ are integers and $F_m = 2^{2^m} + 1$ is Fermat prime. It is easy to see that $\lambda(n)$ is a power of 2. Property (2) can be proved from Theorem 2.3. To prove property (1), we first show that $G_1(n,k)$ does not contain any cycle of length greater than 1. From Theorem 2.4 and the fact that the greatest divisor of $\lambda(n)$ which is relatively prime to k is 1, it follows that all cycles of $G_1(n,k)$ are fixed points. Now from Theorem 2.6, $A_1(G(n,k)) = 1$. Since the number of components in $G_1(n,k)$ is equal to the number of cycles in $G_1(n,k)$, $G_1(n,k)$ consists of only one component containing 1. This along with the fact that $G_2(n,k)$ always consists of one component whenever n is a power of a prime, completes the proof. □

Remark 4.2. In Theorem 4.1, we have taken $n > 2$ as for $n = 2$, the power digraph $G(2,k)$ always consists of two components which are isolated fixed points. It does not depend on value of k. We also note that property (2) is not satisfied in this case.

Corollary 4.3. *Let n be a positive integer and $k = 2^s$, where $s \geq 1$. The power digraph $G(n,k)$ consists of exactly two components containing fixed points 0 and 1 if and only if $n = 2^l$ or $n = F_m$, where $F_m = 2^{2^m} + 1$ is Fermat prime for all $1 \leq i \leq s$ and $l \geq 1$.*

PROOF: Since $k = 2^s$, from Theorem 2.3 $N(n,k,a) = \prod_{i=1}^{r} \gcd(\lambda(p_i^{e_i}), k) = 2^d$ for some $d \geq 1$ or $N(n,k,a) = 0$. Hence, $G_1(n,k)$ is semi-regular of degree 2^d for some $d \geq 1$. Corollary follows from Theorem 4.1. □

Corollary 4.4. *Let k be an even integer ($k \geq 2$). A Fermat number $F_m = 2^{2^m} + 1$ is prime if and only if following are satisfied:*

(1) *$G(F_m, k)$ consists of two components containing fixed points 0 and 1,*

(2) *$G_1(F_m,k)$ is semi-regular of degree 2^d for some $1 \le d \le 2^m$.*

Proof: It is straight forward from Theorem 4.1. $\square$

Corollary 4.5. *Let n be a positive integer and $k = 2^s$, where $s \ge 1$. A Fermat number $F_m = 2^{2^m}+1$ is prime if and only if $G(F_m,k)$ consists of two components containing fixed points 0 and 1.*

Proof: It can be proved from Theorem 2.3 and Corollary 4.4. $\square$

Corollaries 4.3 and 4.5 for $s = 1$ has been proved in [7].

Theorem 4.6. *Let $n > 2$ be a positive integer and $k = q_1^{\beta_1}\dots q_s^{\beta_s}$ be the prime decomposition of k. The power digraph $G(n,k)$ consists of two components if and only if k is even and n has one of the following forms:*

(1) *$n = p$, where $p = 1 + \prod_{1\le i\le s} q_i^{\gamma_i}$ is prime and $\gamma_i \ge 0$ for all i;*
(2) *$n = q_j^{\alpha}$ for some $1 \le j \le s$ and $q_j = 1 + \prod_{1\le i\le s, i\ne j} q_i^{\gamma_i}$, where $\gamma_i \ge 0$ for all i.*

Proof: Suppose the power digraph $G(n,k)$ consists of two components. Now if k is odd then $2 \mid k-1$. Also since $n > 2$, $2 \mid \lambda(p_i^{e_i})$ for all $1 \le i \le r$. Hence, from Theorem 2.6, $A_1(G(n,k)) \ge 3$. This along with the fact that the number of components is equal to the number of cycles in power digraphs implies that the number of components of $G(n,k)$ is greater than or equal to 3 which is a contradiction. Hence, k must be even.

As the vertices 0 and 1 belong to $G(n,k)$, both of its components contain fixed points and there does not exist any other component containing a cycle of length greater than 1. Since $G_2(n,k)$ itself is a component containing 0, n must be of the form $n = p^{\alpha}$, where p is any prime. Suppose on the contrary that n does not satisfy the conditions given in (1) and (2). The following cases arise:

Case 1. If $n = p^{\alpha}$, where $p \ne q_i$ for any $1 \le i \le s$ and $\alpha > 1$, then $p \mid \lambda(n) = \lambda(p^{\alpha}) = p^{\alpha-1}(p-1)$. We can see that $p \nmid k$ which shows that p is a factor of $\lambda(n)$ relatively prime to k. Thus from Theorem 2.4, there exists a cycle of length t such that

$$k^t \equiv 1 \pmod{p}. \tag{4.1}$$

The fact that there does not exist any other component containing the cycle of length greater than 1 forces $t = 1$. But then $p \mid k-1$ from (4.1). Consequently from Theorem 2.7, $A_1(G(n,k)) \ge p+1$. This further implies that the number of components of $G(n,k)$ is greater than or equal to $p+1$ which is a contradiction.

Case 2. Now suppose $n = p$, where p is any prime or $n = q_j^{\alpha}$ for some $1 \le j \le s$, but there exist prime divisors $p_1 \ne q_i$ and $p_2 \ne q_i$ for any i such that $p_1 \mid p-1$ and $p_2 \mid q_j - 1$. Then p_1 and p_2 are prime divisor of $\lambda(n)$ relatively prime to k. Now again by the same argument as in Case 1, we find the contradiction.

Conversely, suppose k is even and n has one of the forms given in (1) and (2). We note that in either case $\lambda(n)$ does not contain any prime factor relatively prime to k. The only factor of $\lambda(n)$ relatively prime to k is $u = 1$. We can see that $k \equiv 1 \pmod{u}$. Thus from Theorem 2.4, every cycle of $G_1(n, k)$ is of length 1, that is a fixed point. Now from Theorem 2.6 there are two fixed points. This implies that $G(n, k)$ consists of two components which completes the proof. □

References

[1] Wilson B., *Power digraphs modulo n*, Fibonacci Quart. **36** (1998), 229–239.

[2] Lucheta C., Miller E., Reiter C., *Digraphs from powers modulo p*, Fibonacc Quart. **34** (1996), 226–239.

[3] Burton D.M., *Elementary Number Theory*, McGraw-Hill, 2007.

[4] Chartrand G., Oellermann O.R., *Applied and Algorithmic Graph Theory*, McGraw-Hill, New York, 1993.

[5] Kramer-Miller J. *Structural properties of power digraphs modulo n*, in Proceedings of the 2009 Midstates Conference for Undergraduate Research in Computer Science and Mathematics, Oberlin, Ohio, 2009, pp. 40–49.

[6] Ellson J., Gansner E., Koutsofios L., North S.C., Woodhull G., *Graphviz - open source graph drawing tools*, version 2.26.3, `http://www.graphviz.org`

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

[8] Somer L., Křížek M., *Structure of digraphs associated with quadratic congruences with composite moduli*, Discrete Math. **306** (2006), 2174–2185.

[9] Somer L., Křížek M., *On semi-regular digraphs of the congruence* $x^k \equiv y \pmod{n}$, Comment. Math. Univ. Carolin. **48** (2007), no. 1, 41–58.

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

[11] Szalay L., *A discrete iteration in number theory*, BDTF Tud. Közl. **8** (1992), 71–91.

[12] MATLAB, *The language of technical computing*, version 7.0.0.19920 (R14).

[13] Deo N. *Graph theory with Application to Engineering and Computer Sciences*, Prentice-Hall of India private Limited, 1990.

[14] Carmichael R.D., *Note on a new number theory function*, Bull. Amer. Math. Soc. **16** (1910), 232–238.

[15] Husnine S.M., Ahmad U., Somer L., *On symmetries of power digraphs*, Utilitas Mathematica, to appear.

[16] Skowronek-Kaziów J., *Properties of digraphs connected with some congruences relations*, Czechoslovak Math. J. **59** (2009), 39–49.

NATIONAL UNIVERSITY OF COMPUTER AND EMERGING SCIENCES (NUCES), LAHORE CAMPUS, PAKISTAN

E-mail: hamdaahmad@gmail.com

NATIONAL UNIVERSITY OF COMPUTER AND EMERGING SCIENCES, LAHORE CAMPUS, PAKISTAN

E-mail: syed.husnine@nu.edu.pk

(*Received* March 27, 2011, *revised* May 31, 2011)