ISSN: 1017-060X (Print)

ISSN: 1735-8515 (Online)

Bulletin of the Iranian Mathematical Society

Vol. 42 (2016), No. 3, pp. 749–759

Title:

The power digraphs of safe primes

Author(s):

U. Ahmad and S. M. Husnine

Published by Iranian Mathematical Society
http://bims.ims.ir

Bull. Iranian Math. Soc.
Vol. 42 (2016), No. 3, pp. 749–759
Online ISSN: 1735-8515

THE POWER DIGRAPHS OF SAFE PRIMES

U. AHMAD* AND S. M. HUSNINE

(Communicated by Ebadollah S. Mahmoodian)

ABSTRACT. A power digraph, denoted by $G(n,k)$, is a directed graph with $Z_n = \{0,1,...,n-1\}$ as the set of vertices and $L = \{(x,y) : x^k \equiv y \pmod n\}$ as the edge set, where n and k are any positive integers. In this paper, the structure of $G(2q+1,k)$, where q is a Sophie Germain prime is investigated. The primality tests for the integers of the form $n = 2q+1$ are established in terms of the structure of components of $G(n,k)$. The digraphs in which all components look like directed star graphs are completely classified. This work generalizes the results of M. Křížek, L. Somer, *Sophie Germain Little Suns*, Math. Slovaca 54(5) (2004), no. 5, 433–442.
Keywords: Iteration digraph, Carmichael lambda function, Fixed point, Sophie Germain primes, Safe primes, Height of vertices.
MSC(2010): Primary: 05C20; Secondary: 11A07, 11A15, 20K01.

1. Introduction

The power digraphs provide an elegant link between graph theory and number theory. By using graph theoretic properties of the power digraphs, one can infer many number theoretic properties of the congruence $a^k \equiv b(\mathrm{mod}\, n)$. Some characteristics of the power digraph $G(n,k)$, where n and k are arbitrary positive integers, have been investigated by Wilson [10], Somer and Křížek [5–9], Kramer-Miller [4], Ahmad and Husnine [1–3]. One of the major problems in number theory is to test the primality of different numbers e.g. Fermat numbers, Mersenne numbers and the numbers of the form $2p+1$, where p is any prime. Many algorithms have been developed for solving these types of problems. Pepin's and Lucas- Lehmer tests are used for checking the primality of Fermat and Mersenne numbers, respectively. These power digraphs provide another way to analyze this problem. Somer and Křížek in [5] proved that a Fermat number F_m is composite if and only if there exists a cycle in $G(F_m, 2)$

Article electronically published on June 29, 2016.
Received: 13 September 2014, Accepted: 24 February 2015.
*Corresponding author.

of length greater than 1. They also proved that the digraph $G(n,2)$ has exactly two components if and only if n is a Fermat prime or n is a power of 2. Then Uzma and Husnine in [1] generalized these results for the general values of n and k. The odd primes q for which $n = 2q+1$ is also a prime are called Sophie Germain primes and n is called its matching safe prime. K$\check{r}\acute{i}\check{z}$ek and Somer in [6] described the structure of power digraphs $G(2q+1,2)$, where q is a Sophie Germain prime. In this paper, the complete structure of $G(2q+1,k)$, where q is a Sophie Germain prime and k is any positive integer is presented. The criteria to test the primality of the integers of the form $2q+1$ are investigated in terms of the components of $G(n,k)$, where $G(n,k)$ is defined below. The digraphs in which each component looks like a directed star graph are completely classified.

2. Preliminaries

Let $g : Z_n \to Z_n$ be a function where $Z_n = \{0,1,...,n-1\}$ and $n \geq 1$. An iteration digraph defined by g is a directed graph such that Z_n is the set of vertices and $D = \{(x,y)|g(x) \equiv y(\mathrm{mod}\, n)\}$ is the edge set. In this paper, we consider $g(x) \equiv x^k(\mathrm{mod}\, n)$. For fixed values of n and k the iteration digraph is represented by $G(n,k)$. A component of $G(n,k)$ is a sub-digraph which is the largest connected subgraph of the underlying non directed graph.
The in-degree of x is the number of directed edges coming into a vertex x, and the number of edges coming out of x is called the out-degree of x. Note that the out-degree of every vertex in $G(n,k)$ is 1.

A digraph $G(n,k)$ is said to be regular if every vertex of $G(n,k)$ has the same in-degree. A digraph $G(n,k)$ is said to be semi-regular of degree j if every vertex of $G(n,k)$ has in-degree 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 $G(n,k)$. A vertex a is said to be an isolated fixed point if it is a fixed point and has in-degree 1. The number of cycles of length t in $G(n,k)$ are denoted by $A_t(G_1(n,k))$. Since each vertex has out-degree one, it follows that each component contains a unique cycle. The height of a vertex in a component is the length of the shortest directed path from the vertex to the unique cycle of the component. The height of the component is the largest height of any vertex in the component. The Carmichael lambda-function $\lambda(n)$ is defined as the smallest positive integer such that $x^{\lambda(n)} \equiv 1(\mathrm{mod}\, n)$ for all x relatively prime to n. The values of the Carmichael lambda-function $\lambda(n)$ are

$$\begin{aligned}
\lambda(1) &= 1\\
\lambda(2) &= 1\\
\lambda(4) &= 2\\
\lambda(2^r) &= 2^{r-2} \text{ for } r \geq 3\\
\lambda(q^r) &= (q-1)q^{r-1}
\end{aligned}$$

for any odd prime q and $r \geq 1$, and

$$\lambda(q_1^{\alpha_1}q_2^{\alpha_2}....q_r^{\alpha_r}) = lcm(\lambda(q_1^{\alpha_1}),\lambda(q_2^{\alpha_2}),...,\lambda(q_r^{\alpha_r})),$$

where $q_1, q_2, ..., q_r$ are distinct primes and $\alpha_i \geq 1$ for all i.
The sub-digraph of $G(n,k)$ containing all vertices relatively prime to n is denoted by $G_1(n,k)$ and the sub-digraph 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 disconnected. We also have $G(n,k) = G_1(n,k) \cup G_2(n,k)$.
Let $n = ml$, where $\gcd(m,l) = 1$. We can easily see with the help of 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 $x_2 \in G(l,k)$. Moreover, 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 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 $G(n,k) \cong G(m,k) \times G(l,k)$. Now if n is of the form:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} .....p_r^{\alpha_r}, \text{ where } p_1 < p_2 < .... < p_r \text{ and } \alpha_i \geq 0 \tag{2.1}$$

then

$$G(n,k) \cong G(p_1^{\alpha_1}, k) \times G(p_2^{\alpha_2}, k) \times ..... \times G(p_r^{\alpha_r}, k). \tag{2.2}$$

Let $N(n,k,a)$ denote the number of incongruent solutions of the congruence $x^k \equiv a (\mathrm{mod}\, n)$.
Then obviously $N(n,k,a) = indeg_n(a)$ and it is easy to see that if $a = (a_1, a_2, \cdots, a_r)$,

$$N(n,k,a) = indeg_n(a) = \prod_{i=1}^{r} N(p_i^{\alpha_i}, k, a_i)$$

Let $Comp(a)$ and $Comp_{\alpha_i}(a)$ denote the components of $G(n,k)$ and $G(p_i^{\alpha_i}, k)$, respectively containing the vertex a.

Theorem 2.1. [10] Let n be an integer having the factorization as given in (2.1) and x be a vertex of $G_1(n,k)$. Then

$$indeg(x) = N(n,k,x) = \prod_{i=1}^{r} N(p_i^{\alpha_i}, k, x) = \prod_{i=1}^{r} \varepsilon_i \gcd(\lambda(p_i^{\alpha_i}), k),$$
$$or N(n,k,x) = 0,$$

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

Lemma 2.2. [9] Let q be a prime and $\beta \geq 1$, $k \geq 2$ be integers. Then $N(q^\beta, k, 0) = q^{\beta - \lceil \frac{\beta}{k} \rceil}$."

Theorem 2.3. [9] Let n be defined as in (2.1). Then

$$A_t(G_1(n,k)) = \frac{1}{t}[\prod_{i=1}^{r}(\delta_i \gcd(\lambda(p_i^{\alpha_i}), k^t - 1)) - \sum_{d|t, d \neq t} dA_d(G(n,k))];$$

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

Theorem 2.4. [10] There exists an s-cycle in $G(n, k)$ if and only if $s = \text{ord}_h k$ for some positive factor h of u, where $\lambda(n) = uv$ and u is the greatest factor of $\lambda(n)$ relatively prime to k, and $\text{ord}_h k$ denotes the multiplicative order of k modulo h.

Theorem 2.5. [9] 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 $G(n_2, k)$.

3. New results on Power digraphs of Safe primes

Definition 3.1. Let S_r be a component of $G(n, k)$ whose set of vertices is $H' = \{x = x_1, x_2, \cdots, x_r\}$ and $E' = \{(x_i, x) : x_i^k \equiv x (\text{mod}\, n)$ for all $x_i \in H'\}$ to be an edge set. In other words the only edges in S_r are from x_i to x for all $x_i \in H'$.

It is clear from the definition that S_r has r edges. Also we note that if we delete the edge (x, x) then the associated non-directed graph of S_r resembles the well known star graph $(K_{s-1,1})$. Thus we may call S_r, the star digraph with loop. Figure 1 is the sub-digraph of $G(49, 35)$ whose three components are the star digraph $K_{6,1}$ with loop, i.e. S_7.

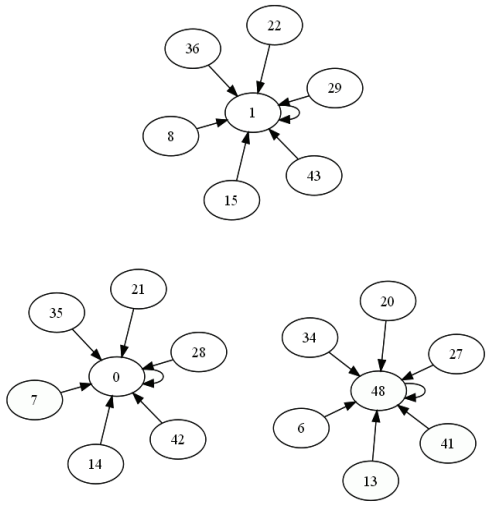

FIGURE 1. sub-digraph of $G(49, 35)$ consisting of 3 S_7

Definition 3.2. Let SW_t, where $t > 1$ be a component of $G(n, k)$ containing a cycle of length t. Corresponding to each cycle vertex $c \in SW_t$, there exists exactly one non-cycle vertex $b \in SW_t$ such that $b^k \equiv c \pmod{n}$ i.e. there is an edge from b to c.

It is obvious from the definition that SW_t consists of $2t$ vertices and $2t$ edges. Also we note that the associated non-directed graph of SW_t looks like a sun graph. Thus we call SW_t, the sun digraph. The two components of $G(147, 2)$ shown in Figure 2 are isomorphic to SW_6. It is also easy to see from

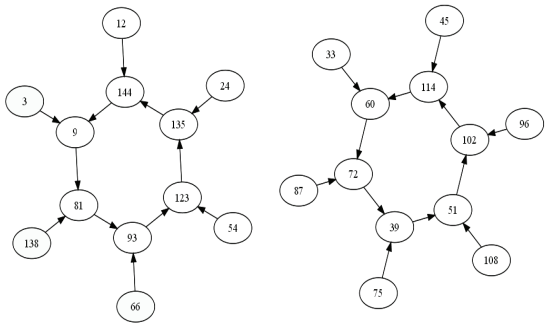

FIGURE 2. sub-digraph of $G(147, 2)$ consisting of 2 SW_6

the definitions that S_r and SW_t both have height 1.

Theorem 3.3. Let $n = 2q + 1$, where q is a Sophie Germain prime and k be any positive integer. Then one of the following holds:

(1) $G(n, k)$ is regular.
(2) $G(n, k)$ contains three components; one is an isolated fixed point and both of the others are isomorphic to S_q.
(3) $G(n, k)$ contains $q + 1$ components; one is an isolated fixed point and each of the others is isomorphic to S_2.
(4) $G(n, k)$ has two components; one is an isolated fixed point and the other is isomorphic to S_{2q}.
(5) $G(n, k)$ has $\frac{q-1}{ord_q k} + 2$ components; one is an isolated fixed point, one is isomorphic to S_2 and each of the other $\frac{q-1}{ord_q k}$components is isomorphic to SW_t, where $t = ord_q k > 1$.

Proof. Since q is a Sophie Germain prime, $n = 2q + 1$ is also a prime. This implies that $G_2(n, k)$ contains only the 0 vertex which is an isolated fixed point. Now $\lambda(n) = 2q$, so there arise four possibilities:

Case 1:
Suppose $2 \nmid k$ and $q \nmid k$. Then $\gcd(\lambda(n), k) = 1$. From Theorem 4.1 of [8], $G(n, k)$ is regular.
Case 2:
Let $2 \nmid k$ but $q \mid k$. Then $\gcd(\lambda(n), k) = q$ which shows that 2 is the highest factor of $\lambda(n)$ which is relatively prime to k. Clearly, $k \equiv 1 \pmod 2$. By Theorem 2.1 and 2.4, $G(n, k)$ contains only fixed points with indegree q. Now by using Theorem 2.3, $A_1(G(n, k)) = \gcd(\lambda(n), k - 1) = 2$. Hence $G_1(n, k)$ contains only 2 components. The height of any component C in $G_1(n, k)$ can be calculated by using Theorem 4.5 of [2] as,

$$height(C) = \lceil \frac{\nu_q(\lambda(n))}{\nu_q(k)} \rceil = 1,$$

where $\nu_q(x)$ means the highest power of q in prime factorization of x. This shows that both components of $G_1(n, k)$ contain a fixed point with in-degree q and have height 1, that is both of them are isomorphic to the directed star graphs S_q.
Case 3:
Let $2 \mid k$ but $q \nmid k$. Then $\gcd(\lambda(n), k) = 2$. This shows that q is the greatest factor of $\lambda(n)$ such that $\gcd(q, k) = 1$. If $q \mid k-1$, then it can be shown by using the same arguments as in case 2 that $G_1(n, k)$ consists of exactly q components, each of which is isomorphic to S_2. Now suppose $q \nmid k - 1$. Then from Theorem 2.4, there must exist a cycle of length $t > 1$. Now from Theorem 2.3,

$$A_1(G_1(n, k)) = \gcd(\lambda(n), k - 1) = 1$$

This along with the fact that q is the only divisor of $\lambda(n)$ that is relatively prime to k implies that $G_1(n, k)$ consists of components such that one of them contains the fixed point and all of the others contain the cycle of length $t > 1$. Now by using Theorem 4.5 of [2], the height of each component C of $G_1(n, k)$ is $height(C) = 1$. Since the in-degree of each cycle vertex is 2, the number of components, say l satisfies $2t \cdot l = 2q - 2$, $l = \frac{q-1}{t}$ By using Theorem 2.4, $l = \frac{p-1}{ord_q k}$. Hence $G_1(n, k)$ consists of $l = \frac{p-1}{ord_q k} + 1$ components, one of them is isomorphic to S_2 and each of the other $l = \frac{p-1}{ord_q k}$ components is isomorphic to SW_t.
Case 4:
Finally, suppose $2 \mid k$ and $q \mid k$ which implies that $N(n, k, 1) = \gcd(\lambda(n), k) = 2q$. Thus the component containing vertex 1 must contain $2q$ vertices. Since $G_1(n, k)$ contains $\lambda(n) = 2q$ vertices, it must consist of exactly one component, say C containing the fixed point with indegree $2q$. Also $height(C) = 1$ by using Theorem 4.5 of [2]. Thus the only component of $G_1(n, k)$ is isomorphic to S_{2q}. This completes the proof. □

Theorem 3.4. Let $k > 1$ be an odd integer and $n = 2q + 1$, where q is any prime such that $q \mid k$. Then q is a Sophie Germain prime if and only if $G(n, k)$ contains three components, one of which is an isolated fixed point and each of the others is isomorphic to S_q.

Proof. Suppose $G(n, k)$ consists of three components one of which is an isolated fixed point and the other two are isomorphic to S_q. Suppose on the contrary, q is not a Sophie Germain prime. This implies that n is not a prime. Hence n can be written as $n = q_1^{\alpha_1} \cdots q_r^{\alpha_r}$, where the q_i's are distinct and none of the q_i's is equal to q. From Lemma 2.2, $N(n, k, 0) = \prod_{i=1}^{r} q_i^{\alpha_i - \lceil \frac{\alpha_i}{k} \rceil}$ But we know that the in-degree of cycle vertices of $G(n, k)$ is either 1 or q. Since none of the q_i's is equal to q, $N(n, k, 0) \neq q$. Thus $N(n, k, 0) = 1$. This is only possible when $\alpha_i = 1$ for all i. This further shows that n is square free, i.e. $n = q_1 \cdots q_r$. Now from Theorem 2.1 and the fact that the in-degree of cycle vertex a of $G(n, k)$ other than 0 is q, we have

$$\begin{aligned} N(n, k, a) &= \prod_{i=1}^{r} N(q_i, k, a) = \prod_{i=1}^{r} \gcd(\lambda(q_i), k) \\ &= \prod_{i=1}^{r} (q_i - 1, k) = q. \end{aligned} \tag{3.1}$$

Equation (3.1) shows that there exists exactly one j for which $\gcd(q_j - 1, k) = q$ and $\gcd(q_i - 1, k) = 1$ for all $1 \leq i \leq r$ but $i \neq j$. Since $q \mid q_j - 1$, we can write $q_j - 1 = qc$. Now we claim that $\gcd(q, c) = 1$. For otherwise either the in-degree of cycle vertices in $G(n, k)$ is greater than q or the height of components of $G(n, k)$ is greater than 1. Both cases lead to a contradiction. Now consider the digraphs $G(q_i, k)$ for all i. Since all the cycle vertices of $G(n, k)$ are fixed points, each cycle vertex of $G(q_i, k)$ is also a fixed point. From Theorem 2.4, $k \equiv 1 (\text{mod } \ q_i - 1)$, if $i \neq j$ and $k \equiv 1 (\text{mod } \ c)$, if $i = j$ i.e $q_i - 1 \mid k - 1$ when $i \neq j$ and $c \mid k - 1$ when $i = j$. From Theorem 2.3,

$$\begin{aligned} A_1(G_1(n, k)) &= \gcd(q_j - 1, k - 1) \prod_{i \neq j, i=1}^{r} \gcd(q_i - 1, k - 1) \\ &= c \prod_{i \neq j, i=1}^{r} (q_i - 1) \end{aligned}$$

Since $2 \mid c$ and $2 \mid (q_i - 1)$, $A_1(G_1(n, k)) > 2$. This along with the fact that 0 is an isolated fixed point contradicts the assumption that $G(n, k)$ contains three components. Hence q must be a Sophie Germain prime.
The proof of the converse is similar to case 2 of the proof of Theorem 3.3. □

Theorem 3.5. Let k be an even integer and $n = 2q + 1$, where q is any prime such that $q \mid k$. Then q is a Sophie Germain prime if and only if $G(n, k)$ contains

two components, one is an isolated fixed point and the other is isomorphic to S_{2q}.

Proof. Suppose $G(n,k)$ contains two components, one is an isolated fixed point and the other is isomorphic to S_{2q}. Then from Theorem 4.6 of [1], either n is a prime or is a power of some prime divisor of k.
Suppose $n = p^\beta$ for some $p \mid k$ and $\beta > 1$. Obviously, $p \neq q$. From Lemma 2.2, $N(n,k,0) = p^{\beta - \lceil \frac{\beta}{k} \rceil}$. Since $\beta > 1$, $N(n,k,0)$ must be some positive power of p. This contradicts the fact that cycle vertices of $G(n,k)$ have in-degree 1 or $2q$. Thus n must be a prime which shows q is a Sophie Germain prime.
The proof of the converse is similar to case 4 of Theorem 3.3. □

Theorem 3.6. Let $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, where $\alpha_i \geq 1$ and $p_1 < p_2 \cdots < p_s$. For some positive integer r, each component of $G(n,k)$ is isomorphic to a directed star graph S_r if and only if following are satisfied

(1) $\alpha_i \leq k$ for all $1 \leq i \leq s$ and $r = p_1^{\alpha_1 - 1} \cdots p_s^{\alpha_s - 1}$.
(2) $\gcd(p_i - 1, k) = 1$ for all $1 \leq i \leq s$
(3) If $8 \nmid n$, $p_i^{\alpha_i - 1} \mid k$ for all $1 \leq i \leq s$. If $p_1 = 2$ and $\alpha_1 \geq 3$ then $p_1^{\alpha_1 - 2} \mid k$ and $p_i^{\alpha_i - 1} \mid k$ for all $2 \leq i \leq s$.
(4) $p_i - 1 \mid k - 1$ for all $1 \leq i \leq s$

Proof. Suppose for some positive integer r, each component of $G(n,k)$ is isomorphic to S_r. Suppose to the contrary there exists a j such that $\alpha_j > k$. Then by Lemma 2.2, the vertex 0 in $G(p_j^{\alpha_j}, k)$ has in-degree $N(p_j^{\alpha_j}, k, 0) = p_j^{\alpha_j - \lceil \frac{\alpha_j}{k} \rceil} \leq p_j^{\alpha_j - 2}$. Since the number of vertices in $Comp_{\alpha_j}(0)$ is $p_j^{\alpha_j - 1}$, there must exist a vertex at height greater than 1. This shows that the height of $Comp_{\alpha_j}(0)$ is greater than 1. Now we know that

$$Comp(0) = Comp_{\alpha_1}(0) \times \cdots \times Comp_{\alpha_s}(0)$$

From Theorem 4.1 of [2], the height of $Comp(0) > 1$. Thus $Comp(0)$ is not a directed star graph. This contradicts the fact that each component of $G(n,k)$ is isomorphic to S_r. Hence

$$\alpha_i \leq k \quad \text{for all } 1 \leq i \leq s. \tag{3.2}$$

Now

$$N(n,k,0) = \prod_{i=1}^{s} p_i^{\alpha_i - \lceil \frac{\alpha_i}{k} \rceil}. \tag{3.3}$$

From (3.2) and (3.3), $N(n,k,0) = \prod_{i=1}^{s} p_i^{\alpha_i - 1}$. Since $Comp(0) \cong S_r$, $r = \prod_{i=1}^{r} p_i^{\alpha_i - 1}$. This proves (1).
To prove (2), suppose on the contrary there exists j such that either $p_j^{\alpha_j - 1} \nmid k$(if

$j = 1$, $p_1 = 2$ and $\alpha_1 \geq 3$, then $p_1^{\alpha_1 - 2} \nmid k)$ or $\gcd(p_j - 1, k) \neq 1$. In any case it is easy to see that $x = N(p_j^{\alpha_j}, k, 1) \neq p_j^{\alpha_j - 1}$. Now consider the component

$$\begin{aligned} C &= Comp_{\alpha_1}(0) \times \cdots \times Comp_{\alpha_{j-1}}(0) \times Comp_{\alpha_j}(1) \times \\ & \quad Comp_{\alpha_{j+1}}(0) \times \cdots \times Comp_{\alpha_s}(0). \end{aligned}$$

Let $M(C)$ equal the maximum in-degree of a vertex in the component C. From Theorem 2.1 and Lemma 2.2,

$$\begin{aligned} M(C) &= M(Comp_{\alpha_1}(0)) \cdots M(Comp_{\alpha_{j-1}}(0)) M(Comp_{\alpha_j}(1)) \\ & \quad M(Comp_{\alpha_{j+1}}(0)) \cdots M(Comp_{\alpha_r}(0)) \\ &= p_1^{\alpha_1 - 1} \cdots p_{j-1}^{\alpha_{j-1} - 1} \cdot x \cdot p_{j+1}^{\alpha_{j+1} - 1} \cdots p_r^{\alpha_r - 1} \\ &= x \prod_{i=1, i \neq j}^{r} p_i^{\alpha_i - 1}, \end{aligned}$$

where $x \neq p_j^{\alpha_j - 1}$. Hence $M(C) \neq r$ which further shows that $C \ncong S_r$. This leads to a contradiction and hence (2) is proved.
Now consider $\lambda(p_i^{\alpha_i}) = p_i^{\alpha - 1}(p_i - 1)$. From (2) it is easy to see that $p_i - 1$ is the largest factor of $\lambda(p_i^{\alpha_i})$ relatively prime to k. From Theorem 2.4,

$$k^t \equiv 1 (\text{mod } \ p_i - 1), \tag{3.4}$$

where t is the length of the longest cycle in $G(p_i^{\alpha_i}, k)$. If $t > 1$, then there exists a component, say C of $G(p_i^{\alpha_i}, k)$ containing cycle of length $t > 1$. Now consider

$$C' = Comp_{\alpha_1}(0) \times \cdots \times Comp_{\alpha_{i-1}}(0) \times C \times Comp_{\alpha_{i+1}}(0) \times Comp_{\alpha_r}(0).$$

Then from Lemma 3.1 of [4], C' is a component of $G(n, k)$ containing a cycle of length $\text{lcm}(1, t) = t > 1$. This leads to a contradiction as each component of $G(n, k)$ is isomorphic to S_r, none of which contains a cycle of length greater than 1. Hence $t = 1$. Therefore, from (3.4), $p_i - 1 | k - 1$ for all $1 \leq i \leq s$.
Suppose that conditions $(1) - (4)$ are satisfied. We will prove the converse implication that each component of $G(n, k)$ is isomorphic to the star graph S_r. For this, let C be any component of $G(n, k)$ and $c \in C$ be a cycle vertex having cycle length t. Then from Theorem 2.5, there exist cycle vertices $c_i \in G(p_i^{\alpha_i}, k)$ for all $1 \leq i \leq s$ such that $c = (c_1, \cdots, c_s)$ Thus

$$N(n, k, c) = \prod_{i=1}^{s} N(p_i^{\alpha_i}, k, c_i). \tag{3.5}$$

If $c_i \in G_2(p_i^{\alpha_i}, k)$, then $c_i \equiv 0 (\text{mod } \ p_i^{\alpha_i})$ as 0 is the only cycle vertex of $G_2(p_i^{\alpha_i}, k)$. Therefore, from Lemma 2.2 and condition (1)

$$\begin{aligned} N(p_i^{\alpha_i}, k, c_i) &= p_i^{\alpha_i - \lceil \frac{\alpha_i}{k} \rceil} \\ &= p_i^{\alpha_i - 1}. \end{aligned} \tag{3.6}$$

Now if $c_i \in G_1(p_i^{\alpha_i}, k)$, then from Theorem 2.1 and conditions $(2)-(3)$

$$\begin{aligned} N(p_i^{\alpha_i}, k, c_i) &= \varepsilon_i \gcd(\lambda(p_i^{\alpha_i}), k), \\ &= p_i^{\alpha_i - 1}. \end{aligned} \tag{3.7}$$

From (3.5), (3.6) and (3.7),

$$N(n, k, c) = \prod_{i=1}^{s} p_i^{\alpha_i - 1} = r.$$

Since t is the length of the cycle of C containing cycle vertex c in $G(n, k)$, from Lemma 3.1 of [4] there exist integers t_i for $1 \leq i \leq s$ such that $t = \text{lcm}(t_1, \cdots, t_s)$, where t_i is length of the cycle containing cycle vertex c_i for $1 \leq i \leq s$. Now from Theorem 2.4,

$$k^{t_i} \equiv 1 (\text{mod } \ d), \tag{3.8}$$

where d is the divisor of the largest factor of $\lambda(p_i^{\alpha_i})$ relatively prime to k. Conditions (2) and (3) imply that $d \mid (p_i - 1)$. This along with condition (4) implies that

$$k \equiv 1 (\text{mod } \ d). \tag{3.9}$$

Since t_i is the least positive integer satisfying (3.8), from (3.9), $t_i = 1$ for all $1 \leq i \leq r$ and hence from (3), $t = 1$. This shows that c is a fixed point. To prove $C \cong S_r$, it is sufficient to show that $height(C) = 1$.
For this, let $x = (x_1, \cdots, x_s)$ be any vertex of in-degree 0 in C. Then from Theorem 4.1 of [2],

$$height(x) = \max\{height(x_1), \cdots, height(x_s)\} \tag{3.10}$$

Suppose $x_i \in G_2(p_i^{\alpha_i}, k)$. From Lemma 4.8 of [2],

$$\begin{aligned} height(G_2(p_i^{\alpha_i}, k)) &= height(Comp_{p_i^{\alpha_i}}(0))) \\ &= \lceil log_k \alpha_i \rceil. \end{aligned} \tag{3.11}$$

Now from condition (1), $\alpha_i \leq k$, $log_k \alpha_i \leq 1$. Hence from (3.11), $height(G_2(p_i^{\alpha_i}, k)) = 1$. This further shows that $height(x_i) \leq 1$.
Now if $x_i \in G_1(p_i^{\alpha_i}, k)$, then from Theorem 4.5 of [2] and conditions $(2)-(3)$, the height of a component containing x_i

$$height(Comp_{p_i^{\alpha_i}}(x_i))) = \lceil \frac{\nu_{p_i}(\lambda(p_i^{\alpha_i}))}{\nu_{p_i}(k)} \rceil = 1,$$

where $\nu_{p_i}(x)$ means the highest power of p_i in x. Thus $height(x_i) \leq 1$. Hence $height(x) \leq 1$. Since $x \in C$ is a vertex of in-degree 0, x is not a cycle vertex. Therefore, $height(x) \neq 0$. This further implies that $height(x) = 1$. Hence $height(C) = 1$. This shows that $C \cong S_r$. □

Acknowledgments

The authors would like to thank the referee for providing his/her valuable comments and suggestions for improving this paper.

References

[1] U. Ahmad and S. Husnine, Characterization of Power Digraphs modulo n, *Comment. Math. Univ. Carolin* **48** (2011), no. 3, 359–367.
[2] U. Ahmad and S. Husnine, On the Heights of Power Digraphs modulo n, *Czechoslovak. Math. J.* **62(137)** (2012), no. 2, 541–556.
[3] S. M. Husnine, U. Ahmad and L. Somer, On symmetries of Power digraphs, *Util. Math* **85** (2011) 257–271.
[4] J. Kramer-Miller, Structural properties of power digraphs modulo n, Proceedings of the 2009 Midstates Conference on Undergraduate Research in Computer Science and Mathematics, 40-49, Oberlin, Ohio, 2009.
[5] L. Somer and M. Krizek, On a connection of number theory with graph theory, *Czechoslovak Math. J.* **54(129)** (2004), no. 2, 465–485.
[6] M. Křížek and L. Somer, Sophie Germain Little Suns, *Math. Slovaca* **54** (2004), no. 5, 433–442.
[7] L. Somer and M. Křížek, Structure of digraphs associated with quadratic congruences with composite moduli, *Discrete Math.* **306** (2006), no. 18, 2174–2185.
[8] L. Somer and M. Křížek, On semiregular digraphs of the congruence $x^k \equiv y(modn)$, *Comment. Math. Univ. Carolin.* **48** (2007), no. 1, 41–58.
[9] L. Somer and M. Křížek, On symmetric digraphs of the congruence $x^k \equiv y \pmod{n}$, *Discrete Math.* **309** (2009), no. 8, 1999–2009.
[10] B. Wilson, Power digraphs modulo n, *Fibonacci Quart.* **36** (1996), no. 3, 229–239.

(U. Ahmad) Department of Mathematics, University of the Punjab, New Campus, Lahore, Pakistan.
E-mail address: uzma.math@pu.edu.pk

(S. M. Husnine) Department of Humanities and Sciences, National University of Computer and Emerging Sciences(FAST), Lahore Campus, Lahore, Pakistan.
E-mail address: syed.husnine@nu.edu.pk