Czechoslovak Mathematical Journal

Uzma Ahmad; Husnine Syed

On the heights of power digraphs modulo n

Czechoslovak Mathematical Journal, Vol. 62 (2012), No. 2, 541–556

Persistent URL: http://dml.cz/dmlcz/142845

Czechoslovak Mathematical Journal, 62 (137) (2012), 541–556

ON THE HEIGHTS OF POWER DIGRAPHS MODULO n

Uzma Ahmad, Husnine Syed, Lahore

(Received March 19, 2011)

Abstract. A power digraph, denoted by $G(n,k)$, is a directed graph with $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$ as the set of vertices and $E = \{(a,b)\colon a^k \equiv b \pmod{n}\}$ as the edge set. In this paper we extend the work done by Lawrence Somer and Michal Křížek: On a connection of number theory with graph theory, Czech. Math. J. 54 (2004), 465–485, and Lawrence Somer and Michal Křížek: Structure of digraphs associated with quadratic congruences with composite moduli, Discrete Math. 306 (2006), 2174–2185. The heights of the vertices and the components of $G(n,k)$ for $n \geqslant 1$ and $k \geqslant 2$ are determined. We also find an expression for the number of vertices at a specific height. Finally, we obtain necessary and sufficient conditions on n such that each vertex of indegree 0 of a certain subdigraph of $G(n,k)$ is at height $q \geqslant 1$.

Keywords: iteration digraph, height, Carmichael lambda function, fixed point, regular digraph

MSC 2010: 11A07, 11A15, 20K01, 05C20

1. Introduction

Power digraphs play an important role in connecting three disciplines of Mathematics, that is, graph theory, number theory and group theory. With the help of power digraphs, we indeed are able to use graph theoretic properties of power digraphs to infer many number theoretic and group theoretic properties of the congruences $a^k \equiv b \pmod{n}$.

The digraphs $G(n,k)$ for arbitrary values of n and k have been studied in [14], [9], [8], [12], [13] and [7]. Many fascinating properties of $G(n,k)$ have been explored like cycle structure, indegree of any vertex in [14], [13], regularity and semi-regularity in [12] and symmetry of $G(n,k)$ in [8], [13] and [7]. The complete structure of $G(p,k)$,

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

p a prime, is discussed in [9]. Yet there are some properties which have been established for $G(n,2)$ but not for general values of k. The height of the vertices and components as well as some of related properties for $G(n,2)$ have been studied in [10], [11], [2]. Similar investigations for $G(p,k)$ have been done in [9]. In this paper we attempt to resolve this problem for $G(n,k)$ where $n \geqslant 1$ and $k \geqslant 2$. The paper is organized as follows.

In Section 2, we discuss the basic concepts about power digraphs modulo n in order to make this paper self contained. Section 3 includes some previous results. In Section 4, we study the heights of the vertices and components in $G_1(n,k)$ and $G_2(n,k)$. We also establish the expression for the number of vertices at a specific height. Finally we find some necessary and sufficient conditions on n such that every vertex of indegree 0 of $G_1(n,p^\alpha)$ and $G_1(n,p)$ is at height $q \geqslant 1$. The figures are created with the help of computational mathematical package MATLAB [15] and displayed by using the Graphviz visualization tool [6].

For notation and definitions, we follow mostly [1], [4], [12] and [5].

2. Preliminaries

Let $g\colon \mathbb{Z}_n \to \mathbb{Z}_n$ be any function where $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$ and $n \geqslant 1$. An iteration digraph defined by g is a directed graph whose vertices are the elements from $\mathbb{Z}_n$, 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 $k \geqslant 2$, and is called power digraph modulo n. Each $x \in G(n,k)$ corresponds uniquely to a residue modulo n.

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 $\mathrm{outdeg}_n(x)$. Note that every vertex in $G(n,k)$ has an outdegree 1.

A digraph $G(n,k)$ is said to be regular if every vertex of $G(n,k)$ has the 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.

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

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

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

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

where $p_1, p_2, \dots, p_r$ are distinct primes and $e_i \geqslant 1$ 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 Chinese Remainder Theorem that corresponding to each vertex $x \in G(n,k)$, there is an ordered pair (x_1, x_2), where $0 \leqslant x_1 < m$ and $0 \leqslant x_2 < l$ 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

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \quad \text{where } p_1 < p_2 < \dots < p_r \text{ and } e_i > 0, \quad \text{i.e. } r = \omega(n), \tag{2.1}$$

then

$$G(n,k) \cong G(p_1^{e_1}, k) \times G(p_2^{e_2}, k) \times \dots \times G(p_r^{e_r}, k). \tag{2.2}$$

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 Chinese Remainder Theorem, we have

$$N(n,k,b) = \operatorname{indeg}_n(b) = \prod_{i=1}^{r} N(p_i^{e_i}, k, b). \tag{2.3}$$

Let $\mathrm{Comp}(a)$ be a component containing a vertex $a \in G(n,k)$ and $d(a,b)$ denote the length of the shortest directed path from a to b. Then height of a vertex $a \in C$, denoted by $\mathrm{height}\, a$, is defined as

$$\mathrm{height}(a) = \min\{d(a,c_i)\colon\ c_i \text{ are cycle vertices of } \mathrm{Comp}(a)\}.$$

The height of any component $C \subseteq G(n,k)$ is defined as

$$\mathrm{height}(C) = \max_{a\in C} \mathrm{height}(a).$$

We also define the height of $G(n,k)$ as

$$\mathrm{height}(G(n,k)) = \max_{C\subseteq G(n,k)} \mathrm{height}(C).$$

A vertex $x \in G(n,k)$ is said to be at level $j \geqslant 1$ if there exists a directed path of least length j which ends at x and does not contain any directed edge from a cycle. A vertex is at level 0 if there does not exist such a path. A component $C \subseteq G(n,k)$ is said to have s levels if the highest level of a vertex in C is $s-1$. It is obvious that the vertex at height 0 and level $s-1$ is a cycle vertex and the vertex at level 0 is a vertex having indegree 0. We can also see that for any component C of $G(n,k)$ having s levels, $s = \mathrm{height}(C) + 1$.

3. Some previous results

Theorem 3.1 (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*

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

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

For the proof of Theorem 3.1, see [3].

Theorem 3.2. *Let n be an integer having factorization as given in* (2.1) *and a be a vertex of $G_1(n,k)$. Then*

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

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

Theorem 3.3. *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 3.4. *If n is a positive integer defined as in (2.1) then there are $\prod_{i=1}^{r} \gcd(u, p_i^{e_i})$ cycle vertices in $G_1(n,k)$ where u is the largest factor of $\lambda(n)$ which is relatively prime to k.*

Theorem 3.5. *Let c_1 and c_2 be any two cycle vertices in $G_1(n,k)$ and $T(c_1)$ and $T(c_2)$ be the trees attached to c_1 and c_2, respectively. Then $T(c_1) \cong T(c_2)$.*

Corollary 3.6. *Let $t \geqslant 1$ be a fixed integer. Then any two components in $G_1(n,k)$ containing t-cycles are isomorphic.*

Theorems 3.2, 3.3, 3.4, 3.5 and Corollary 3.6 are proved in [14].

Theorem 3.7. *Let $n \geqslant 1$ and $k \geqslant 2$ 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 a prime;*
(3) *$G(n,k)$ is regular if and only if n is square free and $\gcd(\lambda(n), k) = 1$.*

For the proof of Theorem 3.7, see [12].

Lemma 3.8. *Let p be a prime and $\alpha \geqslant 1$, $k \geqslant 2$ be integers. Then $N(p^\alpha, k, 0) = p^{\alpha - \lceil \alpha/k \rceil}$.*

Theorem 3.9. *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 $G(n_2,k)$.*

Lemma 3.8 and Theorem 3.9 are proved in [13].

4. Heights in power digraphs

We note that the digraphs $G(n,1)$, $G(1,k)$ and $G(2,k)$ where $n \geqslant 1$ and $k \geqslant 1$ contain components which are isolated fixed points. Thus each vertex in these digraphs is at height 0. Thus for the rest of the paper we take $n > 2$ and $k \geqslant 2$.

Consider a digraph $G(n,k)$, where n has factorization as given in (2.1) and k has factorization

$$k = q_1^{\delta_1} q_2^{\delta_2} \dots q_s^{\delta_s}, \tag{4.1}$$

with $q_1 < q_2 < \ldots < q_s$ and $\delta_i > 0$ i.e. $s = \omega(k)$. Suppose $\lambda(n) = uv$ where u is the the largest divisor of $\lambda(n)$ relatively prime to k. Then we can write

$$\lambda(n) = u q_1^{\gamma_1} q_2^{\gamma_2} \dots q_s^{\gamma_s}, \tag{4.2}$$

where $\gamma_i \geqslant 0$ for all $1 \leqslant i \leqslant s$. Every $x \in G(n,k)$ can be written as

$$x = y p_1^{c_1} p_2^{c_2} \dots p_r^{c_r}, \tag{4.3}$$

where $\gcd(y,n) = 1$ and $c_i \geqslant 0$ for all $1 \leqslant i \leqslant r$. Now we define d_i and n_1 as

$$d_i = \begin{cases} 0, & \text{if } c_i = 0, \\ e_i, & \text{if } 1 \leqslant c_i < e_i, \\ c_i, & \text{if } c_i \geqslant e_i, \end{cases} \tag{4.4}$$

$$n_1 = \prod_{1 \leqslant i \leqslant r} p_i^{e_i - \min\{e_i, d_i\}}, \tag{4.5}$$

so that $\gcd(x, n_1) = 1$. Since $\operatorname{ord}_{n_1} x \mid \lambda(n)$, $\operatorname{ord}_{n_1} x$ can be written as

$$\operatorname{ord}_{n_1} x = u_1 q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}, \tag{4.6}$$

where $1 \leqslant \beta_i \leqslant \gamma_i$ for all $1 \leqslant i \leqslant s$ and $u_1 \mid u$.

Theorem 4.1. *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* $\operatorname{height}(x) = \max\{\operatorname{height}(x_1), \operatorname{height}(x_2)\}$.

Proof. Let $\operatorname{height}(x_1) = j$ and $\operatorname{height}(x_2) = w$. Then there exist cycle vertices c_1 and c_2 in $\operatorname{Comp}(x_1) \subseteq G(m,k)$ and $\operatorname{Comp}(x_2) \subseteq G(l,k)$, respectively such that

$$x_1^{k^j} \equiv c_1 \pmod{m}, \quad \text{and} \quad x_2^{k^w} \equiv c_2 \pmod{l}. \tag{4.7}$$

Now suppose $s = \max\{j, w\}$. It follows that

$$(x_1^{k^s}, x_2^{k^s}) \equiv (c_1', c_2') \pmod{n},$$
$$x^{k^s} \equiv c' \pmod{n},$$

where c_1' and c_2' are cycle vertices in $\mathrm{Comp}(x_1)$ and $\mathrm{Comp}(x_2)$, respectively. Moreover, c' is a cycle vertex in $\mathrm{Comp}(x)$ due to Theorem 3.9. Hence,

$$\mathrm{height}(x) \leqslant s = \max\{\mathrm{height}(x_1), \mathrm{height}(x_2)\}. \tag{4.8}$$

Conversely, let $r = \mathrm{height}(x)$. Then there exists a cycle vertex $b = (b_1, b_2)$ in $\mathrm{Comp}(a)$ such that

$$x^{k^r} \equiv b \pmod{n},$$

where $x^{k^r} = (x_1^{k^r}, x_2^{k^r})$, and $b = (b_1, b_2)$. This implies

$$x_1^{k^r} \equiv b_1 \pmod{m} \quad \text{and} \quad x_2^{k^r} \equiv b_2 \pmod{l}. \tag{4.9}$$

Now b_1, b_2 are cycle vertices due to Theorem 3.9. This along with the fact that j, w are least positive integers satisfying (4.7) lead to

$$j \leqslant r \quad \text{and} \quad w \leqslant r. \tag{4.10}$$

This completes the proof. □

Lemma 4.2. *Let n and k be positive integers defined as in* (2.1) *and* (4.1), *respectively. Suppose x is a vertex of a component C of $G_1(n, k)$. Then*

$$\mathrm{height}(x) = \max_{1 \leqslant i \leqslant s} \left\lceil \frac{\beta_i}{\delta_i} \right\rceil = \max_{1 \leqslant i \leqslant s} \left\lceil \frac{\nu_{q_i}(\mathrm{ord}_n\, x)}{\nu_{q_i(k)}} \right\rceil,$$

where β_i and δ_i are defined in (4.6) *and* (4.1), *respectively and $\nu_{q_i}(x)$ denotes the highest power of q_i in x.*

P r o o f. Suppose $w = \mathrm{height}(x)$. Then there exists a cycle vertex $b \in C$ such that

$$x^{k^w} \equiv b \pmod{n}.$$

Since $\gcd(x, n) = 1$, we have,

$$\mathrm{ord}_n\, b = \mathrm{ord}_n\, x^{k^w} = \frac{\mathrm{ord}_n\, x}{\gcd(k^w, \mathrm{ord}_n\, x)}.$$

Now from (4.6), we obtain

$$\operatorname{ord}_n b = \operatorname{ord}_n x^{k^w} = \frac{u_1 q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}}{q_1^{\min(\beta_1, \delta_1 w)} q_2^{\min(\beta_2, \delta_2 w)} \dots q_s^{\min(\beta_s, \delta_s w)}}.$$

It is easy to see that a vertex $a \in G_1(n,k)$ is a cycle vertex if and only if $\gcd(k, \operatorname{ord}_n a) = 1$ by the proof of Theorem 3.3. Hence, to make sure that b is a cycle vertex, we must have

$$\begin{aligned} \delta_i w &\geqslant \beta_i, \quad \text{for } 1 \leqslant i \leqslant s \\ w &\geqslant \max_{1 \leqslant i \leqslant s} \Big\lceil \frac{\beta_i}{\delta_i} \Big\rceil = \max_{1 \leqslant i \leqslant s} \Big\lceil \frac{\nu_{q_i}(\operatorname{ord}_n a)}{\nu_{q_i}(k)} \Big\rceil. \end{aligned}$$

Since we are considering the least distance,

$$w = \max_{1 \leqslant i \leqslant s} \Big\lceil \frac{\beta_i}{\delta_i} \Big\rceil = \max_{1 \leqslant i \leqslant s} \Big\lceil \frac{\nu_{q_i}(\operatorname{ord}_n a)}{\nu_{q_i}(k)} \Big\rceil.$$

□

Lemma 4.3. *If x is a cycle vertex of $G_2(n,k)$, where n is defined as in* (2.1)*, then $p_i^{e_i} \mid x$ whenever $p_i \mid x$.*

P r o o f. Suppose $x \in G_2(n,k)$ is a cycle vertex. Then there exists $m \geqslant 1$, such that

$$\begin{aligned} x^{k^m} &\equiv x \pmod n, \\ x(x^{k^m - 1} - 1) &\equiv 0 \pmod n. \end{aligned}$$

The Lemma holds due to the fact that $\gcd(x^{k^m-1} - 1, x) = 1$. □

Theorem 4.4. *Let n and k be positive integers defined as in* (2.1) *and* (4.1)*, respectively. If x is a vertex of a component C of $G(n,k)$, then the height of x is*

$$\begin{aligned} \operatorname{height}(x) &= \max\Big\{ \max_{1 \leqslant i \leqslant r} \Big\lceil \log_k \frac{d_i}{c_i} \Big\rceil, \max_{1 \leqslant i \leqslant s} \Big\lceil \frac{\beta_i}{\delta_i} \Big\rceil \Big\} \\ &= \max\Big\{ \max_{1 \leqslant i \leqslant r} \Big\lceil \log_k \frac{d_i}{c_i} \Big\rceil, \max_{1 \leqslant i \leqslant s} \Big\lceil \frac{\nu_{q_i}(\operatorname{ord}_{n_1} a)}{\nu_{q_i}(k)} \Big\rceil \Big\}, \end{aligned}$$

where c_i, d_i, n_1 and β_i are defined as in (4.3), (4.4), (4.5) *and* (4.6)*, respectively and $d_i/c_i = 1$ if $d_i = c_i = 0$.*

P r o o f. Let x and n_1 be defined as in (4.3) and (4.5), $n_2 = n/n_1$ and $\text{height}(x) = l$. Suppose,

$$x \equiv x_1 \pmod{n_1} \quad \text{and} \quad x \equiv x_2 \pmod{n_2}. \tag{4.11}$$

Then from Theorem 4.1,

$$l = \max\{\text{height}(x_1), \text{height}(x_2)\} = \max\{g, h\}. \tag{4.12}$$

Thus to find l, we have to find $\text{height}(x_1)$ in $G(n_1, k)$ and $\text{height}(x_2)$ in $G(n_2, k)$. Since $\gcd(x_1, n_1) = 1$ and $\text{ord}_{n_1} x = \text{ord}_{n_1} x_1$ by (4.11), Lemma 4.2 yields,

$$\text{height}(x_1) = g = \max_{1 \leqslant i \leqslant s} \left\lceil \frac{\beta_i}{\delta_i} \right\rceil = \max_{1 \leqslant i \leqslant s} \left\lceil \frac{\nu_{q_i}(\text{ord}_{n_1} x)}{\nu_{q_i}(k)} \right\rceil. \tag{4.13}$$

Now to determine the height of a_2, we have to find the least positive integer h and a cycle vertex $b \in G_2(n_2, k)$ satisfying

$$x^{k^h} \equiv x_2^{k^h} \equiv b \pmod{n_2}.$$

By using (4.3) we can write,

$$b \equiv x^{k^h} \equiv y^{k^h} p_1^{c_1 k^h} p_2^{c_2 k^h} \dots p_r^{c_r k^h} \pmod{n_2}.$$

For $b \in G_2(n_2, k)$ to be a cycle vertex, we must have due to Lemma 4.3, $p_i^{e_i} \mid b$ whenever $p_i \mid x_2$. Thus for all such i

$$c_i k^h \geqslant e_i. \tag{4.14}$$

If $c_i = 0$, $p_i^{e_i} \nmid b$ and if $c_i \geqslant e_i$, (4.14) is satisfied for $h = 0$. However if $c_i \leqslant e_i$, then from (4.14), $h \geqslant \lceil \log_k e_i/c_i \rceil$. Thus we can write,

$$h \geqslant \max_{1 \leqslant i \leqslant r} \left\lceil \log_k \frac{d_i}{c_i} \right\rceil, \tag{4.15}$$

where d_i are defined as in (4.4). The result follows from (4.12), (4.13) and (4.15) and the fact that we need the least h. □

Theorem 4.5. *Let n and k be positive integers defined as in* (2.1) *and* (4.1), *respectively. Then the height of any component C of $G_1(n, k)$ is*

$$\text{height}(C) = \max_{\leqslant i \leqslant s} \left\lceil \frac{\gamma_i}{\delta_i} \right\rceil = \max_{1 \leqslant i \leqslant s} \left\lceil \frac{\nu_{q_i}(\lambda(n))}{\nu_{q_i}(k)} \right\rceil,$$

where γ_i are defined as in (4.2).

P r o o f. Let $x \in C$ be any vertex in $G_1(n,k)$, by Lemma 4.2, height(x) is given as

$$\text{height}(x) = \max_{1\leqslant i\leqslant s}\Big\lceil \frac{\nu_{q_i}(\text{ord}_n\, x)}{\nu_{q_i}(k)}\Big\rceil.$$

Since $\text{ord}_n\, x \mid \lambda(n)$, we have

$$\text{height}(C) \leqslant \max_{1\leqslant i\leqslant s}\Big\lceil \frac{\nu_{q_i}(\lambda(n))}{\nu_{q_i}(k)}\Big\rceil. \tag{4.16}$$

Since C is arbitrary, (4.16) holds for all components C of $G_1(n,k)$. Now we will show that the equality in (4.16) holds.

By Theorem 3.1, we can find a vertex $g \in G_1(n,k)$ having order $\lambda(n)$. Thus from (4.16), the height of the component C' containing g is

$$\max_{1\leqslant i\leqslant s}\Big\lceil \frac{\nu_{q_i}(\lambda(n))}{\nu_{q_i}(k)}\Big\rceil.$$

By Theorem 3.5, any two cycle vertices of $G_1(n,k)$ have same associated trees. Thus if there is a vertex at height h in C' then there must exist a vertex at height h in C. This implies height(C) = height(C') which completes the proof. □

The following corollaries are immediate consequences of Theorem 4.5 and the definition of level.

Corollary 4.6. *Each component of* $G_1(n,k)$ *has exactly* $\max\limits_{1\leqslant i\leqslant s}\lceil \nu_{q_i}(\lambda(n))/\nu_{q_i}(k)\rceil + 1$ *levels, where* n *and* k *are defined in* (2.1) *and* (4.1)*, respectively.*

Corollary 4.7. *The height and level of any component* C *of* $G_1(n,p)$ *from its cycle is* $\nu_p(\lambda(n))$ *and* $\nu_p(\lambda(n))+1$*, respectively, where* $n \geqslant 1$ *and* p *is any prime.*

The Corollary 4.7 has been proved in [10] for $p = 2$.

Lemma 4.8. *The height of* Comp(0) *in* $G(n,k)$ *is* $\max\limits_{1\leqslant i\leqslant r}\lceil \log_k e_i\rceil$.

P r o o f. For any vertex $a \in$ Comp(0), we have $p_i \mid a$ if and only if $p_i \mid n$. Now the expressions for a and n_1 given in (4.3) and (4.5), respectively imply that $c_i \geqslant 1$ where $1 \leqslant i \leqslant r$ and $n_1 = 1$ for all vertices in Comp(0). By Theorem 4.4, height(Comp(0)) $= \max\{\max\limits_{1\leqslant i\leqslant r}\lceil \log_k e_i/c_i\rceil, 1\} = \max\limits_{1\leqslant i\leqslant r}\lceil \log_k e_i/c_i\rceil$. Since $c_i \geqslant 1$, height(Comp(0)) $\leqslant \max\limits_{1\leqslant i\leqslant r}\lceil \log_k e_i\rceil$. The existence of the vertex $p_1p_2\ldots p_r$ completes the proof. □

Theorem 4.9. *Let n and k be positive integers defined as in* (2.1) *and* (4.1), *respectively. Then the height of $G_2(n,k)$ is*

$$\max\Big\{\max_{1\leqslant i\leqslant r}\lceil\log_k e_i\rceil,\max_{n_1\mid n,\gcd(n/n_1,n_1)=1}\max_{1\leqslant i\leqslant s}\Big\lceil\frac{\nu_{q_i}(\lambda(n_1))}{\nu_{q_i}(k)}\Big\rceil\Big\}.$$

P r o o f. Consider $x\in C$ of $G_2(n,k)$. Then Theorem 4.4 yields

$$\mathrm{height}(x)=\max\Big\{\max_{1\leqslant i\leqslant r}\Big\lceil\log_k\frac{d_i}{c_i}\Big\rceil,\max_{1\leqslant i\leqslant s}\Big\lceil\frac{\nu_{q_i}(\mathrm{ord}_{n_1}a)}{\nu_{q_i}(k)}\Big\rceil\Big\}.$$

Since $d_i/c_i\leqslant e_i$ for all $1\leqslant i\leqslant r$, it follows that

$$\max_{1\leqslant i\leqslant r}\Big\lceil\log_k\frac{d_i}{c_i}\Big\rceil\leqslant\max_{1\leqslant i\leqslant r}\lceil\log_k e_i\rceil. \tag{4.17}$$

Consider n_1 defined as in (4.5). Then Theorem 4.5 gives us

$$\begin{aligned}\max_{1\leqslant i\leqslant s}\Big\lceil\frac{\nu_{q_i}(\mathrm{ord}_{n_1}a)}{\delta_i}\Big\rceil&\leqslant\max_{1\leqslant i\leqslant s}\Big\lceil\frac{\nu_{q_i}(\lambda(n_1))}{\nu_{q_i(k)}}\Big\rceil\\&\leqslant\max_{n_1\mid n,\gcd(n/n_1,n_1)=1}\max_{1\leqslant i\leqslant s}\Big\lceil\frac{\nu_{q_i}(\lambda(n_1))}{\nu_{q_i}(k)}\Big\rceil.\end{aligned} \tag{4.18}$$

Thus from (4.17) and (4.18), we obtain

$$\mathrm{height}(x)\leqslant\max\Big\{\max_{1\leqslant i\leqslant r}\lceil\log_k e_i\rceil,\max_{n_1\mid n,\gcd(n/n_1,n_1)=1}\max_{1\leqslant i\leqslant s}\Big\lceil\frac{\nu_{q_i}(\lambda(n_1))}{\nu_{q_i}(k)}\Big\rceil\Big\}. \tag{4.19}$$

The proof is completed if there exist vertices in $G_2(n,k)$ with heights $\max_{1\leqslant i\leqslant r}\lceil\log_k e_i\rceil$ or $\max_{1\leqslant i\leqslant s}\lceil\nu_{q_i}(\lambda(n_1))/\delta_i\rceil$ for all $n_1\mid n$ such that $\gcd(n/n_1,n_1)=1$.

The existence of vertex having height $\max_{1\leqslant i\leqslant r}\lceil\log_k e_i\rceil$ is shown by Lemma 4.8. By Theorem 4.5, for every $n_1\mid n$ $\mathrm{height}(G_1(n_1,k))=\max_{1\leqslant i\leqslant s}\lceil\nu_{q_i}(\lambda(n_1))/\delta_i\rceil$. Thus we can find a vertex a in $G_1(n_1,k)$ such that $\mathrm{height}(a)=\mathrm{height}(G_1(n_1,k))$. Now consider a fixed point b in $G_2(n/n_1,k)$. Since $\gcd(n/n_1,n_1)=1$, by using (2.2) and Theorem 4.1, we can find a vertex $c=(a,b)\in G_2(n,k)$ such that $\mathrm{height}(c)=\max\{\mathrm{height}(a),\mathrm{height}(b)\}$. Since b is a cycle vertex, $\mathrm{height}(b)=0$ and $\mathrm{height}(c)=\mathrm{height}(a)=\max_{1\leqslant i\leqslant s}\lceil\nu_{q_i}(\lambda(n_1))/\delta_i\rceil$. The result follows immediately. □

Lemma 4.2, Theorem 4.5, Lemma 4.8 and Theorem 4.9 are illustrated by the following Example.

Example 4.10. Let $n = 27 = 3^3$ and $k = 30$. Consider the power digraph

$$G(n,k) = G(27,30) = G(3^3, 2\cdot 3\cdot 5).$$

For $23, 16, 19 \in G_1(27,30)$, $\operatorname{ord}_{27} 23 = 18 = 3^2\cdot 2$, $\operatorname{ord}_{27} 16 = 3^2$ and $\operatorname{ord}_{27} 19 = 3$. Now from Lemma 4.4, $\operatorname{height}(23) = \max\{\lceil \frac{2}{1}\rceil, \lceil \frac{1}{1}\rceil\} = 2$, $\operatorname{height}(16) = \lceil \frac{2}{1}\rceil = 2$ and $\operatorname{height}(19) = \lceil \frac{1}{1}\rceil = 1$ and similarly, heights of the other vertices can be determined. From Theorem 4.5, $\operatorname{height} G_1(27,30) = \max\{\lceil \nu_2(\lambda(27))/1\rceil, \lceil \nu_3(\lambda(27))/1\rceil, \lceil \nu_5(\lambda(27))/1\rceil\} = 2$ and by Lemma 4.8, $\operatorname{height}(\operatorname{Comp}(0)) = \max\{\lceil \log_{30} 3\rceil\} = 1$. The digraph $G(27,30)$ is given in Figure 1.

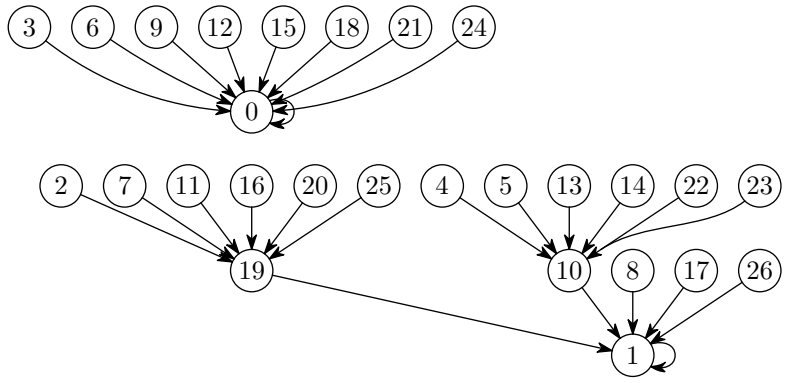

Figure 1. $G(27,30)$

Theorem 4.11. *Let n and k be positive integers defined as in* (2.1) *and* (4.1)*, respectively. Then the number of vertices in $G_1(n,k)$ at height q is given by*

$$\prod_{i=1}^{r} \gcd(\lambda(p_i^{e_i}), u)[N(n,k^q,b) - N(n,k^{q-1},b)],$$

where u is the largest divisor of $\lambda(n)$ relatively prime to k and b is any cycle vertex of $G_1(n,k)$.

P r o o f. From Theorem 3.5 we know that $T(c_1) \cong T(c_2)$ for all cycle vertices c_1 and c_2 of $G_1(n,k)$. Thus in order to find the number of vertices at height q in $G_1(n,k)$, we first find the number of vertices at height q from one cycle vertex, say b. In other words we have to find the number of solutions of the following congruence, where q is the least non negative integer

$$x^{k^q} \equiv b \pmod{n}, \tag{4.20}$$

or equivalently we have to find those vertices which satisfy (4.20) but do not satisfy the following congruence

$$x^{k^{q-1}} \equiv b \pmod{n}. \tag{4.21}$$

Hence, the number of vertices at height q from b in the component containing b is

$$N(n, k^q, b) - N(n, k^{q-1}, b). \tag{4.22}$$

The result follows from Theorem 3.4 and (4.22). □

Theorem 4.12. *Suppose $G_1(n, p^\alpha)$ is not regular, where p is an odd prime. Then the height of $G_1(n, p^\alpha)$ is 1 if and only if n is of one of the following forms*

(1) $n = 2^{w_0} p^{w_1} \prod_{1 \leqslant i \leqslant t} p_i^{h_i}$ *where* $w_0 \geqslant 0$, $1 < w_1 \leqslant \alpha + 1$ *and* $p^{\alpha+1} \nmid p_i - 1$ *for any* i.

(2) $n = 2^{w_0} p^{w_1} \prod_{1 \leqslant i \leqslant t} p_i^{h_i}$ *where* $w_0 \geqslant 0$, $w_1 \in \{0, 1\}$, $p \mid p_i - 1$ *for some* i *but* $p^{\alpha+1} \nmid p_i - 1$ *for any* i.

P r o o f. Suppose every vertex of indegree 0 is at height 1 and

$$n = 2^{w_0} p^{w_1} \prod_{1 \leqslant i \leqslant t} p_i^{h_i}.$$

Suppose $w_1 > 1$ but $w_1 > \alpha + 1$ or $p^{\alpha+1} \mid p_i - 1$ for some i then $p^{\alpha+1} \mid \lambda(n)$. This along with Theorem 4.5 yields height $(G_1(n, k)) \geqslant 2$. Thus there must exists some vertex of indegree 0 at height greater than or equal to 2 which contradicts our assumption. This establishes (1).

Now suppose $w_1 \in \{0, 1\}$ and $p \nmid p_i - 1$ for any i. Then $p \nmid \lambda(n)$ which implies $\gcd(\lambda(n), k) = 1$. From Theorem 3.7 it follows that $G_1(n, k)$ is regular i.e. having height 0 which contradicts our assumption. Hence, we may suppose $p \mid p_i - 1$ but $p^{\alpha+1} \mid p_i - 1$ for some i. Again by the same argument we can show the existence of a vertex having indegree 0 at height greater than or equal to 2 which provides a contradiction. Thus (2) is established.

The converse is straightforward due to Theorem 4.5. □

Theorem 4.13. *Suppose $G_1(n, 2^\alpha)$ is not regular. Then the height of $G_1(n, 2^\alpha)$ is 1 if and only if $n = 2^{w_0} \prod_{1 \leqslant i \leqslant t} p_i^{h_i}$ where $0 \leqslant w_0 \leqslant \alpha + 1$ and $2^{\alpha+1} \nmid p_i - 1$ for any i.*

P r o o f. If $w_0 > \alpha + 1$ or $2^{\alpha+1} \mid p_i - 1$ for some i then $2^{\alpha+1} \mid \lambda(n)$. This along with Theorem 4.5 yields height $(G_1(n, k)) \geqslant 2$. Therefore, there must exist a vertex having indegree 0 at height greater than or equal to 2 which provides a contradiction. □

Theorem 4.12 is illustrated by Examples 4.14 and 4.15.

Example 4.14. Let $n = 36 = 2^2 \cdot 3^2 = 2^{w_0} \cdot p^{w_1}$ and $k = 9 = 3^2 = p^\alpha$, so that $w_0 = 2$, $w_1 = 2$ and $\alpha = 2$. The power digraph $G_1(36, 9)$ satisfies the conditions given in Theorem 4.12 and height $(G_1(36, 9)) = 1$. We also note that $\lambda(36) = 6$ and $\gcd(\lambda(n), p^\alpha) = \gcd(\lambda(36), 9) \neq 1$ so that $G_1(n, p^\alpha)$, by Theorem 3.7, is not regular. See Figure 2 for detailed structure of $G(36, 9)$.

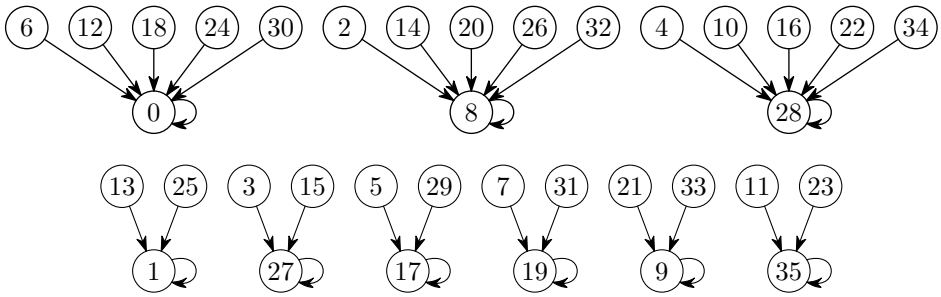

Figure 2. $G(36, 9)$

Example 4.15. Let $n = 81 = 3^4 = p^{w_1}$ and $k = 9 = 3^2 = p^\alpha$, where $w_1 = 4$ and $\alpha = 2$. We note that $w_1 > 3 = \alpha + 1$, the digraph $G_1(81, 9)$ does not satisfy the conditions given in Theorem 4.12, height$(G_1(81, 9)) \neq 1$. In fact from Theorem 4.5, height$(G_1(81, 9)) = 2$.

Theorem 4.16. *Suppose $G_1(n, p)$ is not regular. Then every vertex of indegree 0 in $G_1(n, p)$ is at height $q \geqslant 1$ if and only if n has one of the following forms*

(1) $n = 2^{w_0} p^{w_1} \prod_{1 \leqslant i \leqslant t} p_i^{h_i}$ *where $w_0 \geqslant 0$, $0 \leqslant w_1 \leqslant q$, $p \mid p_i - 1$ for some i and $p^q \parallel p_i - 1$ for all such p_i's.*

(2) $n = 2^{w_0} p^{q+1} \prod_{1 \leqslant i \leqslant t} p_i^{h_i}$ *where $w_0 \geqslant 0$ and either $p \nmid p_i - 1$ for any i or $p^q \parallel p_i - 1$ for all p_i such that $p \mid p_i - 1$.*

P r o o f. Let every vertex of indegree 0 in $G_1(n, p)$ be at height $q \geqslant 1$ and

$$n = 2^{w_0} p^{w_1} \prod_{1 \leqslant i \leqslant t} p_i^{h_i}.$$

Suppose $m = 2^{w_0} \prod_{1 \leqslant i \leqslant t} p_i^{h_i}$ and $l = p^{w_1}$. Since $\gcd(m, l) = 1$, by (2.2), $G(n, p) \cong G(m, p) \times G(l, p)$.

Now suppose $0 \leqslant w_1 \leqslant q$ and there is no i for which $p \mid p_i - 1$. Then $p \nmid \lambda(m)$. Hence, by Theorem 3.7 it follows that $G_1(m, p)$ is regular and has height 0. Now

Theorem 4.5 yields $0 \leqslant \text{height}(G_1(l,p)) \leqslant q-1$. We see by Theorem 4.1 that $0 \leqslant \text{height}(G_1(n,p)) \leqslant q-1$. This implies that the height of every vertex of indegree 0 is less than or equal to $q-1$ which contradicts the assumption that every vertex of indegree 0 in $G_1(n,p)$ is at height $q \geqslant 1$. Thus there must exist some i for which $p \mid p_i - 1$. Now suppose for one such p_j, $p^d \parallel p_j - 1$ where $d \neq q$ Then Theorem 4.5 yields there is a vertex $a \in G_1(p_j^{h_j}, p)$ such that $\text{height}(a) = \text{height}(G_1(p_j^{h_j}, p)) = d$, i.e.

$$a^{k^d} \equiv a_j \pmod{p_j^{h_j}},$$

for some cycle vertex a_j in $G_1(p_j^{h_j}, p)$. Now consider the fixed points b_i in $G_1(p_i^{h_i}, p)$ for all $i \neq j$, c_0 in $G_1(2^{w_0}, p)$ and c_1 in $G_1(p^{w_1}, p)$. Then from (4.1) and Theorem 4.1, $c = (c_0, c_1, b_1, \ldots, b_{j-1}, a, \ldots b_t) \in G_1(n,p)$ and

$$\begin{aligned}\text{height}(c) = \ & \max\{\text{height}(c_0), \text{height}(c_1), \text{height}(b_1), \ldots, \\ & \text{height}(b_{j-1}), \text{height}(a), \ldots, \text{height}(b_t)\}.\end{aligned}$$

Note that being fixed points, $\text{height}(c_0) = \text{height}(c_1) = \text{height}(b_i) = 0$, where $i \neq j$. Thus $\text{height}(c) = \text{height}(a) = d \neq q$. But the vertex c has indegree 0 by (2.3) and the fact that the vertex a has indegree 0. This implies c is a vertex having indegree 0 and height $d \neq q$ which contradicts our assumption. Hence, (1) holds.

Now suppose $w_1 = q+1$ and $p \mid p_j - 1$ for some $1 \leqslant j \leqslant t$ but $p^d \parallel p_j - 1$ where $d \neq q$. Again by the same argument as above, we can prove the existence of a vertex of indegree 0 which is not at height q which leads to a contradiction. This establishes (2).

It remains to show that w_1 can not exceed $q+1$. Indeed if $w_1 > q+1$, Theorem 3.2 forces height $(G_1(p^{w_1}, p)) > q$. Now by Theorem 4.1, height $(G_1(n,p)) > q$ which contradicts the assumption.

The converse is easy to prove using Theorem 4.5. □

The following examples illustrate Theorem 4.16.

Example 4.17. Let $n = 57 = 3 \cdot 19 = p \cdot p_1$ and $k = p = 3$, where $p = 3$, $p_1 = 19$ and $w_1 = 1$. We note that $p^2 = 9 \parallel p_1 - 1 = 18$, the digraph $G_1(57,3)$ satisfies the conditions given in Theorem 4.16. Hence, every vertex of indegree 0 is at height 2. We also note that $\gcd(\lambda(n), p) = \gcd(\lambda(57), 3) = (18, 3) \neq 1$. Thus from Theorem 3.7, $G_1(57,3)$ is not regular.

Example 4.18. Let $n = 133 = 7 \cdot 19 = p_1 \cdot p_2$ and $k = p = 3$, where $p_1 = 7$ and $p_2 = 19$. We can see $p^2 \parallel p_2 - 1$ and $p \mid p_1 - 1 = 6$ but $p^2 \nmid p_1 - 1$. Thus the digraph $G_1(133,3)$ does not satisfy the conditions given in Theorem 4.12. This implies every vertex of indegree 0 is not at height 2. In fact there are some vertices

of indegree 0 which are at height 1, for example by Theorem 3.2, $N(133, 3, 26) = 0$ but by Theorem 4.2, height$(26) = 1$.

References

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

[2] *W. Carlip, M. Mincheva*: Symmetry of iteration graphs. Czech. Math. J. *58* (2008), 131–145.

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

[4] *G. Chartrand, O. R. Oellermann*: Applied and Algorithmic Graph Theory. International Series in Pure and Applied Mathematics, McGraw-Hill, 1993.

[5] *N. Deo*: Graph theory with Application to Engineering and Computer Sciences. Prentice-Hall Series in Automatic Computation. Englewood Cliffs, N.J.: Prentice-Hall, 1974.

[6] *J. Ellson, E. Gansner, L. Koutsofios, S. C. North, G. Woodhull*: Graphviz–open source graph drawing tools.. Mutzel, Petra (ed.) et al., Graph drawing. 9th international symposium, GD 2001, Vienna, Austria, September 23–26, 2001; Revised papers. Berlin: Springer. Lect. Notes Comput. Sci. 2265 (2002), 483–484.

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

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

[9] *C. Lucheta, E. Miller, C. Reiter*: Digraphs from powers modulo p. Fibonacci Q. *34* (1996), 226–239.

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

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

[12] *L. Somer, M. Křížek*: On semiregular digraphs of the congruence $x^k \equiv y \pmod{n}$. Commentat. Math. Univ. Carol. *48* (2007), 41–58.

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

[14] *B. Wilson*: Power digraphs modulo n. Fibonacci Q. *36* (1998), 229–239.

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

Authors' address: U. Ahmad, H. Syed, National University of Computer and Emerging Sciences (NUCES), Lahore Campus, Pakistan, e-mail: `hamdaahmad@gmail.com`, `syed.husnine@nu.edu.pk`.