Amplify Sawkmie; Madan Mohan Singh
On the tree structure of the power digraphs modulo n

Czechoslovak Mathematical Journal, Vol. 65 (2015), No. 4, 923–945

Persistent URL: http://dml.cz/dmlcz/144783

Czechoslovak Mathematical Journal, 65 (140) (2015), 923–945

ON THE TREE STRUCTURE OF THE POWER DIGRAPHS MODULO n

Amplify Sawkmie, Madan Mohan Singh, Shillong

(Received August 19, 2014)

Abstract. For any two positive integers n and $k \geqslant 2$, let $G(n,k)$ be a digraph whose set of vertices is $\{0,1,\ldots,n-1\}$ and such that there is a directed edge from a vertex a to a vertex b if $a^k \equiv b \pmod{n}$. Let $n = \prod_{i=1}^{r} p_i^{e_i}$ be the prime factorization of n. Let P be the set of all primes dividing n and let $P_1, P_2 \subseteq P$ be such that $P_1 \cup P_2 = P$ and $P_1 \cap P_2 = \emptyset$. A fundamental constituent of $G(n,k)$, denoted by $G^*_{P_2}(n,k)$, is a subdigraph of $G(n,k)$ induced on the set of vertices which are multiples of $\prod_{p_i \in P_2} p_i$ and are relatively prime to all primes $q \in P_1$. L. Somer and M. Křížek proved that the trees attached to all cycle vertices in the same fundamental constituent of $G(n,k)$ are isomorphic. In this paper, we characterize all digraphs $G(n,k)$ such that the trees attached to all cycle vertices in different fundamental constituents of $G(n,k)$ are isomorphic. We also provide a necessary and sufficient condition on $G(n,k)$ such that the trees attached to all cycle vertices in $G(n,k)$ are isomorphic.

Keywords: congruence; symmetric digraph; fundamental constituent; tree; digraph product; semiregular digraph

MSC 2010: 68R10, 05C05, 05C20, 11A07, 11A15

1. Introduction

Let n and $k \geqslant 2$ be any positive integers. Let $G(n,k)$ be a digraph whose set of vertices is $\{0,1,\ldots,n-1\}$ and such that there is a directed edge from a vertex a to a vertex b if $a^k \equiv b \pmod{n}$.

The *indegree* of a vertex a in $G(n,k)$, denoted by $\mathrm{indeg}_n(a)$, is the number of directed edges coming into the vertex a, and the *outdegree* of a vertex a is the number of directed edges leaving the vertex a. Cycles of length t are called *t-cycles*, and cycles of length 1 are called *fixed points*. A fixed point is *isolated* if it is not connected to any other vertex in $G(n,k)$.

Attached to each cycle vertex c in $G(n,k)$ is a tree $T(c)$ whose root is c and whose additional vertices are the non-cycle vertices b such that $b^{k^i} \equiv c \pmod{n}$, for some positive integer i, but $b^{k^{i-1}}$ is not congruent modulo n to a cycle vertex in $G(n,k)$.

Let $G_1(n,k)$ denote the subdigraph of $G(n,k)$ induced on the set of vertices which are relatively prime to n, and let $G_2(n,k)$ denote the subdigraph of $G(n,k)$ induced on the set of vertices which are not relatively prime to n. It is clear that the digraph $G(n,k)$ is a disjoint union of the digraphs $G_1(n,k)$ and $G_2(n,k)$.

Let $M \geqslant 2$ be an integer. The digraph $G(n,k)$ is *symmetric* [5] of order M if its set of components can be partitioned into subsets of size M, each containing M isomorphic components. The digraph $G(n,k)$ is *semiregular* [6] if there exists a positive integer d such that each vertex of $G(n,k)$ either has indegree d or 0.

Let $n = \prod\limits_{i=1}^{r} p_i^{e_i}$, where p_i, $i = 1,2,\ldots,r$ are distinct primes. Let P be the set of all primes dividing n. Let P_1, P_2 be subsets of P such that $P_1 \cup P_2 = P$ and $P_1 \cap P_2 = \emptyset$. Let $G^*_{P_2}(n,k)$ denote the subdigraph of $G(n,k)$ induced on the set of vertices which are multiples of $\prod\limits_{p_i \in P_2} p_i$ and are relatively prime to all primes $q \in P_1$. Then $G^*_{P_2}(n,k)$ is called a *fundamental constituent* of $G(n,k)$. These subdigraphs were first introduced by B. Wilson [7].

B. Wilson [7] proved that the trees attached to all cycle vertices in $G_1(n,k)$ are isomorphic. In [4], L. Somer and M. Křížek proved that the trees attached to all cycle vertices in the same fundamental constituent of $G(n,k)$ are isomorphic. They also provide an example of a digraph whose trees attached to all cycle vertices in two distinct fundamental constituents are isomorphic. In Figure 1, the trees in the fundamental constituents $G^*_{\{3,13\}}(39,3)$ and $G^*_{\{13\}}(39,3)$ of $G(39,3)$ are trivial, and the trees attached to cycle vertices in $G^*_{\emptyset}(39,3)$ and $G^*_{\{3\}}(39,3)$ are isomorphic.

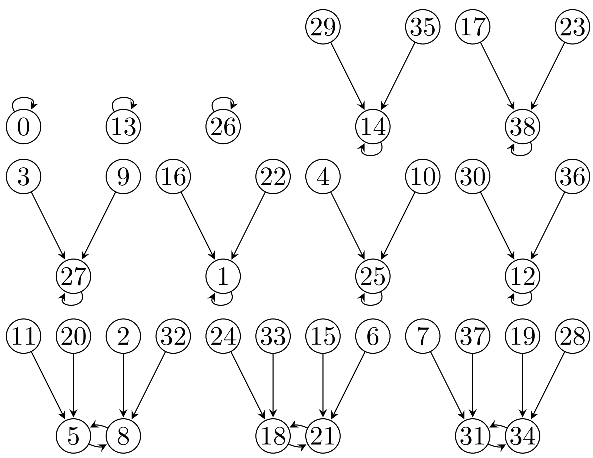

Figure 1. $G(39,3)$.

In this paper, we characterize n and k such that the trees attached to all cycle vertices in different fundamental constituents of $G(n,k)$ are isomorphic. We provide a relation between the tree structure of $G(n,k)$ and the symmetry and semiregularity property of $G(n,k)$. We also provide a necessary and sufficient condition on $G(n,k)$ such that the trees attached to all cycle vertices in $G(n,k)$ are isomorphic.

The outline of this paper is as follows. In Section 2, we give some basic properties of the Carmichael lambda function. In Section 3, we state basic results on $G(n,k)$ proved in [1], [2], [4]–[7]. In Section 4, we discuss important properties of the fundamental constituents of $G(n,k)$, which will be used throughout the paper. In particular, we discuss the product of two distinct fundamental constituents. Section 5 contains some lemmas which will be used in the main results. In Section 6, we prove the main results of this paper.

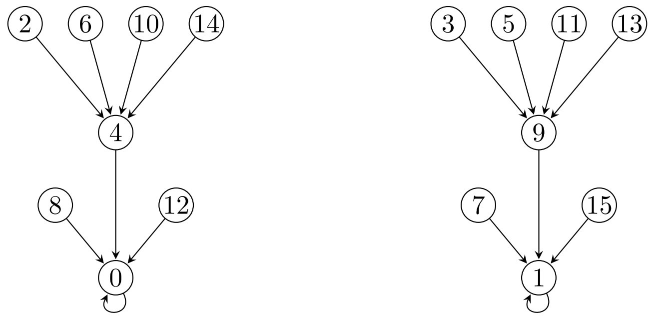

Figure 2. $G(16,2)$.

2. Carmichael lambda function

In this section, we give some basic properties of the Carmichael lambda function.

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

$$\lambda(1) = 1 = \varphi(1),$$
$$\lambda(2) = 1 = \varphi(2),$$
$$\lambda(4) = 2 = \varphi(4),$$
$$\lambda(2^k) = 2^{k-2} = \frac{1}{2}\varphi(2^k), \quad \text{for } k \geqslant 3,$$
$$\lambda(p^k) = p^{k-1}(p-1) = \varphi(p^k), \quad \text{for any odd prime } p \text{ and } k \geqslant 1,$$
$$\lambda\biggl(\prod_{i=1}^{r} p_i^{e_i}\biggr) = \operatorname{lcm}[\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \ldots, \lambda(p_r^{e_r})],$$

where $p_1, p_2, \ldots, p_r$ are distinct primes and $e_i \geqslant 1$ for all $i = 1, 2, \ldots, r$.

Theorem 2.2. *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 $\operatorname{ord}_n(g) = \lambda(n)$, where $\operatorname{ord}_n(g)$ denotes the multiplicative order of g modulo n.*

For more on the Carmichael lambda function, see [3].

3. Some results on $G(n, k)$

Consider a digraph $G(n, k)$. Let

$$\lambda(n) = uv,$$

where u is the largest divisor of $\lambda(n)$ relatively prime to k. We need the following results in this paper.

Lemma 3.1 ([7]). *Let $n = \prod_{i=1}^{r} p_i^{e_i}$, where p_i, $i = 1, 2, \ldots, r$ are distinct primes. Then there are $\prod_{i=1}^{r} \gcd(\lambda(p_i^{e_i}), u)$ cycle vertices in $G_1(n, k)$.*

Lemma 3.2 ([5]). *Every cycle in $G_1(n, k)$ is a fixed point if and only if $k \equiv 1 \pmod{u}$.*

Lemma 3.3 ([6]). *Every vertex in $G(n, k)$ is a cycle vertex if and only if $\gcd(\lambda(n), k) = 1$ and n is square-free.*

Lemma 3.4 ([4]). *Every vertex in $G(n, k)$ is a fixed point if and only if n is square-free and $k \equiv 1 \pmod{\lambda(n)}$.*

Lemma 3.5 ([4]). *The vertex 0 is an isolated fixed point of $G(n, k)$ if and only if n is square-free.*

Let $A_t(G(n, k))$ denote the number of t-cycles in $G(n, k)$.

Lemma 3.6 ([5]). *Let $n = \prod_{i=1}^{r} p_i^{e_i}$, where p_i, $i = 1, 2, \ldots, r$ are distinct primes. 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.

Lemma 3.7 ([7]). *Let c_1 and c_2 be any two cycle vertices in $G_1(n,k)$. Let $T(c_1)$ and $T(c_2)$ be trees attached to c_1 and c_2, respectively. Then $T(c_1) \cong T(c_2)$.*

Lemma 3.8 ([6]). *Let $n = \prod_{i=1}^{r} p_i^{e_i}$, where p_i, $i = 1, 2, \ldots, r$ are distinct primes, and $k \geqslant 2$ be integers. If $\gcd(\lambda(n), k) > 1$, then $G_1(n,k)$ is always semiregular. If a is a vertex in $G_1(n,k)$ and $\mathrm{indeg}_n(a) > 1$, then*

$$\mathrm{indeg}_n(a) = \varepsilon \prod_{i=1}^{r} \gcd(\lambda(p_i^{e_i}), k),$$

where $\varepsilon = 2$ if $2 \mid k$ and $8 \mid n$, and $\varepsilon = 1$ otherwise.

Lemma 3.9 ([6]). *Let p be an odd prime, and let $e \geqslant 1$, $\alpha \geqslant 1$ be integers. Let $k = Qp^e$, where $\gcd(Q,p) = 1$. Then $G_2(p^\alpha, k)$ is semiregular if and only if $1 \leqslant \alpha \leqslant k + e + 1$.*

Lemma 3.10 ([1]). *Let p be an odd prime and let α, $k \geqslant 2$ be two integers. Then $G(p^\alpha, k)$ is semiregular if and only if $\gcd\left(p^{\alpha-1}(p-1), k\right) = p^{\alpha-1}$.*

Lemma 3.11 ([1]). *Let p be an odd prime and $\alpha \geqslant 1$. Then $G(p^\alpha, k)$ is symmetric of order p if and only if $\gcd(p^{\alpha-1}(p-1), k) = p^{\alpha-1}$ and $k \equiv 1 \pmod{p-1}$.*

Lemma 3.12 ([7]). *Let $n = \prod_{i=1}^{r} p_i^{e_i}$, where p_i, $i = 1, 2, \ldots, r$ are distinct primes, and let a be a vertex of positive indegree in $G_1(n,k)$. Then*

$$\mathrm{indeg}_n(a) = \prod_{i=1}^{r} \varepsilon_i \gcd(\lambda(p_i^{e_i}), k),$$

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

Lemma 3.13 ([5]). *Let p be a prime and let $\alpha \geqslant 1$. Then*

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

Lemma 3.14 ([1]). *Let $k \geqslant 2$, $\alpha \geqslant 1$ be integers and let p be a prime. If a and b are two cycle vertices in the same cycle of $G(p^\alpha, k)$, then $\mathrm{indeg}_{p^\alpha}(a) = \mathrm{indeg}_{p^\alpha}(b)$.*

The *height* of a vertex b in $G(n,k)$ is the least non-negative integer i such that b^{k^i} is congruent modulo n to a cycle vertex in $G(n,k)$. We denote the height of a vertex b by $h(b)$. If C is a component of $G(n,k)$, we define $h(C) = \sup_{b \in C}(b)$.

Lemma 3.15 ([1]). *Let p be a prime and $\alpha \geqslant 1$, $k \geqslant 2$ be integers. Suppose that h is the unique positive integer such that $k^{h-1} < \alpha \leqslant k^h$. Then $h = h(G_2(p^\alpha, k))$.*

Lemma 3.16 ([1]). *Let p be a prime and $\alpha \geqslant 1$, $k \geqslant 2$ be integers. Let $\lambda(p^\alpha) = uv$, where u is the largest divisor of $\lambda(p^\alpha)$ relatively prime to k. If C is the component of $G(p^\alpha, k)$ containing 1, then $h(C) = \min\{i\colon\ v \mid k^i\}$.*

Now we discuss the digraph product and some of its properties. Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$, $n_1 > 1$, $n_2 \geqslant 1$. Let $k \geqslant 2$ be an integer. Then it was proved in [5] that we can write

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

The isomorphism is given by $a \mapsto (a_1, a_2)$, where $a \equiv a_i \pmod{n_i}$, for $i = 1, 2$.

In general, if $n = \prod\limits_{i=1}^{r} p_i^{e_i}$, where p_i, $i = 1, 2, \ldots, r$ are distinct primes, then

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

Lemma 3.17 ([2]). *Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$. Let $a = (a_1, a_2)$ be a vertex in $G(n,k) \cong G(n_1,k) \times G(n_2,k)$. Then*

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

Lemma 3.18 ([7]). *Let $n = \prod\limits_{i=1}^{r} p_i^{e_i}$, where p_i, $i = 1, 2, \ldots, r$ are distinct primes. Let $a = (a_1, a_2, \ldots, a_r)$ be a vertex in $G(n,k) \cong G(p_1^{e_1},k) \times G(p_2^{e_2},k) \times \ldots \times G(p_r^{e_r},k)$. Then*

$$\operatorname{indeg}_n(a) = \prod_{i=1}^{r} \operatorname{indeg}_{q_i}(a_i), \quad \text{where } q_i = p_i^{e_i}.$$

Lemma 3.19 ([2]). *Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$. Let C_1 be a component of $G(n_1,k)$ and C_2 be a component of $G(n_2,k)$. Let the cycle length of C_i be t_i. Then $C_1 \times C_2$ is a subdigraph of $G(n,k)$ consisting of $\gcd(t_1,t_2)$ components, each having an $\operatorname{lcm}[t_1,t_2]$-cycle.*

Lemma 3.20 ([5]). *Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$. Let $c = (c_1, c_2)$ be a vertex in $G(n,k) \cong G(n_1,k) \times G(n_2,k)$. 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 $i = 1, 2$.*

Lemma 3.21 ([5]). *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 $G(n,k)\cong G(n_1,k)\times G(n_2,k)$. Moreover, if*

$$L(n_2,k)=\bigcup_{i=1}^{m} L_i(n_2,k),$$

where $L_i(n_2,k)$ are distinct components of $G(n_2,k)$, for $i=1,2,\ldots,m$, then

$$J(n_1,k)\times L(n_2,k)=\bigcup_{i=1}^{m} J(n_1,k)\times L_i(n_2,k),$$

where the union is a disjoint union.

Definition 3.22 ([1]). For any positive integers t and m, we define O_t^m to be the digraph which satisfies the following conditions:

(i) O_t^m has a t-cycle;
(ii) $\operatorname{indeg}(a)=m$ if a is a cycle vertex, and $\operatorname{indeg}(a)=0$ otherwise.

Lemma 3.23 ([1]). *$O_1^m\times G\cong O_1^m\times H$ if and only if $G\cong H$, for any digraphs G and H.*

4. Fundamental constituents of $G(n,k)$

Let $n=n_1n_2$, where $\gcd(n_1,n_2)=1$. Let P be the set of primes dividing n. Let P_1, P_2 be subsets of P such that $P_1\cup P_2=P$ and $P_1\cap P_2=\emptyset$. Suppose that $n_1=\prod_{p_i\in P_1} p_i^{e_i}$ and $n_2=\prod_{p_i\in P_2} p_i^{e_i}$. Let $L(n_2,k)$ denote the subdigraph of $G_2(n_2,k)$ induced on the set of vertices of $G_2(n_2,k)$ which are multiples of $\prod_{p_i\in P_2} p_i$. It is clear that $L(n_2,k)$ is a single component of $G(n_2,k)$ with the fixed point 0.

Then we have (see [4])

$$G^*_{P_2}(n,k)\cong G_1(n_1,k)\times L(n_2,k). \tag{4.1}$$

If $P_1=\emptyset$, then $n_2=n$ and $G^*_{P_2}(n,k)\cong L(n,k)$. If $P_2=\emptyset$, then $n_1=n$ and $G^*_{P_2}(n,k)\cong G_1(n,k)$. It was discussed in [4] that $G^*_{P_1}(n,k)$ and $G^*_{P_2}(n,k)$ are disjoint unions of components of $G(n,k)$, and $G_2(n,k)$ is a disjoint union of $G^*_{P_2}(n,k)$, where P_2 ranges over all the nonempty subsets of P.

Let $l = mn$, where $\gcd(m,n) = 1$. Let $m = \prod_{i=1}^{r} p_i^{e_i}$ and $n = \prod_{i=r+1}^{r+s} p_i^{e_i}$, where p_i, $i = 1,2,\ldots,r+s$ are distinct primes. Let $P = \{p_1,p_2,\ldots,p_r\}$ and $Q = \{p_{r+1},p_{r+2},\ldots,p_{r+s}\}$. Let $G^*_{P_2}(m,k)$ and $G^*_{Q_2}(n,k)$ be fundamental constituents of $G(m,k)$ and $G(n,k)$, respectively, where $P_2 \subseteq P$ and $Q_2 \subseteq Q$. Then from (4.1), we see that

$$G^*_{P_2}(m,k) \times G^*_{Q_2}(n,k) \cong G^*_{P_2\cup Q_2}(l,k).$$

Also note that if $R = \{p_1,p_2,\ldots,p_r,p_{r+1},p_{r+2},\ldots,p_{r+s}\}$ and $R_2 \subseteq R$, then

$$G^*_{R_2}(l,k) \cong G^*_{R_2^i}(l_i,k) \times G^*_{R_2^j}(l_j,k), \tag{4.2}$$

where R_2^i, R_2^j are subsets of R_2 such that $R_2^i \cup R_2^j = R_2$, $R_2^i \cap R_2^j = \emptyset$, and $l_il_j = l$, where $\gcd(l_i,l_j) = 1$ and $R_2^i = \{p_i \in R_2\colon\ p_i \mid l_i\}$, $R_2^j = \{p_j \in R_2\colon\ p_j \mid l_j\}$.

Thus we see that the product of a fundamental constituent of $G(m,k)$ and a fundamental constituent of $G(n,k)$ results in a fundamental constituent of $G(l,k)$. Also, any fundamental constituent of $G(l,k)$ can be decomposed into a product of a fundamental constituent of $G(m,k)$ and a fundamental constituent of $G(n,k)$. This property of the fundamental constituents will be our main technique to prove the main results in this paper.

Note. If $G^*_{Q_2}(m,k)$ is a fundamental constituent of $G(m,k)$, then $G^*_{Q_2}(l,k)$ is also a fundamental constituent of $G(l,k)$, and

$$G^*_{Q_2}(l,k) \cong G^*_{Q_2}(m,k) \times G^*_{\emptyset}(n,k).$$

Let $n = \prod_{i=1}^{r} p_i^{e_i}$ be the prime factorization of n and P be the set of all primes dividing n. Let $P_2 = \{p_1,p_2,\ldots,p_s\}$, for any s such that $1 \leqslant s \leqslant r$. Then

$$\begin{aligned} G^*_{P_2}(n,k) \cong G^*_{\{p_1\}}(p_1,k) &\times G^*_{\{p_2\}}(p_2,k) \times \ldots \\ &\times G^*_{\{p_s\}}(p_s,k) \times G^*_{\emptyset}(p_{s+1},k) \times \ldots \times G^*_{\emptyset}(p_r,k). \end{aligned}$$

Theorem 4.1 ([4])**.** *Let $n = \prod_{i=1}^{r} p_i^{e_i}$, where p_i, $i = 1,2,\ldots,r$ are distinct primes and let P be the set of primes dividing n. Let P_1, P_2 be subsets of P such that $P_1 \cup P_2 = P$ and $P_1 \cap P_2 = \emptyset$. Let c_1, c_2 be two cycle vertices in $G^*_{P_2}(n,k)$ and let $T(c_1)$ and $T(c_2)$ be the trees attached to c_1 and c_2, respectively. Then $T(c_1) \cong T(c_2)$.*

5. Preliminary lemmas

Lemma 5.1. *Let $n = n_1n_2$, where $\gcd(n_1, n_2) = 1$, $n_1 > 1$, $n_2 \geqslant 1$. Let P and Q be the set of all primes dividing n_1 and n_2, respectively. Let $G^*_{P_2\cup Q'}(n,k)$ and $G^*_{Q'}(n,k)$ be fundamental constituents of $G(n,k)$, for any $Q' \subseteq Q$ and $\emptyset \neq P_2 \subseteq P$.*

(i) *Let $n_1 = p_1p_2\dots p_r$, where p_i, $i = 1, 2, \dots, r$ are distinct odd primes. Let $P_2 = \{p_1, p_2, \dots, p_s\}$, for any integer s such that $1 \leqslant s \leqslant r$. Suppose that $k \equiv 1 \pmod{\lambda(n_1)}$. Then $G^*_{Q'}(n,k)$ consists of $(p_1-1)(p_2-1)\dots(p_s-1)$ subgraphs of $G(n,k)$, each isomorphic to $G^*_{P_2\cup Q'}(n,k)$.*

(ii) *Let $n_1 = p^{\alpha}$, where p is an odd prime and $\alpha \geqslant 1$. Suppose that $k \equiv 1 \pmod{p-1}$ and $p^{\alpha-1}/k$. Then $G^*_{Q'}(n,k)$ consists of $(p-1)$ subgraphs of $G(n,k)$, each isomorphic to $G^*_{\{p\}\cup Q'}(n,k)$.*

Proof. We prove the first part. By Lemma 3.2, we see that every vertex in $G_1(n_1,k)$ is a fixed point. Also, by Lemma 3.6, we have

$$A_1(G(n_1,k)) = \prod_{i=1}^{r}(\gcd(\lambda(p_i), k-1)+1) = \prod_{i=1}^{r}[(p_i-1)+1] = \prod_{i=1}^{r} p_i = n_1.$$

Hence, $G(n_1,k)$ consists only of isolated fixed points.

Let $Q' \subseteq Q$ and $\emptyset \neq P_2 \subseteq P$, for any s such that $1 \leqslant s \leqslant r$. Then by (4.2),

$$G^*_{Q'}(n,k) \cong G^*_{\emptyset}(n_1,k) \times G^*_{Q'}(n_2,k),$$
$$G^*_{P_2\cup Q'}(n,k) \cong G^*_{P_2}(n_1,k) \times G^*_{Q'}(n_2,k).$$

By (4.1) and Lemma 3.5, we see that $G^*_{\emptyset}(n_1,k)$ consists of $\varphi(n_1)$ isolated fixed points, and $G^*_{P_2}(n_1,k)$ consists of $(p_{s+1}-1)(p_{s+2}-1)\dots(p_r-1)$ isolated fixed points, for any s such that $1 \leqslant s \leqslant r$.

Let $m = (p_{s+1}-1)(p_{s+2}-1)\dots(p_r-1)$. Then we have

$$G^*_{Q'}(n,k) \cong \bigcup_{i=1}^{\varphi(n_1)} F_i(n_1,k) \times G^*_{Q'}(n_2,k),$$
$$G^*_{P_2\cup Q'}(n,k) \cong \bigcup_{i=1}^{m} E_j(n_1,k) \times G^*_{Q'}(n_2,k),$$

where $F_i(n_1,k)$ and $E_j(n_1,k)$ are components of $G^*_{\emptyset}(n_1,k)$ and $G^*_{P_2}(n_1,k)$, respectively, for $i = 1, 2, \dots, \varphi(n_1)$ and $j = 1, 2, \dots, m$. Also, by Lemma 3.23 we see that

$$F_i(n_1,k) \times G^*_{Q'}(n_2,k) \cong E_j(n_1,k) \times G^*_{Q'}(n_2,k),$$

for all i, j.

Hence, $G^*_{Q'}(n,k)$ consists of $(p_1-1)(p_2-1)\dots(p_s-1)$ subgraphs of $G(n,k)$, for any s such that $1\leqslant s\leqslant r$, each subgraph is isomorphic to $G^*_{P_2\cup Q'}(n,k)$.

We now prove the second part. Assume that $k\equiv 1 \pmod{p-1}$ and $p^{\alpha-1}\mid k$. By Lemma 3.2, we see that every cycle in $G_1(n_1,k)$ is a fixed point. By Lemma 3.6, we have

$$A_1(G(n_1,k)) = \gcd(p^{\alpha-1}(p-1),k-1)+1=(p-1)+1=p.$$

Also, note that the only cycle vertex in $G_2(n_1,k)$ is the fixed point 0. Thus, every cycle in $G(n_1,k)$ is a fixed point.

Let $a_1,a_2,\dots,a_p$ be the fixed points of $G(n_1,k)$. Then by Lemma 3.12 and Lemma 3.13, it follows that

$$\mathrm{indeg}_{p^\alpha}(a_i)=(p^{\alpha-1}(p-1),k)=p^{\alpha-1},\quad \text{for } i=1,2,3,\dots,p.$$

This implies that $\sum\limits_{i=1}^{p}\mathrm{indeg}_{p^\alpha}(a_i)=p^\alpha=n_1$. It follows that the height of each component of $G(n_1,k)$ is 1. Hence, all the components of $G(n_1,k)$ are isomorphic.

Consider $G^*_{\emptyset}(n_1,k)$ and $G^*_{\{p\}}(n_1,k)$, the fundamental constituents of $G(n_1,k)$. We know that $G^*_{\emptyset}(n_1,k)$ consists of $p-1$ isomorphic components and $G^*_{\{p\}}(n_1,k)$ consists of only one component.

Let $G^*_{Q'}(n_2,k)$ be a fundamental constituent of $G(n_2,k)$, for any $Q'\subseteq Q$. Then, by (4.2)

$$G^*_{Q'}(n,k)\cong G^*_{\emptyset}(n_1,k)\times G^*_{Q'}(n_2,k)\cong \bigcup_{i=1}^{p-1} O_{1_i}^{p^{\alpha-1}}\times G^*_{Q'}(n_2,k),$$
$$G^*_{\{p\}\cup Q'}(n,k)\cong G^*_{\{p\}}(n_1,k)\times G^*_{Q'}(n_2,k)\cong O_1^{p^{\alpha-1}}\times G^*_{Q'}(n_2,k).$$

Hence, by Lemma 3.23, it follows that $G^*_{Q'}(n,k)$ consists of $p-1$ subgraphs of $G(n,k)$, each isomorphic to $G^*_{Q'\cup\{p\}}(n,k)$. □

Lemma 5.2. *Let p be a prime, let $\alpha\geqslant 1$ and $k\geqslant 2$ be integers. Suppose that the trees attached to all cycle vertices in $G(p^\alpha,k)$ are isomorphic. Then the trees attached to all cycle vertices in $G(p^\alpha,k^r)$, for any positive integer r, are also isomorphic.*

P r o o f. If C is a component of $G(p^\alpha,k^r)$, then $|C|\leqslant|D|$, where D is a component of $G(p^\alpha,k)$ and D contains all the vertices of C. Note that a is a cycle vertex of $G(p^\alpha,k)$ if and only if a is also a cycle vertex of $G(p^\alpha,k^r)$, for any positive integer r. Let a_0 be a fixed point in $G(p^\alpha,k)$, as well as a fixed point in $G(p^\alpha,k^r)$. If C

is a component of $G(p^\alpha, k^r)$ with the fixed point a_0, then $|C| = |D|$, where D is a component of $G(p^\alpha, k)$ with the fixed point a_0 and containing all the vertices of C. That is, the components C and D have the same vertices but the edges may be different.

Let $T(0)$ and $T(1)$ be the trees attached to the fixed points 0 and 1, respectively, in $G(p^\alpha, k)$. By hypothesis, there exists a digraph isomorphism φ from $T(0)$ onto $T(1)$. Let $T'(0)$ and $T'(1)$ denote the trees attached to the fixed points 0 and 1, respectively, in $G(p^\alpha, k^r)$, for any positive integer r. It is enough to show that $T'(0) \cong T'(1)$.

Let a and b be two vertices in $T'(0)$ such that $a^{k^r} \equiv b \pmod{p^\alpha}$. Then there exist vertices $x_1, x_2, \ldots, x_r = b$ such that

$$a^k \equiv x_1 \pmod{p^\alpha},\ x_1^k \equiv x_2 \pmod{p^\alpha},\ \ldots,\ x_{r-1}^k \equiv b \pmod{p^\alpha}.$$

Since $T'(0)$ and $T(0)$ have the same vertices, and since φ is an isomorphism, we have

$$\varphi(a)^k \equiv \varphi(x_1) \pmod{p^\alpha},\ \varphi(x_1)^k \equiv \varphi(x_2) \pmod{p^\alpha},\ \ldots,\ \varphi(x_{r-1})^k \equiv \varphi(b) \pmod{p^\alpha}.$$

Thus, $\varphi(a)^{k^r} \equiv \varphi(b) \pmod{p^\alpha}$ in $T(1)$ as well as in $T'(1)$. Hence, $T'(0) \cong T'(1)$. □

Theorem 5.3 ([2]). *Let $n = pq_1q_2\ldots q_r$, where p and q_i, $i = 1, 2, \ldots, r$ are distinct odd primes. Suppose $G(p, k)$ is not symmetric of order p. Then $G(n, k)$ is symmetric of order p if and only if both of the following conditions are satisfied.*

(i) $\gcd(p-1, k) = 1$.

(ii) *Let $T = \{q_i \mid \gcd(q_i - 1, k) = 1\}$. Then T is not empty and for all $t \in \mathbb{N}$, $p \mid A_t\Bigl(G\Bigl(\prod_{q_i \in T} q_i, k\Bigr)\Bigr)$ or $\operatorname{ord}_{p-1} k \mid t$.*

Corollary 5.4. *Let $n = pq_1q_2\ldots q_r$, where p and q_i, $i = 1, 2, \ldots, r$ are distinct odd primes. Let $k \geqslant 2$ be an integer such that $\gcd(p-1, k) = \gcd(q_i - 1, k) = 1$, for all i. Suppose that $G(n, k)$ is symmetric of order p and $G(p, k)$ is not symmetric of order p. Then $p \mid A_1(G(q_1q_2\ldots q_r, k))$.*

Proof. This follows from Lemma 3.11 and Theorem 5.3. □

6. Main results

Theorem 6.1. *Let $l = mn$, where $\gcd(m,n) = 1$, and let $k \geqslant 2$ be an integer. Let $G^*_{P_1}(m,k)$ and $G^*_{P_2}(m,k)$ be two distinct fundamental constituents of $G(m,k)$ such that the trees attached to all cycle vertices in $G^*_{P_1}(m,k)$ and $G^*_{P_2}(m,k)$ are isomorphic. Let $G^*_Q(n,k)$ be a fundamental constituent of $G(n,k)$. Then the trees attached to all cycle vertices in the fundamental constituents $G^*_{Q\cup P_1}(l,k)$ and $G^*_{Q\cup P_2}(l,k)$ of $G(l,k)$ are isomorphic.*

Proof. By (4.2), we have

$$G^*_{P_1\cup Q}(l,k) \cong G^*_{P_1}(m,k) \times G^*_Q(n,k),$$
$$G^*_{P_2\cup Q}(l,k) \cong G^*_{P_2}(m,k) \times G^*_Q(n,k).$$

Let $a_1, a_2, \ldots, a_r$ be the cycle vertices of $G^*_{P_1}(m,k)$, $b_1, b_2, \ldots, b_s$ be the cycle vertices of $G^*_{P_2}(m,k)$, and $c_1, c_2, \ldots, c_t$ be the cycle vertices of $G^*_Q(n,k)$, for any positive integers r, s, and t.

Then by Lemma 3.20, the cycle vertices of $G^*_{P_1\cup Q}(l,k)$ and $G^*_{P_2\cup Q}(l,k)$ are of the form (a_i, c_j) and (b_x, c_j), respectively, for all i, j, x such that $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant t$, and $1 \leqslant x \leqslant s$. It now suffices to show that the trees attached to cycle vertices (a_i, c_j) and (b_x, c_j) are isomorphic, for all i, j, x. In view of Theorem 4.1, it is enough to show that $T(a_1, c_1)$ is isomorphic to $T(b_1, c_1)$.

By hypothesis, there exists a digraph isomorphism φ_{ij} from $T(a_i)$ onto $T(b_j)$, for all i, j such that $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$. Note that φ_{ij} maps a vertex at height h in $T(a_i)$ to a vertex at the same height in $T(b_j)$. Now, we define a map F from $T(a_1, c_1)$ into $T(b_1, c_1)$ as $F((u,v)) = (\varphi_{11}(u), v)$, for each vertex (u,v) in $T(a_1, c_1)$. We first show that F is well-defined. Suppose that (u,v) is a cycle vertex in $T(a_1, c_1)$. Then

$$F((u,v)) = F((a_1, c_1)) = (\varphi_{11}(a_1), c_1) = (b_1, c_1).$$

Now assume that a vertex (u,v) is at height $h \geqslant 1$ in $T(a_1, c_1)$. Then h is the least positive integer such that $(u,v)^{k^h} = (a_1, c_1)$. It follows that u is at height h in $T(a_1)$ or v is at height h in $T(c_1)$. If one of u or v is at height h, then the other is at height i such that $i \leqslant h$. Since φ_{11} is a digraph isomorphism, then

$$\begin{aligned}[F((u,v))]^{k^h} &= (\varphi_{11}(u), v)^{k^h} = (\varphi_{11}(u)^{k^h}, v^{k^h}) \\ &= (\varphi_{11}(u^{k^h}), v^{k^h}) = (\varphi_{11}(a_1), c_1) = (b_1, c_1).\end{aligned}$$

If $1 \leqslant i < h$, then it follows from Lemma 3.20 that $[F((u,v))]^{k^i} = (\varphi_{11}(u^{k^i}), v^{k^i})$ is not a cycle vertex in $T(b_1, c_1)$. Hence, F maps a vertex at height h in $T(a_1, c_1)$

to a vertex at the same height in $T(b_1, c_1)$. We now show that F is a digraph isomorphism.

Clearly, F is one-one. We now show that F is onto. First note that $(b_1, c_1) = (\varphi_{11}(a_1), c_1) = F((a_1, c_1))$. Let (u, v) be a vertex at height $h \geqslant 1$ in $T(b_1, c_1)$. Assume that u is at height h in $T(b_1)$ and v is at height i such that $i \leqslant h$ in $T(c_1)$. Since φ_{11} is a digraph isomorphism, there exists a vertex w at height h in $T(a_1)$ such that $\varphi_{11}(w) = u$. Then (w, v) is at height h in $T(a_1, c_1)$ and $F((w, v)) = (\varphi_{11}(w), v) = (u, v)$. Similarly, if v is at height h in $T(c_1)$, then $F((w, v)) = (\varphi_{11}(w), v) = (u, v)$, where w is at height i such that $i \leqslant h$ in $T(a_1)$. Hence, F is onto.

Finally, we show that F preserves direction. Let (u_1, v_1) and (u_2, v_2) be two non-cycle vertices in $T(a_1, c_1)$. Suppose there exists a directed edge from (u_1, v_1) to (u_2, v_2). Since φ_{11} is edge-preserving, we have

$$\begin{aligned}[F((u_1, v_1))]^k &= (\varphi_{11}(u_1), v_1)^k = (\varphi_{11}(u_1)^k, v_1^k) \\ &= (\varphi_{11}(u_1^k), v_1^k) = (\varphi_{11}(u_2), v_2) = F((u_2, v_2)).\end{aligned}$$

□

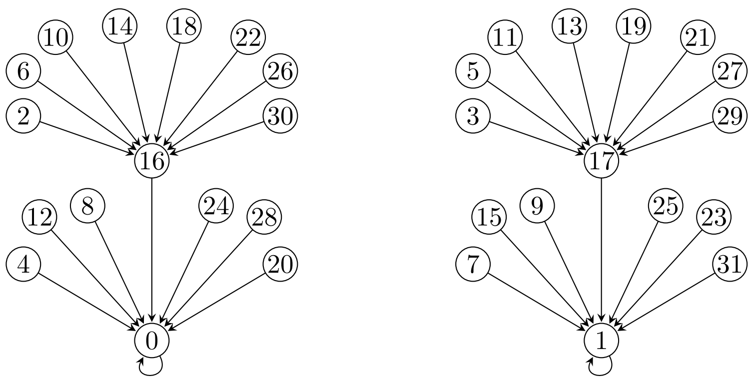

Figure 3. $G(32, 4)$.

Theorem 6.2. *Let $\alpha \geqslant 1$, and let $k \geqslant 2$ be an integer. Then $G(2^\alpha, k)$ is symmetric of order 2 if and only if the trees attached to all cycle vertices in $G(2^\alpha, k)$ are isomorphic.*

P r o o f. If $G(2^\alpha, k)$ is symmetric of order 2, or if the trees attached to all cycle vertices in $G(2^\alpha, k)$ are isomorphic, then $G(2^\alpha, k)$ has exactly two isomorphic components, one containing the fixed point 0 and the other containing the fixed point 1. Hence, the result follows. □

Corollary 6.3. *Let $\alpha \geqslant 1$, and let $k \geqslant 2$ be an integer. Suppose that the trees attached to all cycle vertices in $G(2^\alpha, k)$ are isomorphic. Then k must be an even integer.*

Proof. By Theorem 6.2, the only cycle vertices in $G(2^\alpha, k)$ are the fixed points 0 and 1. Now, $A_1(G(2^\alpha, k)) = \gcd(\lambda(2^\alpha), k-1)+1$. If k is odd, then $A_1(G(2^\alpha, k)) \geqslant 3$, which is a contradiction. Hence, k must be even. $\square$

Theorem 6.4. *Let p be an odd prime and $\alpha \geqslant 1$. Let $k \geqslant 2$ be an integer. Then the trees attached to all cycle vertices in $G(p^\alpha, k)$ are isomorphic if and only if $\gcd(p^{\alpha-1}(p-1), k) = p^{\alpha-1}$.*

Proof. Assume that $\gcd(p-1, k) = d > 1$ or $p \nmid k$ when $\alpha > 1$. Let $h = h(G(p^\alpha, k))$. Then $h(G(p^\alpha, k^h)) = 1$. By Lemma 3.14, we have

$$G(p^\alpha, k^h) = G_2(p^\alpha, k^h) \cup G_1(p^\alpha, k^h) = O_1^{p^{\alpha-1}} \cup a_1 O_1^m \cup a_2 O_2^m \cup \ldots \cup a_t O_t^m,$$

where $a_i = A_i(G_1(p^\alpha, k^h))$ and $m = \gcd(p^{\alpha-1}(p-1), k^h)$. By our assumption, $m \neq p^{\alpha-1}$. This implies that the trees attached to cycle vertices in $G_1(p^\alpha, k^h)$ and $G_2(p^\alpha, k^h)$ are not isomorphic. By Lemma 5.2, the trees attached to cycle vertices in $G_1(p^\alpha, k)$ and $G_2(p^\alpha, k)$ are also not isomorphic. Hence, $\gcd(p-1, k) = 1$ and $p \mid k$ when $\alpha > 1$.

We now assume that $p^r || k$, for some positive integer r. By hypothesis, $h(T(0)) = h(T(1)) = h_0$. By Lemma 3.15 and Lemma 3.16, we have $k^{h_0-1} < \alpha \leqslant k^{h_0}$ and $p^{\alpha-1} \mid k^{h_0}$. Then $r(h_0-1) < \alpha - 1 \leqslant rh_0$. Then $p^{r(h_0-1)} \leqslant k^{h_0-1} \leqslant \alpha - 1 \leqslant rh_0$, which implies that $h_0 = 1$. Thus, the height of all components of $G(p^\alpha, k)$ is 1. Then we can write

$$G(p^\alpha, k) = O_1^{p^{\alpha-1}} \cup a_1 O_1^m \cup a_2 O_2^m \cup \ldots \cup a_t O_t^m,$$

where $a_i = A_i(G_1(p^\alpha, k))$.

Also, $\mathrm{indeg}_{p^\alpha}(a) = p^r$, if a is a cycle vertex in $G_1(p^\alpha, k)$, and $\mathrm{indeg}_{p^\alpha}(a) = 0$ otherwise. By hypothesis, we get $m = p^r = p^{\alpha-1}$, which implies $r = \alpha - 1$. Hence, the result follows.

Now we prove the converse. Assume that $\gcd(p^{\alpha-1}(p-1), k) = p^{\alpha-1}$. Then the indegree of any vertex in $G(p^\alpha, k)$ is 0 or $p^{\alpha-1}$. Also, the indegree of all cycle vertices in $G(p^\alpha, k)$ is $p^{\alpha-1}$. By Lemma 3.1, the number of cycle vertices in $G_1(p^\alpha, k)$ is $p-1$. It follows that the number of cycle vertices in $G(p^\alpha, k)$ is p. Thus, this implies that the height of all components in $G(p^\alpha, k)$ is 1. Hence, the result follows. $\square$

Corollary 6.5. *Let p be an odd prime and $\alpha \geqslant 1$. Let $k \geqslant 2$ be an integer. Then the trees attached to all cycle vertices in $G(p^\alpha, k)$ are isomorphic if and only if $G(p^\alpha, k)$ is semiregular.*

Corollary 6.6. *Let p be an odd prime and $\alpha \geqslant 1$. Let $k \geqslant 2$ be an integer. Suppose that $G(p^\alpha, k)$ is symmetric of order p. Then the trees attached to all cycle vertices in $G(p^\alpha, k)$ are isomorphic.*

The converse of Corollary 6.6 does not hold. For example, the trees attached to all cycle vertices in $G(49, 35)$ are isomorphic, but $G(49, 35)$ is not symmetric (see Figure 4). However, if $k \equiv 1 \pmod{p-1}$, then the converse is also true. This follows from Theorem 6.4 and Lemma 3.11.

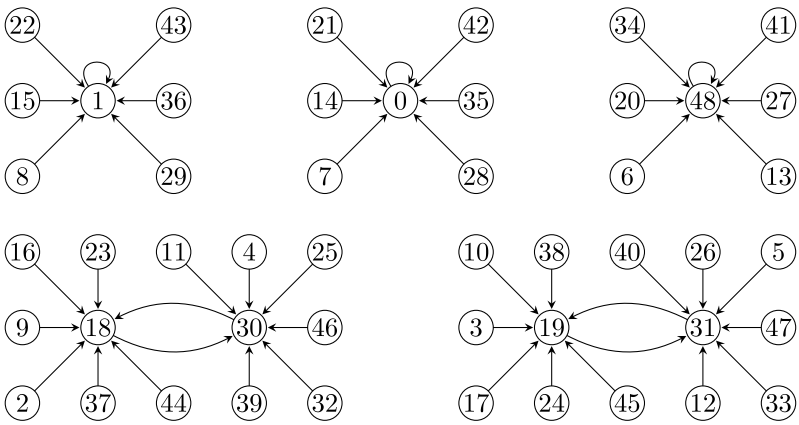

Figure 4. $G(49, 35)$.

Theorem 6.7. *Let $n = p_1 p_2 \ldots p_r$, where p_i, $i = 1, 2, \ldots, r$ are distinct odd primes. Suppose that for any fundamental constituent $G^*_P(n, k)$ of $G(n, k)$, there exists a distinct fundamental constituent $G^*_Q(n, k)$ such that the trees attached to all cycle vertices in $G^*_P(n, k) \cup G^*_Q(n, k)$ are isomorphic. Then, $G(p_i, k)$ consists only of cycles, for at least one i such that $1 \leqslant i \leqslant r$, and conversely. Moreover, if $G(p_i, k)$ consists only of cycles for all i, then the trees attached to all cycle vertices in $G(n, k)$ are isomorphic.*

P r o o f. From Lemma 3.5, we see that 0 is an isolated fixed point of $G(p_i, k)$, for all i. Suppose that $G(p_i, k)$ contains some nontrivial trees, for all i. Then using Lemma 3.7, the indegree of all non-zero cycle vertices in $G(p_i, k)$ is greater than 1, for all i. Note that the cycle vertices of $G(n, k)$ are of the form $a = (a_1, a_2, \ldots, a_r)$, where each a_i is a cycle vertex of $G(p_i, k)$. By Lemma 3.18,

$$\operatorname{indeg}_n(a) = \prod_{i=1}^{r} \operatorname{indeg}_{p_i}(a_i).$$

Thus, $\operatorname{indeg}_n(a) > 1$, unless $a = (0, 0, \ldots, 0)$. That is, the only cycle vertex in $G(n, k)$ with indegree 1 is the fixed point 0. Since $G^*_{\{p_1, p_2, \ldots, p_r\}}(n, k)$ is the only fundamental constituent of $G(n, k)$ with trivial trees, the result follows.

Conversely, assume that $G(p_i, k)$ consists only of cycles for at least one i such that $1 \leqslant i \leqslant r$. Then the trees attached to all cycle vertices in the fundamental constituents $G^*_{\emptyset}(p_i, k)$ and $G^*_{\{p_i\}}(p_i, k)$ are isomorphic, in fact the trees are trivial. Let $G^*_Q(n, k)$ be any fundamental constituent of $G(n, k)$. Let $m_i = p_1 p_2 \ldots p_{i-1} p_{i+1} \ldots p_r$. Then by (4.2),

$$G^*_Q(n, k) \cong G^*_{Q_1}(p_i, k) \times G^*_{Q_2}(m_i, k),$$

where $Q_1 = \{p \in Q \colon\ p \mid p_i\}$, $Q_2 = \{p \in Q \colon\ p \mid m_i\}$. Then there exists a fundamental constituent $G^*_{Q_1'}(p_i, k)$ of $G(p_i, k)$ such that the trees attached to all cycle vertices in $G^*_{Q_1}(p_i, k) \cup G^*_{Q_1'}(p_i, k)$ are isomorphic. By Theorem 6.1, the trees attached to all cycle vertices in $G^*_Q(n, k) \cup G^*_{Q_1' \cup Q_2}(n, k)$ are isomorphic.

The second part follows directly from Lemma 3.20. $\square$

Corollary 6.8. *Let $n = p_1 p_2 \ldots p_r$, where p_i, $i = 1, 2, \ldots, r$ are distinct odd primes, and let $k \geqslant 2$ be an integer. Suppose that $G(n, k)$ is symmetric of order n. Then the trees attached to all cycle vertices in $G(n, k)$ are isomorphic.*

The converse of Corollary 6.8 does not hold. For example, the digraph $G(35, 11)$ has trivial trees but it is not symmetric (see Figure 5).

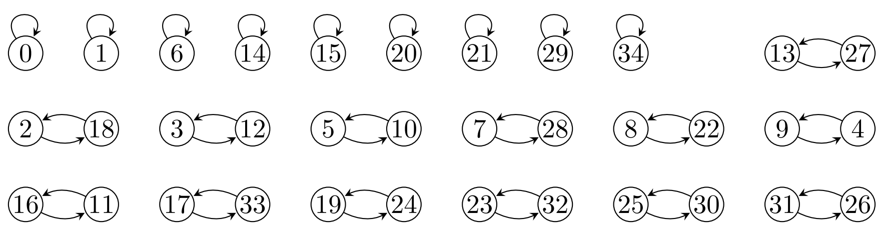

Figure 5. $G(35, 11)$.

Corollary 6.9. *Let $n = pq_1q_2\dots q_r$, where p and q_i, $i = 1,2,\dots,r$ are distinct odd primes. Let $k \geqslant 2$ be an integer such that $\gcd(p-1,k) = \gcd(q_i-1,k) = 1$, for all i. Let $Q \subseteq \{q_1,q_2,\dots,q_r\}$ and consider the fundamental constituent $G^*_Q(q_1q_2\dots q_r,k)$ of $G(q_1q_2\dots q_r,k)$. Suppose that $G(p,k)$ is symmetric of order p. Then $G^*_Q(n,k)\cup G^*_{Q\cup\{p\}}(n,k)$, which is a subdigraph of $G(n,k)$, is symmetric of order p.*

Proof. Since $G(p,k)$ is symmetric of order p, then by Lemma 3.11 we see that $k \equiv 1 \pmod{p-1}$. Let C be a component of $G^*_Q(n,k)$. Then by Lemma 5.1 (ii), there exist distinct components $C_1,C_2,\dots,C_{p-2}$ of $G^*_Q(n,k)$ and one component C_{p-1} of $G^*_{Q\cup\{p\}}(n,k)$ such that each C_i is isomorphic to C, for $i = 1,2,\dots,p-1$. Similarly, it is the case if we take C to be a component of $G^*_{Q\cup\{p\}}(n,k)$. Hence, $G^*_Q(n,k)\cup G^*_{Q\cup\{p\}}(n,k)$ is symmetric of order p. □

Corollary 6.9 does not hold when $G(p,k)$ is not symmetric of order p, even though $G(n,k)$ is symmetric of order p. Consider the following example.

Example. Consider the digraphs $G(5,15)$ and $G(29,15)$. Note that both $G(5,15)$ and $G(29,15)$ consist only of cycles. By Lemma 3.11, $G(5,15)$ is not symmetric of order 5. Now, $A_1(G(5,15)) = 3$, $A_2(G(5,15)) = 1$, $A_1(G(29,15)) = 15$, and $A_2(G(29,15)) = 7$. Also, $A_1(G(5\times 29,15)) = 45$ and $A_2(G(5\times 29,15)) = 50$. Hence, $G(5\times 29,15)$ is symmetric of order 5.

Consider the fundamental consituents $G^*_\emptyset(145,15)$, $G^*_{\{5\}}(145,15)$, $G^*_{\{29\}}(145,15)$ and $G^*_{\{5,29\}}(145,15)$ of $G(145,15)$. By (4.2), we have

$$\begin{aligned} G^*_\emptyset(145,15) &\cong G^*_\emptyset(5,15)\times G^*_\emptyset(29,15),\\ G^*_{\{5\}}(145,15) &\cong G^*_{\{5\}}(5,15)\times G^*_\emptyset(29,15),\\ G^*_{\{29\}}(145,15) &\cong G^*_\emptyset(5,15)\times G^*_{\{29\}}(29,15),\\ G^*_{\{5,29\}}(145,15) &\cong G^*_{\{5\}}(5,15)\times G^*_{\{29\}}(29,15). \end{aligned}$$

Note that $G^*_\emptyset(5,15)$ consists of one 2-cycle and 2 isolated fixed points, and $G^*_\emptyset(29,15)$ consists of 7 2-cycles and 14 isolated fixed points. Then by Lemma 3.19 and Lemma 3.21, $G^*_\emptyset(145,15)$ consists of $14+14+14 = 42$ 2-cycles and 28 isolated fixed points. Similarly, $G^*_{\{5\}}(145,15)$ consists of 7 2-cycles and 14 isolated fixed points, $G^*_{\{29\}}(145,15)$ consists of one 2-cycle and 2 isolated fixed points, and $G^*_{\{5,29\}}(145,15)$ consists of only 1 isolated fixed point. Therefore, we see that $G^*_P(145,15)\cup G^*_Q(145,15)$ is not symmetric of order 5, for any $P,Q \subseteq \{5,29\}$, $P \neq Q$.

Theorem 6.10. *Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$, and $k \geqslant 2$ be positive integers.*

(i) *Let $n_1 = p_1 p_2 \ldots p_r$, where p_i, $i = 1, 2, \ldots, r$ are distinct odd primes and $r \geqslant 2$. Suppose that $\gcd(\lambda(n), k) = 1$.*

(ii) *Let $n_1 = p^\alpha$, where p is an odd prime and $\alpha \geqslant 1$ is an integer. Suppose that $\gcd(p^{\alpha-1}(p-1), k) = p^{\alpha-1}$.*

(iii) *Let $n_1 = 2^\alpha$, where $\alpha \geqslant 1$. Suppose that $G(n_1, k)$ satisfies the following conditions:*

  (a) $\alpha = 5$, $k = 4$.

  (b) $\alpha = 4$, $k = 2$.

  (c) $\alpha \leqslant 2$, $2^{\alpha-1} \mid k$.

  (d) $\alpha \leqslant 2$, $k > 2$, $2^{\alpha-2} \mid k$.

Then for any fundamental constituent $G_P^*(n, k)$ of $G(n, k)$, there exists a distinct fundamental constituent $G_Q^*(n, k)$ such that the trees attached to all cycle vertices in $G_P^*(n, k) \cup G_Q^*(n, k)$ are isomorphic.

Proof. We first show that the trees attached to all cycle vertices in $G(n_1, k)$ are isomorphic. Cases (i) and (ii) follow from Lemma 3.3 and Theorem 6.4, respectively.

Now we consider case (iii). For parts (a) and (b), we see from Figure 2 and Figure 3, respectively, that $G(16, 2)$ and $G(32, 4)$ have exactly two isomorphic components, one with the fixed point 0 and the other with the fixed point 1.

We now prove parts (c) and (d). By Lemma 3.2, every cycle of $G_1(2^\alpha, k)$ is a fixed point. Also, the fixed point 0 is the only cycle in $G_2(2^\alpha, k)$. Since $A_1(G(2^\alpha, k)) = \gcd(\lambda(2^\alpha), k-1) + 1 = 2$, the only cycles in $G(2^\alpha, k)$ are the fixed points 0 and 1. By Lemmas 3.12 and 3.13, we get $\operatorname{indeg}_{n_1}(1) = \operatorname{indeg}_{n_1}(0) = 2^{\alpha-1}$. Thus, $G(2^\alpha, k)$ has exactly two isomorphic components, one component containing the fixed point 0 and the other containing the fixed point 1.

To finish the proof, in all three cases we use Theorem 6.1 and equation (4.2). Let $G_P^*(n, k)$ be any fundamental constituent of $G(n, k)$. By (4.2), we have

$$G_P^*(n, k) \cong G_{P_1}^*(n_1, k) \times G_{P_2}^*(n_2, k),$$

where $P_1 = \{p \in P \colon p \mid n_1\}$, $P_2 = \{q \in P \colon q \mid n_2\}$. Then there exists a fundamental constituent $G_{Q_1}^*(n_1, k)$ of $G(n_1, k)$ such that the trees attached to all cycle vertices in $G_{P_1}^*(n_1, k) \cup G_{Q_1}^*(n_1, k)$ are isomorphic. Now, using equation (4.1), consider the fundamental constituent

$$G_{Q_1}^*(n_1, k) \times G_{P_2}^*(n_2, k) \cong G_{Q_1 \cup P_2}^*(n, k).$$

Hence, by Theorem 6.1, the trees attached to all cycle vertices in $G_P^*(n, k) \cup G_{Q_1 \cup P_2}^*(n, k)$ are isomorphic. $\square$

Corollary 6.11. *Let $n = 3p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, where $p_i \neq 3$ are distinct odd primes. Let $k > 2$ be an odd integer. Then for any fundamental constituent $G_P^*(n,k)$ of $G(n,k)$, there exists a distinct fundamental constituent $G_Q^*(n,k)$ such that the trees attached to all cycle vertices in $G_P^*(n,k) \cup G_Q^*(n,k)$ are isomorphic.*

Corollary 6.12. *Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$. Let $n_1 = p^\alpha$, where p is an odd prime and $\alpha \geqslant 1$. Let $G_Q^*(n_2,k)$ be a fundamental constituent of $G(n_2,k)$. Suppose that $G(n_1,k)$ is symmetric of order p. Then $G_Q^*(n,k) \cup G_{Q\cup\{p\}}^*(n,k)$, which is a subdigraph of $G(n,k)$, is symmetric of order p.*

Proof. By Theorem 6.10, the trees attached to all cycle vertices in $G_Q^*(n,k) \cup G_{Q\cup\{p\}}^*(n,k)$ are isomorphic. Since $G(n_1,k)$ is symmetric of order p, then by Lemma 3.11 we get that $k \equiv 1 \pmod{p-1}$. Let C be a component of $G_{Q\cup\{p\}}^*(n,k)$. Then by Lemma 5.1 (ii), there exist $p-1$ distinct components of $G_Q^*(n,k)$, say, $C_1, C_2, \dots, C_{p-1}$, each isomorphic to C. Similarly, it is the case when C is a component of $G_Q^*(n,k)$. Hence, $G_Q^*(n,k) \cup G_{Q\cup\{p\}}^*(n,k)$ is symmetric of order p. □

The following theorem is a generalization of Theorem 6.4.

Theorem 6.13. *Let $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, where p_i, $i = 1,2,\dots,r$ are distinct odd primes. Let $k \geqslant 2$ be an integer. The trees attached to all cycle vertices in $G(n,k)$ are isomorphic if and only if $\gcd(p_i^{e_i-1}(p_i-1), k) = p_i^{e_i-1}$, for $i = 1,2,\dots,r$.*

Proof. Assume that $\gcd(p_i^{e_i-1}(p_i-1), k) = m \neq p_i^{e_i-1}$, for some i such that $1 \leqslant i \leqslant r$. Our aim is to show that $\operatorname{indeg}_{p_i^{e_i}}(0) \neq \operatorname{indeg}_{p_i^{e_i}}(1)$. We know that $\operatorname{indeg}_{p_i^{e_i}}(0) = p_i^{e_i - \lceil e_i/k \rceil}$ and $\operatorname{indeg}_{p_i^{e_i}}(1) = m$. If $p_i \nmid m$, then we are done. So we consider the case when $p_i \mid m$. By Lemma 3.8, $G_1(p_i^{e_i}, k)$ is always semiregular, and $\operatorname{indeg}_{p_i^{e_i}}(a) = 0$ or m, for any vertex a in $G_1(p_i^{e_i}, k)$.

Suppose that $\operatorname{indeg}_{p_i^{e_i}}(0) = \operatorname{indeg}_{p_i^{e_i}}(1)$, then $m = \gcd(p_i^{e_i-1}(p_i-1), k) = p_i^{e_i - \lceil e_i/k \rceil}$. This implies that $k < e_i$. If $G_2(p_i^{e_i}, k)$ is semiregular, then by Lemma 3.10, we get a contradiction. Now consider the case when $G_2(p_i^{e_i}, k)$ is not semiregular. By Lemma 3.9, we have $e_i \geqslant k + e_i - \lceil e_i/k \rceil + 2$. Note that $e_i - \lceil e_i/k \rceil + 2 \leqslant p_i^{e_i - \lceil e_i/k \rceil} \leqslant k$, for any odd prime p. Then, $e_i \geqslant 2e_i + 4 - 2\lceil e_i/k \rceil$, which is again a contradiction. Thus we can conclude that if $\gcd(p_i^{e_i-1}(p_i-1), k) \neq p_i^{e_i-1}$, then $\operatorname{indeg}_{p_i^{e_i}}(0) \neq \operatorname{indeg}_{p_i^{e_i}}(1)$.

Let $m_i = p_1^{e_1} p_2^{e_2} \dots p_{i-1}^{e_{i-1}} p_{i+1}^{e_{i+1}} \dots p_r^{e_r}$. Then,

$$\operatorname{indeg}_{p_i^{e_i}}(0) \operatorname{indeg}_{m_i}(1) \neq \operatorname{indeg}_{p_i^{e_i}}(1) \operatorname{indeg}_{m_i}(1),$$

which by Lemma 3.17 implies that $\operatorname{indeg}_n((0,1)) \neq \operatorname{indeg}_n((1,1))$. Hence, the trees attached to the cycle vertices $(0,1)$ and $(1,1)$ in $G(n,k)$ are not isomorphic.

We now prove the converse. Assume that $\gcd(p_i^{e_i-1}(p_i-1),k)=p_i^{e_i-1}$, for $i=1,2,\ldots,r$. Then by Theorem 6.4, the trees attached to all cycle vertices in $G(p_i^{e_i},k)$, for all i, are isomorphic. By similar arguments as in the proof of Theorem 6.4, we see that the height of each component of $G(p_i^{e_i},k)$, for all i, is 1. Then it is clear that the height of each non-cycle vertex of $G(n,k)$ is 1.

Let $a=(a_1,a_2,\ldots,a_r)$ and $b=(b_1,b_2,\ldots,b_r)$ be two cycle vertices in $G(n,k)\cong G(p_1^{e_1},k)\times G(p_2^{e_2},k)\times\ldots\times G(p_r^{e_r},k)$. Let φ_i be a digraph isomorphism from $T(a_i)$ onto $T(b_i)$ in $G(p_i^{e_i},k)$, for $i=1,2,\ldots,r$. Consider the trees $T(a)$ and $T(b)$ in $G(n,k)$. It is enough to show that $T(a)\cong T(b)$. Let $u=(u_1,u_2,\ldots,u_r)$ be any vertex in $T(a)$. Define a map $F\colon T(a)\longrightarrow T(b)$ as

$$T((u_1,u_2,\ldots,u_r))=(\varphi_1(u_1),\varphi_2(u_2),\ldots,\varphi_r(u_r)).$$

If $u=(u_1,u_2,\ldots,u_r)$ is a cycle vertex, then

$$\begin{aligned}F((u_1,u_2,\ldots,u_r))&=F((a_1,a_2,\ldots,a_r))\\&=(\varphi_1(a_1),\varphi_2(a_2),\ldots,\varphi_r(a_r))=(b_1,b_2,\ldots,b_r).\end{aligned}$$

Suppose that the vertex $u=(u_1,u_2,\ldots,u_r)$ is at height 1 in $T(a)$. Since φ_i is an isomorphism, then

$$\begin{aligned}[F((u_1,u_2,\ldots,u_r))]^k&=(\varphi_1(u_1),\varphi_2(u_2),\ldots,\varphi_r(u_r))^k=(\varphi_1(u_1^k),\varphi_2(u_2^k),\ldots,\varphi_r(u_r^k))\\&=(\varphi_1(a_1),\varphi_2(a_2),\ldots,\varphi_r(a_r))=(b_1,b_2,\ldots,b_r).\end{aligned}$$

Hence, F is well-defined. Since φ_i are one-one and onto, it is clear that F is also one-one and onto. Finally, we show that F preserves the direction. Let $u=(u_1,u_2,\ldots,u_r)$ be at height 1 in $T(a)$. Then

$$\begin{aligned}[F((u_1,u_2,\ldots,u_r))]^k&=(\varphi_1(u_1),\varphi_2(u_2),\ldots,\varphi_r(u_r))^k=(\varphi_1(u_1^k),\varphi_2(u_2^k),\ldots,\varphi_r(u_r^k))\\&=(\varphi_1(a_1),\varphi_2(a_2),\ldots,\varphi_r(a_r))=F(a).\end{aligned}$$

□

Note. The arguments of the proof of the '⇒' part of Theorem 6.13 will also work to prove the '⇒' part of Theorem 6.4.

Corollary 6.14. *Let $n=p_1^{e_1}p_2^{e_2}\ldots p_r^{e_r}$, where p_i, $i=1,2,\ldots,r$ are distinct odd primes. Let $k\geqslant 2$ be an integer. The trees attached to all cycle vertices in $G(n,k)$ are isomorphic if and only if $G(n,k)$ is semiregular.*

P r o o f. If the trees attached to all cycle vertices in $G(n,k)$ are isomorphic, then the height of each component of $G(n,k)$ is 1. Let $a = (a_1, a_2, \ldots, a_r)$ be a cycle vertex in $G(n,k)$. Then by Lemma 3.18, $\operatorname{indeg}_n(a) = \prod_{i=1}^{r} \operatorname{indeg}_{q_i}(a_i)$, where $q_i = p_i^{e_i}$. Thus it follows that $G(n,k)$ is semiregular.

Conversely, assume that $G(n,k)$ is semiregular. Our aim is to show that $\gcd(p_i^{e_i-1}(p_i-1), k) = p_i^{e_i-1}$, for all i such that $1 \leqslant i \leqslant r$. However, this follows by using similar arguments as in the proof of the '⇒' part of Theorem 6.13. □

Corollary 6.15. *Let n and $k \geqslant 2$ be two integers. The trees attached to all cycle vertices in $G_2(n,k)$ are isomorphic if and only if the trees attached to all cycle vertices in $G(n,k)$ are isomorphic.*

The following theorem is a generalization of Theorem 7.1 in [5].

Theorem 6.16. *Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$. Let $J(n_1,k)$ and $L(n_2,k)$ be subdigraphs of $G(n_1,k)$ and $G(n_2,k)$, respectively. Suppose that $J(n_1,k)$ consists of M isomorphic components, and $L(n_2,k)$ consists of N isomorphic components. Then $J(n_1,k) \times L(n_2,k)$ is a subdigraph of $G(n,k)$ that is symmetric of order MN.*

P r o o f. Let $C_i(n_1,k)$, where $i = 1, 2, \ldots, M$, be M isomorphic components of $J(n_1,k)$, and let $D_j(n_2,k)$, where $j = 1, 2, \ldots, N$, be N isomorphic components of $L(n_2,k)$. Since all $C_i(n_1,k)$ are isomorphic, each cycle in $C_i(n_1,k)$ is a t_1-cycle, for some positive integer t_1. Let the M t_1-cycles in $J(n_1,k)$ be

$$\langle a_1, a_2, \ldots, a_{t_1} \rangle,\ \langle a_{t_1+1}, a_{t_1+2}, \ldots, a_{2t_1} \rangle,\ \ldots,\ \langle a_{(M-1)t_1+1}, a_{(M-1)t_1+2}, \ldots, a_{Mt_1} \rangle.$$

Similarly, each cycle in $D_j(n_2,k)$, for $j = 1, 2, \ldots, N$, is a t_2-cycle, for some positive integer t_2. Let the N t_2-cycles of $L(n_2,k)$ be

$$\langle b_1, b_2, \ldots, b_{t_2} \rangle,\ \langle b_{t_2+1}, b_{t_2+2}, \ldots, b_{2t_2} \rangle,\ \ldots,\ \langle b_{(N-1)t_2+1}, b_{(N-1)t_2+2}, \ldots, b_{Nt_2} \rangle.$$

From Lemma 3.21, we see that

$$J(n_1,k) \times D_j(n_2,k) = \bigcup_{i=1}^{M} C_i(n_1,k) \times D_j(n_2,k),$$

for each j such that $1 \leqslant j \leqslant N$. Thus, from Lemma 3.19, it follows that there are M disjoint subgraphs in $J(n_1,k) \times D_j(n_2,k)$, for each j such that $1 \leqslant j \leqslant N$, each subgraph containing $\gcd(t_1, t_2)$ components. We now show that these M subgraphs are all isomorphic.

For each j, it suffices to show that

$$C_i(n_1,k)\times D_j(n_2,k)\cong C_l(n_1,k)\times D_j(n_2,k),$$

for all positive integers i, l such that $1\leqslant i,\ l\leqslant M$.

By hypothesis, there exists a digraph isomorphism φ_{il} from $C_i(n_1,k)$ onto $C_l(n_1,k)$, for all i, l such that $1\leqslant i,\ l\leqslant M$. Then it is clear that for each j, the map

$$F_{il}\colon\ C_i(n_1,k)\times D_j(n_2,k)\longrightarrow C_l(n_1,k)\times D_j(n_2,k),$$

defined by $F_{il}((u,v))=(\varphi_{il}(u),v)$, for any vertex $(u,v)\in C_i(n_1,k)\times D_j(n_2,k)$, is a digraph isomorphism, for all i, l such that $1\leqslant i,\ l\leqslant M$. Again, by hypothesis, there exists a digraph isomorphism ψ_{ij} from $D_i(n_2,k)$ onto $D_j(n_2,k)$, for all i, j such that $1\leqslant i,\ j\leqslant N$. Define a map

$$F'_{ij}\colon\ J(n_1,k)\times D_i(n_2,k)\longrightarrow J(n_1,k)\times D_j(n_2,k)$$

as $F'_{ij}((u,v))=(u,\psi_{ij}(v))$, for any vertex $(u,v)\in J(n_1,k)\times D_i(n_2,k)$. It is clear that F'_{ij} is a digraph isomorphism from $J(n_1,k)\times D_i(n_2,k)$ onto $J(n_1,k)\times D_j(n_2,k)$, for all i, j such that $1\leqslant i,\ j\leqslant N$.

Then, $J(n_1,k)\times L(n_2,k)$ consists of MN isomorphic subgraphs, each containing $\gcd(t_1,t_2)$ components. Hence, $J(n_1,k)\times L(n_2,k)$ consists of $\gcd(t_1,t_2)$ subgraphs, each containing MN isomorphic components. This implies that $J(n_1,k)\times L(n_2,k)$ is symmetric of order MN. $\square$

Theorem 6.17. *Let* $n=n_1n_2$, *where* $\gcd(n_1,n_2)=1$. *Suppose that* $G(n_1,k)$ *is symmetric of order* M *and* $G(n_2,k)$ *is symmetric of order* N. *Then* $G(n,k)\cong G(n_1,k)\times G(n_2,k)$ *is symmetric of order* MN.

P r o o f. This follows from Lemma 3.21 and Theorem 6.16. $\square$

References

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

[2] *J. Kramer-Miller*: Structural properties of power digraphs modulo n. Mathematical Sciences Technical Reports (MSTR) (2009), 11 pages, `http://scholar.rose-hulman.edu/math_mstr/11`.

[3] *M. Křížek, F. Luca, L. Somer*: 17 Lectures on Fermat Numbers: From Number Theory to Geometry. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC 9, Springer, New York, 2001.

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

[5] *L. Somer, M. Křížek*: On symmetric digraphs of the congruence $x^k \equiv y \pmod{n}$. Discrete Math. *309* (2009), 1999–2009.
[6] *L. Somer, M. Křížek*: On semiregular digraphs of the congruence $x^k \equiv y \pmod{n}$. Commentat. Math. Univ. Carol. *48* (2007), 41–58.
[7] *B. Wilson*: Power digraphs modulo n. Fibonacci Q. *36* (1998), 229–239.

Authors' addresses: Amplify Sawkmie, Department of Mathematics, School of Physical Sciences, North Eastern Hill University, 793022 Shillong, Meghalaya, India, e-mail: `ampsawkmie@gmail.com`, Madan Mohan Singh, Department of Basic Sciences & Social Sciences, School of Technology, North-Eastern Hill University, 793022 Shillong, Meghalaya, India, e-mail: `mmsingh2004@gmail.com`.