On the symmetric digraphs from powers modulo $n$

Guixin Deng$^a$,*, Pingzhi Yuan$^b$

$^a$ School of Mathematics, Guangxi Teachers Education University, Nanning 530001, PR China
$^b$ School of Mathematics, South China Normal University, Guangzhou 510631, PR China

ARTICLE INFO

Article history:
Received 18 August 2010
Received in revised form 24 July 2011
Accepted 6 November 2011
Available online 3 December 2011

Keywords:
Symmetric
Congruence
Digraph products
Component
Height
Cycle length

ABSTRACT

For any positive integers $n$ and $k$, let $G(n, k)$ denote the digraph whose set of vertices is $H = \{0, 1, 2, \ldots, n - 1\}$ and there is a directed edge from a vertex $a$ to a vertex $b$ if $a^k \equiv b \pmod{n}$. The digraph $G(n, k)$ is called symmetric of order $M$ if its set of connected components can be partitioned into subsets of size $M$ with each subset containing $M$ isomorphic components. In this paper, we establish a necessary and sufficient condition for $G(n, k)$ to be symmetric of order $M$, where $M$ has an odd prime divisor.

© 2011 Elsevier B.V. All rights reserved.

1. Introduction

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

In [4], Somer and Křížek called a digraph symmetric if its connected components can be partitioned into isomorphic pairs. They gave the following definition in [6].

Definition 1.1. Let $M \geq 2$ be an integer. A digraph is said to be symmetric of order $M$ if its set of components can be partitioned into subsets of size $M$, each containing $M$ isomorphic components.

In [7], Szalay showed that $G(n, 2)$ is symmetric of order 2 if $n \equiv 2 \pmod{4}$ or $n \equiv 4 \pmod{8}$. In [1], Carlip and Mincheva proved that if $p$ is a Fermat prime, then $G(2^r p, 2)$ is not symmetric of order 2 when $r = 3$ or $r \geq 5$. The following theorem is part of Theorem 5.1 in [6].

Theorem 1.1 ([6, Theorem 5.1]). Let $n = n_1 n_2$, where $n_1 > 1$, $n_2 \geq 1$, and $\gcd(n_1, n_2) = 1$. Then

(i) Suppose that $n_1 = p^\alpha$, where $p$ is an odd prime and $\alpha \geq 1$. Suppose further that $k \equiv 1 \pmod{p - 1}$ and $p^\alpha - 1 | k$. Then $G(n, k)$ is symmetric of order $p$.

(ii) Suppose that $n_1 = q_1 q_2 \cdots q_s$, where the $q_i$s are distinct primes, and $s \geq 2$. Suppose that $k \equiv 1 \pmod{\lambda(n_1)}$. Then $G(n, k)$ is symmetric of order $n_1$.

* Supported by the Guangdong Provincial Natural Science Foundation (No. 8151027501000114) and NSF of China (No. 10571180).
* Corresponding author;
E-mail addresses: oldlao@163.com (G. Deng), mcsypz@mail.sysu.edu.cn (P. Yuan).

0012-365X/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2011.11.007
(iii) Suppose that \( n = p^\alpha q_1q_2 \cdots q_s \), where \( p \) is an odd prime, \( \alpha \geq 2 \), \( s \geq 1 \), and the \( q_i \)'s are distinct primes such that \( p \neq q_i \) and \( p \nmid q_i - 1 \) for \( i = 1, 2, \ldots, s \). Suppose further that \( k \equiv 1 (\text{mod } \lambda(pq_1q_2 \cdots q_s)) \) and \( p^{\alpha-1} | k \). Then \( G(n, k) \) is symmetric of order \( pq_1q_2 \cdots q_s \).

Here the function \( \lambda \) is the Carmichael lambda-function, which will be introduced in Section 2. In [2], Kramer-Miller obtained a necessary and sufficient condition for \( G(n, k) \) to be symmetric of order \( p \), where \( n \) is square free and \( p \) is an odd prime.

**Theorem 1.2** ([2, Theorem 3.15]). Let \( n = pq_1q_2 \cdots q_m \), where \( q_i \) and \( p \) 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) \( \text{gcd}(p - 1, k) = 1 \). (ii) Let \( T = \{q_i : \text{gcd}(q_i - 1, k) = 1\} \). Then \( T \) is not empty and for all \( x \in \mathbb{N} \), \( p|xA_\lambda(G(\prod_{i \in T} q_i, k)) \) or \( \text{ord}_p x | k \).

Here we use \( A_\lambda(G(n, k)) \) to denote the number of \( t \)-cycles contained in \( G(n, k) \), and use \( \mathcal{A}(G(n, k)) \) to denote the set of cycle lengths that appear in \( G(n, k) \).

In this paper, we generalize Theorem 1.2 to any positive integers \( n \) and \( M \), where \( M \) has an odd prime divisor.

The outline of this paper is as follows. In Section 3, we present some preliminary results on the structure of \( G(n, k) \). In Section 4, we treat the case \( n = p^m \). In Section 5, we prove two lemmas for our main results. In Section 6, we state and prove the main theorem of the present paper.

2. The Carmichael lambda-function

Before proceeding further, we need to review some properties of the Carmichael lambda-function \( \lambda(n) \).

**Definition 2.1.** Let \( n \) be a positive integer. The Carmichael lambda-function \( \lambda(n) \) is defined as follows:

\[
\begin{align*}
\lambda(1) & = 1, \\
\lambda(2) & = 1, \\
\lambda(4) & = 2, \\
\lambda(2^k) & = 2^{k-2} \quad \text{for } k \geq 3, \\
\lambda(p^k) & = (p - 1)p^{k-1} \quad \text{for any odd prime } p \text{ and } k \geq 1, \\
\lambda(p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r}) & = \text{lcm}[\lambda(p_1^{k_1}), \lambda(p_2^{k_2}), \ldots, \lambda(p_r^{k_r})], \text{ where } p_1, p_2, \ldots, p_r \text{ are distinct primes and } k_i \geq 1 \text{ for all } i \in \{1, 2, \ldots, r\}.
\end{align*}
\]

The following theorem generalizes the well-known Euler’s theorem which says that \( a^{\phi(n)} \equiv 1 \pmod{n} \) if and only if \( \text{gcd}(a, n) = 1 \).

**Theorem 2.1** (Carmichael). Let \( a, n \in \mathbb{N} \). Then

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

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

\[
\text{ord}_ag = \lambda(n),
\]

where \( \text{ord}_ag \) denotes the multiplicative order of \( g \) modulo \( n \).

For the proof, see [3, p. 21].

3. Some preliminary results on \( G(n, k) \)

There are two particular subdigraphs of \( G(n, k) \). Let \( G_1(n, k) \) be the induced subdigraph of \( G(n, k) \) on the set of vertices which are coprime to \( n \), and \( G_2(n, k) \) be the induced subdigraph of \( G(n, k) \) on the set of vertices which are not coprime with \( n \). We observe that \( G_1(n, k) \) and \( G_2(n, k) \) are disjoint and that \( G(n, k) = G_1(n, k) \cup G_2(n, k) \), that is, no edge goes between \( G_1(n, k) \) and \( G_2(n, k) \).

It is clear that each component of \( G(n, k) \) contains a unique cycle. The following lemma tells us that the structure of each component contained in \( G_1(n, k) \) is determined by its cycle length.

**Lemma 3.1** ([6, Corollary 6.4]). Let \( t \geq 1 \) be a fixed integer. Then any two components in \( G_1(n, k) \) containing \( t \)-cycle are isomorphic.

Now consider a digraph \( G(n, k) \), and factor \( \lambda(n) \) as

\[
\lambda(n) = uv,
\]

where \( u \) is the largest divisor of \( \lambda(n) \) relatively prime to \( k \). We need the following results on the cycles of \( G(n, k) \).
Lemma 3.2 ([8]). There exists a t-cycle in \(G_1(n, k)\) if and only if \(t = \text{ord}_a k\) for some factor \(d\) of \(u\).

Lemma 3.3 ([6, Theorem 6.6]). Let \(n = \prod_{i=1}^{r} p_i^{e_i}\) be the prime factorization of \(n\). If \(t \in A(G(n, k))\), then

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

where \(\delta_i = 2\) if \(2|k - 1\) and \(8|p_i^{e_i}\), and \(\delta_i = 1\) otherwise.

Let \(G\) be a digraph and \(a\) be a vertex in \(G\). The indegree of \(a\), denoted by \(\text{indeg}(a)\), is the number of directed edges coming to \(a\), and the outdegree of \(a\) is the number of edges leaving \(a\). Particularly, let \(\text{indeg}_k^a(a)\) denote the indegree of a vertex \(a \in G(n, k)\). It is clear that each vertex in \(G(n, k)\) has outdegree 1. In the rest of this paper, all digraphs are assumed to be finite and have this property.

Definition 3.1. We define a height function on the vertices and components of \(G(n, k)\). Let \(c\) be a vertex of \(G(n, k)\). Let \(h(c)\) to be the minimal nonnegative integer \(i\) such that \(e^i\) is congruent modulo \(n\) to a cycle vertex in \(G(n, k)\). If \(C\) is a component of \(G(n, k)\), we set \(h(C) = \sup_{c \in C} h(c)\).

The indegree and height function play an important role in the structure of \(G(n, k)\). We need the following results concerning the indegrees and heights.

Lemma 3.4 ([8]). Let \(n = \prod_{i=1}^{r} p_i^{e_i}\) be the prime factorization of \(n\), where \(e_i \geq 1\). Let \(a\) be a vertex of positive indegree in \(G_1(n, k)\). Then

\[
\text{indeg}_n^k(a) = \prod_{i=1}^{r} \text{indeg}_{p_i}^a(a) = \prod_{i=1}^{r} \delta_i \gcd(\lambda(p_i^{e_i}), k),
\]

where \(\delta_i = 2\) if \(2|k\) and \(8|p_i^{e_i}\), and \(\delta_i = 1\) otherwise.

Lemma 3.5 ([5, Theorem 3.2]). Let \(p\) be a prime. Let \(a\) be a vertex of positive indegree in \(G_2(p^e, k)\), and assume that \(p^f \parallel a\) and \(a \neq 0\). Then \(l = kt\) for some positive integer \(t\) and

\[
\text{indeg}_{p^f}^k(a) = \delta p^{(k - 1)e} \gcd(\lambda(p^{f - 1}), k),
\]

where \(\delta = 2\) if \(p = 2\) and \(e - l \geq 3\), and \(\delta = 1\) otherwise.

Lemma 3.6 ([6, Lemma 3.2]). Let \(p\) be a prime and \(e, k\) be two positive integers. Then

\[
\text{indeg}_{p^e}^k(0) = p^{e - \left\lceil \frac{e}{k} \right\rceil}.
\]

Lemma 3.7. Let \(p\) be a prime and let \(e \geq 1, k \geq 2\) be integers. Suppose that \(h\) be the unique positive integer such that \(k^{h-1} < e \leq k^h\). Then \(h = h(G_2(p^e, k))\).

Proof. It is clear that \(p \in G_2(p^e, k)\) and \(h(p) = h(G_2(p^e, k))\). And \(p^{k^i} \equiv 0 \pmod{p^e}\) if and only if \(k^i \geq e\). The proof is completed. \(\square\)

Lemma 3.8. Let \(p\) be a prime and \(e, k \geq 2\) be two positive integers. Let \(\lambda(p^e) = uv\), where \(u\) is the maximal divisor of \(\lambda(p^e)\) relatively prime to \(k\). If \(C\) is the component of \(G(p^e, k)\) containing \(1\), then

\[
h(C) = \min\{i : v|k^i\}.
\]

Proof. Let \(h = \min\{i : v|k^i\}\). Then there exists a divisor \(d\) of \(v\) such that \(d\) is not a divisor of \(k^{h-1}\). By Theorem 2.1, there exists a vertex \(g \in G(p^e, k)\) such that \(\text{ord}_{p^e} g = uv\). Let \(a \equiv g^{\frac{k^i}{v}} \pmod{p^e}\). Then \(\text{ord}_{p^e} a = d, a^{k^i - 1} \equiv 1 \pmod{p^e}\) and \(a^{k^i} \equiv 1 \pmod{p^e}\). Hence, \(h(C) \geq h(a) = h\) by the definition of the height function.

Conversely if \(a \in C\), then there exists \(j \geq 1\) such that \(a^{k^i} \equiv 1 \pmod{p^e}\), so \(\text{ord}_{p^e} a|k^i\). Since \(\text{ord}_{p^e} a|uv\), we have \(\text{ord}_{p^e} a|v\), so \(a^{k^i} \equiv 1 \pmod{p^e}\), that is, \(h(C) \leq h\). \(\square\)

4. The case \(n = p^e\)

Recall that a digraph \(G\) is called semiregular if there exists a positive integer \(d\) such that each vertex of \(G\) either has indegree \(d\) or 0.

[8, Theorem 6.6]
Lemma 4.1. Let \( p \) be an odd prime and let \( e, k \geq 2 \) be two positive integers. Then \( G(p^e, k) \) is semiregular if and only if \( \gcd((p - 1)p^{e-1}, k) = p^{e-1} \).

Proof. The case \( e = 1 \) is trivial. Assume that \( e \geq 2 \) and that \( G(p^e, k) \) is semiregular. Then \( \text{indeg}_{G(p^e)}(0) = \text{indeg}_{G(p^e)}(1) \). By Lemmas 3.4 and 3.6,
\[
\text{indeg}_{G(p^e)}(0) = p^e - \left\lceil \frac{k}{p^e} \right\rceil = \gcd((p - 1)p^{e-1}, k) = \text{indeg}_{G(p^e)}(1).
\]
If \( \left\lceil \frac{k}{p^e} \right\rceil \geq 2 \), then \( \text{indeg}_{G(p^e)}(p^e) = 0 \). By Lemma 3.5
\[
\text{indeg}(p^e) = p^{e-1} \gcd((p - 1)p^{e-1}, k) = p^{e-1+\min\{e-k-1, e-\left\lceil \frac{k}{p^e} \right\rceil\}}.
\]
Since \( \text{indeg}(p^e) = \text{indeg}(0) \), it follows that \( e - \left\lceil \frac{k}{p^e} \right\rceil = k - 1 + \min\{e-k-1, e-\left\lceil \frac{k}{p^e} \right\rceil\} \), so \( e - \left\lceil \frac{k}{p^e} \right\rceil = k - 1 + (e-k-1) = e - 2 \). We find that \( \left\lceil \frac{k}{p^e} \right\rceil = 2 \). Now we have \( k < e \leq 2k \) and \( p^{e-2} \parallel k \). Therefore, \( p^{e-2} < e \), we deduce \( e = 2 \) and \( k = 1 \), which is a contradiction. Hence, \( \left\lceil \frac{k}{p^e} \right\rceil = 1 \) and \( \gcd((p - 1)p^{e-1}, k) = p^{e-1} \).

Conversely, if \( \gcd((p - 1)p^{e-1}, k) = p^{e-1} \), then \( k \geq e \). The vertex 0 is the only vertex in \( G_2(p^e, k) \) with positive indegree and \( \text{indeg}(0) = p^{e-1} = \text{indeg}(a) \) for any vertices \( a \) in \( G_1(p^e, k) \) with positive indegree. So \( G(p^e, k) \) is semiregular. This proves Lemma 4.1. \( \square \)

Corollary 4.1. Let \( p \) be an odd prime and \( e, k \geq 2 \) be two positive integers. Suppose that \( G(p^e, k) \) is semiregular. Then
\[
\sum_{i \in A(G(p^e, k))} a_i(G(p^e, k)) = p.
\]

Theorem 4.1. Let \( p \) be an odd prime. Then \( G(p^e, k) \) is symmetric of order \( p \) if and only if \( \gcd((p - 1)p^{e-1}, k) = p^{e-1} \) and \( k \equiv 1 \pmod{p-1} \).

Proof. Assume that \( G(p^e, k) \) is symmetric of order \( p \). Then there exist at least \( p - 1 \) distinct components \( C_1, C_2, \ldots, C_{p-1} \) contained in \( G_1(p^e, k) \) such that \( C_i \cong G_2(p^e, k) \). But \( |G_2(p^e, k)| = p^{e-1} \), therefore,
\[
|C_1| + |C_2| + \cdots + |C_{p-1}| + |G_2(p^e, k)| = p^e = |G(p^e, k)|.
\]
It follows that \( G(p^e, k) \) is the union of \( C_1, C_2, \ldots, C_{p-1} \), and \( G_2(p^e, k) \). By Lemma 3.3, we have
\[
p = A_1(G(p^e, k)) = \gcd((p - 1)p^{e-1}, k) + 1.
\]
We deduce \( p - 1 |k - 1 \) from this equation.

The converse implication follows immediately from (i) of Theorem 1.1. \( \square \)

5. Properties of digraphs products

Given two digraphs \( G_1 \) and \( G_2 \). Let \( G_1 \times G_2 \) denote the digraph whose vertices are the ordered pairs \((a_1, a_2)\), where \( a_1 \in G_1 \) and there is a directed edge from \((a_1, a_2)\) to \((b_1, b_2)\) if there is a directed edge from \( a_1 \) to \( b_1 \) and a directed edge from \( a_2 \) to \( b_2 \). In [6], Somer and Křížek noted the following fact. Let \( n = n_1n_2 \), where \( \gcd(n_1, n_2) = 1 \). Then \( G(n, k) \cong G(n_1, k) \times G(n_2, k) \). And the canonical isomorphism is given by \( a \mapsto (a_1, a_2) \), where \( a \equiv a_i \pmod{n_i} \), \( i = 1, 2 \). In general,
\[
G(n, k) \cong G(p_1^{e_1}, k) \times G(p_2^{e_2}, k) \times \cdots \times G(p_r^{e_r}, k),
\]
if \( n = \prod_{i=1}^r p_i^{e_i} \) is the prime factorization of \( n \). We need this fact and the following lemmas.

Lemma 5.1 ([2, Lemma 3.1]). Let \( n = n_1n_2 \), 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 \( G(n_2, k) \). And the cycle length of \( C_1 \) is \( t_1 \). Then \( C_1 \times C_2 \) is a subdigraph of \( G(n, k) \) consisting of \( \gcd(t_1, t_2) \) components, each having cycles of length \( \min(t_1, t_2) \).

Corollary 5.1. Let \( n = n_1n_2 \), where \( \gcd(n_1, n_2) = 1 \). If \( G(n_1, k) \) is symmetric of order \( M \), then \( G(n, k) \) is also symmetric of order \( M \).

Proof. It follows immediately from Lemma 5.1 and the fact \( G(n, k) \cong G(n_1, k) \times G(n_2, k) \). \( \square \)

Lemma 5.2 ([2, Lemma 3.12]). Let \( n = \prod_{i=1}^r p_i^{e_i} \) be the prime factorization of \( n \). Let \( a = (a_1, a_2, \ldots, a_r) \) and \( b = (b_1, b_2, \ldots, b_r) \) be two vertices in \( G(n, k) \cong G(p_1^{e_1}, k) \times G(p_2^{e_2}, k) \times \cdots \times G(p_r^{e_r}, k) \). If \( a \) and \( b \) are in the same cycle, then \( a_i \) and \( b_i \) are in the same cycle for each \( i \).

Lemma 5.3. If \( G(n, k) \) is symmetric of order \( M \), then \( G(n^r, k^r) \) is also symmetric of order \( M \) for any \( r \geq 1 \).
Proof. Let $C_1, C_2$ be two components of $G(n, k)$ and there exists an isomorphism of digraphs:

$$\varphi : C_1 \to C_2.$$ 

We first show that each component of $G(n, k)$ splits into one or several components of $G(n, k')$. If two vertices $x, y$ are in the same component of $G(n, k')$, then there exists a vertex $z$ and two positive integers $u, v$ such that $x^u \equiv z \mod n$ and $y^v \equiv z \mod n$. It follows that $x, y$ are in the same component of $G(n, k)$. And if $D$ is a component of $G(n, k')$, then we have $D \subseteq C$, where $C$ is a component of $G(n, k)$.

Now we can assume that $C_1 = \bigcup_{j=1}^{n_1} D_j$ and $C_2 = \bigcup_{j=1}^{n_2} E_j$, where each $D_j$ or $E_j$ is a component of $G(n, k')$. If $x, y \in C_1$ and $x^{k'} \equiv y \mod n$, then there exist $y_1, y_2, \ldots, y_r = y$ such that $x^{\ell_i} \equiv y_i \mod n$ and $y^{k'} \equiv y_{i+1} \mod n$. Hence, $\varphi(x)^{k'} \equiv \varphi(y_1) \mod n$ and $\varphi(y)^{k'} \equiv \varphi(y_{i+1}) \mod n$. So $\varphi(x)^{k'} \equiv \varphi(y) \mod n$. $\varphi$ still preserves arrows if we consider $C_1$ and $C_2$ as subdigraphs of $G(n, k')$.

Since $\varphi$ maps a component $D_j$ into a component $E_i$, we have $s_1 = s_2$. Thus, $\varphi$ is still an isomorphism if we consider $C_1$ and $C_2$ as subdigraphs of $G(n, k')$. It implies that $G(n, k')$ is also symmetric of order $M$. This proves Lemma 5.3. $\square$

Let $G$ be a digraph. Let $|G|$ or $\#G$ denote the number of vertices in $G$. Let $M(G) = \max_{x \in G} \{\deg(x)\}$, $N(G) = \min_{x \in G} \{\deg(x)\}$, $I(G) = \#\{d > 0 : \text{there exists a vertex } a \in G \text{ such that } \deg(a) = d\}$. Note that $G$ is semiregular if and only if $I(G) = 1$.

**Lemma 5.4.** Let $G$ and $H$ be two digraphs, and $a \in G$ and $b \in H$. Then $\deg((a, b)) = \deg(a) \deg(b)$, $M(G \times H) = M(G) M(H)$, $N(G \times H) = N(G) N(H)$ and $|G \times H| = |G| |H|$. Moreover, if $I(G) \geq 2$, $I(H) \geq 2$, then $I(G \times H) \geq \max(I(G), I(H)) + 1$.

**Proof.** It follows immediately from the definitions. $\square$

**Definition 5.1.** For any positive integers $t$, $m$, we define $O_t^m$ to be the digraph which satisfies: (i) it has $tm$ vertices and a $t$-cycle, (ii) $\deg(a) = m$ if $a$ is a cycle vertex and $\deg(a) = 0$, otherwise.

**Lemma 5.5.** $O_t^m \times O_{t_2}^{m_2} \cong \gcd(t_1, t_2) O_{t_1 \min\{t_1, t_2\}}^m \times O_{t_2 \min\{t_1, t_2\}}^{m_2}$.

**Proof.** By Lemma 5.1, there are exactly $\gcd(t_1, t_2)$ cycles contained in the product digraph, each having a cycle of length $\min\{t_1, t_2\}$. It is clear that $(a_1, a_2)$ is a cycle vertex of $O_{t_1}^m \times O_{t_2}^{m_2}$ if and only if $a_1$ is a cycle vertex of $O_{t_1}^m$. Consequently, the indegree of each cycle vertex in $O_{t_1}^m \times O_{t_2}^{m_2}$ is $m_1 m_2$, and the indegree of other vertices is 0. Lemma 5.5 is proved. $\square$

**Lemma 5.6.** Let $k \geq 2$, $e \geq 1$ be integers and $p$ a prime. If $a, b$ are two cycle vertices in the same cycle of $G(p^e, k)$, then $\gcd(a, p) = \gcd(b, p)$.

**Proof.** If $\gcd(a, p) = 1$, then $\gcd(b, p) = 1$ since $a, b$ are two cycle vertices in the same cycle of $G(p^e, k)$, and thus $\gcd(a, p) = \gcd(b, p) = \gcd(p^e - 1, p - 1, k)$. If $\gcd(p, a) > 1$, then $p|a$. Since $a, b$ are two cycle vertices in the same cycle of $G(p^e, k)$, so $a = b = 0$ and $\gcd(a, p) = \gcd(b, p)$. Lemma 5.6 is proved. $\square$

**Remark 5.1.** By Lemmas 5.2, 5.4 and 5.6, we see that if $a$ and $b$ are two cycle vertices in the same cycle of $G(n, k)$, then $\gcd(a, p) = \gcd(b, p)$. So if $C$ is a component of $G(n, k)$ and $h(C) \leq 1$, then $C \cong O_t^m$ where $t$ is the cycle length of $C$ and $m$ is the indegree of a cycle vertex of $C$.

The following two lemmas are very useful in the proof of our main results.

**Lemma 5.7.** $O_t^m \times G \cong O_t^m \times H$ if and only if $G \cong H$ for any digraphs $G$ and $H$.

**Proof.** Assume that $\varphi : O_t^m \times G \to O_t^m \times H$ is an isomorphism of digraphs. Let $G_0 = \{x \in G \mid \deg(x) = 0\}$, $G_1 = \{x \in G \mid \deg(x) > 0\}$, $H_0 = \{x \in H \mid \deg(x) = 0\}$, $H_1 = \{x \in H \mid \deg(x) > 0\}$. Let $a$ be the unique vertex of $O_t^m$ with $\deg(a) > 0$.

If $x \in G_1$ and $\deg((a, x)) = \deg(a) \deg(x) > 0$, then $\deg((a, x)) > 0$ and $\deg((a, x)) = (a, x')$, we have $x' \in H_1$. Now we define a map $\varphi_1 : G_1 \to H_1$ by $\varphi_1(x) = x \cdot x \in G_1$. Obviously, $\varphi_1$ is injective. If $y \in H_1$, then there exists a vertex $(a, y)$ of positive indegree in $O_t^m \times G$ such that $\varphi((a, y)) = (a, y')$. Hence, $\varphi_1(y) = y'$ and $\varphi_1$ is also surjective.

If $x, y \in G_1$ and there is a directed edge from $x$ to $y$. Let $\varphi_1(x) = x' \cdot x \varphi_1(y) = y'$. Then $\varphi((a, x)) = (a, x')$ and $\varphi((a, y)) = (a, y')$ by definition of $\varphi_1$. There is a directed edge from $(a, x')$ to $(a, y')$, since $\varphi$ preserves arrows. So there is a directed edge from $x'$ and $y'$. $\varphi$ preserves arrows.

Next we define a map $\varphi_0$ from $G_0$ to $H_0$. For any $y \in G_1$, let

$$E_0(y) = \{x \in G_0 \mid \text{there is a directed edge from } x \text{ to } y\},$$

$$E_1(y) = \{x \in G_1 \mid \text{there is a directed edge from } x \text{ to } y\}.$$
Then
\[ G_0 = \bigcup_{y \in G_1} E_0(y). \]
And the union is a disjoint union since each vertex has outdegree 1. If \( \varphi_1(y) = y' \), we have
\[
\text{indeg}((a, y)) = m(|E_0(y)| + |E_1(y)|) = \text{indeg}((a, y')) = m(|E_0(y')| + |E_1(y')|),
\]
and \( |E_1(y)| = |E_1(y')| \) since \( \varphi_1 \) maps \( E_1(y) \) into \( E_1(y') \), and so \( |E_0(y)| = |E_0(y')| \). Now we can take \( \varphi_0 \) such that \( \varphi_0 \) is bijective and \( \varphi_0(x) \in E_0(\varphi_1(x)) \) for any \( x \in E_0(y) \).

Finally we define \( \phi : G \to H \),
\[
\phi(x) = \varphi_1(x), \quad \text{if } x \in G_1,
\]
for \( i = 0, 1 \). It is clear that \( \phi \) is bijective.

Now we prove that \( \phi \) preserves arrows. Suppose \( x, y \in G \) and there is a directed edge from \( x \) to \( y \). We only need to treat the case when \( x \in G_0 \) and \( y \in G_1 \). Let \( \phi(y) = \varphi_1(y) = y' \). By the construction of \( \varphi_0 \), we see that \( \phi(x) = \varphi_0(x) \in E_0(\varphi_1(y)) \), thus there is also an arrow from \( \phi(x) \) to \( \phi(y) \). It is easy to show that the number of directed edges of \( G \) is equal to the number of directed edges of \( H \). Thus \( \phi \) is an isomorphism. This proves Lemma 5.7. \( \square \)

**Remark 5.2.** Let \( K \) be a digraph, \( M \) a positive integer, write
\[
K = n_1D_1 \cup n_2D_2 \cup \cdots \cup n_rD_r,
\]
where each \( D_i \) is a component and \( D_i \simeq D_j \) if and only if \( i = j \). Then, by the definition of symmetry, \( K \) is symmetric of order \( M \) if and only if \( |M|/n_i \) for each \( i = 1, 2, \ldots, r \). In particular, \( M \nmid 2K \).

**Lemma 5.8.** Let \( G = O^n/ H \) be a digraph, where \( H \) is a semiregular subdigraph of \( G \), and \( \text{indeg}(a) = 0 \) or \( d \) for any vertex \( a \in H \). Suppose that \( d \neq m \) and \( K \) is a digraph. Then \( G \times K \) is symmetric of order \( M \) if and only if \( K \) is symmetric of order \( M \).

**Proof.** Suppose that \( K \) is not symmetric of order \( M \), we write
\[
K = n_1D_1 \cup n_2D_2 \cup \cdots \cup n_rD_r,
\]
where each \( D_i \) is a component and \( D_i \simeq D_j \) if and only if \( i = j \).

If \( d < m \), without loss of generality, we may assume that \( M(D_1) \leq M(D_2) \leq \cdots \leq M(D_r) \). Let \( j \) be the maximal index such that \( M \nmid n_j \). Then, by Lemma 5.1 and Remark 5.2, \( G \times K \) is symmetric of order \( M \) if and only if \( G \times (n_1D_1 \cup n_2D_2 \cup \cdots \cup n_jD_j) \) is symmetric of order \( M \). Let \( E = O^n \times D_j \). By Lemma 5.1 again, \( E \) is a component of \( G \times (n_1D_1 \cup n_2D_2 \cup \cdots \cup n_jD_j) \). Let \( F \) be a component of \( G \times (n_1D_1 \cup n_2D_2 \cup \cdots \cup n_jD_j) \), if \( F = O^n \times D_j \), where \( 1 \leq i < j \), then \( E \) is not isomorphic to \( F \) according to Lemma 5.7. If \( F \) is a component of \( H \times (n_1D_1 \cup n_2D_2 \cup \cdots \cup n_jD_j) \), then
\[
M(F) = M(H)M(D_j) < mM(D_j) = M(E),
\]
which implies that \( F \) is not isomorphic to \( E \).

If \( d > m \), we assume that \( N(D_1) \geq N(D_2) \geq \cdots \geq N(D_r) \) in this case. Again let \( j \) be the maximal index such that \( M \nmid n_j \). Let \( E = O^n \times D_j \), and \( F \) be a component of \( G \times (n_1D_1 \cup n_2D_2 \cup \cdots \cup n_jD_j) \). If \( F = O^n \times D_j \), where \( 1 \leq i < j \), then \( E \) is not isomorphic to \( F \) according to Lemma 5.7. If \( F \) is a component of \( H \times (n_1D_1 \cup n_2D_2 \cup \cdots \cup n_jD_j) \), then
\[
N(E) = N(O^n)N(D_j) = mN(D_j) < dN(D_j) < N(F),
\]
which again implies that \( E \) is not isomorphic to \( F \).

In both cases, we have showed that there are exactly \( n_j \) components contained in \( G \times (n_1D_1 \cup n_2D_2 \cup \cdots \cup n_jD_j) \) which are isomorphic to \( E \). Thus, \( G \times K \) is not symmetric of order \( M \). The converse implication is trivial. Lemma 5.8 is proved. \( \square \)

### 6. The main result

We begin with a lemma before we prove our main theorem.

**Lemma 6.1.** Let \( p \) be an odd prime and \( n = p^eq \), where \( p \nmid q \). Suppose that \( G(n, k) \) is symmetric of order \( p \). Then \( \gcd((p - 1)p^{e-1}, k) = p^{e-1} \).

**Proof.** Step 1: Assume that \( \gcd(p - 1, k) = u > 1 \) or \( p \mid k \) when \( e > 1 \). Let \( h = h(G(p^e, k)) \). Then \( h(G(p^e, k)) = 1 \) and
\[
G(p^e, k) = G_2(p^e, k^h) \cup G_1(p^e, k^h) \simeq O_1^{p^e-1} \cup a_1O_1^{p^e} \cup a_2O_2^{p^e} \cup \cdots \cup a_lO_l^{p^e},
\]
where \( m = \gcd((p - 1)p^{e-1}, k^h) \) and \( a_i \) is the number of \( i \)-cycles contained in \( G_1(p^e, k^h) \). Obviously, \( m \neq p^{e-1} \). By Lemma 5.8, \( G(p^e, k) \neq G(p^e, k^h) \) is not symmetric of order \( p \), which contradicts Lemma 5.3.
Step 2: It remains to prove that $p^e - 1 | k$, the case $e = 1$ is trivial. Suppose that $e \geq 2$ and $p^e \parallel k$, $r \geq 1$. Let $C_0, C_1$ be the components of $G(p^e, k)$ containing the vertex 0 and 1, respectively. Let $h_0 = h(C_0)$ and $h_1 = h(C_1)$. Then $h_0 \geq 1$ and $h_1 \geq 1$. If $h_0 = h_1$, by Lemmas 3.7 and 3.8, $k^{\nu_1 - 1} - e \leq k^{\nu_1}$ and $r(h_1 - 1) - e - 1 \leq rh_1$, combining with $p^e \parallel k$ we have

$$p^{e(h_1 - 1)} - e - 1 \leq rh_1 = rh_0.$$ 

Therefore, $h_0 = 1$, and

$$G(p^e, k) = G_2(p^e, k) \cup G_1(p^e, k) \simeq \mathcal{O}^{p^e - 1} \cup G_1(p^e, k).$$

Since $\gcd((p - 1)p^{e-1}, k) = p^r$, it follows that $\text{indeg}(a) = p^r$ or 0 for any $a \in G_1(p^e, k)$. From the proof of Step 1, we obtain $m = p^r = p^{e-1}$ and $r = e - 1$.

If $h_0 \neq h_1$, then

$$p^{e(h_0 - 1)} - e - 1 \leq rh_1.$$ 

We must have $h_0 < h_1$. Then $h(G_2(p^e, k^{h_0})) = 1$, $G_2(p^e, k^{h_0}) \simeq \mathcal{O}^{p^e - 1}$. In this case

$$G(p^e, k^{h_0}) = G_2(p^e, k^{h_0}) \cup G_1(p^e, k^{h_0}) \simeq \mathcal{O}^{p^e - 1} \cup G_1(p^e, k^{h_0}).$$

For any vertices $a \in G_1(p^e, k^{h_0})$ with positive indegree,

$$\text{indeg}_{p^e}(a) = \gcd((p - 1)p^{e-1}, k^{h_0}) = p^r,$$

since $rh_0 \leq r(h_1 - 1) < e - 1$. Again we have $M(G_1(p^e, k^{h_0})) < p^{e-1}$, which implies that $G(p^e, q, k^{h_0}) \cong G(p^e, k^{h_0}) \times G(q, k^{h_0})$ is not symmetric of order $p$ by the same argument in Step 1. But this contradicts Lemma 5.3. Lemma 6.1 is proved.

**Theorem 6.1.** Let $n, k \geq 2$ be two positive integers. Let $2|M$ be a positive integer such that $M$ has an odd prime divisor. If $G(n, k)$ is symmetric of order $M$, then $2 \parallel n$. Moreover, in this case we have $2 \parallel M$ and $G(M, k)$ is symmetric of order $\frac{M}{2}$.

**Proof.** Assume that $2^e \parallel n$. Let $n = 2^m m$ and $h = h(G(2^e, k))$, where $2 \not\parallel m$. Then

$$G(2^e, k^h) = G_2(2^e, k^h) \cup G_1(2^e, k^h) \simeq \mathcal{O}^{2^{e-1}} \cup G_1(2^e, k^h).$$

$G(n, k)$ is symmetric of order $M$, where $M$ has an odd prime divisor $p$, so $p|n$ by Remark 5.2. By Lemma 6.1, we get $\gcd(p - 1, k) = 1$, so $k$ is odd. Therefore, $\text{indeg}_{p^e}(a) = \gcd(a, 2^e)$, $k = 1$ or 0 for any vertex $a$ in $G_1(2^e, k^h)$, by Lemma 5.8, $G(n, k) \simeq G(2^e, k^h) \times G(m, k^h)$ is not symmetric of order 2, since $G(m, k^h)$ is not symmetric of order 2. This contradicts Lemma 5.3. Thus $r = 1$ and $G(2, k) \simeq 2_1^1$. Let

$$G(m, k) \simeq \bigcup_1 n_i H_i \cup \bigcup_2 n_i H_2 \cup \cdots \cup \bigcup_s n_i H_s,$$

where $H_i \simeq H_j$ if and only if $i = j$. We have

$$G(n, k) \simeq G(2, k) \times G(m, k) \simeq \bigcup_2 n_i H_1 \cup \bigcup_2 n_i H_2 \cup \cdots \cup \bigcup_2 n_i H_s.$$ 

Now, by Remark 5.2, $M|2n_i$ for $1 \leq i \leq s$, and $m$ is odd. Thus, there exists a $j$, $1 \leq j \leq s$ such that $2 \not\parallel n_j$. Therefore, $2 \not\parallel M$ and $G(m, k)$ is symmetric of order $M \not\parallel 2$. Theorem 6.1 is proved.

**Theorem 1.2** is a special case of the following lemma. We include the proof here for its simplicity.

**Theorem 6.2.** Let $n = p^e \prod_{i=1}^r p_i^{\nu_i}$, where $p$ is an odd prime, and the $p_i$’s are distinct odd primes such that $p \neq p_i$. Suppose that $\gcd((p - 1)p^{e-1}, k) = p^{e-1}$ and $\gcd((p_i - 1)p_i^{\nu_i - 1}, k) = p_i^{\nu_i - 1}$. Then $G(n, k)$ is symmetric of order $p$ if and only if $p|\text{gcd}(\prod_{i=1}^r p_i^{\nu_i})$ or $\text{ord}_{p-1}(k|t)$ for any $t \in \mathbb{N}$.

**Proof.** We know that $G(p^e, k) \simeq a_1 \mathcal{O}_1^{p^{e-1}} \cup a_2 \mathcal{O}_2^{p^{e-1}} \cup \cdots \cup a_0 \mathcal{O}_r^{p^{e-1}}$, where $a_i = A_i(G(p^e, k))$ and $a_i \neq 0$. By Lemma 3.3, we see that $A_i(G(p^e, k)) = A_i(G(p, k))$ for any $i \in \mathbb{N}$. It follows that $G(p, k) \simeq a_1 \mathcal{O}_1 \cup a_2 \mathcal{O}_2 \cup \cdots \cup a_0 \mathcal{O}_r$. By Lemma 5.5,

$$G(p^e, k) \simeq \mathcal{O}_1^{p^{e-1}} \times G(p, k).$$

Similarly, $G(p_i^{\nu_i}, k) \simeq \mathcal{O}_i^{\nu_i - 1} \times G(p_i, k)$ for $1 \leq i \leq r$. Let $m = p^{e-1} \prod_{i=1}^r p_i^{\nu_i - 1}$. We observe that

$$G(n, k) \cong G(p^e, k) \times \prod_{i=1}^r G(p_i^{\nu_i}, k) \cong \mathcal{O}_1^{m} \times G(p, k) \times \left(\prod_{i=1}^r \mathcal{O}_i^{\nu_i - 1} \times G(p_i, k)\right) \cong \mathcal{O}_1^m \times G\left(p \prod_{i=1}^r p_i, k\right).$$
By Lemma 5.7, \( G(n, k) \) is symmetric of order \( p \) if and only if \( G(p \prod_{i=1}^{r} p_i, k) \) is symmetric of order \( p \). The rest of the proof follows from Theorem 1.2. Theorem 6.2 is proved. \( \square \)

By Theorem 6.1 and Lemma 6.1, we only need to treat the case that \( M \) is an odd integer and \( k \geq 3 \) in the following theorem.

**Theorem 6.3** (Main Theorem). Let \( M \geq 3 \) be an odd integer. Suppose that \( n = \prod_{i=1}^{r} p_i^j \), where the \( p_i \)'s are distinct odd primes.

Let \( k \geq 3 \) be an integer and \( T = \{p_j, \text{gcd}(p_j - 1)p_j^{-1}, k\} = p_j^{e_j-1}, 1 \leq j \leq r \). Then \( G(n, k) \) is symmetric of order \( M \) and only if \( G(\prod_{p \in T} p, k) \) is symmetric of order \( M \).

**Proof.** If \( X \) is a set of prime divisors of \( n \), we denote

\[
n_X = \prod_{p_i \in X} p_i^{e_i}.
\]

Suppose that \( G(n, k) \) is symmetric of order \( M \). Our method is to show that the subgraph \( G(n_T, k) \times (\prod_{p \in T} G_2(p_i^j, k)) \) of \( G(n, k) \) is also symmetric of order \( M \). If it is true, note that \( L' = \prod_{i=1}^{r} G_2(p_i^j, k) \) is a single component of cycle length 1 and that

\[
G(n_T, k) \simeq a_1 O_1^{m_1} \cup a_2 O_2^{m_2} \cup \cdots \cup a_r O_r^{m_r},
\]

where \( m = \prod_{p \in T} p_i^{e_j-1} \) and \( a_i \) is the number of \( i \)-cycles contained in \( G(n_T, k) \). Therefore, \( O_1^{m_1} \times L' \) is a single component. By comparing the cycle length, \( O_1^{m_1} \times L' \simeq O_j^{m_j} \times L' \) if and only if \( i = j \). We get \( M|a_i \) and \( G(n_T, k) \) is symmetric of order \( M \).

Step 1: We do some reductions in this step. Let \( T' = \{p_j : p_j|n, p_j \notin T\} \). By the proof of Theorem 6.2,

\[
G(n, k) \simeq G(n_T, k) \times G(n_{T'}, k)
\]

\[
\simeq O_1^{m_1} \times G\left(\prod_{p_j \in T} p_j, k\right) \times G(n_{T'}, k)
\]

\[
\simeq O_1^{m_1} \times G\left(n_T \prod_{p_j \in T} p_j, k\right).
\]

Here \( m = \prod_{p \in T} p_i^{e_j-1} \). Hence, \( G(n, k) \) is symmetric of order \( M \) if and only if \( G(n_T \prod_{p \in T} p_j, k) \) is symmetric of order \( M \). In the following, we can assume that \( e_j = 1 \) if \( p_j \in T \).

If there exists an index \( i \) such that \( e_i = k \) and \( G(p_i^j, k) \) is not semiregular, then \( p_i \notin T \). And

\[
G(p_i^j, k) = G_2(p_i^j, k) \cup G_1(p_i^j, k) \simeq O_1^{p_i^{e_i-1}} \cup G_1(p_i^j, k).
\]

Let \( X = \{p_1, p_2, \ldots, p_{r-1}, p_r, \ldots, p_r, \ldots, p_r\} \). Then \( G(n, k) \simeq G(n_X, k) \times G(p_i^j, k) \). By Lemma 5.8, \( G(n_X, k) \) is symmetric of order \( M \), since \( G_1(p_i^j, k) \) is always semiregular. By induction, we can assume that if \( e_i \leq k \), then \( p_i \in T \).

Step 2: Let \( S = \{p_j|p_j \notin T, G_2(p_i^j, k) \text{ is semiregular}\}, R = \{p_j|p_j \notin T, G_2(p_i^j, k) \text{ is not semiregular}\} \). Then, by a permutation of indices if necessary, we may assume that \( T = \{p_1, p_2, \ldots, p_{i-1}, p_{i+1}, \ldots, p_k\}, S = \{p_{i+1}, p_{i+2}, \ldots, p_r\} \), and \( R = \{p_1, p_2, \ldots, p_i\} \).

We show that \( G(n_{T\cup S}, k) \times \prod_{i=1}^{r} G_2(p_i^j, k) \) is symmetric of order \( M \) in this step. We write

\[
G(n, k) \simeq H_1 \cup H_2 \cup \cdots \cup H_t,
\]

where \( H_t \neq \emptyset \) and each \( H_t \) is a union of components of \( G(n, k) \) such that \( I(D) = t \) for each component \( D \subseteq H_t \). Then each \( H_t \) is symmetric of order \( M \). We claim that \( H_t \simeq G(n_{T\cup S}, k) \times G_2(p_i^{e_i+1}, k) \times G_2(p_i^{e_i+2}, k) \times \cdots \times G_2(p_i^{e_i}, k) \).

Let \( C \) be a component of \( G(n, k) \). By Lemma 5.1, there exist \( E_1, E_2, \ldots, E_r \), such that \( E_i \) is a component of \( G(p_i^j, k) \) and \( C \) is a component of \( \prod_{i=1}^{r} E_i \). Since \( E_i \) is not semiregular only if \( i \geq s + 1 \) and \( E_i = G_2(p_i^j, k) \), it follows that

\[
I(C) \leq I\left(\prod_{i=1}^{r} E_i\right) = I\left(\prod_{i=s+1}^{r} E_i\right) \leq I\left(\prod_{i=s+1}^{r} G_2(p_i^j, k)\right).
\]

But we observe that \( \prod_{i=s+1}^{r} G_2(p_i^j, k) \) is a component by Lemma 5.1. Hence, \( C \subseteq H_t \) if and only if \( E_i = G_2(p_i^j, k) \) for each \( i \geq s + 1 \). It implies that \( G(n_{T\cup S}, k) \times \prod_{i=s+1}^{r} G_2(p_i^j, k) \simeq H_t \) is symmetric of order \( M \).

Step 3: We claim that if \( p_i \in S \), then \( M(G_2(p_i^j, k)) > M(G_1(p_i^j, k)) \). We have \( e_i > k \), since \( p_i \notin T \). Thus

\[
\text{indeg}_{p_i^j}^k(p_i^j) = p_i^{k-e_j} - \frac{1}{2} k, \quad \text{for } i \geq s + 1.
\]
since \( G_2(p_i^{e_i}, k) \) is semiregular. Then \( k \) is odd and \( e_i \geq 4 \). Assume that \( p^{e_i} \parallel k \), \( 0 \leq r_i \leq e_i - 2 \). Then

\[
k - 1 + \min\{e_i - k - 1, r_i\} = e_i - \left\lceil \frac{e_i}{k} \right\rceil.
\]

If \( r_i \leq e_i - k - 1 \), then \( k - 1 + r_i = e_i - \left\lceil \frac{e_i}{k} \right\rceil \). Thus \( M(G_1(p_i^{e_i}, k)) = \gcd((p_i - 1)p_i^{e_i-1}, k) = p_i^{e_i} < p_i^{e_i-1+\left\lceil \frac{e_i}{k} \right\rceil} = M(G_2(p_i^{e_i}, k)) \).

If \( e_i - k - 1 \leq r_i \), then \( \left\lceil \frac{e_i}{k} \right\rceil = 2 \) and \( M(G_1(p_i^{e_i}, k)) = p_i^{e_i} \leq p_i^{e_i-2} \), where the equality holds if and only if \( r_i = e_i - 2 \). But \( k < e_i \leq p_i^{e_i-2} \), since \( e_i \geq 4 \), thus \( r_i < e_i - 2 \).

Step 4: Let \( L = \prod_{t=1}^{s} G_2(p_i^{e_i}, k) \). We write

\[
H_i \simeq G(n_T, k) \times L
\]

\[
\simeq G(n_T, k) \times G(n_S, k) \times L
\]

\[
\simeq K_i \cup K_2 \cup \cdots \cup K_u,
\]

where \( K_u \neq \emptyset \) and \( K_i \) is a union of components of \( H_i \) such that \( M(D) = i \) for each component \( D \subseteq K_i \). Then each \( K_i \) is symmetric of order \( M \), since \( H_i \) is symmetric of order \( M \).

Now if \( C \) is a component of \( H_i \), there exist \( F \) and \( E_{t+1}, E_{t+2}, \ldots, E_s \), where \( F \) is a component of \( G(n_T, k) \) and \( E_i \) is a component of \( G(p_i^{e_i}, k) \) such that \( C \) is a component of \( F \times \prod_{t=1}^{s} E_i \times L \). But \( M(F) = 1 \), since \( M(G(n_T, k)) = 1 \). Consequently, by the result in Step 3

\[
M(C) \leq M(L) \prod_{i=1}^{s} M(E_i) \leq M(L) \prod_{i=1}^{s} M(G_2(p_i^{e_i}, k)),
\]

and the last equality holds if and only if \( E_i = G_2(p_i^{e_i}, k) \) for \( t + 1 \leq i \leq s \). But \( F \times L \times \prod_{t=1}^{s} G_2(p_i^{e_i}, k) \) is a single component by Lemma 5.1. We see that \( C \subseteq K_u \) if and only if \( E_i = G_2(p_i^{e_i}, k) \) for \( t + 1 \leq i \leq s \). Hence, \( G(n_T, k) \times \prod_{t=1}^{s} G_2(p_i^{e_i}, k) \simeq K_u \) is symmetric of order \( M \). Theorem 6.3 is proved. \( \square \)

**Corollary 6.1.** Let \( M \geq 2 \) be an integer such that \( M \) has an odd prime divisor. Then there exist \( n \) and \( k \geq 2 \) such that \( G(n, k) \) is symmetric of order \( M \) if and only if \( M \) is square free.

**References**


