

Structural Properties of Power Digraphs Modulo n

Joe Kramer-Miller

July 2009

Abstract

We define $G(n, k)$ to be a directed graph whose set of vertices is $\{0, 1, \dots, n-1\}$ and whose set of edges is $\{(a, b) : a^k \equiv b \pmod{n}\}$. We say that $G(n, k)$ is symmetric of order m if we can partition $G(n, k)$ into subgraphs, each containing m components, such that all the components in a subgraph are isomorphic. We develop necessary and sufficient conditions for $G(n, k)$ to contain symmetry when n is odd and square-free. Additionally, we use group theory to describe the structural properties of $G_1(n, k)$, the subgraph of $G(n, k)$ containing only those vertices relatively prime to n .

1 Introduction

Modular exponentiation has been of interest to number theorists since Fermat. However, much less has been said about the process of iteratively applying exponentiation to a residue. By representing iterated modular exponentiation with digraphs, we are able to use aspects of graph theory to describe the nature of iterated modular exponentiation.

This paper extends the results from the papers [1] and [3], which explore a basic number theory function, modular exponentiation, by making novel connections to graph theory and group theory. We continue their work by generalizing previous results, as well as exploring specific cases that have not been covered previously. Specifically, we first develop necessary and sufficient conditions for power digraphs to contain symmetry, when our modulus is square-free and odd. We then utilize some basic concepts from group theory to prove two theorems, which prove as corollaries several of the results discovered by Wilson in [3].

2 Some Preliminary Results

2.1 Basic Definitions

Fix $n \geq 1$ and let $H = \{0, 1, \dots, n-1\}$. Let $f : H \rightarrow H$. A *functional digraph* of f is a directed graph whose vertices are the elements in H , such that there exists an edge from a to b if and only if $f(a) = b$. For this paper, if $x \in H$, then $f(x)$ denotes x^k modulo n , for a fixed k and n . We denote the described directional graph as $G(n, k)$.

If a is a vertex in $G(n, k)$, then it corresponds uniquely to a residue modulo n . We will treat a as a number in statements such as $\text{ord}_p a$ and $\text{gcd}(a, n)$. In addition, a^k will refer to $f(a)$ (i.e., reduced modulo n).

A *component* of $G(n, k)$ is a maximal connected subgraph of the associated nondirected graph. The number of edges coming into a vertex $a \in G(n, k)$ is referred to as the *indegree* of a and is

denoted by $N(n, k, a)$. The number of edges leaving a is referred to as the *outdegree* of a . Note that every vertex in $G(n, k)$ has an outdegree of 1.

A *cycle* is a path from one vertex to itself, and a cycle is a *t-cycle* if it contains exactly t vertices. It is evident that each component contains a unique cycle, because each vertex has outdegree one and because there are finitely many vertices. The number of t -cycles in a graph $G(n, k)$ is denoted $A_t(G(n, k))$.

The subgraph of $G(n, k)$ containing all vertices relatively prime to n is denoted as $G_1(n, k)$. Also, the subgraph of $G(n, k)$ containing all vertices not relatively prime to n is denoted as $G_2(n, k)$.

2.2 The Carmichael Function

Let n be a positive integer. The *Carmichael lambda-function* $\lambda(n)$ is defined as the smallest positive integer such that $a^{\lambda(n)} \equiv 1 \pmod{n}$ for all a relatively prime to n . We know from chapter 2 in [2] that,

$$\begin{aligned}\lambda(1) &= 1 \\ \lambda(2) &= 1 \\ \lambda(4) &= 2 \\ \lambda(2^k) &= 2^{k-2} \text{ for } k \geq 3, \\ \lambda(p^k) &= (p-1)p^{k-1} \text{ for any odd prime } p \text{ and } k \geq 1, \\ \lambda(p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}) &= \text{lcm}[\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \dots, \lambda(p_r^{e_r})],\end{aligned}$$

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

2.3 Symmetries of $G(n, k)$

We say that a graph G is symmetric of order m if G can be partitioned into subgraphs, each subgraph containing exactly m components, such that any two components in a given subgraph are isomorphic. The symmetries of $G(n, k)$ have been studied by Somer and Křížek in [1]. Their main results include specifying conditions for n and k , under which $G(n, k)$ is symmetric of order p , where p is a prime that divides n . They also came up with a useful recursive formula for the number of cycles of length t .

2.4 Products of Graphs

Let $n = n_1 n_2$, where $\text{gcd}(n_1, n_2) = 1$. We know by the Chinese Remainder Theorem that a vertex a in $G(n, k)$ corresponds to the ordered pair (a_1, a_2) , where $0 \leq a_1 < n_1$ and $0 \leq a_2 < n_2$. Additionally, the Chinese Remainder Theorem tells us that a^k corresponds to (a_1^k, a_2^k) . We will define the product of graphs, $G(n_1, k) \times G(n_2, k)$ as follows: a vertex in $G(n_1, k) \times G(n_2, k)$ is an ordered pair (a_1, a_2) such that $a_1 \in G(n_1, k)$ and $a_2 \in G(n_2, k)$. Also, there is an edge from (a_1, a_2) to (b_1, b_2) if and only if there is an edge from a_1 to b_1 in $G(n_1, k)$ and there is an edge from a_2 to b_2 in $G(n_2, k)$. This implies that (a_1, a_2) has an edge leading to (a_1^k, a_2^k) . We then see that $G(n, k) \cong G(n_1, k) \times G(n_2, k)$. We can further assert that if n 's prime decomposition is $p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, then

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

If $G(n, k) \cong G(n_1, k) \times G(n_2, k)$, where $\gcd(n_1, n_2) = 1$, then we call $G(n_1, k)$ and $G(n_2, k)$ *factors* of $G(n, k)$.

2.5 Distribution with Graph Products

Suppose G is a functional graph. Also, suppose E and F are disjoint functional graphs. We will explain why $G \times (E \cup F) = (G \times E) \cup (G \times F)$, which is a property used frequently throughout this paper. Suppose (a_1, a_2) is a vertex in $G \times (E \cup F)$. Then $a_1 \in G$ and a_2 is in either E or F . If $a_2 \in E$, then $(a_1, a_2) \in G \times E$, meaning that $(a_1, a_2) \in (G \times E) \cup (G \times F)$. The same argument works for when $a_2 \in F$. If (a_1, a_2) is in $(G \times E) \cup (G \times F)$, we can use similar reasoning to assert that $(a_1, a_2) \in G \times (E \cup F)$. This means that $G \times (E \cup F)$ and $(G \times E) \cup (G \times F)$ have the same vertices.

We still need to verify that $G \times (E \cup F)$ and $(G \times E) \cup (G \times F)$ have the same set of edges. Suppose (a_1, a_2) has an edge leading to (b_1, b_2) in $G \times (E \cup F)$. This implies that a_1 has an edge leading to b_1 in G . Suppose the edge from a_2 to b_2 is in E . This implies that there is an edge from (a_1, a_2) to (b_1, b_2) in $G \times E$. Therefore there is an edge from (a_1, a_2) to (b_1, b_2) in $(G \times E) \cup (G \times F)$. A similar argument works if the edge from a_2 to b_2 is in F . If (a_1, a_2) has an edge leading to (b_1, b_2) in $(G \times E) \cup (G \times F)$, we can use similar reasoning to show that there is an edge from (a_1, a_2) to (b_1, b_2) in $G \times (E \cup F)$. It follows that $G \times (E \cup F) = (G \times E) \cup (G \times F)$. This property can be extended to the union of an arbitrary number of disjoint graphs, and proves extremely helpful when proving results on $G(n, k)$.

2.6 Some Useful Previous Results

These next two results provide us with a useful connection between $G(n, k)$ and its factors. We make use of them several times throughout this paper.

Theorem 2.1. *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 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 $G(n_2, k)$.*

Proof. This is Theorem 6.7 in [1]. □

Theorem 2.2. *Let $n = n_1 n_2$ where $\gcd(n_1, n_2) = 1$. Let $J(n_1, k)$ be a union of components of $G(n_1, k)$ and let $L(n_2, k)$. Then $J(n_1, k) \times L(n_2, k)$ is a union of components of $G(n, k) \cong G(n_1, k) \times G(n_2, k)$.*

Proof. This is Theorem 6.8 in [1]. □

Our main results on symmetry is dependent on $A_t(G(n, k))$, for several values of t . Hence, it is useful to have a formula for $A_t(G(n, k))$ that is completely dependent on n and k .

Theorem 2.3. *Let n 's prime decomposition be $p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$.*

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

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

Proof. This is Theorem 6.6 in [1]. □

3 Results on Symmetry

We will now establish necessary and sufficient conditions for $G(n, k)$ to be symmetric of order p , where $p|n$ and n is square-free. To do this, we first will prove a less general result. We will then be able to generalize that result for all square-free n . However, before we are able to prove anything meaningful, we need a few lemmas and theorems.

Lemma 3.1. *Let $n = n_1n_2$ where $\gcd(n_1, n_2) = 1$. Let $E(n_1, k)$ be a component of $G(n_1, k)$ and let $J(n_2, k)$ be a component of $G(n_2, k)$. Let s be the length of $J(n_2, k)$'s cycle and let t be the length of $E(n_1, k)$'s cycle. Then $C(n, k) = E(n_1, k) \times J(n_2, k)$ is a subdigraph of $G(n, k)$ consisting of $\gcd(s, t)$ components, each having cycles of length $\text{lcm}[s, t]$.*

Proof. By Theorem 2.2, we know that $C(n, k)$ is a union of components of $G(n, k)$. Also, by Theorem 2.1, (c_i, d_i) is a cycle vertex of $C(n, k)$ if and only if c_i is a cycle vertex of $E(n_1, k)$ and d_i is a cycle vertex of $J(n_2, k)$. Therefore there are precisely st cycle vertices in $C(n, k)$. Let

$$\langle c_1, c_2, \dots, c_t \rangle$$

be the cycle in $E(n_1, k)$ and let

$$\langle d_1, d_2, \dots, d_s \rangle$$

be the cycle in $J(n_2, k)$. Evidently, $\text{lcm}[s, t] = e$ is the least positive integer such that $(c_i, d_j)^e = (c_i^e, d_j^e) = (c_i, d_j)$. Hence each cycle has is of length $\text{lcm}[s, t]$. It follows that there are $\frac{st}{\text{lcm}[s, t]} = \gcd(s, t)$ cycles. \square

Corollary 3.2. *Let $n = n_1n_2$ where $\gcd(n_1, n_2) = 1$. Let $E(n_1, k)$ be a component of $G(n_1, k)$ and let $J(n_2, k)$ be a component of $G(n_2, k)$. Let s be the length of $J(n_2, k)$'s cycle and let t be the length of $E(n_1, k)$'s cycle. Then $C(n, k) = E(n_1, k) \times J(n_2, k)$ consists of components whose cycle length is greater than or equal to $\max(t, s)$.*

Lemma 3.3. *Let n be an odd integer. Let n 's prime decomposition be $p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$ and let a be a vertex of $G_1(n, k)$. Then*

$$N(n, k, a) = \prod_{i=1}^r N(p_i^{e_i}, k, a) = \prod_{i=1}^r \gcd(\lambda(p_i^{e_i}), k),$$

or $N(n, k, a) = 0$.

Proof. This is Lemma 2 in [3]. \square

Corollary 3.4. *Suppose $\gcd(p-1, k) = 1$. Then $G(p, k)$ is a permutation.*

Proof. First note that $G_2(p, k)$ is a permutation, since it consists of a single vertex with an edge leading to itself. Next, since each of the $p-1$ vertices in $G_1(p, k)$ has outdegree 1, the sum of the indegrees of the $p-1$ vertices in $G_1(p, k)$ should be $p-1$. By Lemma 3.3, if a is a vertex in $G_1(p, k)$ then a has indegree $\gcd(p-1, k) = 1$ or 0. If there were a vertex in $G_1(p, k)$ whose indegree was 0, then the sum of the indegrees of each vertex of $G_1(p, k)$ would be less than $p-1$. Therefore, each vertex in $G_1(p, k)$ has indegree 1. It follows that $G(p, k)$ is a permutation. \square

Lemma 3.5. *Let $x, a, b \in \mathbb{N}$. If $a|b$, then $\text{ord}_a x | \text{ord}_b x$.*

Proof. Let $t = \text{ord}_b x$. Then $x^t \equiv 1 \pmod{b}$. Since $a|b$, $x^t \equiv 1 \pmod{a}$. Therefore $\text{ord}_a x | t$, or $\text{ord}_a x | \text{ord}_b x$. \square

This next result is a specific case of Theorem 2 [3].

Lemma 3.6. *Let p be an odd prime. Let $c \neq 0$ be a cycle vertex in $G(p, k)$ where $\text{gcd}(p-1, k) = 1$. Let $s = \text{ord}_p c$. The length of c 's cycle is $r = \text{ord}_s k$.*

Proof. The cycle length of c is the smallest integer r such that $c^{k^r} \equiv c \pmod{p}$. First note that $\text{gcd}(s, k) = 1$, because $s|(p-1)$ and $\text{gcd}(p-1, k) = 1$. This implies that $\text{ord}_s k$ is defined. Since $\text{ord}_s k = r$, we know that $k^r \equiv 1 \pmod{s}$. This means that there exists $n \in \mathbb{N}$ such that $k^r = 1 + ns$. It follows that

$$\begin{aligned} c^{k^r} &\equiv c^{ns+1} \pmod{p} \\ &\equiv c^{ns} c \pmod{p} \\ &\equiv c \pmod{p}. \end{aligned}$$

Note that r is minimal by the definition of $\text{ord}_s k$. The claim follows. \square

Corollary 3.7. *Let p be prime. Suppose $\text{gcd}(p-1, k) = 1$. The longest cycle in $G(p, k)$ has a length of $\text{ord}_{p-1} k$ and the cycle lengths of all cycles in $G(p, k)$ divide $\text{ord}_{p-1} k$.*

Proof. We know that there exists $g \in \mathbb{Z}_p^*$, such that $\text{ord}_p g = p-1$, because \mathbb{Z}_p^* is a cyclic group. We know that $G(p, k)$ is a permutation, by Corollary 3.4. Thus g is a cycle vertex. It follows from Lemma 3.6 that there is a cycle of length $\text{ord}_{p-1} k$ in $G(p, k)$. Now let $g' \in G(p, k)$. We will show that the length of the cycle containing g' divides $\text{ord}_{p-1} k$. If g' is in $G_2(p, k)$, then g' is 0, and contained in a 1-cycle. Thus the length of the cycle containing g' divides $\text{ord}_{p-1} k$. Next, suppose g' is in $G_1(p, k)$. Let $r = \text{ord}_p g'$. Note that $r|p-1$. We know that the length of the cycle containing g' is $\text{ord}_r k$. By Lemma 3.5, since $r|p-1$, we know that $\text{ord}_r k | \text{ord}_{p-1} k$. Since g' is an arbitrary vertex in $G(p, k)$ it follows that the cycle lengths of all cycles in $G(p, k)$ divide $\text{ord}_{p-1} k$. \square

For the following theorems, we will use an equivalence relation on the components of $G(n, k)$. Two components are in the same equivalence class if and only if they are isomorphic. The number of components in a specific equivalence class, C , is denoted by $S(C)$ and is referred to as the size of C . Each component in an equivalence class C has a cycle of the same length and we denote this length by $K(C)$. If $U = \{C_1, C_2, \dots, C_m\}$ is a set of equivalence classes where $K(C_i) = K(C_j)$, for $0 < i, j \leq m$, then $K(U)$ refers to $K(C_i)$. Also, if J is a component in equivalence class C where every cycle vertex in J has the same indegree, then $M(C)$ refers to that indegree. If $M(C_i) = M(C_j)$, for all i and j , then $M(U)$ refers to $M(C_i)$. Also, $G(C)$ refers to the graph consisting entirely of the components in C . Likewise $G(U)$ refers to the graph $\cup_{i=1}^m G(C_i)$.

Theorem 3.8. *Let $n = pq_1q_2\dots q_m$, where each q_i and p are distinct odd primes. Let J be a subgraph of $G(q_1q_2\dots q_m, k)$ that is symmetric of order p . Then $G(p, k) \times J$ is symmetric of order p .*

Proof. Let E_1, E_2, \dots, E_s be the equivalence classes of $G(q_1q_2\dots q_m, k)$. Let $0 < i \leq s$. Note that since $G(q_1q_2\dots q_m, k)$ is symmetric of order p , $S(E_i) = rp$, for some $r \in \mathbb{N}$. Let C_1, C_2, \dots, C_{rp} be the components in E_i . We will first show that if C is a component in $G(p, k) \times G(E_i)$, then C is isomorphic to a component in $G(p, k) \times C_1$. Then we will show that if C' is a component in $G(p, k) \times C_1$, then the number of components in $G(p, k) \times G(E_i)$ that are isomorphic to C' is a multiple of p . It will follow that $G(p, k) \times G(E_i)$ has xp components isomorphic to C , where $x \in \mathbb{N}$. Since C is an arbitrary component in $G(p, k) \times G(E_i)$, we will know that $G(p, k) \times G(E_i)$ is symmetric of order p . We also know that

$$G(n, k) \cong G(p, k) \times G(q_1q_2\dots q_m, k) \quad (1)$$

$$= G(p, k) \times \bigcup_{j=1}^s G(E_j) \quad (2)$$

$$= \bigcup_{j=1}^s (G(p, k) \times G(E_j)). \quad (3)$$

Furthermore, since E_i is an arbitrary equivalence class, the graph in Equation (3) is symmetric of order p , implying that $G(n, k)$ is symmetric of order p .

We will show that if C is a component in $G(p, k) \times G(E_i)$ then C is isomorphic to a component in $G(p, k) \times C_1$. Since $G(E_i) = \bigcup_{j=1}^{rp} C_j$, we find that

$$G(p, k) \times G(E_i) = G(p, k) \times \bigcup_{j=1}^{rp} C_j \quad (4)$$

$$= \bigcup_{j=1}^{rp} (G(p, k) \times C_j). \quad (5)$$

This implies that C is a component in $G(p, k) \times C_{i_1}$, where $0 < i_1 \leq rp$. However, since $C_{i_1} \cong C_1$, we know that $G(p, k) \times C_{i_1} \cong G(p, k) \times C_1$. It follows that C is isomorphic to a component in $G(p, k) \times C_1$.

Next, we will show that if C' is a component in $G(p, k) \times C_1$, then the number of components in $G(p, k) \times G(E_i)$ that are isomorphic to C' is a multiple of p . Let F be the equivalence class of $G(p, k) \times C_1$ which contains C' . Evidently, $G(p, k) \times C_1$ contains $S(F)$ components isomorphic to C' . Let $0 < j \leq rp$. Since $C_1 \cong C_j$, we know $G(p, k) \times C_1 \cong G(p, k) \times C_j$. Therefore $G(p, k) \times C_j$ contains $S(F)$ components isomorphic to C' . Since C_j is an arbitrary component in E_i , and since there are rp components in E_i , we see that $\bigcup_{j=1}^{rp} G(p, k) \times C_j$ has $rp \cdot S(F)$ components isomorphic to C' . Therefore, by Equation (5), we know that the number of components of $G(p, k) \times G(E_i)$ isomorphic to C' is a multiple of p . □

Lemma 3.9. *Let $n = n_1n_2$, where $(n_1, n_2) = 1$. Let $a = \gcd(a_1, a_2)$ be a vertex in $G(n, k) = G(n_1, k) \times G(n_2, k)$. Then $N(n, k, a) = N(n_1, k, a_1)N(n_2, k, a_2)$.*

Proof. There is an edge from $b = (b_1, b_2)$ to a in $G(n, k)$ if and only if there is an edge from b_1 to a_1 in $G(n_1, k)$ and there is an edge from b_2 to a_2 in $G(n_2, k)$. The result follows. □

Corollary 3.10. *Let $n = n_1n_2$, where $(n_1, n_2) = 1$. Let $a = (a_1, a_2)$ be a vertex in $G(n, k) = G(n_1, k) \times G(n_2, k)$. Then $N(n, k, a) \geq \max(N(n_1, k, a_1), N(n_2, k, a_2))$.*

Lemma 3.11. *Let $n = p_1 p_2 \dots p_m$, where each p_i is a distinct prime. Suppose there exists $0 < j \leq m$ such that $\gcd(p_i - 1, k) = 1$ when $i \leq j$ and $\gcd(p_i - 1, k) \neq 1$ when $i > j$. Note that $G(n, k) = G(p_1, k) \times G(p_2, k) \times \dots \times G(p_m, k)$. A vertex a has indegree 1 if and only if it is of the form $(a_1, a_2, \dots, a_j, 0, 0, \dots, 0)$.*

Proof. \Leftarrow Let a be a vertex of the form $(a_1, a_2, \dots, a_j, 0, 0, \dots, 0)$. Since $\gcd(p_i - 1, k) = 1$, when $i \leq j$, we know that $G(p_i, k)$ is a permutation when $i \leq j$, by Corollary 3.4. This implies that $N(p_i, k, a_1) = 1$, when $i \leq j$. Next, we know that 0 is the only vertex in $G_2(p_i, k)$, for all i . This implies that $G_2(p_i, k)$ consists of a single fixed point, and consequently, $N(p_i, k, 0) = 1$. We know by Lemma 3.9 that

$$N(n, k, a) = N(p_1, k, a_1) \cdot N(p_2, k, a_2) \cdot \dots \cdot N(p_j, k, a_j) \cdot N(p_{j+1}, k, 0) \cdot \dots \cdot N(p_m, k, 0).$$

It follows that $N(n, k, a) = 1$, as desired.

\Rightarrow We will prove the contrapositive. Let a be a vertex of the form (a_1, a_2, \dots, a_m) , where $a_i \neq 0$ for some $i > j$. Let x be the smallest integer such that $x > j$ and $a_x \neq 0$. There are two cases:

Case 1. For some y , $N(p_y, k, a_y) = 0$,

Case 2. $N(p_i, k, a_i) \neq 0$ for all i .

Note that

$$N(n, k, a) = N(p_1, k, a_2) \cdot N(p_2, k, a_3) \cdot \dots \cdot N(p_m, k, a_m), \quad (6)$$

by Lemma 3.9.

In the first case, Equation (6) tells us that $N(n, k, a) = 0$. Next consider the second case. Note that since $a_x \neq 0$, $a_x \in G_1(p_x, k)$. We know that $N(p_x, k, a_x)$ is 0 or $\gcd(p_x - 1, k)$, by Lemma 3.3. However, we are assuming that $N(p_x, k, b_x) \neq 0$, so $N(p_x, k, a_x) = \gcd(p_x - 1, k)$. By our assumption, $\gcd(p_x - 1, k) \neq 1$, implying that $N(p_x, k, a_x) \neq 1$. It follows from Equation (6) that $N(n, k, a) \neq 1$. □

Lemma 3.12. *Let $n = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$, where each p_i is a distinct prime. Let $a = (a_1, a_2, \dots, a_m)$ and $b = (b_1, b_2, \dots, b_m)$ be vertices in $G(n, k) \cong G(p_1^{e_1}, k) \times G(p_2^{e_2}, k) \times \dots \times G(p_m^{e_m}, k)$. If a and b are in the same cycle, then a_i and b_i are in the same cycle, for each i .*

Proof. First note that a_i and b_i are cycle vertices, for each i , by Theorem 2.1. Next, since a and b are in the same cycle, there exists $x \in \mathbb{N}$ such that $a^{k^x} \equiv b \pmod{n}$. This implies that $(a_1^{k^x}, a_2^{k^x}, \dots, a_m^{k^x}) = (b_1, b_2, \dots, b_m)$. Hence $a_i^{k^x} \equiv b_i \pmod{p_i^{e_i}}$, implying that a_i and b_i are in the same cycle, for all i . □

Lemma 3.13. *Let $n = p_1 p_2 \dots p_m$. If a and b are cycle vertices in $G(n, k)$ in the same cycle, then $N(n, k, a) = N(n, k, b)$.*

Proof. We know that $G(n, k) \cong G(p_1, k) \times G(p_2, k) \times \dots \times G(p_m, k)$. Thus, a and b correspond to the m -tuples (a_1, a_2, \dots, a_m) and (b_1, b_2, \dots, b_m) respectively, where $0 \leq a_i, b_i < p_i$. By Lemma 3.14, we know that a_i and b_i are in the same cycle in $G(p_i, k)$, for all i . Now suppose $a_i, b_i \in G_2(p_i, k)$. Since $G_2(p_i, k)$ consists of a single fixed point, it's evident that $N(p_i, k, a_i) = N(p_i, k, b_i)$. Also,

if $a_i, b_i \in G_1(p_i, k)$, it is evident by Lemma 3.3 that $N(p_i, k, a_i) = N(p_i, k, b_i)$. It follows from Lemma 3.9 that

$$N(n, k, a) = N(p_1, k, a_1) \cdot N(p_2, k, a_2) \cdot \dots \cdot N(p_m, k, a_m) \quad (7)$$

$$= N(p_1, k, b_1) \cdot N(p_2, k, b_2) \cdot \dots \cdot N(p_m, k, b_m) \quad (8)$$

$$= N(n, k, b), \text{ as desired.} \quad (9)$$

□

Theorem 3.14. *Suppose $\gcd(p-1, k) = 1$. Let X be a directed graph that is a permutation. Then $G(p, k) \times X$ is symmetric of order p if and only if for every $x \in \mathbb{N}$ that $p \nmid A_x(X)$, $\text{ord}_{p-1}k|x$.*

Proof. \Leftarrow Suppose that for every $x \in \mathbb{N}$ such that $p \nmid A_x(X)$, $\text{ord}_{p-1}k|x$. We will show that $G(p, k) \times X$ is symmetric of order p .

Let X_1 be the subgraph of X containing all cycles of length t , such that $p|A_t(X)$, and let $X_2 = X - X_1$. Note that X_1 and X_2 are disjoint, since X is composed entirely of cycles. Also note that X_2 precisely the cycles of length t such that $p \nmid A_t(X)$ and $\text{ord}_{p-1}k|x$. By our definition, X_1 is symmetric of order p . Therefore, by Theorem 3.8, $G(p, k) \times X_1$ is symmetric of order p . We will show that $G(p, k) \times X_2$ is also symmetric of order p . Since

$$G(p, k) \times X = G(p, k) \times (X_1 \cup X_2) \quad (10)$$

$$= (G(p, k) \times X_1) \cup (G(p, k) \times X_2), \quad (11)$$

it will follow that $G(p, k) \times X$ is symmetric of order p .

Let C_1, C_2, \dots, C_m denote the cycles in X_2 . Note that since X_2 is a permutation, it is comprised entirely of cycles and $X_2 = \bigcup_{i=1}^m C_i$. Let j be between 1 and m . We will show that $G(p, k) \times C_j$ is symmetric of order p . Since C_j is an arbitrary cycle of X_2 , we know

$$G(p, k) \times X_2 = G(p, k) \times \bigcup_{i=1}^m C_i \quad (12)$$

$$= \bigcup_{i=1}^m (G(p, k) \times C_i). \quad (13)$$

It will follow that $G(p, k) \times X_2$ is symmetric of order p .

We will now show that $G(p, k) \times C_j$ is symmetric of order p . Let y denote $L(C_j)$. Recall that X_2 precisely the cycles of length t such that $p \nmid A_t(X)$ and $\text{ord}_{p-1}k|x$. This implies that $p \nmid A_y(X)$ and $\text{ord}_{p-1}k|y$, since C_j is in X_2 . Let D_1, D_2, \dots, D_l be the cycles in $G(p, k)$. Since $\gcd(p-1, k)$, we know by Corollary 3.7 that $G(p, k)$ is a permutation. This implies that $G(p, k) = \bigcup_{i=1}^l D_i$ and $p = \sum_{i=1}^l L(D_i)$. By Corollary 3.5, we know that if D is a cycle in $G(p, k)$, then $L(D)|\text{ord}_{p-1}k$. Since $\text{ord}_{p-1}k|y$, we can then conclude that $L(D_i)|y$, for all i . We know by Lemma 3.1 that $D_i \times C_j$ is going to consist entirely of $\gcd(L(D_i), y)$ cycles of length $\text{lcm}[L(C_j), y]$, for all i . Since $L(D_i)|y$, it follows that $D_i \times C_j$ consists entirely of $L(D_i)$ cycles of length y .

$$G(p, k) \times C_j = \left(\bigcup_{i=1}^l D_i \right) \times C_j \quad (14)$$

$$= \bigcup_{i=1}^l (D_i \times C_j). \quad (15)$$

It follows that $G(p, k) \times C_j$ consists entirely of $\sum_{i=1}^l L(D_i) = p$ cycles of length y . Therefore $G(p, k) \times C_j$ is isomorphic of order p .

\Rightarrow Suppose there exists some x such that $p \nmid A_x(X)$ and $\text{ord}_{p-1} k \nmid x$. We will show that $G(p, k)$ is not symmetric of order p . Let X_1 be a subgraph of X consisting of each cycle of length t , such that $p \mid A_t(X)$, or $p \nmid A_t(X)$ and $\text{ord}_{p-1} k \mid t$. Let X_2 be a subgraph of X consisting of each cycle of length t , such that $p \nmid A_t(X)$ and $\text{ord}_{p-1} k \nmid t$. Note that $X = X_1 \cup X_2$. We know that $G(p, k) \times X_1$ is symmetric of order p , by the other direction of this theorem. We will show that $G(p, k) \times X_2$ is not symmetric of order p . Since

$$G(p, k) \times X = G(p, k) \times (X_1 \cup X_2) \quad (16)$$

$$= (G(p, k) \times X_1) \cup (G(p, k) \times X_2), \quad (17)$$

it will follow that $G(p, k) \times X$ is not symmetric of order p .

Let s denote the length of the smallest cycle in X_2 . We will show that the number of s -cycles in $G(p, k) \times X_2$ is not a multiple of p , implying that $G(p, k) \times X_2$ is not symmetric of order p . Let $X_{2,1}$ denote the subgraph of X_2 containing all cycles of length s and let $X_{2,2} = X_2 - X_{2,1}$. We will show that $G(p, k) \times X_{2,2}$ contains no s -cycles and that the number of s -cycles in $X_{2,1}$ is not a multiple of p . Since

$$G(p, k) \times X_2 = G(p, k) \times (X_{2,1} \cup X_{2,2}) \quad (18)$$

$$= (G(p, k) \times X_{2,1}) \cup (G(p, k) \times X_{2,2}), \quad (19)$$

it will follow that the number of s -cycles in $G(p, k) \times X_2$ is not a multiple of p .

Let C_1, C_2, \dots, C_a be the cycles of $X_{2,2}$. Let j be between 1 and a . We know that $L(C_j) > s$. We also know that the length of a cycle in $G(p, k) \times C_j$ is greater than or equal to $L(C_j)$, by Corollary 3.2. This implies that if C is a cycle in $G(p, k) \times C_j$, then $L(C) > s$. Therefore $G(p, k) \times C_j$ contains no cycles of length s , as desired. Since C_j is an arbitrary cycle in $X_{2,2}$, we know that $G(p, k) \times C_i$ has no cycles of length s for all i . We know that

$$G(p, k) \times X_{2,2} = G(p, k) \times \bigcup_{i=1}^a C_i \quad (20)$$

$$= \bigcup_{i=1}^a (G(p, k) \times C_i). \quad (21)$$

It follows that $G(p, k) \times X_{2,2}$ has no cycles of length s .

Let D_1, D_2, \dots, D_b be the cycles of $X_{2,1}$, each of which is a s -cycle. Note that $p \nmid b$, because otherwise each D_i would be in X_1 . Let E be the subgraph of $G(p, k)$ containing all cycles

whose length divides s and let F be the subgraph of $G(p, k)$ containing all cycle whose length does not divide s . We know that $X_{2,1} = E \cup F$, because $X_{2,1}$ is a permutation and therefore has no non-cycle vertices. Note that E is not empty because $G(p, k)$ has at least two fixed points. We know that $G(p, k)$ has a cycle of length $\text{ord}_{p-1}k$, by Corollary 3.7. We also know that $\text{ord}_{p-1}k \nmid s$ because X_2 is defined as the subgraph of X consisting of cycles of length t , such that $p \neq |A_t(X)$ and $\text{ord}_{p-1}k \nmid t$. It follows that F is not empty because $G(p, k)$ has a cycle length of $\text{ord}_{p-1}k$ and $\text{ord}_{p-1}k \nmid s$. Let r denote the number of cycle vertices in E . We know that r is not 0 because E is not empty. Also note that r is less than p , because $F \cup E = G(p, k)$ and F is not empty. It follows that $p \nmid r$. We will show that $E \times D_i$ contains exactly r s -cycles, for each i . Then we will show that $F \times D_i$ has no s -cycles, for each i . We know that

$$G(p, k) \times X_{2,1} = (E \cup F) \times \bigcup_{i=1}^b D_i \quad (22)$$

$$= (E \times \bigcup_{i=1}^b D_i) \cup (F \times \bigcup_{i=1}^b D_i) \quad (23)$$

$$= \bigcup_{i=1}^b (E \times D_i) \cup \bigcup_{i=1}^b (F \times D_i). \quad (24)$$

It follows that $G(p, k) \times X_{2,1}$ contains exactly rb s -cycles. Since $p \nmid b$ and $p \nmid r$, we know that $p \nmid rb$, and consequently, $G(p, k) \times X_{2,1}$ is not symmetric of order p .

Let E_1, E_2, \dots, E_c be the cycles of E . Note that $\bigcup_{i=1}^c E_i = E$ and $\sum_{i=1}^c L(E_i) = r$. Let E_j be an arbitrary cycle in E . By our definition of E , $L(E_j) \nmid s$. Since $L(D_i)$, for all i , it follows from Lemma 3.1 that $E_j \times D_i$ consists of $L(E_j)$ cycles of length s , for all i . We know that

$$E \times D_i = \left(\bigcup_{j=1}^c E_j \right) \times D_i \quad (25)$$

$$= \bigcup_{j=1}^c (E_j \times D_i), \text{ for all } i. \quad (26)$$

This implies that $E \times D_i$ consists of $\sum_{j=1}^c L(E_j) = r$ s -cycles, for all i .

We will now show that $F \times D_i$ has no s -cycles for each i . Let F_1, F_2, \dots, F_d be the cycles in F and let F_j be an arbitrary cycle in F . We know that $L(D_i) = s$, for all i , and that $L(F_j) \nmid s$. This implies that $\text{lcm}[L(D_i), L(F_j)] > s$, for all i . We know by Lemma 3.1 that the cycles in $F_j \times D_i$ have length $\text{lcm}[L(D_i), L(F_j)]$, for all i . It follows that $F_j \times D_i$ has no s -cycles, for all i . Since F_j is an arbitrary cycle in F , we know that

$$F \times D_i = \left(\bigcup_{j=1}^d F_j \right) \times D_i \quad (27)$$

$$= \bigcup_{j=1}^d (F_j \times D_i), \quad (28)$$

for all i . This implies that $F \times D_i$ has no s -cycles, for all i . Since D_i is an arbitrary cycle in $X_{2,1}$, it follows that $F \times D_i$ has no s -cycles for all i . □

If $T = \{p_1, p_2, \dots, p_m\}$, where each p_i is prime, then $G(T, k)$ denotes $G(p_1 p_2 \dots p_m, k)$. Also, if X is a functional graph and C is a component, $I(X, C)$ denotes the number of components in X isomorphic to C . We now have the machinery to provide necessary and sufficient conditions for $G(n, k)$ to be symmetric of order p , when n is odd and square free.

Theorem 3.15. *Let $n = pq_1 q_2 \dots q_m$, where q_i and p are distinct odd primes. Suppose $G(p, k)$ is not symmetric of order p . $G(n, k)$ is symmetric of order p if and only if both of the following conditions are met*

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

ii *Let $Q = \{q_1, q_2, \dots, q_m\}$. Let $T = \{q \in Q : \gcd(q-1, k) = 1\}$. Then T is nonempty and for all $x \in \mathbb{N}$ such that $p \nmid A_x(G(T, k))$, $\text{ord}_{p-1} k \mid x$.*

Proof. \Rightarrow First we will assume that condition i is not satisfied, and then show that $G(n, k)$ is not symmetric of order p . Then we will assume that condition i is satisfied and condition ii is not satisfied. We will show that under these assumptions that $G(n, k)$ is not symmetric of order p . It will follow that if condition i or condition ii is not satisfied, then $G(n, k)$ is not symmetric of order p .

Claim (1). *If $\gcd(p-1, k) \neq 1$, then $G(n, k)$ is not symmetric of order p .*

Consider the set of equivalency classes of $G(q_1 q_2 \dots q_m, k)$, which we will denote as γ . Since $p \nmid q_1 q_2 \dots q_m$, there must exist some equivalence class whose size is not a multiple of p . Let t denote the smallest positive integer, such that there exists $R \in \gamma$, such that $t = K(R)$ and $p \nmid S(R)$. By Lemma 3.13, we know that if x and y are in the same cycle, then $N(q_1 q_2 \dots q_m, k, x) = N(q_1 q_2 \dots q_m, k, y)$. Thus if $C \in \gamma$, $M(C)$ is defined. Let s denote the smallest positive integer such that there exists an equivalence class, R' , where $K(R') = t$, $p \nmid S(R')$ and $M(R') = s$. Let $Z = \{V \in \gamma : p \nmid S(V), K(V) = t, \text{ and } M(V) = s\}$. Also, let Z_1, Z_2, \dots, Z_l , denote the equivalence classes in Z .

Let C_1 be a component in γ . We will now show that the number of components in $G(n, k)$ that are isomorphic to C_1 is not a multiple of p , implying that $G(n, k)$ is not symmetric of order p . To do this, we will partition γ into three disjoint subsets. The first partition is Z . The second partition, X , is the union of every equivalency class in $\gamma - Z$ whose size is a multiple of p . Finally, the last partition, Y , consists of the remaining classes that aren't in X or Z . First we will show that $I(G(p, k) \times G(X), C_1)$ is a multiple of p , $x'p$, and that $I(G(p, k) \times G(Y), C_1) = 0$. Then we will show that $I(G(p, k) \times G(Z), C_1) = S(Z_1)$, which by definition is not a multiple of p . Note that

$$G(n, k) \cong G(p, k) \times G(q_1 q_2 \dots q_m, k) \tag{29}$$

$$= G(p, k) \times (G(X) \cup G(Y) \cup G(Z)) \tag{30}$$

$$= (G(p, k) \times G(Z)) \cup (G(p, k) \times G(X)) \cup (G(p, k) \times G(Y)). \tag{31}$$

This implies that

$$\begin{aligned} I(G(n, k), C_1) &= I(G(p, k) \times G(X), C_1) + I(G(p, k) \times G(Y), C_1) + I(G(p, k) \times G(Z), C_1) \\ &= x'p + 0 + S(Z_1). \end{aligned}$$

Since $x'p + 0 + S(Z_1)$ is not divisible by p , we know that $p \nmid I(G(n, k), C_1)$. Therefore $G(n, k)$ is not symmetric of order p .

Claim (1.a). $p \mid I(G(p, k) \times G(X), C_1)$.

By definition the, size of each of X 's equivalency classes is a multiple of p . This implies that $G(X)$ is symmetric of order p . It follows from Theorem 3.8 that $G(p, k) \times G(X)$ is symmetric of order p as well. Hence, $p \mid I(G(p, k) \times G(X), C_1)$.

Claim (1.b). $I(G(p, k) \times G(Y), C_1) = 0$.

Let $\phi \in Y$. By definition, $Y = (\gamma - X) - Z$. Since X contains every equivalence class of $G(Q, k)$ whose size is a multiple of p , we know that $p \nmid S(\phi)$. By the definition of Z , we know that if $C \in \gamma$ such that $p \nmid S(C)$, then $K(C) \geq K(Z) = t$. This is because t is defined as the least positive integer such that there exists a class C' where $p \nmid S(C')$ and $K(Z) = t$. Since $p \nmid S(\phi)$, it follows that $K(\phi) \geq K(Z)$. We will now show that if $K(\phi) > K(Z)$, then $I(G(p, k) \times G(\phi), C_1) = 0$. Following that, we will show that if $K(\phi) = K(Z)$, then $I(G(p, k) \times G(\phi), C_1) = 0$. Let $Y_1, Y_2, \dots, Y_{m'}$ be all of the elements in Y . Since ϕ is an arbitrary element in Y , we will know that $I(G(p, k) \times G(Y_i), C_1) = 0$, for all i . It follows that

$$I(G(p, k) \times G(Y), C_1) = I(G(p, k) \times \bigcup_{i=1}^{m'} G(Y_i), C_1) \quad (32)$$

$$= I(\bigcup_{i=1}^m (G(p, k) \times G(Y_i)), C_1) \quad (33)$$

$$= \sum_{i=1}^{m'} I(G(p, k) \times G(Y_i), C_1) \quad (34)$$

$$= 0. \quad (35)$$

Suppose $K(\phi) > K(Z)$. We know by Corollary 3.2 that the cycle length of any component in $G(p, k) \times G(\phi)$ is greater than or equal to $K(\phi)$. This implies that the cycle length of any component in $G(p, k) \times G(\phi)$ is greater than $K(Z)$. Since $L(C_1) = K(Z)$, we know $I(G(p, k) \times G(\phi), C_1) = 0$.

Next, suppose $K(\phi) = K(Z) = t$. By the definition of Z , if C is an equivalence class of $G(Q, k)$ such that $p \nmid S(C)$ and $t = K(C)$, then $M(C) \geq M(Z) = s$. This is because s is defined as the least positive integer such that there exists an equivalence class, C' , such that $p \nmid S(C')$, $t = K(C')$ and $M(C') = s$. Therefore, $M(\phi) \geq M(Z)$. Note that if $M(\phi) = M(Z)$, then $p \nmid S(\phi)$, $t = K(\phi)$ and $M(\phi) = s$, which would imply that $\phi \in Z$. Since $\phi \notin Z$, we can conclude that $M(\phi) > M(Z)$.

By Corollary 3.10 we know that any component in $G(p, k) \times G(\phi)$ has cycle vertices whose indegree is greater than or equal to $M(\phi)$. This implies that every component in $G(p, k) \times G(\phi)$ has cycle vertices whose indegree is greater than $M(Z)$, since $M(\phi) > M(Z)$. Since the indegree of any cycle vertex in C_1 is $M(Z)$, we can conclude that no component in $G(p, k) \times G(\phi)$ is isomorphic to C_1 . Thus $I(G(p, k) \times G(Y), C_1) = 0$.

Claim (1.c). *The number of components in $G(p, k) \times G(Z)$ isomorphic to C_1 is not a multiple of p .*

Finally we will show that $I(G(p, k) \times G(Z), C_1) = S(Z_1)$. To do this we will first show that $I(G_1(p, k) \times G(Z), C_1) = 0$. Next we will show that if $j \neq 1$, then $I(G_2(p, k) \times G(Z_j), C_1) = 0$. Finally, we will show that $I(G_2(p, k) \times G(Z_1), C_1) = S(Z_1)$. It will follow that

$$I(G(p, k) \times G(Z), C_1) = I((G_1(p, k) \cup G_2(p, k)) \times G(Z), C_1) \quad (36)$$

$$= I((G_1(p, k) \times G(Z)) \cup (G_2(p, k) \times G(Z)), C_1) \quad (37)$$

$$= I((G_1(p, k) \times G(Z)) \cup (G_2(p, k) \times \bigcup_{i=1}^l G(Z_i)), C_1) \quad (38)$$

$$= I((G_1(p, k) \times G(Z)) \cup (\bigcup_{i=1}^l (G_2(p, k) \times G(Z_i))), C_1) \quad (39)$$

$$= I(G_1(p, k) \times G(Z), C_1) + \sum_{i=1}^l I(G_2(p, k) \times G(Z_i), C_1) \quad (40)$$

$$= S(Z_1), \text{ as desired.} \quad (41)$$

Claim (1.c.i). $I(G_1(p, k) \times G(Z), C_1) = 0$.

Let $c = (c_1, c_2)$ be a cycle vertex in $G_1(p, k) \times G(Z)$. We know by Theorem 2.1 that c_1 is a cycle vertex in $G_1(p, k)$ and c_2 is a cycle vertex in $G(Z)$. By our definition of Z , $M(Z) = s$. This implies that every cycle vertex in $G(Z)$, including the cycle vertices in C_1 , has indegree s . Hence, $N(q_1 q_2 \dots q_m, k, c_2) = s$. Also, since $c_1 \in G_1(p, k)$, we know by Lemma 3.3 that $N(p, k, c_1)$ is $\gcd(p-1, k)$ or 0. Since c_1 is a cycle, it must have indegree of at least 1, implying that $N(p, k, c_1) = \gcd(p-1, k)$. We know by Lemma 3.9 that

$$N(n, k, c) = N(p, k, c_1) \cdot N(q_1 q_2 \dots q_m, k, c_2) \quad (42)$$

$$= \gcd(p-1, k) \cdot s. \quad (43)$$

By our assumption, $\gcd(p-1, k) \neq 1$, implying that $N(n, k, c) \neq s$. However, the cycle vertices in C_1 have indegree s . Therefore the component containing c is not isomorphic to C_1 . Since c is an arbitrary cycle vertex, we know that no component in $G_1(p, k) \times G(Z)$ is isomorphic to C_1 , or $I(G_1(p, k) \times G(Z), C_1) = 0$.

Claim (1.c.ii). $I(G_2(p, k) \times G(Z_j), C_1) = 0$, where $j \neq 1$.

The only vertex in $G_2(p, k)$ is 0, implying that $G_2(p, k) \times G(Z_j) \cong G(Z_j)$. Therefore, if C is a component in $G_2(p, k) \times G(Z_j)$, then C is isomorphic to a component in $G(Z_j)$. However, since Z_j and Z_1 are different equivalence classes, we know that no component in $G(Z_j)$ is isomorphic to any component in $G(Z_1)$. It follows that C is not isomorphic to any component in $G(Z_1)$. Since C_1 is a component in $G(Z_1)$, we can conclude that C is not isomorphic to C_1 . Because C is an arbitrary component in $G_2(p, k) \times G(Z_j)$, we can conclude that $I(G_2(p, k) \times G(Z_j), C_1) = 0$, when $j \neq 1$.

Claim (1.c.iii). $I(G_2(p, k) \times G(Z_1), C_1) = S(Z_1)$.

It remains to show that $G_2(p, k) \times G(Z_1)$ consists of $S(Z_1)$ components isomorphic to C_1 . We know that $G_2(p, k)$ consists entirely of a single fixed point, implying $G_2(p, k) \times G(Z_1) \cong G(Z_1)$. Since $G(Z_1)$ consists of $S(Z_1)$ components isomorphic to C_1 , it follows that $G_2(p, k) \times G(Z_1)$ also consists of exactly $S(Z_1)$ components isomorphic to C_1 .

Claim (2). *If condition i is satisfied but condition ii is not, then $G(n, k)$ is not symmetric of order p .*

We will first assume that T is empty and that $\gcd(p-1, k) = 1$. Under these conditions, we will conclude that $G(n, k)$ is not symmetric of order p . Then we will assume $\gcd(p-1, k) = 1$ and that T is nonempty. Additionally, we will assume that there exists an $x \in \mathbb{N}$ such that $p \nmid A_x(G(T, k))$ and $\text{ord}_{p-1} k \nmid x$. We will then arrive at the conclusion that $G(n, k)$ is not symmetric of order p . It will follow that if condition i is satisfied and condition ii is not satisfied, then $G(n, k)$ is not symmetric of order p .

Claim (2.a). *If T is empty and $\gcd(p-1, k) = 1$, then $G(n, k)$ is not symmetric of order p .*

Since T is empty, we know that $\gcd(q_i - 1, k) \neq 1$, for all i , because otherwise q_i would be an element in T . We also know that

$$G(n, k) \cong G(p, k) \times G(q_1, k) \times G(q_2, k) \times \dots \times G(q_m, k).$$

Thus, each vertex $a \in G(n, k)$ corresponds to the $m+1$ -tuple, $(b_1, b_2, \dots, b_{m+1})$. By Lemma 3.11, we know that the only vertices in $G(n, k)$ with indegree 1 are the set of vertices L , corresponding to $m+1$ -tuples of the form $(b_1, 0, 0, \dots, 0)$. Note that the subgraph of $G(n, k)$ containing the vertices L is isomorphic to $G(p, k)$, and $G(p, k)$ is not symmetric of order p . It follows that the subgraph of $G(n, k)$ containing vertices with indegree 1 is not symmetric of order p , implying that $G(n, k)$ is not symmetric of order p .

Claim (2.b). *Suppose T is not empty and $\gcd(p-1, k) = 1$. Also suppose that there exists $x \in \mathbb{N}$ such that $p \nmid A_x(G(q_{a_1}q_{a_2}\dots q_{a_j}, k))$ and $\text{ord}_{p-1} k \nmid x$. Then $G(n, k)$ is not symmetric of order p .*

Let $R = \{q_{d_1}, q_{d_2}, \dots, q_{d_l}\}$ be $Q - T$. Note that if $q \in R$, then $\gcd(q-1, k) \neq 1$. We know that

$$G(n, k) \cong G(p, k) \times G(q_{a_1}, k) \times G(q_{a_2}, k) \times \dots \times G(q_{a_j}, k) \times G(q_{d_1}, k) \times G(q_{d_2}, k) \times \dots \times G(q_{d_l}, k).$$

By Lemma 3.11, we know that the only vertices in $G(n, k)$ with indegree 1 are vertices of the form $(b_1, b_2, \dots, b_{j+1}, 0, 0, \dots, 0)$. Thus the vertices with indegree 1 form a subgraph of $G(n, k)$ isomorphic to $G(pq_{a_1}q_{a_2}\dots q_{a_j}, k)$. Since there exists $x \in \mathbb{N}$ such that $p \nmid A_x(G(q_{a_1}q_{a_2}\dots q_{a_j}, k))$ and $\text{ord}_{p-1} k \nmid x$ we know by Theorem 3.11 that $G(pq_{a_1}q_{a_2}\dots q_{a_j}, k)$ is not symmetric of order p . It follows that the subgraph of $G(n, k)$ containing vertices with indegree 1 is not symmetric of order p , implying that $G(n, k)$ is not symmetric of order p .

\Leftarrow We must now show that if both conditions are satisfied, $G(n, k)$ is symmetric of order p . Let $R = \{q_{d_1}, q_{d_2}, \dots, q_{d_l}\}$ be $Q - T$. We know that

$$G(n, k) \cong G(pq_{a_1}q_{a_2}\dots q_{a_j}, k) \times G(q_{d_1}q_{d_2}\dots q_{d_l}, k).$$

We know that $\gcd(p-1, k) = 1$ and $\gcd(q_{a_i} - 1, k)$ for all i , by our assumption. Additionally, by our assumption we know that for all $x \in \mathbb{N}$ such that $p \nmid A_x(G(q_{a_1}q_{a_2}\dots q_{a_j}, k))$, $\text{ord}_{p-1} k \nmid x$. It follows from Theorem 3.9 that $G(pq_{a_1}q_{a_2}\dots q_{a_j}, k)$ is symmetric of order p . Since $G(pq_{a_1}q_{a_2}\dots q_{a_j}, k)$ is symmetric of order p and since $G(n, k) \cong G(pq_{a_1}q_{a_2}\dots q_{a_j}, k) \times G(q_{d_1}q_{d_2}\dots q_{d_l}, k)$, we know by Theorem 3.8 that $G(n, k)$ is symmetric of order p .

□

4 Some Results on $G_1(n, k)$

We will now generalize some of the results discovered by Wilson in [3]. To do this, we must first prove a natural connection between $G_1(n, k)$ and the functional graph formed by scalar multiplication by k over a finite abelian group. We will now define some notation that will be used throughout the remainder of this section.

If $H = \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \dots \times \mathbb{Z}_{a_m}$, let $f_k : H \rightarrow H$ be the function such that if $h = (h_1, h_2, \dots, h_m)$ is an element in H , then $f_k(h) = (kh_1, kh_2, \dots, kh_m)$. Also, we let $F(H, k)$ denote the functional graph formed by f_k on H .

We will use n as an odd natural number whose prime factorization is $p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$. We define u and v to be natural numbers such that $\lambda(n) = uv$, where v is the largest divisor of $\lambda(n)$ relatively prime to k . Also, let $\lambda(p_i^{e_i}) = u_i v_i$, where v_i is the largest divisor of $\lambda(p_i^{e_i})$ relatively prime to k , for all i . Note that $\gcd(v, u) = 1$ and $\gcd(v_i, u_i) = 1$, for all i .

Theorem 4.1. *Let $H = \mathbb{Z}_{p_1^{e_1-1}(p_1-1)} \times \mathbb{Z}_{p_2^{e_2-1}(p_2-1)} \times \dots \times \mathbb{Z}_{p_m^{e_m-1}(p_m-1)}$. Then $F(H, k) \cong G_1(n, k)$.*

Proof. We know that $G_1(n, k) \cong G_1(p_1^{e_1}, k) \times G_1(p_2^{e_2}, k) \times \dots \times G_1(p_m^{e_m}, k)$, so it suffices to prove that $A = G_1(p_1^{e_1}, k) \times G_1(p_2^{e_2}, k) \times \dots \times G_1(p_m^{e_m}, k)$ is isomorphic to $F(H, k)$. Let g_1, g_2, \dots, g_m be primitive roots in $\mathbb{Z}_{p_1}^*, \mathbb{Z}_{p_2}^*, \dots, \mathbb{Z}_{p_m}^*$, respectively. Suppose $a = (a_1, a_2, \dots, a_m)$ is in A . Since g_i is a primitive root modulo $p_i^{e_i}$, there exists a unique d_i between 0 and $p_i^{e_i-1}(p_i-1) - 1$ such that $g_i^{d_i} \equiv a_i \pmod{p_i^{e_i}}$. Define $\gamma : A \rightarrow H$ such that $\gamma(a) = (d_1, d_2, \dots, d_m)$. Note that d_i is between 0 and $p_i^{e_i-1}(p_i-1) - 1$, so $d_i \in \mathbb{Z}_{p_i^{e_i-1}(p_i-1)}$. Next, define $\gamma^{-1} : H \rightarrow A$ such that if $d = (d_1, d_2, \dots, d_m)$, then $\gamma^{-1}(d) = (g_1^{d_1}, g_2^{d_2}, \dots, g_m^{d_m})$. It's evident that γ and γ^{-1} are inverses, implying that γ describes a bijection from A to H . Thus, it remains to show that γ and γ^{-1} preserves edges.

Let $a = (g_1^{d_1}, g_2^{d_2}, \dots, g_m^{d_m})$ be a vertex in A . We know that a has exactly one outgoing edge, which leads to $a^k = (g_1^{kd_1}, g_2^{kd_2}, \dots, g_m^{kd_m})$. It follows that $\gamma(a) = (d_1, d_2, \dots, d_m)$ and $\gamma(a^k) = (kd_1, kd_2, \dots, kd_m)$. Since H has an edge from (d_1, d_2, \dots, d_m) to $(kd_1, kd_2, \dots, kd_m)$, we know that γ preserves edges.

Let $d = (d_1, d_2, \dots, d_m)$ be a vertex in A . We know that d has exactly one outgoing edge, which leads to $(kd_1, kd_2, \dots, kd_m)$. We see that $\gamma^{-1}(d) = (g_1^{d_1}, g_2^{d_2}, \dots, g_m^{d_m})$ and $\gamma^{-1}(kd) = (g_1^{kd_1}, g_2^{kd_2}, \dots, g_m^{kd_m})$. Since A has an edge from $(g_1^{d_1}, g_2^{d_2}, \dots, g_m^{d_m})$ to $(g_1^{kd_1}, g_2^{kd_2}, \dots, g_m^{kd_m})$, we know that γ^{-1} preserves edges, verifying our claim. □

This next result provides us with an easier way to compute v_i and u_i .

Theorem 4.2. $\gcd(\lambda(p_i^{e_i}), v) = v_i$ and $\gcd(\lambda(p_i^{e_i}), u) = u_i$.

Proof. Since $\lambda(p_i^{e_i}) | \lambda(n)$, and v is the largest divisor of $\lambda(n)$ relatively prime to k , it is evident that $v_i | v$. Also since $(v, k) = 1$ and since every prime divisor of u_i is also a divisor of k , we can conclude that $\gcd(u_i, v) = 1$. This implies $\gcd(\lambda(p_i^{e_i}), v) = v_i$. Because $\lambda(p_i^{e_i}) | \lambda(n)$, we know that $\gcd(\lambda(p_i^{e_i}), \lambda(n)) = \lambda(p_i^{e_i}) = u_i v_i$. Since $\gcd(u, v) = 1$, we find

$$\gcd(\lambda(p_i^{e_i}), \lambda(n)) = u_i v_i \tag{44}$$

$$\gcd(\lambda(p_i^{e_i}), u) \gcd(\lambda(p_i^{e_i}), v) = u_i v_i \tag{45}$$

$$\gcd(\lambda(p_i^{e_i}), u) v_i = u_i v_i \tag{46}$$

$$\gcd(\lambda(p_i^{e_i}), u) = u_i. \tag{47}$$

□

Before we prove our first main result, we need a definition. We denote the subgraph of $G_1(n, K)$ containing precisely the cycles of $G_1(n, k)$ by $G_c(n, k)$.

Theorem 4.3. *Let $H = \mathbb{Z}_{v_1} \times \mathbb{Z}_{v_2} \times \dots \times \mathbb{Z}_{v_m}$. Then $F(H, k) \cong G_c(n, k)$.*

Proof. Let $H_1 = \mathbb{Z}_{p_1^{e_1-1}(p_1-1)} \times \mathbb{Z}_{p_2^{e_2-1}(p_2-1)} \times \dots \times \mathbb{Z}_{p_m^{e_m-1}(p_m-1)}$. We know that that $G_1(n, k)$ is isomorphic to $F(H_1, k)$, by Theorem 4.1. We also know that

$$H_1 \cong (\mathbb{Z}_{u_1} \times \mathbb{Z}_{v_1}) \times (\mathbb{Z}_{u_2} \times \mathbb{Z}_{v_2}) \times \dots \times (\mathbb{Z}_{u_m} \times \mathbb{Z}_{v_m}),$$

because $\gcd(u_i, v_i) = 1$ and $\lambda(p_i^{e_i}) = u_i v_i$, for all i . Let

$$H_2 = (\mathbb{Z}_{u_1} \times \mathbb{Z}_{v_1}) \times (\mathbb{Z}_{u_2} \times \mathbb{Z}_{v_2}) \times \dots \times (\mathbb{Z}_{u_m} \times \mathbb{Z}_{v_m}).$$

We then see that that $F(H_2, k) \cong G_1(n, k)$. We will now show that $h \in H_2$ is a cyclic node in $F(H_2, k)$ if and only if h is of the form $((0, h_1), (0, h_2), \dots, (0, h_m))$. Since the subgroup of H_2 whose elements are of the form $((0, h_1), (0, h_2), \dots, (0, h_m))$ is isomorphic to

$$\mathbb{Z}_{v_1} \times \mathbb{Z}_{v_2} \times \dots \times \mathbb{Z}_{v_m},$$

our claim will be satisfied.

Suppose $h \in H_2$ is of the form $((0, h_1), (0, h_2), \dots, (0, h_m))$. Since $\gcd(k, v_i) = 1$, there exists an positive integer y_i , such that $k^{y_i} \equiv 1 \pmod{v_i}$, for each i . Let $y = \text{lcm}[y_1, y_2, \dots, y_m]$. It follows that

$$f^y(h) = ((0, k^y h_1), (0, k^y h_2), \dots, (0, k^y h_m)) \quad (48)$$

$$= ((0, h_1), (0, h_2), \dots, (0, h_m)) \quad (49)$$

$$= h. \quad (50)$$

Therefore h is a cycle vertex in $F(H_2, k)$.

Next, suppose $h' \in H_2$ is not of the form $((0, h_1), (0, h_2), \dots, (0, h_m))$. That is, h' is of the form $((h'_1, h_1), (h'_2, h_2), \dots, (h'_m, h_m))$, where $h'_i \neq 0$, for at least one value of i . Suppose $h'_j \neq 0$. Since every prime divisor of u_j is also a divisor of k , there exists an integer a_j such that $u_j | k^{a_j}$. This implies that for any integer $a = a_j + b$, where $b \in \mathbb{N}$,

$$f^a(h') = ((k^a h'_1, k^a h_1), (k^a h'_2, k^a h_2), \dots, (k^a h'_j, k^a h_j), \dots, (k^a h'_m, k^a h_m)) \quad (51)$$

$$= ((k^a h'_1, k^a h_1), (k^a h'_2, k^a h_2), \dots, (k^{a_j+b} h'_j, k^a h_j), \dots, (k^a h'_m, k^a h_m)) \quad (52)$$

$$= ((k^a h'_1, k^a h_1), (k^a h'_2, k^a h_2), \dots, (k^{a_j} k^b h'_j, k^a h_j), \dots, (k^a h'_m, k^a h_m)) \quad (53)$$

$$= ((k^a h'_1, k^a h_1), (k^a h'_2, k^a h_2), \dots, (0, k^a h_j), \dots, (k^a h'_m, k^a h_m)) \quad (54)$$

$$\neq h'. \quad (55)$$

We know that if h' were a cycle vertex, there would exist $s \in \mathbb{N}$ such that $f^s(h') = h'$. Additionally, for all $r \in \mathbb{N}$, $f^{rs}(h') = h'$. Let x denote a multiple of s that is greater than a . If h' is a cycle vertex, then $f^x(h') = h'$. However, from the previous equation, we know that $f^x(h') \neq h'$. It follows that h' is not a cycle vertex.

□

The following corollaries were originally proven, for both odd and even numbers, in [3] using elementary number theory techniques.

Corollary 4.4. *There are $\prod_{i=1}^m \gcd(v, \lambda(p_i^{e_i}))$ cycle vertices in $G_1(n, k)$.*

Proof. This result follows from Theorem 4.3 and because $\gcd(v, \lambda(p_i^{e_i})) = v_i$. □

Corollary 4.5. *The longest cycle in $G(n, k)$ is $\text{ord}_v k$.*

Our next theorem will provide a similar result regarding vertices in $G_1(n, k)$ that are not cycle vertices. But first, we need two quick lemmas.

Lemma 4.6. *Let C be a cycle in $G(n, k)$ and let c be a vertex in C . Let f denote the mapping $f(x) \equiv x^k \pmod{n}$. For any $y \in \mathbb{N}$, there exists a vertex $d \in C$, such that $f^y(d) = c$. Furthermore, d is the only vertex in C that satisfies this property.*

Proof. We know that there exists $r, s \in \mathbb{N}$ such that $0 \leq s < L(C)$ and $y = L(C)r + s$. Let $d = f^{L(C)-s}(c)$. Note that since c is a cycle vertex in C , d is also a cycle vertex in C . It follows that

$$f^y(d) = f^y(f^{L(C)-s}(c)) \tag{56}$$

$$= f^{y+L(C)-s}(c) \tag{57}$$

$$= c. \tag{58}$$

Now we will prove that d is unique. Suppose there is a vertex d' in C such that $f^y(d') = c$. Let t be a natural number such that $tL(C) \geq y$. We see that

$$d' = f^{tL(C)}(d') \tag{59}$$

$$= f^{tL(C)-y}(c) \tag{60}$$

$$= f^{tL(C)-y}(f^y(d)) \tag{61}$$

$$= f^{tL(C)}(d) \tag{62}$$

$$= d. \tag{63}$$

□

Lemma 4.7. *Let $H = \mathbb{Z}_{u_1} \times \mathbb{Z}_{u_2} \times \dots \times \mathbb{Z}_{u_m}$. Let $h = (h_1, h_2, \dots, h_m)$ be an element in H . There exists $t \in \mathbb{N}$ such that $f_k^t(h) = (0, 0, \dots, 0)$.*

Proof. By our definition of u_i , if $p|u_i$, then $p|k$, for all i . This implies that there exists t_i such that $u_i|k^{t_i}$, for all i . Let $t = \max(t_1, t_2, \dots, t_m)$. It follows that

$$f_k^t(h) = (k^t h_1, k^t h_2, \dots, k^t h_m) \tag{64}$$

$$= (0, 0, \dots, 0), \text{ as desired.} \tag{65}$$

□

We let $T(n, k, a)$ denote the tree connected to the vertex a in the graph $G(n, k)$, where a has no outgoing edge. We now have the machinery needed to prove our second main theorem on $G_1(n, k)$.

Theorem 4.8. *Let*

$$H = \mathbb{Z}_{u_1} \times \mathbb{Z}_{u_2} \times \dots \times \mathbb{Z}_{u_m}.$$

Let A be $F(H, k)$ with the edge from $(0, 0, \dots, 0)$ to itself removed. If c is any cycle node in $G_1(n, k)$, then $T(n, k, c) \cong A$.

Proof. Let $H_1 = (\mathbb{Z}_{u_1} \times \mathbb{Z}_{v_1}) \times (\mathbb{Z}_{u_2} \times \mathbb{Z}_{v_2}) \times \dots \times (\mathbb{Z}_{u_m} \times \mathbb{Z}_{v_m})$. Recall from the proof of Theorem 4.3 that $G_1(n, k) \cong F(H_1, k)$. Thus, any node, a corresponds to an element $((a_1, b_1), (a_2, b_2), \dots, (a_m, b_m))$. Let c be a cycle vertex. We know c corresponds to $((0, c_1), (0, c_2), \dots, (0, c_m))$ by Theorem 4.3. Let C denote the cycle containing a . Define $\gamma : T(n, k, c) \rightarrow H$ as follows

$$\gamma(((a_1, b_1), (a_2, b_2), \dots, (a_m, b_m))) = (a_1, a_2, \dots, a_m).$$

Next, we will define $\gamma^{-1} : H \rightarrow T(n, k, c)$. If $b \in H$, to compute $\gamma^{-1}((a_1, a_2, \dots, a_m))$, we let t be the smallest integer such that $(k^t a_1, k^t a_2, \dots, k^t a_m) = (0, 0, \dots, 0)$. We know that t exists by Lemma 4.7. We let $d = ((0, d_1), (0, d_2), \dots, (0, d_m))$ be the unique vertex in C satisfying $f^t(d) = c$. We know that d exists and is unique by Lemma 4.6. Then $\gamma^{-1}((a_1, a_2, \dots, a_m)) = ((a_1, d_1), (a_2, d_2), \dots, (a_m, d_m))$.

We will now show that γ^{-1} is the inverse of γ , confirming that γ is a bijection. First we see

$$\gamma(\gamma^{-1}((a_1, a_2, \dots, a_m))) = \gamma(((a_1, d_1), (a_2, d_2), \dots, (a_m, d_m))) \quad (66)$$

$$= (a_1, a_2, \dots, a_m). \quad (67)$$

Let $a = ((a_1, b_1), (a_2, b_2), \dots, (a_m, b_m))$ be a vertex in $T(n, k, c)$. We will evaluate

$$\gamma^{-1}(\gamma(((a_1, b_1), (a_2, b_2), \dots, (a_m, b_m))))).$$

First we must show that if we let t' be the smallest natural number such that $(k^{t'} a_1, k^{t'} a_2, \dots, k^{t'} a_m) = (0, 0, \dots, 0)$, then $b = ((0, b_1), (0, b_2), \dots, (0, b_m))$ is the unique vertex in C satisfying $f^{t'}(b) = c$. Since $f^{t'}(a) = c$, we know

$$f_k^{t'}(a) = ((k^{t'} a_1, k^{t'} b_1), (k^{t'} a_2, k^{t'} b_2), \dots, (k^{t'} a_m, k^{t'} b_m)) \quad (68)$$

$$= ((0, c_1), (0, c_2), \dots, (0, c_m)). \quad (69)$$

This means that $k^{t'} b_i \equiv c_i \pmod{v_i}$, for each i . Thus,

$$f^{t'}(b) = ((0, k^{t'} b_1), (0, k^{t'} b_2), \dots, (0, k^{t'} b_m)) \quad (70)$$

$$= ((0, c_1), (0, c_2), \dots, (0, c_m)). \quad (71)$$

It follows that $b = ((0, b_1), (0, b_2), \dots, (0, b_m))$ is the unique vertex in C satisfying $f^{t'}(b) = c$. We then find that

$$\gamma^{-1}(\gamma(((a_1, b_1), (a_2, b_2), \dots, (a_m, b_m)))) = \gamma^{-1}((a_1, a_2, \dots, a_m)) \quad (72)$$

$$= ((a_1, b_1), (a_2, b_2), \dots, (a_m, b_m)). \quad (73)$$

Therefore γ is a bijection.

It remains to show that γ and γ^{-1} preserve edges. Let $((a_1, b_1), (a_2, b_2), \dots, (a_m, b_m))$ be a vertex in C . Then there is an edge from $((a_1, b_1), (a_2, b_2), \dots, (a_m, b_m))$ to $((ka_1, kb_1), (ka_2, kb_2), \dots, (ka_m, kb_m))$. We see that

$$\gamma(((a_1, b_1), (a_2, b_2), \dots, (a_m, b_m))) = (a_1, a_2, \dots, a_m), \text{ and} \quad (74)$$

$$\gamma(((ka_1, kb_1), (ka_2, kb_2), \dots, (ka_m, kb_m))) = (ka_1, ka_2, \dots, ka_m). \quad (75)$$

Since $F(H, k)$ has an edge from (a_1, a_2, \dots, a_m) to $(ka_1, ka_2, \dots, ka_m)$, γ preserves edges. Letting (a_1, a_2, \dots, a_m) be a vertex in $F(H, k)$, we know that $F(H, k)$ has a edge from (a_1, a_2, \dots, a_m) to $(ka_1, ka_2, \dots, ka_m)$. It evident that

$$\gamma^{-1}((a_1, a_2, \dots, a_m)) = ((a_1, b_1), (a_2, b_2), \dots, (a_m, b_m)).$$

We will show that $\gamma^{-1}((ka_1, ka_2, \dots, ka_m)) = ((ka_1, kb_1), (ka_2, kb_2), \dots, (ka_m, kb_m))$. Since $F(H_2, k)$ has an edge from $((a_1, b_1), (a_2, b_2), \dots, (a_m, b_m))$ to $((ka_1, kb_1), (ka_2, kb_2), \dots, (ka_m, kb_m))$, it will follow that γ^{-1} also preserves edge.

Let t be the least positive integer such that $(k^t a_1, k^t a_2, \dots, k^t a_m) = (0, 0, \dots, 0)$. By Equations (68)- (71), $b = ((0, b_1), (0, b_2), \dots, (0, b_m))$ is the unique vertex in C satisfying $f^t(b) = c$. It is evident that $t-1$ is the least positive integer such that $(k^{t-1}ka_1, k^{t-1}ka_2, \dots, k^{t-1}ka_m) = (0, 0, \dots, 0)$. We see that

$$c = f^t(((0, b_1), (0, b_2), \dots, (0, b_m))) \tag{76}$$

$$= f^{t-1}(((0, kb_1), (0, kb_2), \dots, (0, kb_m))). \tag{77}$$

This implies that $b' = ((0, kb_1), (0, kb_2), \dots, (0, kb_m))$ is the unique vertex in C satisfying $f^{t-1}(b') = c$. It follows that $\gamma^{-1}((ka_1, ka_2, \dots, ka_m)) = ((ka_1, kb_1), (ka_2, kb_2), \dots, (ka_m, kb_m))$, as desired. \square

This corollary was originally proved in [3] using elementary number theory.

Corollary 4.9. *Let c_1 and c_2 be cycle vertices in $G_1(n, k)$. Then $T(n, k, c_1) \cong T(n, k, c_2)$.*

5 Conclusion

The graphs $G(n, k)$ and $G_1(n, k)$ are rich with many fascinating properties, many of which remain unexplored. They not only provide us with an interesting class of graphs to study, but also shed light on the nature of discrete exponentiation. In this paper, we have explored the conditions in which symmetry occurs; specifically when our modulus is odd and square free. However, the case when our modulus is not square free and odd is largely still open to investigation. We have also discovered a useful connection between $G_1(n, k)$ and the theory of finite abelian groups. This connection opens up possibilities to find properties of $G_1(n, k)$ using group theory.

References

- [1] Lawrence Somer and Michal Křížek. On symmetric digraphs of the congruence $x^k \equiv y \pmod{n}$. *Discrete Mathematics*, 309:1999–2009, 2009.
- [2] Lawrence Somer, Florian Luca, and Michal Křížek. *17 Lectures on Fermat Numbers: From Number Theory to Geometry*. Springer-Verlag, New York, 2001.
- [3] Brad Wilson. Power digraphs modulo n . *The Fibonacci Quarterly*, 36:229–239, 1996.