Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 6(5): 4581–4596.
DOI: 10.3934/math.2021270
Received: 05 November 2020
Accepted: 08 February 2021
Published: 22 February 2021

Research article

Structures of power digraphs over the congruence equation $x^p \equiv y \pmod{m}$ and enumerations

M. Haris Mateen[1,*], **Muhammad Khalid Mahmmod**[1], **Dilshad Alghazzawi**[2] **and Jia-Bao Liu**[3]

[1] Department of Mathematics, University of the Punjab, Lahore 54590, Pakistan
[2] Department of Mathematics, King Abdulaziz University, Rabigh 21589, Saudi Arabia
[3] Department of Mathematics, School of Mathematics and Physics, Anhui Jianzhu University, Hefei 230601, China

* **Correspondence:** Email: harism.math@gmail.com; Tel: +923466118150.

Abstract: In this work, we incorporate modular arithmetic and discuss a special class of graphs based on power functions in a given modulus, called power digraphs. In power digraphs, the study of cyclic structures and enumeration of components is a difficult task. In this manuscript, we attempt to solve the problem for pth power congruences over different classes of residues, where p is an odd prime. For any positive integer m, we build a digraph $G(p, m)$ whose vertex set is $\mathbb{Z}_m = \{0, 1, 2, 3, ..., m - 1\}$ and there will be a directed edge from vertices $u \in \mathbb{Z}_m$ to $v \in \mathbb{Z}_m$ if and only if $u^p \equiv v \pmod{m}$. We study the structures of $G(p, m)$. For the classes of numbers 2^r and p^r where $r \in \mathbb{Z}^+$, we classify cyclic vertices and enumerate components of $G(p, m)$. Additionally, we investigate two induced subdigraphs of $G(p, m)$ whose vertices are coprime to m and not coprime to m, respectively. Finally, we characterize regularity and semiregularity of $G(p, m)$ and establish some necessary conditions for cyclicity of $G(p, m)$.

Keywords: cycles; components; power digraphs; congruence equation
Mathematics Subject Classification: 05C25, 11E04, 20G15

1. Introduction

In fields such as data structures, computer algorithms, data encryption, security, and networking, computer science relies heavily on graph theory. For instance, designs of a database, routing problems, and networking based on the key ideas of graph theory, namely cycles and trees. Many computer security algorithms and ciphers are similarly based on modular arithmetic from number theory. In these areas, a strong mathematical background and a clear understanding of modular arithmetic, graph theory and algorithms needs to be developed to enjoy the subject. Computer software or a program without adequate knowledge of mathematics is often difficult to understand. The entire structure of an algorithm can be understood through a flow chart or its graph (or digraph). Graphs (or digraphs) are thus much more useful for a better understanding of structurally dependent algorithms and/or outputs. Digraphs based on congruence equations are a primary interest in the field of discrete mathematics for number theorists and computer scientists. Power digraphs have a broad range of applications that are easily recognizable in almost every field and presented with the basic properties of integers. For instance, if a typical power digraph is described and its loops are discovered. Then, instead of ordinary integers, one can consider these vertices (that is, loops) in forming a new cipher. Obviously, it would be difficult to decode this type of cipher unless one knows the correct mapping and its reverse mapping (if possible). In fact, a typical corresponding congruence must be solved to decode such a produced cipher. The problem of factorization in computer science is a very difficult problem for large integers. For such an integer, a digraph which assigns a component to its divisor can always be described. The divisor number can therefore be enumerated as the number of components that are non-isomorphic. The required integer may therefore be written canonically. Let's define our power digraph before proceeding further.

Let $m > 0$ be any integer and $\overline{r}$ denotes the set of all integers which leave remainder r under modulo m, also referred as a residue class of m. Thus, $\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \ldots,\ \overline{m-1}\}$ is the set of all residue classes of m. This set is called a complete residue system (CRS). We construct a digraph $G(p, m)$ on this set of complete residue classes of m and build a directed edge from u to v if and only if $u^p \equiv v \pmod{m}$. The vertices $u_1, u_2, ..., u_s$ will form a cycle of length s if

$$\begin{aligned} u_1^p &\equiv u_2 \pmod{m}, \\ u_2^p &\equiv u_3 \pmod{m}, \\ &\vdots \\ u_s^p &\equiv u_1 \pmod{m}. \end{aligned} \tag{1.1}$$

The indegree of a vertex a is the count of edges incident with it and the number of edges leaving from a vertex a is called outdegree of a. The indegree and outdegree are labeled as $indeg(a)$ and $outdeg(a)$, respectively. The cycles of length one are called fixed points of the map $f(u) = u^p$ and cycles of length q are called q-cycles. A maximal connected simple subgraph of the corresponding digraph $G(p, m)$ is termed as a component. Since every integer lies in a unique residue class of m, so its outdegree must be one.

If indegrees and outdegrees of all vertices are the same then the corresponding digraph is called a regular digraph. In this case, a digraph is regular if the indegree of every vertex is one (since the outdegree of each vertex is already one). If the indegrees of all vertices are either a positive integer d or 0, we then call it a semiregular digraph. Let $G_1(p, m)$ and $G_2(p, m)$ denote the subdigraphs induced by the proposed digraph $G(p, m)$ over the set of vertices which are either coprime to m or not, respectively. Note that the digraphs $G_1(p, m)$ and $G_2(p, m)$ are disjoint and their union is $G(p, m)$. The digraph $G(11, 17)$ is depicted in Figure 1.

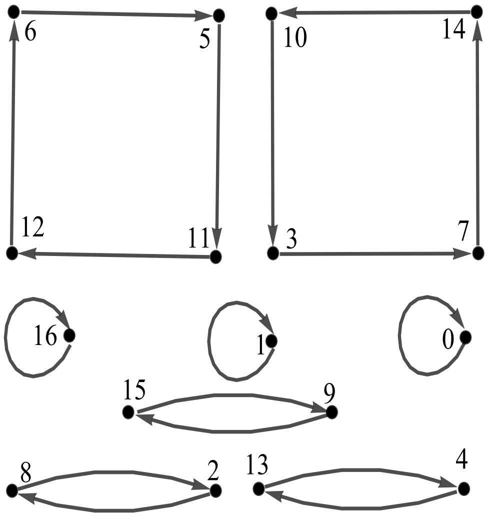


Figure 1. The digraph $G(11, 17)$.

Power digraphs have been of great interest for the last few decades. In 1967, Bryant [1] employed quadratic digraphs and enumerated isomorphic subgroups of a finite group. Szalay [2] investigated some interesting properties of power digraphs based on congruences and established the existence of cycles in components. In 1996, Rogers [3] and Somer et al. [4] investigated the structures of quadratic maps and explored a few results on fixed points, existence of cycles and few decomposition of components. Mahmood and Ahmad [5] established many results for k-array digraphs and completely described an enumeration of squares of 2^k using modular arithmetic for any intger k. Aslam and Mahmood introduced and investigated simple graphs over exponential congruences and characterized all cycles and components completely in [6]. Yangjiang et al. [7] and Somer et al. [8] introduced and investigated the symmetric structures (isomorphic components) of such digraphs. For a fixed k, many useful results on loops, cycles, components and symmetry of power digraphs for the congruence equation $x^k \equiv y \pmod{m}$ have been proposed and proved in [9–13]. Akbari [14] established a relation between edge chromatic number of $G(R)$ with the maximum degree of $G(R)$, where $G(R)$ denotes the zero-divisor graph over of a finite commutative ring R. Wei et al. and Rezaei et al. [15–17] discussed graphs based on quadratic and cubic congruences over finite integral rings. Carlip and Mincheva [18] defined an M-ordered symmetric digraph of G based on M-size subsets, each containing M-isomorphic components. Deng and Yuan [19] investigated symmetric digraphs for a fixed power modulo n. Meemark and Wiroonsri [20, 21] discussed the structure of $G(R, k)$, where R is the quotient ring of polynomials over finite fields and k is the modulus. Mahmood and Ali [22, 23, 29] investigated new numbers on euler totient, super euler function and labeling algorithm on several classes of graphs with application . Alolaiyan et al. [24] studied non-conjugate graphs associated with finite groups. Portilla et al. [25] generalize the classical definition of Gromov hyperbolicity to the context of directed graphs. It is worth mentioning that the problem of enumeration of components of power digraphs is still open. In fact, previously all structures have been established for a fixed power k. In this piece of work, we generalize the structures of these digraphs when power is an odd prime p. That is, we incorporate the congruence, $x^k \equiv y \pmod{m}$.

We organize our paper as follows. In Section 1, we introduce our digraph with some important definitions and also provide some new results on fixed points. In Section 2, we prove some results that enumerate cyclic vertices as well as the existence of a t-cycle in $G(p,m)$. Then, we define two subdigraphs $G_1(p,m)$ and $G_2(p,m)$. Then after, we elaborate cyclic structures and enumerate components of these subdigraphs for $m = 2^r$ and $m = p^r$ for all positive integers r. Finally, we prove that the digraph $G_1(p,m)$ consists of $p-1$ isomorphic trees where as $G_2(p,m)$ is a tree with root at 0 with indeg(0) $= p^{k-\lceil \frac{k}{p} \rceil}$. In Section 3, we characterize regularity and semiregularity of $G_1(p,m)$. We need the following definitions for use in sequel.

Definition 1.1. *[26] Euler totient function counts the positive integers up to a given integer m that are relatively prime to m. It is written using the Greek letter phi as $\phi(m)$, also called Euler phi function.*

Definition 1.2. *[26] Let $m > 0$ be any integer. For a prime p, the Carmichael λ-function (or $\lambda(m)$) is defined as follows: $\lambda(1) = 1 = \phi(1)$, $\lambda(2) = 1 = \phi(2)$, $\lambda(4) = 2 = \phi(4)$, $\lambda(2^k) = \frac{1}{2}\,\phi(2^k)$, $k \geq 3$, and $\lambda(p^k) = \phi(p^k)$, $k \geq 1$.*

Theorem 1.3. *[27] (Carmichael). Let $a, m \in \mathbb{N}$. Then $a^{\lambda(m)} \equiv 1 \pmod{m}$ if and only if $gcd(a,m) = 1$. Here, $gcd(a,m)$ is the greatest common divisor of a and m.*

Theorem 1.4. *The Chinese Remainder Theorem (for detail see page 230, Fact 4 of [28])*
Define

$$\eta_1 = \begin{cases} 0 & if \;\; b = 0, 1 \\ 1 & if \;\; b \geq 2, \end{cases}$$

and

$$\eta_2 = \begin{cases} 0 & if \;\; b < 3 \\ 1 & if \;\; b \geq 3, \end{cases}$$

If $gcd(2^b, u) = 1$, then the number of solutions for the congruence $u^t \equiv a \pmod{2^b}$ is either 0 or $(gcd(2,t))^{\eta_1}(gcd(2^{b-2},t))^{\eta_2}$.

The following inequality can easily be proved using mathematical induction.

Lemma 1.5. *For $t \geq 2$, $t \leq \beta(t-1), \beta = 2,\ 3,\ 4, \ldots$.*

Lemma 1.6. *For a prime p of the type $p \equiv 3 \pmod 4$, $k \geq 4$, then, $1,\ 2^{k-1} \pm 1,\ 2^k - 1$ are fixed points in $G_1(p,\ 2^k)$ and 0 is the only fixed point in $G_2(p,\ 2^k)$.*

Proof. For $k \geq 4$, $\alpha = 1 + 2^{k-1}$ is a fixed point if $\alpha^p \equiv \alpha \pmod{2^k}$. For this, note that

$$(1 + 2^{k-1})^p = 1 + p\, 2^{k-1} + \sum_{\beta=2}^{p} \binom{p}{\beta} 2^{\beta(k-1)}. \tag{1.2}$$

As $k \geq 4$, Lemma 1.5 invokes, $k \leq \beta(k-1)$, $\beta = 2,\ 3,\ 4, \ldots,\ n$ which further gives $2^k | 2^{\beta(k-1)}$. But then,

$$\sum_{\beta=2}^{p} \binom{p}{\beta} 2^{\beta(k-1)} \equiv 0 \pmod{2^k}. \tag{1.3}$$

Also, $p = 4t + 3$ for some integer $t = 0, 1, 2, \ldots.$ Using the expression of p together with Eqs (1.2) and (1.3), we get

$$\begin{aligned}(1+2^{k-1})^p &\equiv 1+(3+2^2t)2^{k-1} \pmod{2^k}\\ &\equiv 1+(1+2+2^2t)2^{k-1} \pmod{2^k}\\ &\equiv 1+(2^{k-1}+2^k+2^{k+1}) \pmod{2^k}\\ &\equiv 1+2^{k-1} \pmod{2^k}.\end{aligned}$$

Similarly, we can follow the same procedure to prove the remaining fixed points. Also by Theorem 1.4, the number of solutions of $u^{p-1} \equiv 1 \pmod{2^b}$ with $2 \nmid u$ is $(gcd(2, p-1))^{\eta_1}(gcd(2^{b-2}, p-1))^{\eta_2}$. Note that, in our case, $\eta_1 = \eta_2 = 1$, with $b \geq 3$. As $p \equiv 3 \pmod 4$ can also be written as $p - 1 = 2(1 + 2t)$, $t \in \mathbb{Z}^+$. Hence, we get $gcd(2, 2(1 + 2t)) \cdot gcd(2^{b-2}, 2(1 + 2t)) = 2 \cdot 2 = 4$. This shows that there are exactly four fixed points. □

Proposition 1.7. *The graph $G_1(p, 2^k)$ has 8 fixed points which are 1, $\pm\ 1+2^{k-1}$, $\pm\ 1+2^{k-2}$, 2^{k-1}, $-(2^{k-2} \pm\ 1) + 2^k$ and $G_2(p, 2^k)$ contains only 0 as a fixed point where $k \geq 4$ and $p\ \equiv\ 5 \pmod 8$.*

Proof. For $k \geq 4$, $\alpha = 1 + 2^{k-2}$ is fixed point if $\alpha^p \equiv \alpha \pmod{2^k}$. For this, note that

$$(1+2^{k-2})^p = 1 + p\,2^{k-2} + \sum_{\beta=2}^{p}\binom{p}{\beta}2^{\beta(k-2)}. \tag{1.4}$$

As $k \geq 4$, Lemma 1.5 invokes, $k \geq 4$, $k \leq \beta(k-2)$, $\beta = 2, 3, 4, \ldots, n$. Then $2^k | 2^{\beta(k-2)}$. Hence

$$\sum_{\beta=2}^{p}\binom{p}{\beta}2^{\beta(k-2)} \equiv 0 \pmod{2^k}. \tag{1.5}$$

Also, $p = 8t + 5$ for some integer $t = 0, 1, 2, \ldots$. Using p together with Eq (1.5) in (1.4), we get

$$\begin{aligned}(1+2^{k-2})^p &\equiv 1+(5+8t)2^{k-2} \pmod{2^k}\\ &\equiv 1+(1+2^2+2^3t)2^{k-2} \pmod{2^k}\\ &\equiv 1+(2^k+2^{k-2}+2^{k+1}t) \pmod{2^k}\\ &\equiv 1+2^{k-2} \pmod{2^k}.\end{aligned}$$

The remaining fixed points can be proved in a similarly technique. Also by Theorem 1.4, the number of solutions of $u^{p-1} \equiv 1 \pmod{2^b}$ with $2 \nmid u$ is $(gcd(2, p-1))^{\eta_1} \cdot (gcd(2^{b-2}, p-1))^{\eta_2}$. In our case, take $\eta_1 = \eta_2 = 1$, with $b \geq 4$. As $p \equiv 5 \pmod 8$ implies that $p - 1 = 4(1 + 2t)$, $t \in \mathbb{Z}^+$. Hence, we get $gcd(2, 4(1 + 2t)) \cdot gcd(2^{b-2}, 4(1 + 2t)) = 2 \cdot 4 = 8$. This shows that there are exactly eight fixed points. □

Figure 2 reflects Proposition 1.7.

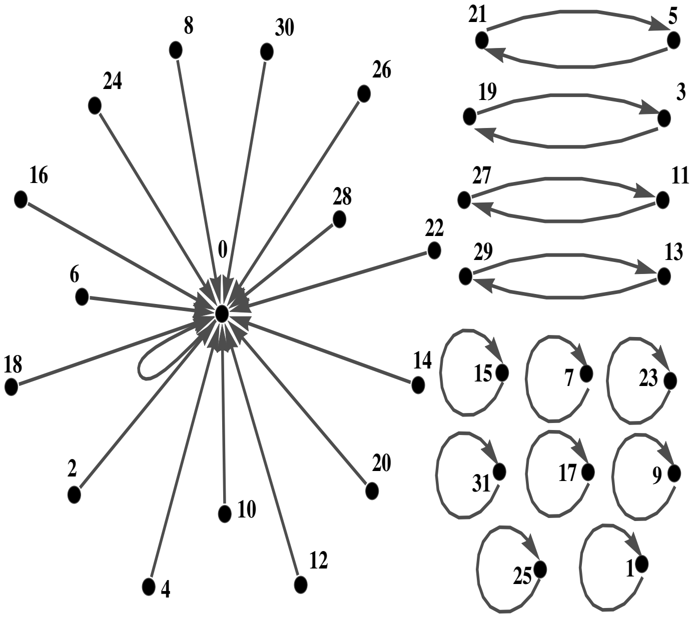


Figure 2. The digraph $G(29, 2^5)$.

2. Enumeration of cyclic vertices and components

The vertices $v_1, v_2, v_3, \ldots, v_t$ compose a component if for every $j, 1 \leq j \leq t$, there exists some i, $1 \leq i \leq t$, such that $v_j^p \equiv v_i^p \pmod{m}$, for all $j \neq i$. By [8], it has been established that there exists one and only one cycle in every component of such digraphs. While the enumeration of components is still an open problem. In this section, an enumeration of cycles and components (up to isomorphism) of $G(p, 2^k)$ is proposed for certain classes of p. Also, we examine all integers for which there are p number of components. The following theorem also validates a similar result given in [4] for a quadratic congruences.

Theorem 2.1. *For an odd prime p, define $m = 2^i p^t$, $i = 0, 1, 2$, $t \geq 1$. Then $G(p, m)$ contains an s-cycle if and only if $p^s \equiv 1 \pmod{d}$ for a smallest integer $s > 0$ provided $d > 0$ with $d \mid \lambda(m)$.*

Proof. Let $m = 2^i p^t$, $i = 0, 1, 2$, $t \geq 1$ and suppose $G(p, m)$ contains an s-cycle. Assume that u is an arbitrary vertex on this cycle. Then $u^{p^s} \equiv u \pmod{2^i p^t}$ for a smallest integer $s > 0$. That is, $u(u^{p^s-1} - 1) \equiv 0 \pmod{2^i p^t}$. Clearly, $gcd(u, u^{p^s-1} - 1) = 1$. Thus if we let $m_1 = gcd(u, m)$ and $m_2 = m/m_1$, then $s > 0$ must be smallest such that $u \equiv 0 \pmod{m_1}$ and $v^{p^s-1} \equiv 1 \pmod{m_2}$. Using Chinese Reminder Theorem, we get a solution x to satisfying $x \equiv 1 \pmod{m_1}$ and $x \equiv a \pmod{m_2}$. Consequently, the integer $s > 0$ is, in fact, least such that $x^{p^s-1} \equiv 1 \pmod{m_1}$ and $x^{p^s-1} \equiv 1 \pmod{m_2}$. Both yields that, $x^{p^s-1} \equiv 1 \pmod{2^i p^t}$. Let $d = ord_m^x$ ($d = ord_m^x$ if d is the least positive integer such that $x^d \equiv 1 \pmod{m}$). Then, $x \equiv 1 \pmod{m_1}$ enforces that $s > 0$ is the least integer such that $p^s \equiv 1 \pmod{d}$. Also, if $d = ord_m^x$, then $(x, 2^i p^t) = 1$, so by Carmichael Theorem, it is evident that $d \mid \lambda(2^i p^t)$.

Conversely, suppose $d > 0$ with $d \mid \lambda(m)$ and let $u = g^{\lambda(2^i p^t) \mid d}$. Then $d = ord_m^u$. As $d \mid p^s - 1$

but $d \nmid p^l - 1$ for $0 \leq l < s$. We deduce that the integer $s > 0$ is least so that $u^{p^s - 1} \equiv 1 \pmod{2^i p^t}$. Equivalently, $u \cdot u^{p^s-1} \equiv u^{p^s} \equiv u \pmod{2^i p^t}$. □

Theorem 2.2. *For any prime p with $p \equiv 3 \pmod 8$, the vertices $1 + p^s 2^{k-2}, k \geq 4$ for $s = 0,\ 1$ form a cycle of length 2 in $G(p, 2^k)$.*

Proof. The vertices α_0 and α_1 form a cycle of length 2 in $G(p, 2^k)$ if and only if $\alpha_0^p \equiv \alpha_1 \pmod{2^k}$, $\alpha_1^p \equiv \alpha_0 \pmod{2^k}$. Now

$$(1 + p^s 2^{k-2})^p = 1 + p^{s+1} 2^{k-2} + \sum_{\beta=2}^{p} \binom{p}{\beta} p^{\beta s} 2^{\beta(k-2)}. \tag{2.1}$$

As $k \geq 4$, Lemma 1.5 invokes, $k \geq 4,\ k \leq \beta(k-2),\ \beta = 2,\ 3,\ 4, \dots, n$. That is, $2^k \mid 2^{\beta(k-2)}$. Therefore,

$$\sum_{\beta=2}^{p} \binom{p}{\beta} p^{\beta s} 2^{\beta(k-2)} \equiv 0 \pmod{2^k}. \tag{2.2}$$

$$(1 + p^s 2^{k-2})^p \equiv 1 + p^{s+1} 2^{k-2} \pmod{2^k}, \tag{2.3}$$

$s = 0,\ 1$ and $p \equiv 3 \pmod 8$. Also, $p = 8t + 3$ for some integer $t = 0,\ 1,\ 2, \dots$. Using this together with Eq (2.3), for $s = 1$ we get that

$$\begin{aligned}
(1 + p^s 2^{k-2})^p &\equiv 1 + (3 + 2^3 t)^2 2^{k-2} \pmod{2^k} \\
&\equiv 1 + (9 + 2^6 t^2 + 3.2^4 t) 2^{k-2} \pmod{2^k} \\
&\equiv 1 + (1 + 2^3 + 2^6 t^2 + 3.2^4 t) 2^{k-2} \pmod{2^k} \\
&\equiv 1 + (1 + 2^3 + 2^6 t^2 + 3.2^4 t) 2^{k-2} \pmod{2^k} \\
&\equiv 1 + 2^{k-2} \pmod{2^k}.
\end{aligned} \tag{2.4}$$

From Eqs (2.3) and (2.4), we find that the vertices $1 + p^s 2^{k-2}$ for $s = 0,\ 1$ form a cycle of length 2 in $G(p,\ 2^k)$, where $k \geq 4$ and $p \equiv 3 \pmod 8$. □

Theorem 2.3. *For any prime p such that $p \equiv 3 \pmod 8$, the vertices $2^k + p^{p^s},\ k > 2$ for $s = 0,\ 1,\ 2,\ 3, \dots,\ 2^{k-2} - 1$ form a cycle of length 2^{k-2} in $G(p,\ 2^k)$.*

Proof. The vertices $\alpha_0,\ \alpha_1,\ \alpha_2, \dots,\ \alpha_{2^{(k-2)}-1}$ form a cycle of length 2^{k-2} in $G(p,\ 2^k)$ if and only if $\alpha_0^p \equiv \alpha_1 \pmod{2^k}$, $\alpha_1^p \equiv \alpha_2 \pmod{2^k}, \dots,\ \alpha_{2^{(k-2)}-1}^p \equiv \alpha_0 \pmod{2^k}$. Now

$$(2^k + p^{p^s})^p = 2^k + (p^{p^s})^p + \sum_{\beta=2}^{p} \binom{p}{\beta} (p^{p^s})^{p-\beta} 2^{(\beta(k))}, \tag{2.5}$$

Since $k > 2,\ k \leq \beta(k),\ \beta = 1, 2,\ 3,\ 4, \dots, n$. Then $2^k | 2^{\beta(k)}$. Hence,

$$\sum_{\beta=2}^{p} \binom{p}{\beta} (p^{p^s})^{p-\beta} 2^{\beta(k)} \equiv 0 \pmod{2^k}, \tag{2.6}$$

putting in Eq (2.5), we get

$$(2^k + p^{p^s})^p \equiv 2^k + p^{p^{s+1}} \pmod{2^k}, \tag{2.7}$$

$s = 0,\ 1,\ 2,\ 3, \dots, 2^{(k-2)} - 1$ and $p \equiv 3 \pmod 8$. Finally, we noted that

$$(2^k + p^{p^{2^{(k-2)}-1}}) \equiv 2^k + p \pmod{2^k}. \tag{2.8}$$

Since, $p^{2^{(k-2)}-1} \equiv 1 \pmod{2^k}$, for any $k > 2$ it implies that,

$$p^{p^{2^{(k-2)}-1}} \equiv p \pmod{2^k}.$$

Eqs (2.7) and (2.8) give that vertices $2^k + p^{p^s}, k > 2$ for $s = 0,\ 1,\ 2,\ 3, \dots, 2^{(k-2)} - 1$ form a cycle of length 2^{k-2} in the graph $G(p,\ 2^k)$, where $p \equiv 3 \pmod 8$. □

Theorem 2.4. *For any prime p such that* $p \equiv 3 \pmod 8$, *the vertices* $2^k + (p+2)^{p^s}, k > 2$ *for* $s = 0,\ 1,\ 2,\ 3, \dots, 2^{k-2} - 1$ *form a cycle of length* 2^{k-2} *in the graph* $G(p,\ 2^k)$.

The proof is on similar lines as illustrated in the proof of Theorem 2.3.

The following result is a simple consequence of last two theorems.

Corollary 2.5. *For any prime p such that* $p \equiv 3 \pmod 8$, *the graph* $G(p,\ 2^k)$ *has cycle of length* $2^{k-(r+2)}$, *where* $k > 2,\ 0 \le r \le k-3$.

In the following theorem, we find all integers for which there are p components.

Theorem 2.6. *(1) The number of components of* $G(p,m)$ *is p if* $m = p^k$ *for some positive integer k and p is an odd prime.*

(2)The number of components of $G(p,m)$ *is p if m is prime of the form* $m = (p-1) \times p^k + 1$ *for some positive integer k, where* $p \equiv 3 \pmod 4$.

Proof. (1) If $m = p^k$ then by [[8], Theorem 6.6 on page 2005], we have exactly p fixed points. Now these are either isolated or the roots of their respective components. Thus, if m is any number for which we have more than p components then there must be a cycle of length $s > 1$. But then by Theorem 2.1, s is the least positive integer such that $p^s \equiv 1 \pmod d$, where $d \mid \lambda(p^k)$ and $d > 0$. That is, $d \mid p^s - 1$ and $d \mid \lambda(m) = (p-1) \times p^k$ as well. This clearly enforces that $d = p - 1$. But then $p^k \equiv 1 \pmod{p-1}$ for each value of k. In particular, if $1 \le r < s$, then $p^r \equiv 1 \pmod{p-1}$ as well. This has certainly provided a contradiction against the minimality of s. Thus, this case is not all possible. Consequently, $G(p,m)$ has p components.

(2) If m is prime of the form $m = (p-1) \times p^k + 1$ for some positive integer k, where $p \equiv 3 \pmod 4$. Then it can easily be seen that there are p fixed points by [[8], see Theorem 6.6 on page 2005] and by similar argument as part 1 there does not exist cycle of length greater than 1. Thus, there are exactly p components. □

If d is the least positive integer such that $n^d \equiv 1 \pmod m$ then d will be termed as order of n modulo m, it is denoted as $d = ord_m^n$. In the following result, we show that the digraph $G_1(p, 2^k),\ k > 0$ contains only the cycles of lengths which are the powers of 2 (excluding fixed points) and $G_2(p, 2^k)$ form a tree with root 0.

Theorem 2.7. *For any positive integer k, the digraph* $G_1(p, 2^k)$, *contains cycles of lengths as integral powers of 2. That is, the length of any cycle in* $G_1(p, 2^k)$ *must be of the form* $2^t,\ t \in \mathbb{Z}^+$ *and* $t < k$ *(excluding fixed points) while* $G_2(p, 2^k)$ *form a tree with root* 0. *Moreover, indeg*$(0) = 2^{k - \lceil \frac{k}{p} \rceil}$.

Proof. It is well known that there must be an equal number of residues of $m = 2^k$ which are prime to m and those which are not prime to m. Thus the digraphs $G_1(p, m)$ and $G_2(p, m)$ contains equal number of vertices 2^{k-1}, by Lemma 1.6. It can be seen that, $\pm\ 1 + 2^{k-1},\ -1 + 2^k,\ 1$, are the only fixed points of $G_1(p,\ 2^k p)$, where $p\ \equiv\ 3 \pmod 4$, and by Proposition 1.7. $G_1(p, 2^k)$ has 8 fixed points which are $1, 2^{k-1} \pm 1,\ \pm 1 + 2^{k-2},\ 2^{k-1},\ -(2^{k-2} \pm\ 1) + 2^k$, where $p\ \equiv\ 5 \pmod 8$, and if $p = 2^u a + 1$ ($p \equiv 1 \bmod 8$) with an odd a, then $G_1(p, 2^k)$ contains 2^{u+1} fixed points, the elements of order dividing 2^u, provided that $k\ \geq\ u + 2$. By Theorem 2.1, there would be a cycle of length s if and only if $s\ =\ ord_d^p$, for some divisor d of $\lambda(m)\ =\ 2^{k-2}$. Now if there exists such a cycle, then s being order of p modulo a divisor of 2^{k-1} must be of the form 2^t, for some integer $t\ >\ 0$. As far the other case is concerned, we note that all, even residues of 2^k, will be connected by a tree. Thus, $(2^{k-\lceil \frac{k}{p} \rceil})$ numbers, namely $2^{\lceil \frac{k}{p} \rceil},\ 2 \cdot 2^{\lceil \frac{k}{p} \rceil},\ 3 \cdot 2^{\lceil \frac{k}{p} \rceil},\ \ldots, 2^{k-\lceil \frac{k}{p} \rceil} \cdot 2^{\lceil \frac{k}{p} \rceil}$ are mapped onto 0. Consequently, $indeg(0) = (2^{k-\lceil \frac{k}{p} \rceil})$. □

In the following theorem, we investigate the structure of isomorphic trees.

Theorem 2.8. *Let t be any positive integer and $m = p^t$. Then the digraph $G_1(p,\ m)$ consists of $p - 1$ isomorphic trees. Moreover, $G_2(p,\ m)$ is a tree with root at* 0 *and $indeg(0) = p^{t-\lceil \frac{t}{p} \rceil}$.*

Proof. We know that the digraph $G(p,\ m)$ has exactly p components with p fixed points (For detail, see Theorem 6.6 on page 205 in [8]). Note that $p^{t-\lceil \frac{t}{p} \rceil}$ elements, namely, $p^{\lceil \frac{t}{p} \rceil}, 2 \cdot p^{t-\lceil \frac{t}{p} \rceil}, 3 \cdot p^{t-\lceil \frac{t}{p} \rceil}, \ldots,$ $p^{t-\lceil \frac{t}{p} \rceil} \cdot p^{\lceil \frac{t}{p} \rceil}$ are adjacent to 0 in $G_2(p,\ m)$. Also, $p|\phi(m) = (p - 1) \cdot p^{t-1}$, by Theorem 3.3, we obtain that the digraph $G_1(p,\ m)$ is semiregular and every vertex, either has degree 0 or p. It is clear that this digraph has a tree with root 0. Now assume the set of non-zero fixed points as $\{1,\ a_2,\ a_3, \ldots, a_{\frac{p-1}{2}},\ m - 1,\ m - a_2,\ m - a_3, \ldots, m - a_{\frac{p-1}{2}}\}$. Define $T_1,\ T_{m-1},\ T_{a_2},\ T_{m-a_2}$ so on $T_{a_{\frac{p-1}{2}}}$ and $T_{m-a_{\frac{p-1}{2}}}$ trees containing the fixed points $\{1,\ m - 1,\ a_2,\ m - a_2,\ a_3,\ m - a_3, \ldots,\ a_{\frac{p-1}{2}},\ m - a_{\frac{p-1}{2}}\}$, respectively. we can easily deduce that $T_1\ \cong\ T_{m-1},\ T_{a_2}\ \cong\ T_{m-a_2}, \ldots,\ T_{a_{\frac{p-1}{2}}}\ \cong\ T_{m-a_{\frac{p-1}{2}}}$. Now, if we multiply each vertex of the tree T_1 by number a_2, we have tree T_{a_2}. Similarly, if we multiply each vertex of the tree T_1 by number a_3, we have a tree T_{a_3}. By continuing this fashion if we multiply T_1 by $a_{\frac{p-1}{2}}$ have a tree $T_{a_{\frac{p-1}{2}}}$. This is possible if $gcd(a_i, m)\ =\ 1$, where $i\ =\ 1, 2, 3, \ldots, a_{\frac{p-1}{2}}$. Consequently, it yields that, $T_1\ \cong\ T_{a_2},\ T_1\ \cong\ T_{a_3}, \ldots, T_1 \cong T_{a_{\frac{p-1}{2}}}$. □

Figures 3 and 4 reflect Theorem 2.7 and Theorem 2.8, respectively.

Now, we discuss the components of the digraph $G(p,\ m)$. The notation $A_t(G(p,\ m))$ denotes the number of cycles of length t in the digraph $G(p, m)$.

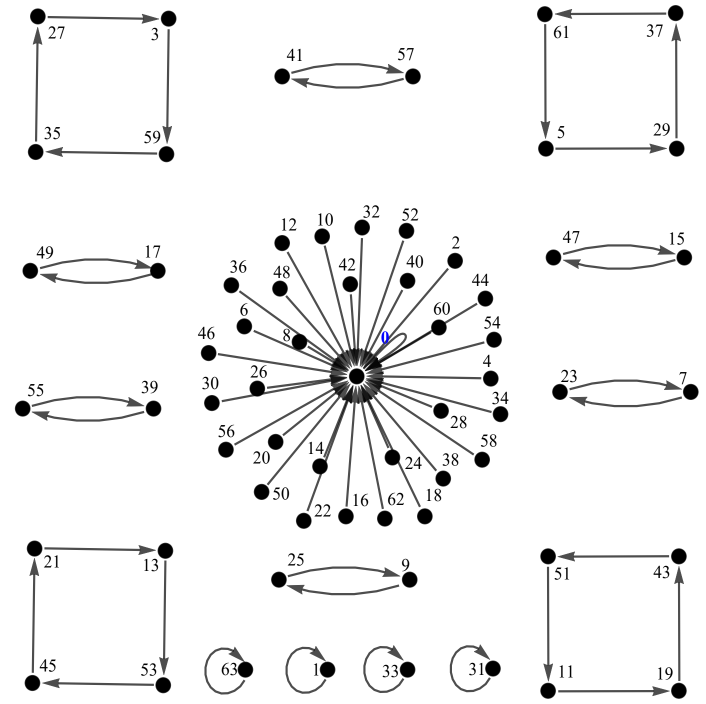


Figure 3. The digraph $G(11, 2^6)$.

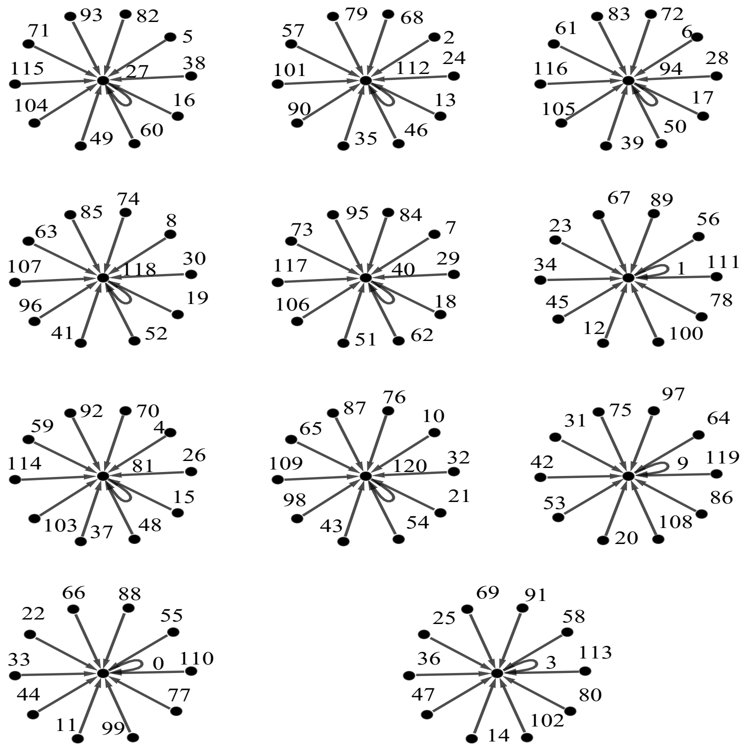


Figure 4. The digraph $G(11, 11^2)$.

Theorem 2.9. *For any prime p such that* $p \equiv 3 \pmod 8$, *the graph* $G(p,\ 2^k)$ *has* $11 + 4(k-5)$ *components, where* $k > 4$.

Proof. To prove this result, first we find the number of cycles of length $2^{k-(r+4)}$, where $k > 4,\ 0 \leq r \leq k-5$ and $p \equiv 3 \pmod 8$. By Lemma 1.5, it is found that $A_1(G(p,\ 2^k)) = 5$ and obtained the number of cycles of length two $A_2(G(p,\ 2^k))$ by using Theorem 6.6 of [8] for $\delta_i = 2$, given as

$$\begin{aligned} A_2(G(p,\ 2^k)) &= \frac{1}{2}[(2gcd(\lambda(2^k), p^2-1)+1) \\ &- \sum_{\substack{d|2 \\ d\neq 2}} dA_d(2^k, p)]. \end{aligned}$$

Now $gcd(\lambda(2^k), p^2-1) = 8$, where $p \equiv 3 \pmod 8),\ k > 4$ and $A_1(p,\ 2^k) = 5$, hence, $A_2(G(2^k, p)) = 6$

$$\begin{aligned} A_{2^2}(G(p,\ 2^k)) &= \frac{1}{2^2}[(\ 2gcd(\lambda(2^k), p^{2^2}-1)+1) \\ &- \sum_{\substack{d|2^2 \\ d\neq 2^2}} dA_d(p,\ 2^k)], \end{aligned}$$

$gcd(\lambda(2^k), p^{2^2}-1) = 2^4 = 16,\ p \equiv 3 \pmod 8),\ k > 4, A_1(p,\ 2^k) = 5$ and $A_2(p,\ 2^k) = 6$.

$$\begin{aligned} A_{2^2}(G(p,\ 2^k)) &= 4. \\ A_{2^3}(G(p,\ 2^k) &= \frac{1}{2^3}[(2gcd(\lambda(2^k), p^{2^3}-1)+1) \\ &- \sum_{\substack{d|2^3 \\ d\neq 2^3}} dA_d(p,\ 2^k)]. \end{aligned}$$

$gcd(\lambda(2^k), p^{2^3}-1) = 2^5 = 32,\ p \equiv 3 \pmod 8),\ k > 4,\ A_1(p,\ 2^k) = 5, A_2(p,\ 2^k) = 6$, and $A_3(p,\ 2^k) = 4$.

$$A_{2^3}(G(p,\ 2^k)) = 4.$$

$$\vdots$$

$$\begin{aligned} A_{2^{k-4}}(G(p,\ 2^k)) &= \frac{1}{2^{k-4}}[(2gcd(\lambda(2^k), p^{2^{k-4}}-1)+1) \\ &- \sum_{\substack{d|2^{k-4} \\ d\neq 2^{k-4}}} dA_d(p,\ 2^{k-4})], \end{aligned}$$

$gcd(\lambda(2^k), p^{2^{k-4}}-1) = 2^{k-2},\ p \equiv 3 \pmod 8),\ k > 4,\ A_1(p,\ 2^k) = 5, A_2(p,\ 2^k) = 6,\ A_{2^2}(p,\ 2^k) = A_{2^3}(p,\ 2^k) = \ldots = A_{2^{k-4}}(p,\ 2^k) = 4$.

$$A_{2^{k-4}}(G(p,\ 2^k)) = 4.$$

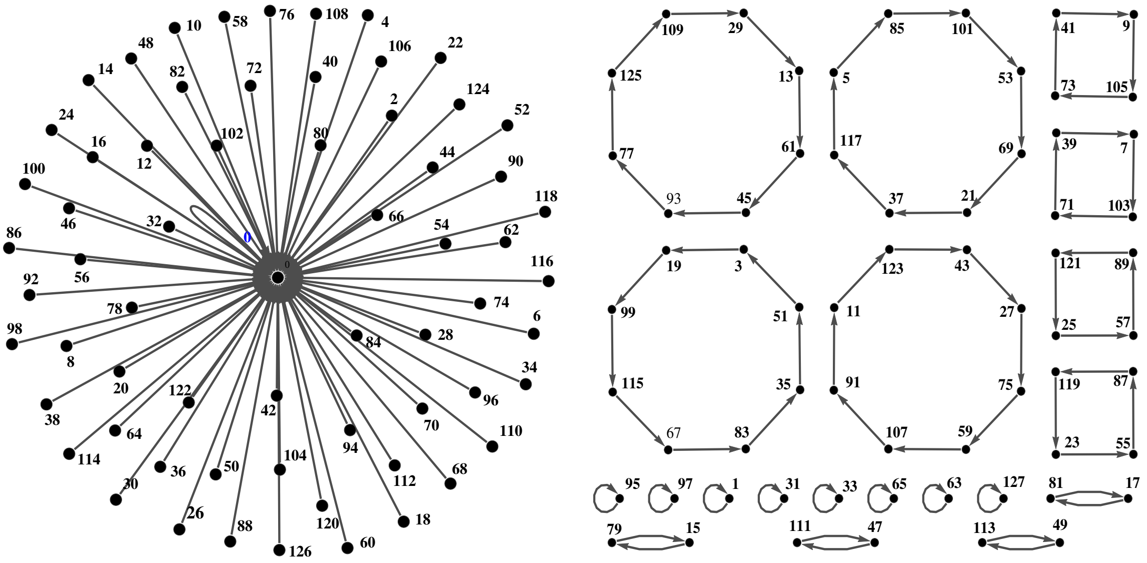
So by counting principle adding $A_1(p,\ 2^k) = 5,\ A_2(p,\ 2^k) = 6,\ A_{2^2}(p,\ 2^k) = A_{2^3}(p,\ 2^k), \ldots, A_{2^{k-4}}(2^k, p) = 4$. We get $11 + 4(k-5)$ components, for $k > 4$, and $p \equiv 3 \pmod 8$. □

Theorem 2.10. *For any prime p such that* $p \equiv 5 \pmod 8$, *the graph* $G(p,\ 2^k)$ *has* $13 + 4(k-5)$ *components, where* $k > 4$.

The proof is on similar lines as illustrated in the proof of Theorem 2.9.

Theorem 2.11. *Let p be any prime such that* $p \equiv 7 \pmod{2^4}$. *Then graph* $G(p,\ 2^k)$ *has* $19 + 8(k-6)$ *components, where* $k > 5$.

The proof is on similar lines as illustrated in the proof of Theorem 2.9.
Figure 5(a) and (b) reflect Theorem 2.9.



(a) (b)

Figure 5. The digraph $G(19, 2^7)$.

3. Regularity and semiregularity

In this section, we give conditions for the regularity and semiregularity of our proposed graph. In the following result, we characterize the regularity of the digraph $G_1(p, m)$.

Lemma 3.1. *The digraph* $G_1(p, m)$ *is regular if and only if* $p \nmid \phi(m)$, *where* ϕ *is the Euler's function.*

Proof. We suppose that $G_1(p, m)$ is regular. The regularity of $G_1(p, m)$ yields that the indeg$(v) = 1$ for every vertex v in $G_1(p, m)$. This means that $x^p \equiv v \pmod m$ has a unique solution. Without loss of generality, assume $v \equiv 1 \pmod m$ and let β be the unique solution of the congruence $x^p \equiv 1 \pmod m$. That is, $\beta^p \equiv 1 \pmod m$. Now, if $p \mid \phi(m)$ then $\phi(m) = p \cdot t$ for some integer t. Note that, $t = 1$ is impossible as $\phi(m)$ is always even. Also by Euler Theorem, $\beta^{\phi(m)} \equiv 1 \pmod m$ as $(\beta,\ m) = 1$ (by definition of $G_1(m)$). Then, $\beta^{p \cdot t} \equiv 1 \pmod m$ or $(\beta^t)^p \equiv 1 \pmod m$. This shows that $\beta^t,\ t > 1$ is another solution of $x^p \equiv 1 \pmod m$. This means that $indeg(1) = 2$, a contradiction against the fact that $G_1(p, m)$ was regular. Therefore, $p \nmid \phi(m)$. Conversely, let $p \nmid \phi(m)$ and we suppose that $G_1(p, m)$ is not regular. Then there must be at least one vertex α such that $indeg(\alpha) > 1$. For the sake of convenience, take $\alpha = 1$ with $indeg(\alpha) = 2$. This means that $x^p \equiv 1 \pmod m$ has two solutions. Let these be α and $\alpha^t,\ t > 1$. Then, $\alpha^p \equiv 1 \pmod m$ and $\alpha^{p't} \equiv 1 \pmod m$. But, $\alpha^{\phi(m)} \equiv 1 \pmod m$. Hence, we deduce that either $\phi(m) = p$ or $\phi(m) = p \cdot t$. As $\phi(m)$ is always even, so $\phi(m) = p \cdot t$. That is, $p \mid \phi(m)$, a contradiction. □

Lemma 3.2. *Let $m > 0$ be any square free integer and p be any odd prime. The digraph $G(p, m)$ is cyclic if and only if $p \nmid \phi(m)$.*

Proof. Recall that a digraph is cyclic if all of its components are cycles. Also, every regular digraph is cyclic. Hence, by Lemma 3.1, $G_1(p,\ m)$ is cyclic if and only if $p \nmid \phi(m)$. For $G_2(p,\ m)$, suppose $p \nmid \phi(m)$ and let α be any vertex in $G_2(p,\ m)$. Let $p^{'}$ be an odd prime such that $p^{'} \mid gcd(\alpha, m)$. Then we can find integers r and s such that $\alpha = rp^{'}$ and $m = p^{'}s$ with $gcd(r, s) = 1$. Now if β is the solution of the congruence $x^p \equiv \alpha \pmod m$, then $\beta^p \equiv \alpha \pmod m$ yields that $\beta^p = \alpha + mt$ for some integer t. But then $\beta^p = rp^{'} + sp^{'}t$. Consequently, $p^{'} \mid \beta$ such that $p^{'} \mid gcd(\alpha, m)$. This means that $\beta^p \equiv \alpha \ \equiv 0 \pmod{p^{'}}$. Thus we conclude that a number β exists such that it is a solution of $x^p \equiv \alpha \pmod m$. Next we show that this solution is unique modulo m. Since $p \nmid \phi(m)$, so $gcd(p, \phi(p^{'})) = 1$. Then the linear congruence $py \equiv 1 \pmod{p^{'} - 1}$ has a unique solution in y. Finally, we put $\beta \equiv \alpha^y \pmod{p^{'}}$ to get $\beta^p \equiv \alpha^{p \cdot y} \equiv a \pmod{p^{'}}$. By Chinese Reminder Theorem, we get that β is a unique solution of $x^p \equiv \alpha \pmod m$. Thus, indegree of this arbitrary vertex is one. This certainly implies that every vertex is either a loop (a cycle of length one) or at some cycle. The converse is a direct consequence of Lemma 3.1. □

For further result on semiregularity, we define a function η as,

$$\eta(m) = \begin{cases} \eta_o(m) + 1 & if \ \ p^{\,2} | m \\ \eta_o(m) & if \ \ p^{\,2} \nmid m \end{cases},$$

where $\eta_o(m)$ is the number distinct prime divisors of m such that $p^{'} \equiv 1 (\text{mod } p)$. In the following theorem, we characterize the semiregularity of $G_1(p, m)$, where p is an odd prime.

Theorem 3.3. *The digraph $G_1(p, m)$ is semiregular if and only if $p | \phi(m)$, Also the indegrees in $G_1(p, m)$ are either $p^{\,\eta(p)}$ or zero.*

Proof. By definition of digraph $G_1(p, m)$, it is indicated, that $\beta^{\phi(m)} \equiv 1 \pmod m$ for each vertex β in $G_1(p, m)$. This means that the indegrees of the vertices of $G_1(p, m)$ are same if $indeg(\beta) > 0$. To find the $indeg(\beta) > 0$, we just count the indegrees of 1. For this purpose we just count the number of solutions of the congruence, $x^p \equiv 1 \pmod{p^r}$. Let p be an odd prime and r be any positive integer. Then we see that, $(p^{r-1} + 1)^p \equiv 1 \pmod{p^r}$. Likewise, we see that the numbers, $2 \times p^{r-1} + 1, 3 \times p^{r-1} + 1, 4 \times p^{r-1} + 1, 5 \times p^{r-1} + 1, 6 \times p^{r-1} + 1, \ldots, p \times p^{r-1} + 1$ also solutions of the congruence, $x^p \equiv 1 \pmod{p^r}$. While modulo $p^{'}$, there are always $p^{'}$ solutions whenever $p^{'} \equiv 1 \pmod p$ and there is a trivial solution if $p^{'} \not\equiv 1 \pmod p$ (for detail see [26], page 104). Using the canonical representation of m into odd primes and Chinese Remainder Theorem, simultaneously, we must get that $\alpha^p \equiv 1 \pmod m$ either have $p^{\,\eta(m)}$ solutions or have no solution for each vertex α in $G_1(p, m)$. On the other hand, we let $G_1(p, m)$ is semiregular and $indeg(\alpha) = p^{\,\eta(m)}$ for $\alpha \in G_1(p, m)$. This means that $\alpha^p \equiv 1 \pmod m$. Using multiplicative order and Euler Theorem for α, we deduce that $p \mid \phi(m)$. Conversely, assume that $p \nmid \phi(m)$. then by Lemma 3.2 indegree of each vertex is one which is contradiction. Hence $p \mid \phi(m)$. □

Figure 6 reflects Theorem 3.3.

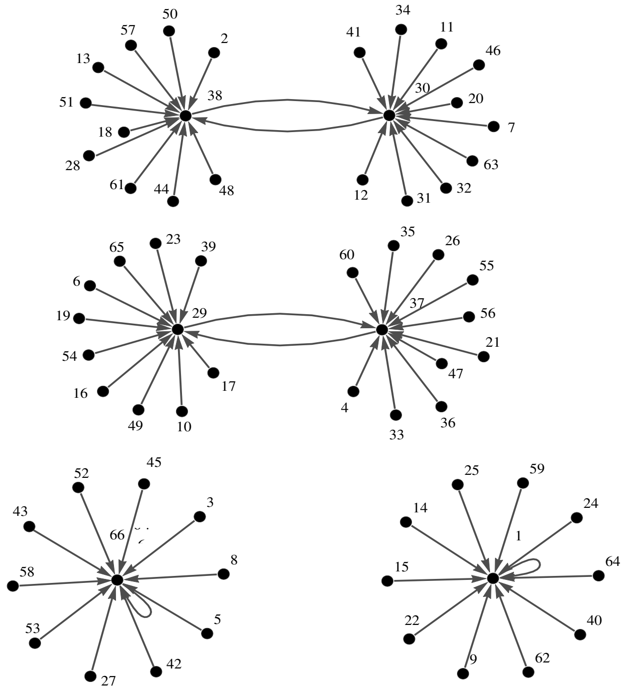


Figure 6. The digraph $G(11, 67)$.

4. Conclusions

Until the date, several papers on power diagraphs have been published for the fixed power of the congruences modulo an integer. For example, power diagraphs corresponding to $x^2 = y \pmod{m}$, $x^3 = y \pmod{m}$ or else fixed powers have been discussed earlier. In this work, we discussed and generalized the results of power diagraphs for any odd prime p as x power rather fixing. That is, for the congruence of $x^p = y \pmod{m}$, where p is any odd prime. We addressed the number of loops, cyclic structures, tree structures and the enumeration of components over residue classes of integers. In Section 1, the fixed points of such diagraphs are described and enumerated. These fixed points are referred to as loops. The existence and enumeration of cycles along with their sizes are discussed in Theorems 2.1–2.4 and in Corollary 2.5. In Theorems 2.6–2.11, we have discussed the enumeration of components and trees for classes of integers. These findings have also been shown in Figures 2–5 for better comprehension and confirmation. Finally, the results on regularity and semi-regularity are discussed and generalized in Section 3. In fact, we have fully established and defined the desired ideas for power diagraphs with an odd prime power. We believe that the characterizations can be built on the basis of these findings for all composite modules, which can serve as a basis for solving many difficult and open challenges.

Acknowledgment

This work was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah. The authors, therefore, acknowledge with thanks DSR for technical and financial support.

Conflict of interest

The authors declare that they have no conflict of interest regarding the publication of the research article.

References

1. S. Bryant, Groups, graphs, and Fermat's last theorem, *Am. Math. Monthly*, **74** (1967), 152–155.
2. L. Szalay, A discrete iteration in number theory, *BDTF Tud. Közl.*, **8** (1992), 71–91.
3. T. D. Rogers, The graph of the square mapping on the prime fields, *Discrete Math.*, **148** (1996), 317–324.
4. L. Somer, M. Krizek, On a connection of number theory with graph theory, *Czech. Math. J.*, **5** (2004), 465–485.
5. M. K. Mahmood, F. Ahmad, An informal enumeration of squares of 2^k using rooted trees arising from congruences, *Utilitas Math.*, **105** (2017), 41–51.
6. M. A Malik, M. K Mahmood, On simple graphs arising from exponential congruences, *J. Appl. Math.*, **2012** (2012), 1–10.
7. Y. J. Wei, G. Tang, The iteration digraphs of finite commutative rings, *Turk. J. Math.*, **39** (2015), 872–883.
8. L. Somer, M. Krizek, On symmetric digraphs of the congruence $x^k \equiv y \pmod{m}$, *Discrete Math.*, **309** (2009), 1999–2009.
9. J. Skowronek-Kazió, Some digraphs arising from number theory and remarks on the zero-divisor graph of the ring Z_n, *Inf. Process. Lett.*, **108** (2008), 165–169.
10. M. H. Mateen, M. K. Mahmood, A new approch for the enumeration of components of digraphs over the quadratic maps, *J. Prime Res. Math.*, **16** (2020), 56–66.
11. M. K. Mahmood, F. Ahmad, A classification of cyclic nodes and enumerations of components of a class of discrete graphs, *Appl. Math. Inf. Sci.*, **9** (2015), 103–112.
12. M. H. Mateen, M. K. Mahmood, Power digraphs associated with the congruence $x^n \equiv y \pmod{m}$, *Punjab Univ. J. Math.*, **51** (2019), 93–102.
13. M. H. Mateen, M. K. Mahmood, S. Ali, Importance of power digraph in computer science, *International conference on innovative computing (ICIC), Lahore, Pakistan*, (2019), 1–6.
14. S. Akbari, A. Mohammadian, On the zero-divisor graph of a commutative ring, *J. Algebra*, **274** (2004), 847–855.
15. Y. J. Wei, J. Z. Nan, G. H. Tang, H. D. Su, The cubic mapping graphs of the residue classes of integers, *Ars Combin.*, **97** (2010), 101–110.
16. Y. Wei, G. Tang, H. Su, The square mapping graphs of finite commutative rings, *Algebra Colloq.*, **19** (2012), 569–580.
17. M. Rezaei, S. U. Rehman, Z. U. Khan, A. Q. Baig, M. R. Farahani, Quadratic residues graph, *Int. J. Pure Appl. Math.*, **113** (2017), 465–470.

18. W. Carlip, M. Mincheva, Symmetry of iteration graphs, *Czechoslovak Math. J.*, **58** (2008), 131–145.

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

20. Y. Meemark, N. Wiroonsri, The quadratic digraph on polynomial rings over finite fields, *Finite Fields Appl.*, **16** (2010), 334–346.

21. Y. Meemark, N. Wiroonsri, The digraph of the kth power mapping of the quotient ring of polynomials over finite fields, *Finite Fields Appl.*, **18** (2012), 179–191.

22. M. K. Mahmood, S. Ali, A novel labeling algorithm on several classes of graphs, *Punjab Univ. J. Math.*, **49** (2017), 23–35.

23. S. Ali, M. K. Mahmood, New numbers on euler totient function with application, *J. Math. Ext.*, **14** (2019), 61–83.

24. H. Alolaiyan, A. Yousaf, M. Ameer, A. Razaq, Non-conjugate graphs associated with finite groups, *IEEE Access*, **7** (2019), 122849–122853.

25. A. Portilla, J. M. Rodrguez, J. M. Sigarreta, E. Tours, Gromov hyperbolicity in directed graphs, *Symmetry*, **12** (2020), 105–117.

26. I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, Hoboken: John Wiley & Sons Inc., 1991.

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

28. B. Wilson, Power digraphs modulo n, *Fibonacci Quart.*, **36** (1996), 229–239.

29. M. K. Mahmood, S. Ali, On super totient numbers with applications and algorithms to graph labeling, *Ars Combinatoria*, **143** (2019), 29–37.