Journal of Prime Research in Mathematics Vol. **16(2)***(2020), 56-66*

A NEW APPROACH FOR THE ENUMERATION OF COMPONENTS OF DIGRAPHS OVER QUADRATIC MAPS

M. HARIS MATEEN[1], M. KHALID MAHMOOD[2,*]

Abstract. Various partial attempts to count cycles and components of digraphs from congruences have been made earlier. While the problem is still open till date. In this work, we introduce a new approach to solve the problem over quadratic congruence equations. Define a mapping $g : Z_m \mapsto Z_m$ by $g(t) = t^2$, where Z_m is the ring of residue classes modulo m. The digraph $G(2, m)$ over the set of residue classes assumes an edge between the residue classes $\overline{x}$ and $\overline{y}$ if and only if $g(\overline{x}) \equiv \overline{y} \pmod{m}$ for $m \in Z^+$. Classifications of cyclic and non-cyclic vertices are proposed and proved using basic modular arithmetic. Finally, explicit formulas for the enumeration of non-isomorphic components are proposed followed by simple proofs from number theory.

Key words: Digraphs, Loops, Cycles, Components, Carmichael λ-function.
MSC: Primary 11A07, 05C30, 05C25.

1. Introduction

The modular arithmetic has great importance to explore the discrete graphs and their structures based on the congruence equations $x^k \equiv y \pmod{m}$ from last few decades. These congruence equations are very helpful to express the relationship between graphs and number theory. The present work is also devoted to discuss the digraphs through congruence equations. For this purpose, we consider an integer $m > 0$ and define a class $\overline{r}$, which contains the set of all integers having remainder r modulo m. The corresponding set of complete residue classes of all integers modulo m is defined as $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{m-1}\}$. Furthermore, we construct a diagraph through the following set of residue

[1] Department of mathematics, University of Punjab, Lahore, 54590, Pakistan.
[2] Department of mathematics, University of Punjab Lahore, 54590, Pakistan.
*Corresponding Author: khalid.math@pu.edu.pk.

classes of m, i.e., there exists an edge between two vertices x and y if and only if $x^2 - y \equiv 0 \pmod{m}$.
Consequently, the vertices $x_1, x_2, ..., x_t$ form a cycle of length t if and only if

$$\begin{aligned} x_1^2 &\equiv x_2 \pmod{m}, \\ x_2^2 &\equiv x_3 \pmod{m}, \\ &\vdots \\ x_t^2 &\equiv x_1 \pmod{m}. \end{aligned} \tag{1}$$

A component is a maximal connected subgraph of the corresponding undirected graph. The number of edges coming to a vertex x is called indegree of x which is denoted by $indeg(x)$ and the number of edges leaving the vertex is referred as outdegree, assigned by $outdeg(x)$. Since, remainder of every number modulo m is unique, therefore the outdegree of each vertex is one.

Let $G_1(2, m)$ and $G_2(2, m)$ be two subdigraphs of $G(2, m)$ induced by coprime and not coprime vertices to m, respectively. These subdigraphs define a partition of $G(2, m)$. The digraph $G(2, 38)$ is depicted in Figure.1.

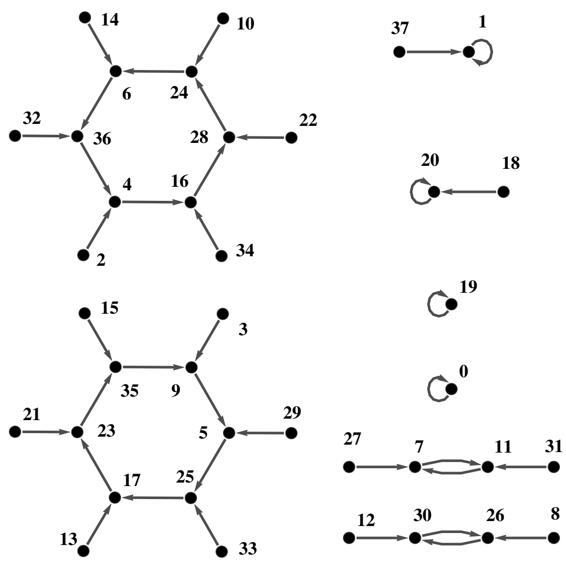

Figure 1. The digraph $G(2, 38)$

Elahi *et al.* discussed an algorithm for zero divisor graphs of finite commutative rings and their vertex-based eccentric topological indices in [1]. It is proved in [2] that each component of such digraphs modulo a prime number p contains a unique cycle. Rogers [3] and Wilson [4] considered and investigated the digraphs associated with the congruence $a^2 \equiv b \pmod{m}$ as well. Number of fixed points and cyclic subdigraphs for the quadratic congruences have also been explored in [3, 4]. The symmetric structures (isomorphic components) and few previous results of these power digraphs have been proposed in [5]. An informal enumeration of squares of 2^k through similar derive established in [6]. Moreover, the power digraphs associated with $x^4 \equiv y \pmod{m}$ and a similar work by employing the exponential congruence $a^x \equiv y \pmod{m}$ have been studied in [7, 8], respectively. Mahmood and Anwar [9, 10] discussed structures of loops, components and cycles in digraphs over Lambert's mapping. Ali and Mahmood introduced and investigated new numbers on Eular's totientnt function with applications in graph labeling [11, 12]. The structures of power digraphs together with their applications in computer science have been discussed in [13, 14]. To make this paper self readable, readers are suggested to read [15, 16, 17, 18, 19, 20, 21, 22, 23] as well.

2. Cyclic Vertices and Components

This section is devoted to investigate the components of the congruence $x^n \equiv y \pmod{m}$, for $n = 2$. We formulate an explicit formula to enumerate the cyclic vertices of the digraph $G(2, p^e)$, where p is prime and e is any positive exponent. By using mathematical induction the inequality given below can easily be shown.

Lemma 1. *For $e > 3,\ e \leq \beta(e-2),\ \beta = 2,\ 3$.*

Theorem 2. *In the graph $G(2, 3^e)$, the vertices $1 + 2^s 3^{e-1}$ form a cycle of length 2, for $s = 0,\ 1$ and $e > 1$.*

Proof. In the graph $G(2, 3^e)$, the vertices β_0 and β_1 construct a cycle of length 2 if and only if $\beta_0^2 \equiv \beta_1 \pmod{3^e}$ and $\beta_1^2 \equiv \beta_0 \pmod{3^e}$. This can be expressed as

$$(1+2^s3^{e-1})^2 = 1 + 2^{s+1}3^{e-1} + 2^{2s}3^{2e-2} \equiv 1 + 2^{s+1}3^{e-1} (\mathrm{mod} 3^e),\ s = 0, 1 \quad (2)$$

$$(1+2^2 3^{e-1})^2 = 1 + 2^4 3^{2e-2} + 2^3 3^{e-1} \pmod{3^e} \quad (3)$$

$$= 1 + (2+6)3^{e-1} + 2^4 3^{2e-2} \pmod{3^e}$$

$$= 1 + 2.3^{e-1} + 2.3^e + 2^4 3^{2(e-1)} \pmod{3^e}$$

$$\equiv 1 + 2.3^{e-1} \pmod{3^e}. \quad (4)$$

Hence, by using equation (3) and (4), we conclude that in the graph $G(2, 3^e)$ the vertices $1 + 2^e 3^{e-1}$ for $s = 0, 1$ and $e > 1$, form a cycle of length 2. □

Theorem 3. *In the graph $G(2, 3^e)$, the vertices $1 + 2^s 3^{e-2}$ form a cycle of length 6, for $s = 0,\ 1,\ 2,\ 3,\ 4,\ 5$ and $e > 2$.*

Proof. The graph $G(2, 3^e)$ and vertices $\beta_0,\ \beta_1,\ \beta_2,\ \beta_3,\ \beta_4,\ \beta_5$ form a cycle of length 6 if and only if $\beta_0^2 \equiv \beta_1 \pmod{3^e}$, $\beta_1^2 \equiv \beta_2 \pmod{3^e}$, $\beta_2^2 \equiv$

$\beta_3 \pmod{3^e}$, $\beta_3^2 \equiv \beta_4 \pmod{3^e}$, $\beta_4^2 \equiv \beta_5 \pmod{3^e}$, $\beta_5^2 \equiv \beta_0 \pmod{3^e}$. Now, for $s = 0,\ 1,\ 2,\ 3,\ 4,\ 5$ and $e > 2$.

$$\begin{aligned}(1+2^s3^{e-2})^2 &= 1+2^{2s}3^{2e-4}+2^{s+1}3^{e-2} \qquad (5)\\ 2^{2s}3^{2e-4} &\equiv 0 \pmod{3^e}\\ (1+2^s3^{e-2})^2 &\equiv 1+2^{s+1}3^{e-2} \pmod{3^e}. \qquad (6)\end{aligned}$$

We observe that

$$\begin{aligned}1+2^63^{e-2} &= 1+(1+7.3^2)3^{e-2}\\ &\equiv 1+3^{e-2} \pmod{3^e}. \qquad (7)\end{aligned}$$

Hence, by considering the equations (6) and (7), we conclude that in the graph $G(2,3^e)$, the vertices $1+2^s3^{e-2}$ for $s = 0,\ 1,\ 2,\ 3,\ 4,\ 5$ and $e > 3$ form a cycle of length 6. □

Corollary 2.1. *If the vertices $1+2^s3^{e-2}$ in $G(2,3^e)$ with $s = 0,\ 1,\ 2,\ 3,\ 4,\ 5$ and $e > 2$ form a cycle of length 6 then, the vertices $1+2^s3^{e-1}$ in $G(2,3^{e+1})$ with $s = 0,\ 1,\ 2,\ 3,\ 4,\ 5$ and $e > 2$ also give a cycle of length 6.*

The proof of this corollary is straightforward if we put $e = v+1$ and apply Theorem 3.

Theorem 4. [3] *Let q does not divide b and $b \neq \pm 1$, where $ord_q\ b = l$ and assume that q is an odd prime. Let t_0 be the largest integer such that $q^{t_0} \mid b^t - 1$. Then $ord_{q^t}\ b = l$ for $1 \leq t \leq t_0$ and $l.q^{t-t_0}$ for $t \geq t_0$*

Theorem 5. [15] *The digraph $G_1(m)$ contains a cycle of length l if and only if $l = ord_d\ k$ where $d|\lambda(m)$.*

Theorem 6. (1) *In the graph $G(2,3^e)$, the vertices $1+2^s3^{e-v-1}$ form a cycle of length 2.3^v, for $s = 0,1,2,3,\dots,2.3^v-1$, $e > 3$ and $v = 1,2,3,\dots,\ u$, where*

$$u = \begin{cases} 2 & \text{if } e = 4\\ \frac{e}{2}-1 & \text{for even } e \geq 5\\ \frac{e-1}{2} & \text{for odd } e \geq 5\end{cases}$$

(2) *In the graph $G(2,3^e)$, the vertices $1+2^{s+1}3^{e-v-1}$ form a cycle of length 2.3^v, for $u < v \leq e-2$ and $e > 4$.*

Proof. Firstly, we prove that in the graph $G(2,3^e)$ there exist cycles of length 2.3^e, where $0 \leq v \leq e-2$. Here, we represent the order of 2 modulo 3^v by $ord_{3^v}2$. Obviously, $ord_3 2 = 2$ and $ord_{3^2}\ 2 = 6$, then by applying Theorem 4, we have $e_0 = 1$, $d = 2$. Hence, $ord_{3^v}\ 2 = 2.3^{v-1}$. But the only divisor of $\phi(3^v)$ are $1,3,3^2,\dots 3^{v-1}$, where $ord_{3^{v-1}}\ 2 = 2.3^{v-2}$. So by applying Theorem

5, there exists a cycles of length 2.3^v, $0 \le v \le e-2$. Now, for $e > 4$, it is straightforward to observe that

$$3^e \mid 2^{2s}.3^{2(e-v-1)}. \tag{8}$$

By using the above result, the following equation

$$(1+2^s3^{e-v-1})^2 \equiv 1+2^{2s}3^{2(e-v-1)}+2^{s+1}3^{e-v-1}$$

can be expressed as

$$(1+2^s3^{e-v-1})^2 \equiv 1+2^{e+1}3^{e-v-1} \pmod{3^e}. \tag{9}$$

The proof is simple for $e = 4$. So, we examine the following two cases to complete the proof.

Case: (**a**) Assume that e is an even integer and by considering $u = \frac{e}{2}-1$, we find a cycle of length 2.3^v, provided $v = u$, then equation (9) becomes

$$(1+2^s3^{\frac{e-1}{2}})^2 \equiv 1+2^{s+1}3^{\frac{e-1}{2}} \pmod{3^e},\ s=0,1,2,3,\dots,2.3^u-1. \tag{10}$$

and if $s = 2.3^v-1 = 2.3^u-1$, then we get

$$\begin{aligned} 1+2^{s+1}3^{\frac{e-1}{2}} &= 1+4^{3^{\frac{e-1}{2}}}3^{\frac{e-1}{2}} && (11)\\ &= 1+(1+3)^{3^{\frac{e}{2}-1}}3^{\frac{e}{2}}\\ &= 1+(1+3.3^{\frac{e-1}{2}}+,\dots)3^{\frac{e-1}{2}}\\ &= 1+3^{\frac{e-1}{2}}+3^e+\dots \text{ terms involving } 3^e\\ &\equiv 1+3^{\frac{e-1}{2}} \pmod{3^e}. && (12) \end{aligned}$$

Case: (**b**) Now, we suppose that e is an odd integer. Then by definition $u = \frac{e-1}{2}$, we find a cycle of length 2.3^u. Again by equation (9), we get

$$(1+2^s3^{\frac{e}{2}})^2 \equiv 1+2^{s+1}3^{\frac{e}{2}} \pmod{3^e},\ s=0,1,2,3,\dots,2.3^v-1. \tag{13}$$

and if $s = 2.3^v-1 = 2.3^u-1$, then we have

$$\begin{aligned} (1+2^{s+1}3^{\frac{e}{2}})^2 &= 1+4^{3^{\frac{e}{2}-1}}3^{\frac{e}{2}}\\ &= 1+(1+3)^{3^{\frac{e}{2}-1}}3^{\frac{e}{2}}\\ &= 1+(1+3.3^{\frac{e}{2}}+,\dots)3^{\frac{e}{2}}\\ &= 1+3^{\frac{e}{2}}+3^e+\dots \text{ terms involving } 3^e.\\ &\equiv 1+3^{\frac{e}{2}} \pmod{3^e}. && (14) \end{aligned}$$

Let $\beta_0 = 1 + 2^0 3^{e-u-1}$, $\beta_1 = 1 + 2^1 3^{e-u-1}, \dots, \beta_{2.3^u-1} = 1 + 2^{2.3^u-1} 3^{e-u-1}$. Then equations (9), (12) and (14) implies that

$$\begin{aligned}
\beta_0^2 &\equiv \beta_1 \pmod{3^e}, \\
\beta^2 &\equiv a_2 \pmod{3^e}, \\
&\vdots \\
\beta_{2.3^u-1}^2 &\equiv \beta_o \pmod{3^e}.
\end{aligned}$$

which shows that the vertices $\beta_0, \beta_1 \dots, \beta_{2.3^u-1}$ form a cycle of length $2.3^u - 1$.

In a similar way we can prove part 2. □

Corollary 2.2. *In the graph $G(2, 3^e)$, the vertices $1 + 2^{s+1}3^{e-v-1}$ and $1 + 2^s 3^{e-v-1}$ are always at a cycle of length 2.3^v, for $s = 0, 1, 2, \dots, 2.3^v - 1$, $e > 2$ and $0 \leq v \leq e - 2$.*

Corollary 2.3. *In the graph $G(2, 3^e)$, the maximum possible length of any cycle is 2.3^{e-2}.*

Corollary 2.4. *In the digraph $G(2, 3^e)$, there are $e - 1$ non-isomorphic cycles of length > 1.*

In the digraph of $G(2, 3^e)$, the classification of non-cyclic vertices are given by the following theorems.

Theorem 7. (1) *In the digraph $G(2, 3^e)$, the vertices $-(2^{s+1}3^{e-v-1} + 1) + 3^e$ and $-(2^s 3^{e-v-1} + 1) + 3^e$ are non-cyclic vertices and always mapped on the cyclic vertices, for $s = 0, 1, 2, \dots, 2.3^v - 1$, $e > 2$.*
(2) *The vertices $1 + 3^{e-1}$, $2.3^{e-1} - 1$, $\pm(3^e + 1)$, ± 1 are mapped on $3^{e-1} + 1$, $2.3^{e-1} + 1, 3^e + 1$, 1, $e > 2$.*

Proof.
(1) The proof is simple. Since $(-(2^{s+1}3^{e-v-1} + 1) + 3^e)^2 \not\equiv -(2^{s+1}3^{e-v-1} + 1) \pmod{3^e}$. In fact the vertices $(1 + 2^{s+1}3^{e-v-1})$ are always mapped on cycle of length 2.3^v, for $s = 0, 1, \dots, 2.3^v - 1$. In similar way we prove for the vertices $-(1 + 2^s 3^{e-v-1}) + 3^e$.
(2) Now, $(2.3^{e-1} + 1)^2 = 4.3^{2(e-1)} + 1 - 4.3^{(e-1)} \equiv 1 - 3^{(e-1)} \pmod{3^e}$ this implies $(2.3^{e-1} + 1)$ mapped on $1 - 3^{(e-1)}$. Similarly, the vertices ± 1, $3^{e-1} - 1$, $\pm(1 + 3^e)$ are mapped on 1, $3^{e-1} + 1$, $1 + 3^e$.

□

The figure 2 depicted the Theorem 2.5, Corollary 2.2, 2.3, 2.4.

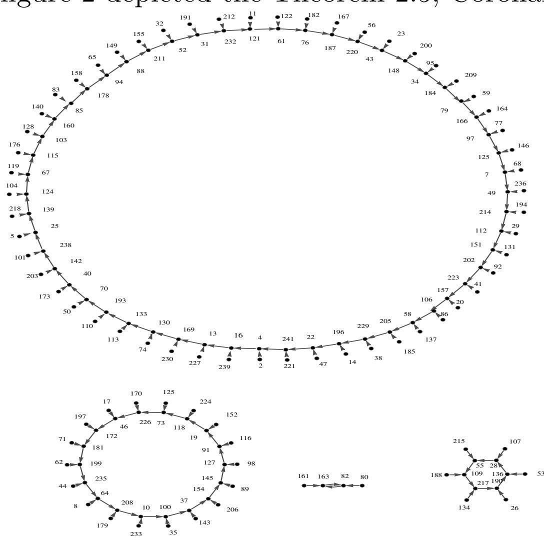

Figure 2: Shows the cycles $2,\ 2.3,\ 2.3^2,\ 2.3^3$ **of** $G(2,3^5)$

Theorem 8. *In the graph* $G(2,p^e)$*, the maximum possible length of a cycle is* $2d.p^v, v=0,1,2,...,e-1,$ *where* $d=$ $ord_p 2$ *and* $p \geq 5$ *be any prime.*

Theorem 9. *For any prime* $p \geq 5$ *and* d *be the positive divisor of* $\frac{\phi(p)}{2}$*. If* $2^d \equiv 1(\ mod\ p^e)$*. Then in the graph* $G(2,p^e)$*, the vertices* $1+2^s p^{e-v-1},\ e \geq 2,\ s=0,1,2,...,2dp^v-1$ *construct cycles of length* $2d.p^v, v=0,1,2,...,q,$ *where*

$$q=\begin{cases}\frac{e}{2}-1 & \textit{for even } e\\ \frac{e-3}{2} & \textit{for odd } e\end{cases}$$

Proof. We observe that

$$q=\begin{cases}\frac{e}{2}-1 & \text{for even } e\\ \frac{e-3}{2} & \text{for odd } e\end{cases}$$

for any v,

$$e-v-1\ =\begin{cases}\ \frac{e}{2}, & \text{for even } e\\ \ \frac{e+1}{2}, & \text{for odd } e\end{cases}$$

Then, $e \leq 2.\ (e-v-1)$, So, $p^e \mid p^{2(e-v-1)}$, where p be prime. This implies that, $p^{2(k-r-1)} \equiv 0\ (\ \text{mod}\ p^e)$. Then the equation $(1+2^s p^{e-v-1})^2 = 1+2^{s+1}p^{e-v-1}+2^{2s}p^{2(e-v-1)}$ reduced to this expression

$$(1+2^s p^{e-v-1})^2 \equiv 1+2^{s+1}p^{e-v-1}\ (\ \text{mod}\ p^e) \tag{15}$$

Moreover, if $2^d \equiv 1(\mod p^e)$ where, d be the positive divisor of $\frac{\phi(p)}{2}$. Then

$$2^{2dp^v} = (2^d)^{2p^v} \equiv (1)^{2p^v} \equiv 1(\mod p^e). \quad (16)$$

Now, we investigate about the cycle of maximum length $2dp^v$. Using equation (15),

$$\begin{aligned} (1+2^s p^{e-v-1})^2 &\equiv 1+2^{s+1}p^{e-v-1} \ (\mod p^e) \\ &\equiv 1+p^{e-v-1} \ (\mod p^e), \text{ using (16)} \\ \text{That is, } (1+2^{2dp^v-1}p^{e-v-1})^2 &\equiv 1+p^{e-v-1} \ (\mod p^e). \quad (17) \end{aligned}$$

Let $\beta_0 = 1+2^0 p^{e-v-1}$, $\beta_1 = 1+2^1 p^{e-v-1}$,..., $\beta_{2.dp^v-1} = 1+4^{2.dp^v-1}p^{e-v-1}$.

Then equations (15) and (17) gives that

$$\begin{aligned} \beta_0^2 &\equiv \beta_1 \ (\mod p^e) \\ \beta_1^2 &\equiv \beta_2 \ (\mod p^e) \\ &\vdots \\ \beta_{2dp^v-1}^2 &\equiv \beta_0 \ (\mod p^k). \end{aligned}$$

Hence, the vertices β_0, β_1,..., β_{2dp^v-1} construct a cycle of length $2dp^v$. □

The simple consequences of Theorem 8 gives the following corollary.

Corollary 2.5. *For any prime $p \geq 5$ and d be the positive divisor of $\frac{\phi(p)}{2}$. If $2^d \equiv 1(\mod p^e)$. Then, in the graph $G(2,p^e)$, $e \geq 2$, the sets of vertices $\{1+2^s p : 0 \leq s \leq 2d.p^{e-2}-1\}, \{1+2^s p : 0 \leq s \leq 2d.p^{e-3}-1\}, ..., \{1+2^s p : 0 \leq s \leq 2d-1\}$ construct cycles of length $2.d.p^{e-2}, 2.d.p^{e-3}$,..., and $2.d$, respectively.*

Now, we discuss the digraph $G_2(2,3^e)$ that contain the vertices which are not prime to 3 and established a tree with root at zero. We observe that if $e > 5$ is odd then the vertices $3\beta,\ \beta = 1,2,...,3^e-1$ has $3^{e-5}+1$ branch points with no root. In the graph $G_2(2,3^e)$, the vertices $(9\alpha)^2$ and 3^{e-1} for $\alpha = 1,4,9,...,(\frac{3^{e-4}-1}{2})^2$, where $gcd(\alpha,3)=1$, are called branch points. We also investigate that the vertices $3\beta,\ \beta = 1,2,3,...,3^e-1$ are mapped either on the children of branch point or any of the branch points of the graph. The vertices $3\beta,\ \beta = 1,2,...,3^e-1$ has 3^{e-5} branch points excluding root in the case of $e > 5$ is even. For $\alpha = 1,4,9,...,(\frac{3^{e-4}-1}{2})^2$, where $gcd(\alpha,3)=1$, the vertices $(9\alpha)^2$ are the branch points of the graph $G_2(2,3^e)$. In other words we see that the vertices $3\beta,\ \beta = 1,2,3,...,3^e-1$ are mapped on any of the branch point or children of the branch point.

Lemma 10. *In the digraph $G(2,p^e), e \geq 1$ there are two fixed points 0 and 1.*

Lemma 11. (1) *In the digraph $G(2,p^e)$, corresponding to all fixed points there are two possible non-isomorphic components.*

(2) *There are* $e+1$ *non-isomorphic components in the digraph* $G(2, 3^e)$, $e > 1$.

Proof. (1) In the graph $G(2, p^e)$, the vertices 1 and 0 are the only fixed points. Because $1 \not\equiv 0(\mod p^e)$, so the vertices 0 and 1 are not adjacent. Now, assume (if possible) that the vertices α and β of the components attaining the fixed points 0 and 1, respectively satisfied $\alpha^2 \equiv \beta \ (\mod p^e)$. This implies, α and β are the adjacent vertices. The integers $l_1, l_2, ..., l_s$ must exits in such a way that $\alpha^2 \equiv l_1p \ (\mod p^e)$, $(l_1p)^2 \equiv l_2p \ (\mod p^e)$,..., $(l_sp)^2 \equiv 0 \ (\mod p^e)$. Then obviously $\alpha^{2l} \equiv 0 \ (\mod p^e)$ for some integer l. In similar fashion there must exist integers $r_1, r_2, ..., r_l$ in such a way that $\beta^2 \equiv r_1 \ (\mod p^e)$ and $r_1^2 \equiv r_2 \ (\mod p^e)$ and so on $r_l^2 \equiv 1 \ (\mod p^e)$. Then , we obtain, $\alpha^{2r} \equiv 1 \ (\mod p^e)$, for some integer r. Let $k = Lcm(2l, 2r)$ and if $\alpha^2 \equiv \beta \ (\mod p^e)$, then $(\alpha^2)^k \equiv \beta^k \ (\mod p^e)$. This implies that $(\alpha^k)^2 \equiv \beta^k \ (\mod p^e)$ or $1 \equiv 0 \ (\mod p^e)$ which is impossible. Consequently, the disjoint components contain the vertices 0 and 1. Lastly, the number of incongruent solutions of the congruence $\alpha^2 \equiv 1 \ (\mod p^e)$ is known as the $deg(1)$. Thus $deg(1) \leq 2$ but $deg(0)$ is at least $p^{\frac{e}{2}-1}$ as $(lp)^2 \equiv 0 \ (\mod p^e)$. Hence, the components attaining the fixed points 0 and 1 are non-isomorphic.

(2) By Theorem 6, there are $e-1$ possible cycles except the fixed points. Also by using Theorem 5, a cycle is contains in each component, so in the digraph $G(2, 3^e)$ there are $e-1$ possible non-isomorphic components. Furthermore, by considering Lemma 11(i), in the graph $G(2, 3^e)$ corresponding to all fixed points there are 2 non-isomorphic components. Hence, there are $e - 1 + 2 = e + 1$ non-isomorphic components in the digraph $G(2, 3^e)$. □

Theorem 12. *In the graph* $G(2, p)$, *For any prime* $p \geq 5$ *such that* $\phi(p) = 2^s q'^e$, *where* $q' \geq 3$ *be any prime.*

(1) *If 3 divide* $\phi(p)$, *then there are* $e + 2$ *non-isomorphic components in* $G(2, p)$.
(2) *If 3 does not divide* $\phi(p)$, *then* $G(2, p)$ *have* $e - t_0 + 3$ *non-isomorphic components, where* t_0 *is the greatest integer such that* $2^\beta \equiv 1 \ (\mod q'^{t_0})$.

Proof. (1) If 3 divide $\phi(p)$ then $q' = 3$. As $\text{ord}_{3^e}2 = 2.3^{e-1} \mid \phi(p) = 2^s3^e$, by applying Theorem 5, we conclude that cycles of lengths $2, 2.3, 2.3^2, ..., 2.3^{e-1}$ are exist in the digraph $G(2, p)$. Thus, except the fixed points there exist e possible cycles. Also, by Lemma 11(1), corresponding to all fixed points there are 2 non-isomorphic possible components. Because each component has a cycle, we infer that when 3 divides $\phi(p)$, then there exist $e+2$ non-isomorphic components.

(2) Now, we assume that 3 does not divide $\phi(p)$, then $q' \geq 5$. Obviously, $\text{ord}_{q'}2 > 1$. As t_0 is the greatest integer such that $2^\beta \equiv 1 \ (\mod q'^{t_0})$, by applying Theorem 4, order of 2 modulo q'^e is β for $e = 1, 2, ..., t_0$ and $\beta q'^{e-t_0}$

for $e \geq t_0$. We conclude that cycles of lengths $\beta, \beta q', ..., \beta q'^{e-t_0}$ exist. So, except the fixed points there exist $e-t_0+1$ non-isomorphic cycles. By Lemma 11(i), corresponding to all fixed points there exist 2 possible non-isomorphic components. Hence, we conclude that there are $e-t_0+3$ cycles of different lengths and these cycles are non-isomorphic. Therefore, we find that when 3 divides $\phi(p)$, then there exist $e+2$ non-isomorphic components. If 3 does not divide $\phi(p)$, in the digraph $G(2,p)$, there are $e-t_0+3$ non-isomorphic components. □

Example 1. *If we choose* $p = 487$. *Then* $\phi(p) = 2.3^5$, *3 divide* $\phi(p)$. *Take* $q' = 3$. *As* $ord_{3^5}2 = 2.3^4 \mid \phi(p) = 2.3^5$, *by applying Theorem 5, we conclude that cycles of lengths* $2, 2.3, 2.3^2, 2.3^3, 2.3^4$ *exist in the digraph* $G(2,p)$. *Thus, other then fixed points there exist* 5 *possible cycles. Also, by Lemma 11(1), corresponding to all fixed points there are 2 non-isomorphic possible components. Because each component has a cycle, we infer that there exist* $5+2=7$ *non-isomorphic components when 3 divide* $\phi(p)$.

(2) Now, take $p = 5477$. *Then* $\phi(p) = 2^2(37)^2$. $q' = 37$. *Here,* $e = 2$ *and* $t_0 = 1$ *as* $ord_{q'}2 = 36$, $ord_{q'^2}2 = 1332 = 36q'$. *Thus, there exist 2 non-isomorphic components attaining cycles of lengths 36 and 1332. Also, by Lemma 11(1), corresponding to all fixed points there exist* 2 *non-isomorphic possible components. Because each component has a cycle. Hence, we infer that there exist 4 = 2 - 1 + 3 =* $e-t_0+3$ *possible non-isomorphic components.*

References

[1] Elahi, K., Ahmad, A., & Hasni, R. (2018). Construction algorithm for zero divisor graphs of finite commutative rings and their vertex-based eccentric topological indices. *Mathematics, 6*(12), 301.

[2] Lucheta, C., Miller, E., & Reiter, C. (1996). Digraphs from powers modulo p. *Fibonacci Quarterly, 34*, 226-238.

[3] Rogers, T. D. (1996). The graph of the square mapping on the prime fields. *Discrete Mathematics, 148*(1-3), 317-324.

[4] Wilson, B. (1998). Power digraphs modulo *n*. *Fibonacci Quart 36*, 229-239.

[5] Skowronek-Kaziw, J. (2009). Properties of digraphs connected with some congruence relations. *Czechoslovak mathematical journal, 59*(1), 39-49.

[6] Mahmood, M. K., & Ahmad, F. (2017). An Informal Enumeration of Squares of 2k using Rooted Trees Arising from Congruences. *Utilitas Mathematica, 105*, 41-51.

[7] Mahmood, M. K., & Ahmad, F. (2015). A Classification of Cyclic Nodes and Enumeration of Components of a Class of Discrete Graphs. Applied Mathematics & Information Sciences, 9(1), 103.

[8] Malik, M. A., & Mahmood, M. K. (2012). On simple graphs arising from exponential congruences. *Journal of Applied Mathematics*, 2012.

[9] Mahmood, M. K., & Anwar, L. (2016). Loops in Digraphs of Lambert Mapping Modulo Prime Powers: Enumerations and Applications. *Advances in Pure Mathematics, 6*(8), 564-570.

[10] Mahmood, M. K., & Anwar, L. The Iteration Digraphs of Lambert Map Over the Local Ring $\mathbb{Z}/p^k\mathbb{Z}$, *Iranian Journal of Mathematical Sciences and Informatics* (To Appear).

[11] Ali, S., & Mahmood, K. (2019). New numbers on euler's totient function with applications. *Journal of Mathematical Extension, 14*(2020) 61-83.

[12] Ali, S., Mahmood, M. K., & Mateen, M. H. (2019, November). New Labeling Algorithm on Various Classes of Graphs with Applications. In *2019 International Conference on Innovative Computing (ICIC)* (pp. 1-6). IEEE.

[13] Mateen, M. H., & Mahmood, M. K. (2019). Power digraphs associated with the congruence $x^n \equiv y \pmod{m}$. *Punjab Univ. j. math, 51*, 93-102.

[14] M. Mateen, M. H., Mahmood, M. K., & Ali, S. (2019, November). Importance of Power Digraph in Computer Science. In *2019 International Conference on Innovative Computing* (ICIC) (pp. 1-6). IEEE.

[15] Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1991). *An introduction to the theory of numbers.* John Wiley & Sons.

[16] Rosen, K. H. (2011). *Elementary number theory.* Pearson Education.

[17] Carmichael, R. D. (1910). Note on a new number theory function. *Bulletin of the American Mathematical Society, 16*(5), 232-238.

[18] Cao, X., Liu, S. X., Shum, K. P., & Yang, C. C. (Eds.). (1996). *Rings, groups, and algebras* (Vol. 181). CRC Press.

[19] Ali, U., Ahmad, Y., & Sardar, M. S. On 3-total edge product cordial labeling of tadpole, book and flower graphs. *Open Journal of Mathematical Sciences , 4*(1), 48-55.

[20] Tabassum, A., Umar, M. A., Perveen, M., & Raheem, A. (2020). Antimagicness of subdivided fans. *Open journal of mathematical sciences, 4*(1), 18-22.

[21] Shah, A., & Bokhary, S. A. U. H. (2019). On chromatic polynomial of certain families of dendrimer graphs. *Open journal of mathematical sciences, 3*(1), 404-416.

[22] Cary, M. (2019). A Linear Algorithm for Minimum Dominator Colorings of Orientations of Paths. Engineering and Appled Science Letter, 3(3), 10-14.

[23] Asif, F., Zahid, Z., & Zafar, S. (2020). Leap Zagreb and leap hyper-Zagreb indices of Jahangir and Jahangir derived graphs. *Engineering and Applied Science Letter, 3*(2), 1-8.