Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/090115

A Classification of Cyclic Nodes and Enumeration of Components of a Class of Discrete Graphs

M. Khalid Mahmood[1,*] *and Farooq Ahmad*[2]

[1] Department of Mathematics, University of the Punjab, Lahore, Pakistan
[2] Faculty of Information Technology, University of Central Punjab, Lahore, Pakistan

Received: 15 Mar. 2014, Revised: 15 Jun. 2014, Accepted: 16 Jun. 2014
Published online: 1 Jan. 2015

Abstract: Let Z_n be the ring of residue classes modulo n. Define $f : Z_n \mapsto Z_n$ by $f(x) = x^4$. Action of this map is studied by means of digraphs which produce an edge from the residue classes $\underline{a}$ to $\underline{b}$ if $f(\underline{a}) \equiv \underline{b}$. For every integer n, an explicit formula is given for the number of fixed points of f. It is shown that the graph $G(p^k),\ k \geq 1$ has four fixed points if and only if $3 \mid p-1$ and has two fixed points if and only if $3 \nmid p-1$. A classification of cyclic vertices of the graph $G(p^k)$ has been determined. A complete enumeration of non-isomorphic cycles and components of $G(p^k)$ has been explored.

Keywords: Congruences, Multiplicative Order, Cyclic Vertices, Components

1 Introduction

The notion of congruence is of great interest in number theory. A strong emphasis on modular arithmetic leads in a natural way to jump over many of new destinations especially in pure mathematics. It has become a useful device to solve most of the mathematical problems which are integral based. Use of modular arithmetic in studying discrete graphs and digraphs is becoming an increasingly useful device to explore a broad range of applications. Let f be any function assuming its values as the residues after division by an integer n. We can draw a graph that has the remainders as vertices when divided by n and a directed edge (a,b) if and only if $f(a) \equiv b(\mathrm{mod}\ n)$. For $f(x) = x^k$, the associated digraph is denoted by $G(n,k)$. The digraph of squaring modulo a prime p, has been studied in [2]. Earle L. Blanton [4], L. Somer and M.Křížek [7], L. Szalay [9], T.D. Rogers [12], Troy Vasiga [13] and Y. Meemark [14] have considered and investigated properties of a variety of digraphs corresponding to the congruence $a^2 \equiv b(\mathrm{mod}\ n)$. The conditions for regularity, semi regularity and symmetrically structured digraphs have been discussed in [1] and [8]. The structures of graphs of exponential congruences has been discussed in [10]. Though many fascinating features like regularity, semi-regularity and symmetry of such digraphs by means of sub-diagraphs have been explored, yet there are some topographies like classifications of vertices, number of all possible cycles of all lengths , number of components etc for which no explicit formula is present. In this piece of work, a complete characterization free from sub-diagraphs in terms of explicit formulas for the number of fixed points, classifications of cyclic vertices, number of non-isomorphic cycles and number of non-isomorphic components of the graph $G(4,p^k),\ k \geq 1$, where p is an odd prime, has been discussed in detail.

2 Preliminaries

The vertices $v_1, v_2, ..., v_{t-1}, v_t$ form a cycle of length t if and only if

$$\begin{aligned} v_1^4 &\equiv v_2 \ (\mathrm{mod}\ n) \\ v_2^4 &\equiv v_3 \ (\mathrm{mod}\ n) \\ &\vdots \\ v_t^4 &\equiv v_1 \ (\mathrm{mod}\ n) \end{aligned}$$

The graph $G(n)$ is said to be connected if for each vertex pair u and v, there exist some integral number m such that $u^{4m} \equiv v \ (\mathrm{mod}\ n)$. A maximal connected subgraph is termed as component, [5]. A vertex z is referred to be a fixed point if $z^4 \equiv z \ (\mathrm{mod}\ n)$.

* Corresponding author e-mail: khalid.math@pu.edu.pk

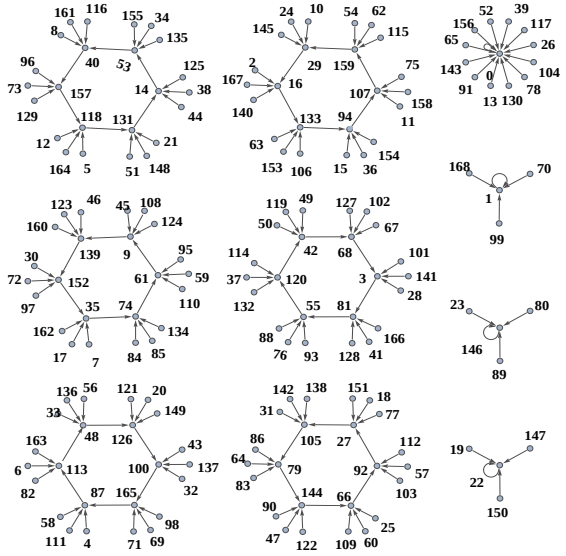

Fig. 1: G(169)

In Fig 1, the digraph $G(169)$ has ten components. Among these six are cyclic and four are the rooted trees. The graph has four fixed points. That is, the vertices which has self loops. These are 0, 1, 22 and 146. Precisely the graph $G(169)$ has three non-isomorphic components, one of which contains a non-isomorphic cycle of length six, one is a rooted tree with root at 0 and one with a non-zero fixed point (containing isomorphic cycles of length one). We first recall a few definitions and some previous results for use in the sequel.

Definition 2.1. [3] The function $\phi(n)$ is defined as the number of divisors d such that $d \mid n$, where $1 \leq d < n$ and $(d,n) = 1$. It is trivial that $\phi(1) = 1$, as $gcd(1,1) = 1$.

Theorem 2.2. [3] (Euler) Let a be any integer such that $(a,m) = 1$, where $m \geq 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

The following result can be derived using Theorem 2.2.

Theorem 2.3. [3] Let $k > 0$ and p be a prime, then

$$\phi(p^k) = p^k(1 - \frac{1}{p})$$

Definition 2.4. [3] Let $n > 1$ and gcd(a,n)=1. The order of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$. It is denoted as $ord_n a = k$.

Theorem 2.5. [6] Let $f(x)$ be a fixed polynomial with integral coefficients, and for any positive integer m let $N(m)$ denote the number of solutions of the congruence $f(x) \equiv 0 \pmod{m}$. If $m = m_1 m_2$ where $(m_1, m_2) = 1$, then $N(m) = N(m_1)N(m_2)$. If $m = \prod p^{\alpha}$ is the canonical factorization of m, then $N(m) = \prod N(p^{\alpha})$.

Theorem 2.6. [11] Consider an odd prime p, and let $p \nmid a \neq \pm 1$, where $\text{ord}_p a = d$. Let k_0 be the greatest integer such that $p^{k_0} \mid a^d - 1$. Then $\text{ord}_p^k a = d$ for $1 \leq k \leq k_0$ and dp^{k-k_0} for $k \geq k_0$.

Theorem 2.7. [11] Let $p, q,\ p \neq q$ be odd primes. Then,

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Theorem 2.8. [7] There exists a cycle of length t in $G_1(n)$ if and only if $t = \text{ord}_d k$ for some divisor d of $\lambda(n)$.

3 Basic Results and Fixed Points of the Map

A point x is said to be a fixed point of the map f if $f(x) \equiv x \pmod{p}$. To find the fixed point of the map, we give the following elementary result whose proof is simple and straight forward.

Lemma 3.1. Let $x \neq 0, 1$ be a fixed point of the mapping f over Z_p, then

(i) $x + x^2 \equiv p - 1 \pmod{p}$ (ii) $xx^2 \equiv 1 \pmod{p}$

The following result describes a relationship between non-trivial fixed points of the map f.

Theorem 3.2. Let $x \neq 0, 1$. Then, x is a fixed point of the mapping f over Z_p if and only if x^2 is a fixed point of f over Z_p.

Proof. Let $x \neq 0, 1$. Suppose x is a fixed point of f. That is, $x^4 \equiv x \pmod{p}$. Then, x^2 is a fixed point of f as

$$(x^2)^4 = (x^4)^2 \equiv x^2 (\text{mod } p).$$

Conversely, Suppose x^2 is a fixed point of f. That is,

$$(x^2)^4 \equiv x^2 (\text{mod } p). \text{ Or}$$

$$x^8 \equiv x^2 (\text{mod } p). \tag{1}$$

Now $x \not\equiv 0 \pmod{p}$ implies that $x^4 \not\equiv 0 \pmod{p}$.

$$\text{Let} \qquad x^4 \equiv \alpha \pmod{p}, \alpha \in Z_p, \alpha \neq 0. \tag{2}$$

Then by (1), $x^2 \equiv \alpha^2 \pmod{p}$. This further implies that

$$x^4 \equiv \alpha^4 (\text{mod } p). \tag{3}$$

Thus $p \mid x^2 + \alpha^2$ or $p \mid x + \alpha$ or $p \mid x - \alpha$. We will exhibit, the first two are not possible. This will complete the proof. Let $p \mid x^2 + \alpha^2$. That is, $x^2 + \alpha^2 \equiv 0 \pmod{p}$. Then by equation (2), $x^2 + x^8 \equiv 0 \pmod{p}$ or $x^8 \equiv -x^2 \pmod{p}$, a contradiction against (1). Otherwise, $x^2 \equiv -x^2 \pmod{p}$ yields that $2x^2 \equiv 0 \pmod{p}$. But p is an odd prime, so $x^2 \equiv 0 \pmod{p}$ reveals that $x \equiv 0 \pmod{p}$, a contradiction as $x \not\equiv 0 \pmod{p}$. Hence $p \mid x^2 + \alpha^2$ is not possible.

Now, let $p \mid x + \alpha$. That is, $x + \alpha \equiv 0 \pmod{p}$. Then by equation (2), $x + x^4 \equiv 0 \pmod{p}$. This gives, $x \equiv -1 \pmod{p}$ or $x^2 - x + 1 \equiv 0 \pmod{p}$. But $x \not\equiv -1 \pmod{p}$ since $(-1)^4 \not\equiv -1 \pmod{p}$. Thus $x^2 - x + 1 \equiv 0 \pmod{p}$. This further can be written as, $x + x^2 + 1 \equiv 2x \pmod{p}$. Also by Lemma 3.1, $x + x^2 + 1 \equiv 0 \pmod{p}$. Hence, $2x \equiv 0 \pmod{p}$. Since p is an odd prime, so $x \equiv 0 \pmod{p}$ yields a contradiction as $x \not\equiv 0 \pmod{p}$. Hence $p \nmid x + \alpha$. □

The following corollaries are the simple consequences of Theorem 3.2.

Corollary 3.3 Fixed points of $G(p^k)$ are the quadratic residues of p^k.

Corollary 3.4 The non zero fixed points of the graph $G(p^k),\ k \geq 1$ form a cyclic subgroup of the group Z_p^*.

Before giving the cardinality of fixed points of $G(n)$ for any integer n, we need the following important lemmas.

Lemma 3.5. The numbers 0, 1, $3^{k-1}+1$ and $2.3^{k-1}+1$ are the fixed points of the graph $G(3^k)$.

Proof. For $k=1$, it is easy to see that 0 and 1 are the only solutions of the congruence $x^4 \equiv x \pmod{3^k}$. Let $k>1$ and suppose x is a fixed point of $G(3^k),\ k>1$. Clearly 0 and 1 are the fixed points for $k>1$ as well. For the numbers $3^{k-1}+1$ and $2.3^{k-1}+1$, it is easy to see that

$$(3^{k-1}+1)^2+(3^{k-1}+1)+1 \equiv 3 \pmod{3^k} \text{ as } k>1 \quad (4)$$

Using (4), we get,

$$\begin{aligned}(3^{k-1}+1)^4-(3^{k-1}+1) &= 3^{k-1}(3^{k-1}+1)\{(3^{k-1}+1)^2 \\ &\quad +(3^{k-1}+1)+1)\} \\ &\equiv 3^{k-1}(3^{k-1}+1)(3) \pmod{3^k} \\ &\equiv 3^k(3^{k-1}+1) \pmod{3^k} \\ &\equiv 0 \pmod{3^k},\ k>1\end{aligned}$$

This shows that $3^{k-1}+1$ is a fixed point of the graph $G(3^k),\ k>1$. For the number $2.3^{k-1}+1$, we note that $(2.3^{k-1}+1)^2 \equiv 3^{k-1}+1 \pmod{3^k}$. Hence by Theorem 3.2, $2.3^{k-1}+1$ is a fixed point of the graph $G(3^k),\ k>1$. □

Lemma 3.6. Let $p>3$ be any prime. Then the graph $G(p^k),\ k \geq 1$ has four fixed points if and only if $3 \mid p-1$.

proof. Suppose $3 \mid p-1$. Let x be a fixed point of the graph $G(p^k),\ k \geq 1$. Then, $x^4 \equiv x \pmod{p^k}$ yields that $x^4 \equiv x \pmod{p}$. This gives, $p \mid x$ or $p \mid x-1$ or $p \mid x^2+x+1$. Thus the graph $G(p^k),\ k \geq 1$ has four fixed points if and only if the congruence $x^2+x+1 \equiv 0 \pmod{p}$ is solvable. Now $x^2+x+1 \equiv 0 \pmod{p}$ is solvable if and only if $y^2 \equiv -3 \pmod{p}$, where $2x \equiv y-1 \pmod{p}$ is solvable for y. By Theorem 2.7, it is easy to establish that -3 is a quadratic residue modulo p if and only if p is a quadratic residue modulo 3. But $3 \mid p-1$ implies that $p \equiv 1 \pmod 3$. This clearly shows that p is a quadratic residue modulo 3 and hence -3 is a quadratic residue modulo p. consequently, the congruence $y^2 \equiv -3 \pmod{p}$ is solvable. Thus the graph $G(p^k),\ k \geq 1$ has four fixed points if and only if $3 \mid p-1$. □

Lemma 3.7. Let p be a prime of the form $6k+1$. Then the numbers 0, 1, $\frac{(-3)^{\frac{3k+1}{2}}-1}{2}$ and $\frac{(-3)^{\frac{3k+1}{2}}+1}{2}$ are the fixed points of the of the graph $G(p^k)$.

Proof. Since $p \equiv 1 \pmod 6$, -3 is a quadratic residue of p. Then by Euler's Theorem, $(-3)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. This means that $(-3)^{3k+1} \equiv -3 \pmod{p}$. This can also be written as $((-3)^{\frac{3k+1}{2}})^2 \equiv -3 \pmod{p}$. This shows that $(-3)^{\frac{3k+1}{2}}$ is a solution of the congruence $y^2 \equiv -3 \pmod{p}$. Hence by Lemma 3.6, $\frac{(-3)^{\frac{3k+1}{2}}-1}{2}$ is a fixed point of the graph $G(p)$. Also by Theorem 3.2, $\frac{(-3)^{\frac{3k+1}{2}}+1}{2}$ is a fixed point since

$$\left(\frac{(-3)^{\frac{3k+1}{2}}-1}{2}\right)^2 = \frac{(-3)^{\frac{3k+1}{2}}+1}{2}. \quad \square$$

Lemma 3.8. Let $p>3$ be any prime. Then the graph $G(p^k),\ k \geq 1$ has two fixed points if and only if $3 \nmid p-1$.

Proof. Since $p \not\equiv 1 \pmod 3$, so p is not a quadratic residue modulo 3. Hence the congruence $x^2+x+1 \equiv 0 \pmod{p}$ is not solvable. Thus 0 and 1 are the only fixed points of $G(p^k),\ k \geq 1$. □

For any integer n. We define the functions $\xi(n)$ and $\omega(n)$ as

$$\xi(n) = \begin{cases} 0, & \text{if } 3 \nmid n \text{ or } 3 \,||\, n \\ 1, & \text{if } 3^k \mid n,\ k>1 \end{cases}$$

and

$$\omega(n) = \begin{cases} 0, & \text{if } 3 \nmid n \text{ or } 3^k \mid n,\ k>1 \\ -1, & \text{if } 3 \,||\, n \end{cases}$$

Theorem 3.9. Let $p_1^{k_1}p_2^{k_2}...p_r^{k_r}$ be the canonical representation of any integer n, where $p_1, p_2, ..., p_r$ are distinct odd primes. Let $L(n)$ denote the number of fixed points of the graph $G(n)$, then,

$$L(n) = \begin{cases} 2^{r+\xi(n)}, & \text{if } 3 \nmid p_i-1,\ 1 \leq i \leq r \\ 2^{2r+\omega(n)}, & \text{if } 3 \mid p_i-1,\ 1 \leq i \leq r \\ 2^{2r-t+\xi(n)}, & \text{if } 3 \nmid p_i-1,\ 1 \leq i \leq t \\ & \text{and } 3 \mid p_i-1,\ t+1 \leq i \leq r \end{cases}$$

Proof. To find the number $L(n)$, we need to count the number of solutions of the congruence $x^4 \equiv x \pmod{n}$. We note that the congruence $x^4 \equiv x \pmod{p_1^{k_1}p_2^{k_2}...p_r^{k_r}}$ is solvable if and only if $x^4 \equiv x \pmod{p_i^{k_i}}$ is solvable for each $i=1,2,...,r$. Let $3 \nmid p_i-1$ for each $i=1,2,...,r$, then by Lemma 3.8, $L(p_i^{k_i})=2$ for each i. Since $p_1<p_2<...<p_r$ are distinct primes, so by Theorem 2.5, $L(n)=2^r$. Now if $3 \mid p_i-1$ for each $i=1,2,...,r$, then by Lemma 3.6, $L(p_i^{k_i})=4$ for each i. Hence by Theorem 2.5, $L(n)=4^r$. Finally, without any loss, we assume that $3 \nmid p_i-1$ for each $i=1,2,...,t$, then $3 \mid p_i-1$ for each $i=t+1,t+2,...,r$. Hence by Lemmas 3.6, 3.8, $L(p_i^{k_i})=2$ for $i=1,2,...,t$ and $L(p_i^{k_i})=4$ for $i=t+1,t+2,...,r$. Thus again by Theorem 2.5, $L(n)=2^t4^{r-t}=2^{2r-t}$. Now we discuss the following three cases.

(1) Let $3 \nmid n$. Then by definition, $\xi(n)=\omega(n)=0$. Thus result is true in this case.

(2) Let $3 \,||\, n$. Then by definition $\xi(n)=0$ and $\omega(n)=-1$. Now since $3 \,||\, n$, so one of the $p_i^{k_i}=3$ for some ith factor of n. Without any loss, we let $p_1^{k_1}=3$. Then the condition $3 \mid p_i-1,\ 1\le i\le r$ must reduces to $3 \mid p_i-1,\ 2\le i\le r$. Thus in this case, we must get, $L(n)=2^{2r-1}=2^{2r+\omega(n)}$ when $3 \mid p_i-1,\ 2\le i\le r$. Therefore, we set $\xi(n)=0$ and $\omega(n)=-1$ to get the desired result.

(3) Let $3^k \mid n,\ k>1$. Then by definition $\xi(n)=1$ and $\omega(n)=0$. Now since $3^k \mid n,\ k>1$, so one of the $p_i^{k_i}=3^k,\ k>1$ for some ith factor of n. Without any loss, we let $p_1^{k_1}=3^k,\ k>1$. Then by Theorem 2.5 and by Lemma 3.5, we have,

$$L(n)=L(3^k)L(p_2^{k_2}...p_r^{k_r})=2^2L(p_2^{k_2}...p_r^{k_r}).$$

Now if $3 \nmid p_i-1,\ 2\le i\le r$, then $L(p_2^{k_2}...p_r^{k_r})=2^{r-1}$. Hence, $L(n)=2^2L(p_2^{k_2}...p_r^{k_r})=2^{r+1}=2^{r+\xi(n)}$. Thus in this case we set $\xi(n)=1$ and $\omega(n)=0$ to get the desired result. □

Remark 3.10. The number $L(n)$ is always even.

Corollary 3.11. Let p be an odd prime and $\alpha\neq 0,1$, a fixed point of the graph $G(p^k)$ such that $\alpha,\alpha^2\in Z_p=\{0,1,2,...,p-1\}$. Then $\alpha \mid p-1$ if and only if $4p=3+(2\alpha+1)^2$.

4 Classifications of Cyclic Vertices

In this section we present explicit formulas to enumerate cyclic vertices of the graph $G(p^k)$, where p is prime. The following inequalities can easily be proved using mathematical induction.

Lemma 4.1. For $k\ge 4,\ k\le\alpha(k-2),\ \alpha=2,3,4$

Theorem 4.2. The vertices $1+4^l3^{k-2}$ and $1+2.4^l3^{k-2}$ for $l=0,1,2$ form cycles of length 3 in the graph $G(3^k)$.

Proof. The vertices a_0,a_1 and a_2 form a cycle of length 3 in $G(3^k)$ if and only if $a_0^4\equiv a_1 \pmod{3^k}$, $a_1^4\equiv a_2 \pmod{3^k}$ and $a_2^4\equiv a_0 \pmod{3^k}$. Now,

$$(1+4^l3^{k-2})^4=1+4^{l+1}3^{k-2}+\sum_{\alpha=2}^{4}\binom{4}{\alpha}4^{\alpha l}3^{\alpha(k-2)} \quad (5)$$

Since $k\ge 4$, by Lemma 3.1, $k\le\alpha(k-2),\ \alpha=2,3,4$. Then, $3^k \mid 3^{\alpha(k-2)}$. Hence,

$$\sum_{\alpha=2}^{4}\binom{4}{\alpha}4^{\alpha l}3^{\alpha(k-2)}\equiv 0 \pmod{3^k}.$$

Putting in (5), we obtain,

$$(1+4^l3^{k-2})^4\equiv 1+4^{l+1}3^{k-2} \pmod{3^k},\ \ l=0,1,2 \quad (6)$$

Finally,we note that

$$\begin{aligned}1+4^33^{k-2}&=1+(1+3)^33^{k-2}\\&=1+(1+3.3+3.3^2+3^3)3^{k-2}\\&=1+3^{k-2}+3^k+2.3^{k+1}\\&\equiv 1+3^{k-2} \pmod{3^k} \quad (7)\end{aligned}$$

Equations (6) and (7) yields that the vertices $1+4^l3^{k-2}$ for $l=0,1,2$ form a cycle of length 3 in the graph $G(3^k),\ k\ge 4$. Similarly, it is easy to see that the vertices $1+2.4^l3^{k-2}$ for $l=0,1,2$ form a cycle of length 3 in the graph $G(3^k),\ k\ge 3$. □

Corollary 4.3. If the vertices $1+4^l3^{k-2}$ for $l=0,1,2$ are at a 3-cycle in $G(3^k),\ k\ge 3$ then $1+4^l3^{k-1}$ for $l=0,1,2$ are at a 3-cycle in $G(3^{k+1}),\ k\ge 3$.

The proof of above corollary is evident if we take $k=r+1$ and apply Theorem 4.2. However, the importance of this result is of great interest as we are lifting the vertices of a 3-cycle of a graph to a 3-cycle in its higher modulo graph.

Theorem 4.4. (i) The vertices $1+4^l3^{k-r-1}$ for $l=0,1,2,...,3^r-1$ form cycles of length $3^r,\ r=1,2,...,q$ in the graph $G(3^k),\ k\ge 4$, where

$$q=\begin{cases}2, & \text{if } k=4\\ \frac{k-1}{2}, & \text{if } k \text{ is odd, } k>4\\ \frac{k}{2}-1, & \text{if } k \text{ is even, } k>4\end{cases}$$

(ii) For $q<r\le k-2$, the vertices $1+2.4^l3^{k-r-1}$ form cycles of length 3^r in the graph $G(3^k),\ k\ge 5$.

Proof. First, we prove that there exist cycles of length $3^r,\ 0\le r\le k-2$ in the graph $G(3^k)$. Let's denote the order of 4 modulo 3^k by $\text{ord}_{3^r}4$. Clearly $\text{ord}_34=1$ and $\text{ord}_{3^2}4=3$. Then by Theorem 2.6, $k_0=1$. Hence $\text{ord}_{3^r}4=3^{r-1}$. But the only odd divisors of $\phi(3^r)=2*3^{r-1}$ are $1,3,3^2,...,3^{r-1}$, where, $\text{ord}_{3^{r-1}}4=3^{r-2}$. Thus by Theorem 2.8, there exist cycles of length $3^r,\ 0\le r\le k-2$. Next for $k>4$ and $r=1,2,...,q$, it is easy to see that

$$k\le\alpha(k-r-1),\ \text{where, } \alpha=3,4.$$

$$\text{Thus, } 3^k \mid 3^{\alpha(k-r-1)} \text{ for } \alpha=3,4.$$

Also for $\alpha=2$,

$$3^k \mid \binom{4}{2}3^{\alpha(k-r-1)}$$

This shows that

$$\binom{4}{\alpha}3^{\alpha(k-r-1)}\equiv 0 \pmod{3^k},\ \alpha=2,3,4$$

Then the following equation

$$(1+4^l3^{k-r-1})^4=1+4^{l+1}3^{k-r-1}+\sum_{\alpha=2}^{4}\binom{4}{\alpha}4^{\alpha l}3^{\alpha(k-r-1)}$$

reduces to

$$(1+4^l3^{k-r-1})^4\equiv 1+4^{l+1}3^{k-r-1} \pmod{3^k} \quad (8)$$

For $k=4$, proof is simple and straight forward. So we complete the proof in the following two cases.

Case (a). Let k be even. Then by definition of q, $q=\frac{k}{2}-1$. We discuss the cycle of length 3^q. In this case, $r=q$, then equation (8) becomes

$$(1+4^l3^{\frac{k}{2}})^4\equiv 1+4^{l+1}3^{\frac{k}{2}} \pmod{3^k},\ \ l=0,1,...,3^r-1 \quad (9)$$

Finally, if $l = 3^r - 1 = 3^q - 1$, where $q = \frac{k}{2} - 1$, then

$$\begin{aligned} 1+4^{l+1}3^{\frac{k}{2}} &= 1+(1+3)^{3^{\frac{k}{2}-1}}3^{\frac{k}{2}} \\ &= 1+(1+3.3^{\frac{k}{2}-1}+...)\,3^{\frac{k}{2}} \\ &= 1+3^{\frac{k}{2}}+3^k+ \text{ terms involving } 3^k \\ &\equiv 1+3^{\frac{k}{2}} \pmod{3^k} \end{aligned} \quad (10)$$

Case(b). Let k be odd. Then $q = \frac{k-1}{2}$. For a cycle of length 3^q. Again by equation (8), we obtain,

$$(1+4^l3^{\frac{k-1}{2}})^4 \equiv 1+4^{l+1}3^{\frac{k-1}{2}} (\text{mod} 3^k), l = 0,...,3^q-1 \quad (11)$$

Take $l = 3^q - 1$, then

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

Let $a_0 = 1 + 4^0 3^{k-q-1}$, $a_1 = 1 + 4^1 3^{k-q-1}$,..., $a_{3^q-1} = 1 + 4^{3^q-1}3^{k-q-1}$. Then equations (8), (10) and (12) implies that

$$\begin{aligned} a_0^4 &\equiv a_1 \pmod{3^k} \\ a_1^4 &\equiv a_2 \pmod{3^k} \\ &\vdots \\ a_{3^q-1}^4 &\equiv a_0 \pmod{3^k} \end{aligned}$$

This clearly shows that the vertices a_0, a_1,..., a_{3^q-1} form a cycle of length 3^q. The proof of part (ii) is similar. □

The below results can be proved using Theorem 4.4.

Corollary 4.5. The vertices $1 + 4^l3^{k-r-1}$ and $1 + 2.4^l3^{k-r-1}$ for $l = 0,1,2,...,3^r - 1$ are always at a cycle of length 3^r where, $1 \le r \le k-2$ in the graph $G(3^k)$, $k \ge 3$.

Corollary 4.6. There exist $k-2$ non-isomorphic cycles of length greater than one in $G(3^k)$.

Corollary 4.7. The maximum length of any cycle in $G(3^k)$ is 3^{k-2}.

The following theorem gives the classifications of non-cyclic vertices in the graph $G(3^k)$.

Theorem 4.8 (i) The vertices $3^k - (1+4^l3^{k-r-1})$ and $3^k - (1+2.4^l3^{k-r-1})$ for l= 0,1,2,...,$3^r - 1$ are the non-cycle vertices of the graph $G(3^k)$ and are always mapped on the cyclic vertices.

(ii) The vertices ± 1, $\pm(1+3^k)$ and $\pm(1+2.3^k)$ are mapped on 1, $1+3^k$ and $1+2.3^k$ respectively.

Proof.(i) This is simple since

$$(3^k - (1+4^l3^{k-r-1}))^4 \equiv 1+4^{l+1}3^{k-r-1} \pmod{3^k}$$

and

$$(1+4^{l+1}3^{k-r-1})^4 \not\equiv -(1+4^l3^{k-r-1}) \pmod{3^k}$$

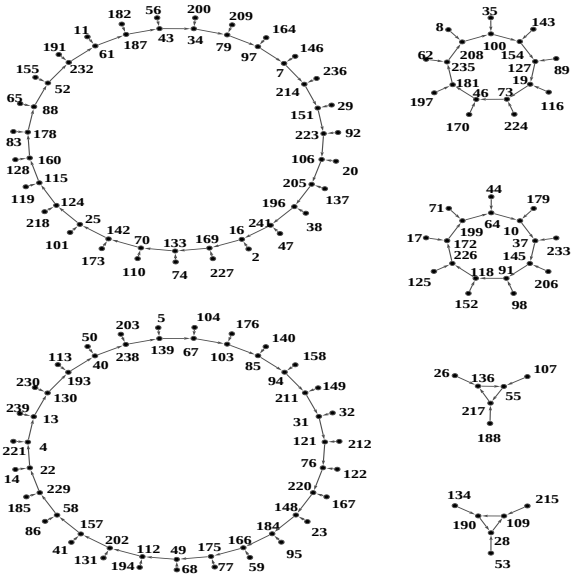

Fig. 2: shows the $3, 3^2$ and 3^3 Cycles of $G(3^5)$

where the vertices $1+4^l3^{k-r-1}$ for $l = 0,1,2,...,3^r-1$ are always at a cycle of length 3^r. The proof for the vertices $3^k - (1+2.4^l3^{k-r-1})$ is similar.

(ii) By Lemma 3.5, the vertices 1, $1+3^k$ and $1+2.3^k$ are the fixed points of $G(3^k)$, so they mapped on themselves. Since $(-1)^4 \equiv 1$. □

Finally we classify the vertices in $G(3^k)$ which are not prime to 3. We see that these vertices always form a tree in $G(3^k)$ with root at 0. First we note that the vertices 3α, $\alpha = 1,2,...,3^k-1$ has 3^{k-5} branch points except root. For $\beta = 1,2,4,...,\frac{3^{k-4}-1}{2}$, where $gcd(3,\beta) = 1$, the vertices $(3\beta)^4$ are the branch points of the graph $G(3^k)$. That is the vertices 3α, $\alpha = 1,2,...,3^k-1$ are mapped on any of the branch points. It can easily be seen that if 3α are mapped on $(3\beta)^4$, then by definition

$$\begin{aligned} (3\alpha)^4 &= (3\beta)^4 \pmod{3^k} \quad \text{gives,} \\ (\alpha-\beta)(\alpha+\beta)(\alpha^2+\beta^2) &\equiv 0 \pmod{3^{k-4}} \end{aligned}$$

But $\alpha^2+\beta^2 \equiv 0 \pmod{3^{k-4}}$ is not solvable for any α as proved in the proof of Theorem 3.2. Hence, the only possibilities are $\alpha = \pm\beta + 3^{k-4}t$. That is, $\alpha \equiv \beta \pmod{3^{k-4}}$ where $\beta = \pm1, \pm2, \pm4, ..., \pm\frac{3^{k-4}-1}{2}$, $k \ge 4$ and $gcd(3,\beta) = 1$. Note that there are 2.3^{k-5} residues namely $\pm1.3, \pm2.3, , ..., \pm3^{k-5}.3$ modulo 3^{k-4} which are divisible by 3. Thus to count the branch points excluding 0, we count the number of $\beta's$ such that $\beta = \pm1, \pm2, \pm4, ..., \pm\frac{3^{k-4}-1}{2}$, $k \ge 4$ in CRS modulo 3^{k-4}. Thus the total number of such $\beta's$ is $3^{k-4} - 2.3^{k-5} = 3^{k-5}$. This shows that there are 3^{k-5} branch points other than 0 in the tree component of the graph $G(3^k)$.

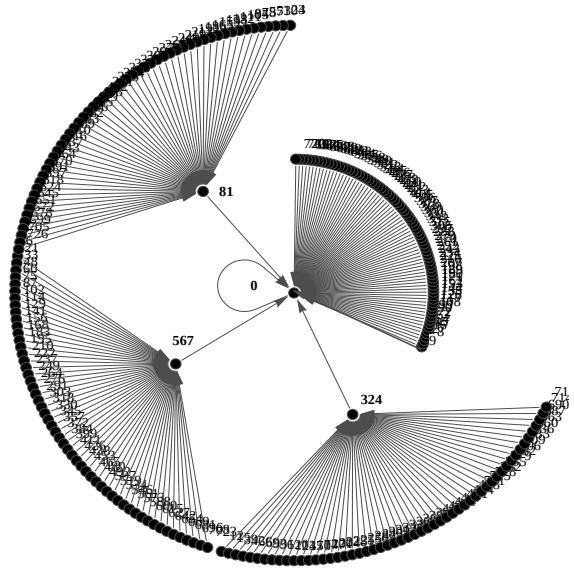

Fig. 3: shows the three branch points of the tree component of $G(3^6)$ with root at 0.

The above discussion leads to the following result.

Theorem 4.9. The undirected graph of the vertices 3α, $\alpha = 1,2,...,3^k-1$ form a tree with root at 0 and have 3^{k-5} branch points.

Espousing the steps elucidated above, we can cheer to extant the formula for finding the cycle vertices even to higher powers of any prime p. This can be entertained in Theorem 4.11. The proof of the following proposition is analogous to Theorem 2.6.

Proposition 4.10. Let $p > 3$ be any prime. The possible cycle length of the graph $G(p^k)$ is at most $d.p^r, r = 0,1,2,...,k-1$, where $\text{ord}_p 4 = d$.

Theorem 4.11. (i) Let $p > 3$ be any prime and $d > 0$ divides $\frac{\phi(p)}{2}$. If $4^d \equiv 1(\text{mod } p^k)$. Then the vertices $1 + 4^l p^{k-r-1}$, $k > 1$ form cycles of length $d.p^r, r = 0,1,2,...,\lfloor\frac{k}{2}\rfloor - 1$ in the graph $G(p^k)$ where, $l = 0,1,2,...,d.p^r - 1$.

(ii) For $\lfloor\frac{k}{2}\rfloor \le r \le k-2$, the vertices $1 + 2.4^l 3^{k-r-1}$ form cycles of length $d.p^r$ in the graph $G(p^k)$, $k \ge 5$.

Proof. We prove (i). The proof of (ii) can be derived in a similar fashion. Note that

$$\lfloor\frac{k}{2}\rfloor - 1 = \begin{cases} \frac{k-3}{2}, & \text{if } k \text{ is odd} \\ \frac{k}{2} - 1, & \text{if } k \text{ is even} \end{cases}$$

Now for any r, we have,

$$k - r - 1 = \begin{cases} k - \frac{k-3}{2} - 1, & \text{if } k \text{ is odd} \\ k - (\frac{k}{2} - 1) - 1, & \text{if } k \text{ is even} \end{cases}$$

$$= \begin{cases} \frac{k+1}{2}, & \text{if } k \text{ is odd} \\ \frac{k}{2}, & \text{if } k \text{ is even} \end{cases}$$

Then, $k \le \alpha(k-r-1), \alpha = 2,3,4$. So, $p^k \mid p^{\alpha(k-r-1)}$ for any prime p.

This means that, $p^{\alpha(k-r-1)} \equiv 0 \pmod{p^k}$. Then the following equation

$$(1+4^l p^{k-r-1})^4 = 1 + 4^{l+1} p^{k-r-1} + \sum_{\alpha=2}^{4} \binom{4}{\alpha} 4^{\alpha l} p^{\alpha(k-r-1)}$$

reduces to

$$(1+4^l p^{k-r-1})^4 \equiv 1 + 4^{l+1} p^{k-r-1} \pmod{p^k} \quad (13)$$

Also if $4^d \equiv 1(\text{mod } p^k)$ where, $d > 0$ divides $\frac{\phi(p)}{2}$. Then

$$4^{dp^r} = (4^d)^{p^r} \equiv (1)^{p^r} \equiv 1(\text{mod } p^k) \quad (14)$$

Finally we discuss a cycle of maximum length dp^r. By equation (13) and (14), we obtain

$$\begin{aligned}(1+4^{dp^r-1}p^{k-r-1})^4 &\equiv 1 + 4^{dp^r} p^{k-r-1} \pmod{p^k} \\ &\equiv 1 + p^{k-r-1} \pmod{p^k}\end{aligned}$$

That is, $(1+4^{dp^r-1}p^{k-r-1})^4 \equiv 1 + p^{k-r-1} \pmod{p^k}$ (15)

Let $a_0 = 1+4^0 p^{k-r-1}$, $a_1 = 1+4^1 p^{k-r-1}$,..., and $a_{dp^r-1} = 1+4^{dp^r-1}p^{k-r-1}$. Then equations (13) and (15) yields that

$$\begin{aligned} a_0^4 &\equiv a_1 \pmod{p^k} \\ a_1^4 &\equiv a_2 \pmod{p^k} \\ &\vdots \\ a_{dp^r-1}^4 &\equiv a_0 \pmod{p^k} \end{aligned}$$

This clearly shows that the vertices a_0, a_1,..., a_{dp^r-1} form a cycle of length dp^r. □

The below results can be proved using Theorem 4.11.

Corollary 4.12. Let p be any prime and $d > 0$ divides $\frac{\phi(p)}{2}$. If $4^d \equiv 1(\text{mod } p^k)$. Then for $k > 1$, the sets of vertices $\{1+4^l p : 0 \le l \le d.p^{k-2} - 1\}, \{1+4^l p : 0 \le l \le d.p^{k-3} - 1\}, ..., \{1+4^l p : 0 \le l \le d-1\}$ form cycles of length $d.p^{k-2}, d.p^{k-3}$,..., and d respectively in the graph $G(p^k)$.

Corollary 4.13. If $v_1, v_2, ..., v_r$ form a cycle of length r in $G(p^k)$ then for any integer s, the vertices $v_1^s, v_2^s, ..., v_r^s$ also form a cycle of length r in $G(p^k)$.

Proof. Since $(v_1^s)^4 = (v_1^4)^s \equiv v_2^s, (v_2^s)^4 = (v_2^4)^s \equiv v_3^s, ..., (v_r^s)^4 = (v_r^4)^s \equiv v_1^s$. Hence $v_1^s, v_2^s, ..., v_r^s$ form a cycle of length r in $G(p^k)$. □

Corollary 4.14. If $v_1, v_2, ..., v_r$ form a cycle of length r in $G(p)$ then $v_1, v_2, ..., v_r$ are the quadratic residues of p.

Proof. Since $(v_n^2)^2 \equiv v_1, (v_1^2)^2 \equiv v_2, ..., (v_{n-1}^2)^2 \equiv v_n$. Hence $v_1, v_2, ..., v_r$ are the quadratic residues of p. □

5 Enumeration of Cycles and Components

The vertices $v_1, v_2, ..., v_s$. constitutes a component $G(p^k)$ if for each i, $1 \le i \le s$, there exist some j, $1 \le j \le s$ such

that $v_i^4 \equiv v_j(\ mod\ p^k)$, for all $i \neq j$. It is well known that each component contains exactly one cycle in the graph $G(p^k),\ k \geq 1$ but yet it is desirable to know that how many components does $G(p^k),\ k \geq 1$ have? In this section we address this problem and enumerate number of cycles of all lengths, and hence number of non-isomorphic components of the graph $G(p^k),\ k \geq 1$. In the following theorems, we discuss the possible cases and enumerate the number of non-isomorphic components in detail. Before giving the detail of non-isomorphic components, we first give the following simple Lemma.

Lemma 5.1. (1) There are two non-isomorphic possible components corresponding to all fixed points of the graph $G(p^k)$.

(2) The graph $G(3^k), k > 1$ has k non-isomorphic components.

Proof. Let $3 \nmid p$, then by Lemma 3.8, the vertices 0 and 1 are the only fixed points of the graph $G(p^k)$. Since $0 \not\equiv 1(\text{mod } p^k)$, so 0 and 1 are not adjacent to each other. Let (if possible) x and y be the vertices of the components containing the fixed points 0 and 1 respectively such that $x^4 \equiv y(\text{mod } p^k)$. That is, x and y are the adjacent vertices. By definition, there must exist integers $t_1, t_2, ..., t_r$ such that $x^4 \equiv t_1 p(\text{mod } p^k)$, $(t_1 p)^4 \equiv t_2 p(\text{mod } p^k)$,..., $(t_r p)^4 \equiv 0(\text{mod } p^k)$. Then clearly $x^{4t} \equiv 0(\text{mod } p^k)$ for some integer t. Similarly there exist integers $s_1, s_2, ..., s_t$ such that $y^4 \equiv s_1(\text{mod } p^k)$ and $s_1^4 \equiv s_2(\text{mod } p^k)$ and so on $s_r^4 \equiv 1(\text{mod } p^k)$. Then for some integer s, we obtain, $y^{4s} \equiv 1(\text{mod } p^k)$. Let l be the least common multiple of the integers $4t$ and $4s$. Now if $x^4 \equiv y(\text{mod } p^k)$, then $(x^4)^l \equiv y^l(\text{mod } p^k)$. This means that $(x^l)^4 \equiv y^l(\text{mod } p^k)$ or $0 \equiv 1(\text{mod } p^k)$ which is not possible. Thus the fixed points 0 and 1 are the vertices of disjoint components. Finally, as $deg(1)$ is the number of incongruent solutions of the congruence $x^4 \equiv 1(mod\ p^k)$. Thus $deg(1) \leq 4$ whereas $deg(0)$ is at least $p^{\frac{k}{4}-1}$ as $(tp)^4 \equiv 0(mod\ p^k)$. Thus the components containing the fixed points 0 and 1 are the non-isomorphic components.

Again by Lemma 3.6, there are four fixed points of the graph $G(p^k)$ if and only if $3 \mid p$. Then by Lemma 3.7, if α is a non zero fixed point of the graph $G(p^k)$ then $1, \alpha$ and α^2 are the possible non zero fixed points of the graph $G(p^k)$. As α is a fixed point so, $(p^k - \alpha)^4 \equiv (-\alpha)^4 \equiv \alpha^4 \equiv \alpha\ (mod\ p^k)$. This shows that α and $p^k - \alpha$ are adjacent to each other. The rest of the proof can easily be completed adopting the steps explained above.

(2) By Theorem 4.4, there exist $k-2$ possible cycles of length greater then one. Also by Theorem 2.8, each component contains a cycle, so there exist $k-2$ non-isomorphic components in $G(3^k)$. Moreover by Theorem 5.1 (i), there exist two non-isomorphic components corresponding to all fixed points of the graph $G(3^k)$. Thus, $G(3^k)$ has $k-2+2 = k$ non-isomorphic components. □

Theorem 5.2. Let $p > 3$ be any prime such that $\phi(p) = 2^l q^r$, where q is an odd prime and $\text{ord}_q 4 = \alpha$. If $3 \mid \phi(p)$ then $G(p)$ contains $r+1$ non-isomorphic components. If $3 \nmid \phi(p)$ then $G(p)$ contains $r - k_0 + 3$ non-isomorphic components, where k_0 is the largest integer such that $4^\alpha \equiv 1\ (\text{mod } p^{k_0})$.

Proof. If $3 \mid \phi(p)$ then $q = 3$. As $\text{ord}_{3^r} 4 = 3^{r-1} \mid \phi(p) = 2^l 3^r$, so by Theorem 2.8, we infer that there exist cycles of lengths $3, 3^2, ..., 3^{r-1}$ in $G(p)$. That is, there exist $r-1$ possible cycles of length > 1. Also by Lemma 5.1 (i), there exist two non-isomorphic components corresponding to cycles of lengths one. Since each component contains a cycle, we conclude that there exist $r-1+2 = r+1$ non-isomorphic components when $3 \mid \phi(p)$. Next we suppose that $3 \nmid \phi(p)$, then $q > 3$. Clearly $\text{ord}_q 4 > 1$. Since k_0 is the largest integer such that $4^\alpha \equiv 1\ (\text{mod } p^{k_0})$, so by Theorem 2.6, order of 4 modulo q^r is α for $r = 1, 2, ..., k_0$ and αp^{r-k_0} for $r \geq k_0$. This shows that there exist cycles of lengths $\alpha, \alpha q, ..., \alpha q^{r-k_0}$. Thus there exist $r - k_0 + 1$ non-isomorphic cycles of length > 1. By Lemma 5.1, there exist two non-isomorphic components corresponding to cycles of lengths one. Hence, we find that there exist $r - k_0 + 3$ non-isomorphic cycles of different lengths. Consequently, if $3 \mid p$, then the graph $G(p)$ has $r - k_0 + 3$ non-isomorphic components. □

Example 5.3 (1) Take $p = 2431326594378257$. Then $\phi(p) = 2^4(3511)^4$. Take $q = 3511$. Here, $r = 4$ and $k_0 = 2$ as $\text{ord}_q 4 = \text{ord}_{q^2} 4 = 1755$, $\text{ord}_{q^3} 4 = 6161805 = 1755q$ and $\text{ord}_{q^4} 4 = 21634097355 = 1755q^2$. Thus there exist three non-isomorphic components containing cycles of lengths 1755, 6161805 and 21634097355. Since $3 \nmid \phi(p)$, so by Lemma 3.8, 0 and 1 are the only fixed points of the graph $G(p)$. By Lemma 5.1, there are two non-isomorphic components containing the fixed points 0 and 1. Hence, there are 5 = 4 - 2 + 3 = $r - k_0 + 3$ possible non-isomorphic components.

(2) Take $p = 1373$. Then $\phi(p) = 2^2 7^3$. Here, $q = 7$, $r = 3$ and $k_0 = 1$ as $\text{ord}_7 4 = 3$, $\text{ord}_{7^2} 4 = 21$ and $\text{ord}_{7^3} 4 = 147$. Thus there exist three non-isomorphic components containing cycles of lengths 3, 21 and 147 plus two non-isomorphic components containing corresponding to fixed points 0 and 1. Hence, there are 5 = 3 - 1 + 3 = $r - k_0 + 3$ possible non-isomorphic components in $G(p)$.

Theorem 5.4. Let $p > 3$ be any prime such that $\phi(p) = 2^l q_1^{k_1} q_2^{k_2} ... q_r^{k_r}$, where $l > 0, k_i \geq 1$ and $q_1, q_2, ..., q_r$ are distinct odd primes. Let $\text{ord}_{q_i} 4 = \alpha_i > 1$. Then,

(a) If α_i for each i, are pairwise relatively prime integers. Then the graph $G(p)$ has $2^r + 1$ non-isomorphic components.

(b) If $\alpha_i \mid \alpha_j$ for each $i < j$. Then there does not exist any cycle of length $\prod \alpha_j, j > 1$. In this case $G(p)$ has $r+2$ non-isomorphic components.

(c) Let $\alpha_i \nmid \alpha_j$ for all i and j. If $\text{lcm}(\alpha_i, \prod_{j \geq 1} \alpha_j) = l \neq \alpha_k$ for all $k = 1, 2, ..., r$. Then there exist a cycle of length l. In this case $G(p)$ has $2^r + 1$ non-isomorphic components as well.

Proof. (a) Let $\text{ord}_{q_i}4 = \alpha_i$ and $\text{ord}_{q_j}4 = \alpha_j$ where $(\alpha_i, \alpha_j) = 1$ for $i \neq j$. That is α_i and α_j are the least positive integers such that

$$4^{\alpha_i} \equiv 1 \pmod{q_i} \text{ and } 4^{\alpha_j} \equiv 1 \pmod{q_j} \quad (16)$$

Let t be a least positive integer such that

$$4^t \equiv 1 \pmod{q_i q_j} \quad (17)$$

Since $(q_i, q_j) = 1$, so by equation (16), it is easy to find that

$$4^{\alpha_i \alpha_j} \equiv 1 \pmod{q_i q_j} \quad (18)$$

But t is the least positive integer such that $4^t \equiv 1 \pmod{q_i q_j}$, we must get,

$$t \mid \alpha_i \alpha_j \quad (19)$$

By equation (17), we get

$$4^t \equiv 1 \pmod{q_i} \text{ and } 4^t \equiv 1 \pmod{q_j} \quad (20)$$

But by equation (16), $\alpha_i \mid t$ and $\alpha_j \mid t$ as α_i, α_j are least positive integers. Since $(\alpha_i, \alpha_j) = 1$, so

$$\alpha_i \alpha_j \mid t \quad (21)$$

By equations (19) and (21), we get $\alpha_i \alpha_j = t$. This shows that there exist a cycle of length $\alpha_i \alpha_j$ in $G(p)$. Now since each $\alpha_i > 1$ and are pairwise prime to each other, so there must exist a cycle of length $d = \prod \alpha_j$ for all j factors. As there are r different odd primes in $\phi(p)$. Therefore the total number of cycles of length greater then one must be

$$\binom{r}{1} + \binom{r}{2} + ... + \binom{r}{r} = 2^r - 1 \quad (22)$$

Moreover, by Lemma 5.1 (i), there exist two non-isomorphic components containing cycles of length one. Consequently, there exist $2^r - 1 + 2 = 2^r + 1$ components.

(b) On contrary we suppose that there exist a cycle of length $\alpha_i \alpha_j$ corresponding to some odd divisor $q_i q_j$. That is $\alpha_i \alpha_j$ is the least positive integer such that

$$4^{\alpha_i \alpha_j} \equiv 1 \pmod{q_i q_j} \quad (23)$$

Since $\alpha_i \mid \alpha_j$, so there exist some integer α such that $\alpha_j = \alpha \alpha_i$. Then by equation(16), $4^{\alpha_j} \equiv 1 \pmod{q_i q_j}$. Now by equation (18), $\alpha_i \alpha_j \mid \alpha_j$. Hence $\alpha_i \alpha_j = \alpha_j$. This shows that $\alpha_i = 1$, which is a contradiction as $\alpha_i > 1$ for each i. This clearly shows that there does not exist any cycle of length $\prod \alpha_j, j > 1$. Thus there exist only cycles of lengths α_i, $i = 1, 2, ..., r$. Using Lemma 5.1(i), the number of non-isomorphic components is

$$\binom{r}{1} + 2 = r + 2 \quad (24)$$

(c) Note that if $\alpha_i \mid t$ and $\alpha_j \mid t$ and $(\alpha_i, \alpha_j) \neq 1$, then this is false in general that $\alpha_i \alpha_j \mid t$. However, $\text{lcm}(\alpha_i, \alpha_j) \mid t$ is true in either case. That is, $l \mid t$. The rest of the proof is similar to part (a). □

Remark 5.5. In view of Theorem 5.2, we note that the number of non-isomorphic cycles of different lengths > 1 are actually the number of distinct orders modulo prime powers appearing in the canonical form of $\phi(p)$. Thus to count the non-isomorphic cycles of length > 1, our task is to count the number of distinct orders modulo all possible divisors of $\phi(p)$. For instance, if $\phi(p) = 2^l q_1^{r_1} q_2^{r_2}$, $r_1, r_2 > 1$. Suppose for each i, there does not exist any integer $k_{i_0} > 1$ such that $4^\alpha \equiv 1 \pmod{q_i^{k_{i_0}}}$. Then there must exist cycles of lengths $\alpha, \alpha q_1, \alpha q_1^2, ..., \alpha q_1^{r_1 - 1}$ and $\beta, \beta q_2, \beta q_2^2, ..., \beta q_2^{r_2 - 1}$ in $G(p)$ if $\text{ord}_{q_1}4 = \alpha$ and $\text{ord}_{q_2}4 = \beta$ provided $\alpha \neq \beta$. Finally, we need to know whether there exist some more orders modulo $q_1^i q_2^j$, for all i, j where, $1 \leq i \leq r_1 - 1$ and $1 \leq j \leq r_2 - 1$. Thus by Theorem 5.4 (c), we need to know all possible distinct lcm's of all possible products of integers $\alpha, \alpha q_1, \alpha q_1^2, ..., \alpha q_1^{r_1 - 1}$ and $\beta, \beta q_2, \beta q_2^2, ..., \beta q_2^{r_2 - 1}$ different from αq_1^i and βq_2^j for all i, j. To generalize the concept, we define the following notation.

Notation. Let $\alpha_i q_i^j$, where, $1 \leq i \leq r$ and $1 \leq j \leq k_i - 1$ be distinct integers. Let $l \neq \alpha_i q_i^j$ for all i, j. We denote $N(l)$ as the number of distinct lcm's of all possible products of the integers $\alpha_i q_i^j$ for all i, j.

Theorem 5.6. Let $q_1, q_2, ..., q_r$ and $p > 3$ be distinct odd primes such that $\phi(p) = 2^l q_1^{k_1} q_2^{k_2} ... q_r^{k_r}$, $l > 0$, where $\text{ord}_{q_i}4 = \alpha_i > 1$. Suppose for each i, there does not exist any integer $k_{i_0} > 1$ such that $4^\alpha \equiv 1 \pmod{q_i^{k_{i_0}}}$. Then the graph $G(p)$ has $\sum_{i=1}^r k_i + N(l) + 2$ non-isomorphic components, where $N(l)$ is defined above.

Proof. Let $\text{ord}_{q_i}4 = \alpha_i$. Since for each i, there does not exist any integer $k_{i_0} > 1$ such that $4^\alpha \equiv 1 \pmod{p^{k_{i_0}}}$. Then by Theorem 2.6, $\text{ord}_{q_i^{k_i}}4 = \alpha_i q_i^{k_i - 1}$. Thus there exist cycles of length $\alpha_i q_i^j$, $1 \leq j \leq k_i - 1$, where $i = 1, 2, ..., r$. That is, there exist $\sum_{i=1}^r k_i$ non-isomorphic components containing cycles of length $\alpha_i q_i^j$, $1 \leq j \leq k_i - 1$. Also if $\text{lcm}(\text{ord}_{q_m^u}4, \prod_{n \geq 1} \text{ord}_{q_n^v}4) = l \neq \alpha_i q_i^j$ for all i, j, where $1 \leq u \leq k_m - 1$ and $1 \leq v \leq k_n - 1$, then by Theorem 5.4 (c), there exist a cycle of length l in $G(p)$. Now if $N(l)$ is the number of distinct lcm's of all possible products of the orders $\alpha_i q_i^j$ for all i, j. Then there exist $\sum_{i=1}^r k_i + N(l)$ non-isomorphic cycles of length > 1. Using Lemma 5.1, we conclude that the graph $G(p)$ contains $\sum_{i=1}^r k_i + N(l) + 2$ non-isomorphic components. □

Theorem 5.7. Let $p > 3$ be any prime such that $\phi(p^k) = 2^l q^r p^{k-1}$, where q is an odd prime. Let $\text{ord}_q 4 = \alpha$ and $\text{ord}_p 4 = \beta$. Suppose there does not exist any integers $s_0, t_0 > 1$ such that $4^\alpha \equiv 1 \pmod{q^{s_0}}$ and $4^\beta \equiv 1 \pmod{p^{t_0}}$

(a) If $\alpha q^{i-1} \mid \beta$ for all $i = 1, 2, ..., r$. Then the graph $G(p^k)$ has $r + k + 1$ non-isomorphic components.

(b) If αq^{i-1} and βp^{j-2} are pairwise relatively prime integers for all $i = 1, 2, ..., r$ and $j = 2, 3, ..., k$. Then the

graph $G(p^k)$ has $(r+1)k+1$ non-isomorphic components.

Proof. Let $\text{ord}_q 4 = \alpha$ and $\text{ord}_p 4 = \beta$. Since there does not exist any integers $s_0, t_0 > 1$ such that $4^\alpha \equiv 1 \pmod{q^{s_0}}$ and $4^\beta \equiv 1 \pmod{p^{t_0}}$. Then by Theorem 2.6, we must obtain, $\text{ord}_{q^i} 4 = \alpha q^{i-1}$ and $\text{ord}_{p^{j-1}} 4 = \beta p^{j-2}$ for $i = 1,2,...,r$ and $j = 2,3,...,k$. This shows that there exist $r+k-1$ cycles of lengths $\alpha, \alpha q, \alpha q^2, ..., \alpha q^{r-1}, \beta, \beta p, \beta p^2, ..., \beta p^{k-3}$ and βp^{k-2}. Next we show that there does not exist any other cycle of length> 1. Let $t \neq \alpha\beta q^{i-1} p^{j-2}$ for all i, j. We suppose that there exist integers u and v such that $\text{ord}_{q^u p^v} 4 = t$, $1 \leq u \leq r-1$, $1 \leq v \leq k-2$. Then t is the least positive integer such that

$$4^t \equiv 1 \pmod{q^u p^v} \tag{25}$$

Since p and q are distinct primes, so we have

$$4^t \equiv 1 \pmod{q^u} \text{ and } 4^t \equiv 1 \pmod{p^v} \tag{26}$$

But $\text{ord}_{p^v} 4 = \beta p^{v-1,}$ so by (25), $\beta p^{v-1} \mid t$. Also $\text{ord}_{q^u} 4 = \alpha q^{u-1}$ and $\alpha q^{u-1} \mid \beta$, hence, $\text{ord}_{q^u p^v} 4 = \beta p^{v-1}$, since $\text{lcm}(\alpha q^{u-1}, \beta p^{v-1}) = \beta p^{v-1}$. As $\text{ord}_{q^u p^v} 4 = t$. This clearly shows that $t \mid \beta p^{v-1}$. Consequently $t = \beta p^{v-1}$, which is a contradiction as $t \neq \alpha\beta q^{i-1} p^{j-2}$ for all i, j. Thus the only cycles of lengths > 1 are of lengths $\alpha, \alpha q, \alpha q^2, ..., \alpha q^{r-1}, \beta, \beta p, \beta p^2, ..., \beta p^{k-3}$ and βp^{k-2}. Moreover there exist two non-isomorphic components containing cycles of length one. Thus in this case, graph $G(p^k)$ contains $r+k+1$ non-isomorphic components. For the proof of part (b), it is enough to show that there exist a cycle of length $\alpha\beta q^{u-1} p^{v-2}$, $1 \leq u \leq r$, $2 \leq v \leq k$. Since $\text{ord}_{q^u} 4 = \alpha q^{u-1}$ and $\text{ord}_{p^v} 4 = \beta p^{v-1}$. That is αq^{u-1} and βp^{v-1} are the least positive integers such that

$$4^{\alpha q^{u-1}} \equiv 1 \pmod{q^u} \text{ and } 4^{\beta p^{v-1}} \equiv 1 \pmod{p^v} \tag{27}$$

Since $(\alpha q^{i-1}, \beta p^{j-2}) = 1$, for all i, j so we deduce that

$$4^{\alpha\beta q^{i-1} p^{j-2}} \equiv 1 \pmod{q^u p^v} \tag{28}$$

then by equation (25),

$$t \mid \alpha\beta q^{i-1} p^{j-2} \tag{29}$$

Aa $\text{ord}_{q^u} 4 = \alpha q^{u-1}$ and $\text{ord}_{p^v} 4 = \beta p^{v-1}$, so (27) yields that, $\alpha q^{i-1} \mid t$ and $\beta p^{j-2} \mid t$. Since $(\alpha q^{i-1}, \beta p^{j-2}) = 1$, so

$$\alpha\beta q^{i-1} p^{j-2} \mid t \tag{30}$$

Hence, $\alpha\beta q^{i-1} p^{j-2} = t$. This shows that there exist a cycle of length $\alpha\beta q^{i-1} p^{j-2}$ for all i, j. Since there exist $r(k-1)$ such products, so we must get $r(k-1)$ more cycles of lengths > 1. Finally, the total number of non-isomorphic components is

$$r+k+1+r(k-1) = (r+1)k+1. \quad \square$$

The following corollary is a simple consequence of Theorem 5.7.

Corollary 5.8. If $\alpha q^{i-1} \nmid \beta p^{j-2}$ and $\beta p^{j-2} \nmid \alpha q^{i-1}$ for all $i = 1,2,...,r$ and $j = 2,3,...,k$. Then the graph $G(p^k)$ has $(r+1)k+1$ non-isomorphic components.

The below result is the more general case of Theorem 5.6, and can be established easily by adopting the technique explained in the proof of Theorems 5.6 and 5.7.

Theorem 5.9 Let $q_0 > 3$ be any prime and $q_1, q_2, ..., q_r$ be distinct odd primes such that $\phi(q_0^{k_0}) = 2^l q_1^{k_1} q_2^{k_2} ... q_r^{k_r} q_0^{k_0-1}$, $l > 0$. If $\text{ord}_{q_i} 4 = \alpha_i > 1$. Then the graph $G(p^k)$ has at most $\sum_{i=0}^{r} k_i + N(l) + 1$ non-isomorphic components, where $N(l)$ denote the number of distinct lcm's of all possible products of the integers $\alpha_i q_i^j$, where, $0 \leq i \leq r$ and $1 \leq j \leq k_i - 1$.

References

[1] B. Wilson, Power Digraphs Modulo *n*, Fibonacci Quart, **36**, 229-239 (1998).

[2] C. Lucheta, E. Miller and C. Reiter, Digraphs from Powers Modulo *p*, Fibonacci Quart, **34**, 226-239 (1996).

[3] D.M. Burton, Elementary Number Theory, McGraw-Hill, 2007.

[4] Earle L. Blanton, Jr., Spencer P. Hurd, and Judson S. McCranie, On a Digraph Defined by Squaring Modulo *n*, The Fibonacci Quarterly, **30**, 322-34 (1992).

[5] G. Chartrand and L. Lesnidk, Graphs and Digraphs, third edition, Chapman Hall, London, (1996).

[6] Ivan Nivan, Herbert S. Zuckerman, An introduction to the Theory of Numbers, John Wiley, Inc., (2005).

[7] L. Somer and M.Křížek, On a connection of number theory with graph theory, Czechoslovak Math. J., **54**, 465-485 (2004).

[8] L. Somer and M.Křížek, On symmetric digraphs of the congruence $x^k \equiv y \pmod{n}$. Discrete Math., **309** 1999-2009 (2009).

[9] L. Szalay, A discrete iteration in number theory. BDTF Tud. Közl., **8**, 71-91 (1992).

[10] M. Aslam Malik and M. Khalid Mahmood, On Simple Graphs Arising From Exponential Congruences, Journal of Applied Mathematics, **2012**, Article ID 292895, 10 pages. doi:10.1155/2012/292895.

[11] Melvyn B. Nathanson, Methods in Numbers Theory, Springer, **2005**.

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

[13] Troy Vasiga, Jeffrey Shallit, On the iteration of certain quadratic maps over GF(p), Discrete Mathematics **277**, 219-240 (2004).

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

M. Khalid Mahmood is Assistant Professor of Mathematics at University of the Punjab, Pakistan. He is pursuing his PhD degree in Mathematics at University of the Punjab, Pakistan. His research interests are in the areas of Pure Mathematics and Combinatorics. Specifically, his main interests are Number Theory, Graph Theory, Analysis and Algebra.

Farooq Ahmad is Associate Professor of Computer science at University of Central Punjab, Lahore, Pakistan. He received his PhD degree in Computer Science at HIT, China. He is referee and Editor of several international journals in the frame of Discrete Algorithms, Graph Theory and Combinatorics. He has published research articles in reputed international journals of Computer and engineering sciences. His main research interests are: Petrinets, Graph Theory, Discrete Mathematics and Computer Algorithms.