Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. 51(5)(2019) pp. 93-102

Power Digraphs Associated with the Congruence $x^n \equiv y \pmod{m}$

Muhammad Haris Mateen[1], Muhammad Khalid Mahmood[2]

[1,2] Department of Mathematics, University of Punjab, Lahore, Pakistan.
[1,2] Email: harism.math@gmail.com, khalid.math@pu.edu.pk

Received: 06 July, 2018 / Accepted: 17 January, 2019 / Published online: 05 March, 2019

Abstract: For any positive integer m, we assign a digraph $G(m)$ for which $\{0, 1, 2, 3, ..., m-1\}$ is the set of vertices and there is an edge from a vertex u to a vertex v if m divides $u^7 - v$. We enumerate the self and isolated loops and study the structures of this digraph for the numbers 2^r and 7^r, for every positive integer r. Further, we characterize the existence of cycles by employing Carmichael's Theorem. Also, we discuss the subdigraphs of proposed digraph induced by the vertices coprime to m and not coprime to m. Lastly, we characterize the regularity, semiregularity and results regarding components of these subdigraphs.

AMS (MOS) Subject Classification Codes: 35S29; 40S70; 25U09
Key Words: Digraphs, Loops, Cycles, Carmichael λ-function

1. Introduction

In recent years, modular arithmetic has become a useful tool in studying structures of discrete graphs based on congruence equations $x^k \equiv y \pmod{m}$. It has developed a strong relationship between number theory and graph theory. In this work, we also employ this device to define our digraph as follows.

Let m be a positive integer and $\overline{r}$ denote the set of all integers which leave remainder r when divided by m. Thus, $\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \ldots,\ \overline{m-1}\}$ is the set of complete residue classes of all integers when divided by m. We define a digraph $G(m)$ over these residue classes of m and build a directed edge from a vertex u to a vertex v if m divides $u^7 - v$. That is, $u^7 \equiv v \pmod{m}$. The vertices $u_1, u_2, ..., u_s$ will form a cycle of length s if

$$u_1^7 \equiv\ u_2 \pmod{m}, u_2^7 \equiv u_3 \pmod{m},\ \ldots,\ u_s^7 \equiv\ u_1 \pmod{m}.$$

A cycle of length one will be termed as a loop or a fixed point. A maximal connected subgraph of the corresponding undirected graph is called a component. The number of edges incident with u as the terminal vertex is called indegree of u and is assigned by $indeg(u)$ and the number of edges with u as the initial vertex is called outdegree and is denoted by $outdeg(u)$. Since the residue of a number modulo m is unique, we note that the outdegree

of each vertex is one.

A digraph is regular if the indegree and outdegree of every vertex are same. Thus, in our case, a digraph is regular if the indegree of every vertex is one (since the outdegree of each vertex is already one). Likewise, a digraph is semiregular if there exists an integer $m > 0$ such that each vertex has m or 0 indegree. Let $G_1(m)$ and $G_2(m)$ be subdigraphs of $G(m)$ induced by the vertices coprime to m and not coprime to m respectively. It is evident that $G_1(m)$ and $G_2(m)$ define a partition of $G(m)$. The digraph $G(19)$ is depicted in Fig.1 given below.

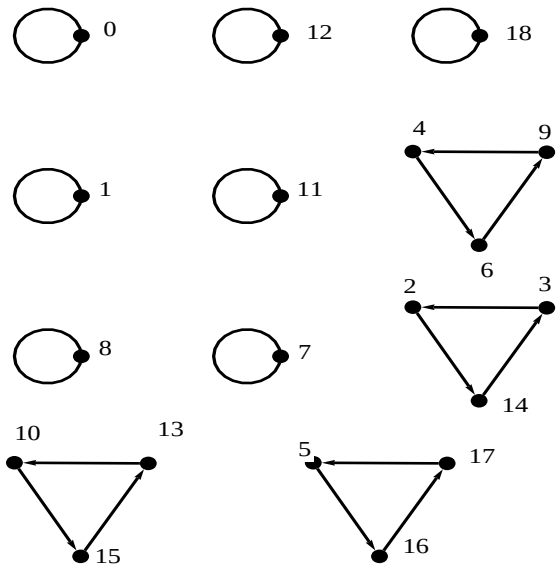

Figure 1. The digraph $G(19)$

In this paper, we extend the investigations of M. Rahmati [1] and J. Skowronek-Kaziow [2] for higher powers and propose some interesting characterizations to study its structures. It has been shown in [3], that each component of a power digraph modulo a prime number p contains a cycle. The digraphs associated with the congruence $a^2 \equiv b \pmod{m}$ have been considered and explored by T.D. Rogers [4], B. Wilson [5] and L. Somer and M.Křížek [6]. Also, explicit formulas for fixed points, cyclic subdigraphs and decomposition of components for the quadratic congruences have been explored in [3, 4, 5] and [6]. The symmetric structures (isomorphic components) and few previous results of these power digraphs have been generalized in [7] and [8]. The power digraphs associated with $x^4 \equiv y \pmod{m}$ and simple graphs associated with the exponential congruence $a^x \equiv y \pmod{m}$ have been discussed in [9] and [10] respectively. Many useful algebraic techniques to study combinatorial number theory, generalized Farmat's numbers, graph labeling and power digraphs via number theory have been proposed earlier in [11, 13, 14, 15]. We organize our paper as follows.

In Section 1, we define our digraph and few important definitions. Also, we discuss some previous work similar to our defined digraph. In Section 2, we give a generalized formula to enumerate fixed points of the digraph $G(m)$ for every positive integer m. In Section 3, we discuss the conditions of regularity and semiregularity of the subdigraph $G_1(m)$. We characterize that the subdigraph $G_1(m)$ is regular if and only if $7 \nmid \phi(m)$, where ϕ is the Euler's Phi function. In Section 4, we explore cyclic structures and components of $G_1(2^r)$ and $G_1(7^r)$, for all positive integers r. In Theorem 4.1, we show that there exists a cycle of length s in the digraph $G(m)$ if and only if $s = ord_d^7$ for some divisor $d > 0$ of $\lambda(m)$ (for $\lambda(m)$, see Definition 3.1 of [6] and we write $s = ord_d^7$ if s is the least positive integer such that $7^s \equiv 1 (\text{mod } d)$). Finally, we propose that the digraph $G_1(m)$ consists of six isomorphic trees. While, $G_2(m)$ is a tree with root 0 and indeg$(0) = 7^{k-\lceil \frac{k}{7} \rceil}$.

2. Fixed Points

Recall that the vertex associated with the number ρ is said to be fixed in $G(m)$ (or $G(m)$ has a loop at ρ) if $\rho^7 \equiv \rho \pmod{m}$. The fixed points of the digraph are actually the solutions of the congruence $x^7 \equiv x \pmod{m}$. Instead of m, we use its canonical representation as $2^\alpha 3^\beta p_1^{l_1} p_2^{l_2} \dots p_t^{l_t} q_1^{r_1} q_2^{r_2} \dots q_s^{r_s}$, where $p_i's$ and $q_j's$ are distinct odd primes such that $p_i \equiv 1 \pmod{6}$ and $q_j \equiv 5 \pmod{6}$. We will find solutions of $x^7 \equiv x$ modulo prime powers and then by using Chinese Remainder Theorem, we will count all solutions modulo m. Likewise a cubic congruence discussed in [2], we employ the solutions of the congruence, $x^7 \equiv y \pmod{m}$, and give the following simple and straightforward results.

Lemma 2.1. *Let m be any positive integer.*

1. *The numbers $0, \pm 1$ are the fixed points of $G(m)$.*
2. *If m is square free then, 0 is an isolated fixed point of $G(m)$ and conversely.*
3. *For any vertices α and β in $G(m)$, (α, β) is an edge in $G(m)$ if and only if $(-\alpha, -\beta)$ is an edge in $G(m)$.*
4. *A number r is an isolated fixed point only if $-r$ is an isolated fixed point and conversely.*
5. *Let k ba any odd integer. A number r is at some k-cycle only if $-r$ is at k-cycle and conversely.*

Proof. (1) Note that, $x^7 \equiv x \pmod{m}$, for $x = 0, \pm 1$ is trivially hold.

(2) Suppose 0 is isolated and $p^2 t = m$ for some integer t and p is prime. But then $(pt)^7 = p^2 t p^5 t^6 = m p^5 t^6 \equiv 0 \pmod{m}$. This shows the vertex pt is adjacent to 0 as well, which is a contradiction against the fact that 0 was isolated. Thus m is square free. Conversely, let m be square free and suppose α is any vertex such that $\alpha^7 \equiv 0 \pmod{m}$. Then, $m \mid \alpha^7$. Since m is square free, so $m \mid \alpha^7$ gives $m \mid \alpha$. Equivalently, $\alpha \equiv 0 \pmod{m}$. Thus, 0 is isolated.

(3) Since $(-\alpha)^7 \equiv -\alpha^7 \pmod{m}$. Thus $\alpha^7 \equiv \beta \pmod{m}$ if and only if $(-\alpha)^7 \equiv -\beta \pmod{m}$.

(4) Using (3), $m | \alpha^7$ if and only if $m | -\alpha^7$. Equivalently, $m \nmid \alpha^7$ if and only if $m \nmid -\alpha^7$.

(5) If a number r is at some k-cycle, then k is the least positive integer such that $(r^7)^k \equiv r \pmod{m}$. But then for the least positive integer k, we see that $(-r^7)^k = ((-r)^k)^7 \equiv -r \pmod{m}$, as k is odd. This shows that $-r$ is at k-cycle as well.

□

In the following theorem, we enumerate fixed points of the digraph $G(m)$.

Theorem 2.2. *If $L(m)$ denote the number of fixed point of $G(m)$, where $m = 2^{\alpha}3^{\beta}p_1^{l_1}p_2^{l_2}\dots p_t^{l_t}q_1^{r_1}q_2^{r_2}\dots q_s^{r_s}$, provided $p_i's$ and $q_j's$ are distinct odd primes with $p_i \equiv 1 \pmod 6$ and $q_j \equiv 5 \pmod 6$. Then,*

$$L(m) = \left\{ \begin{array}{ll} 7^{\,t} \times 3^{\,s} & if\ \alpha = 0,\ \beta = 0 \\ 2 \times 7^{\,t} \times 3^{\,s} & if\ \alpha = 1,\ \beta = 0 \\ 2 \times 7^{\,t} \times 3^{\,s+1} & if\ \alpha = 1,\ \beta = 1 \\ 2 \times 7^{\,t+1} \times 3^{\,s} & if\ \alpha = 1,\ \beta > 1 \\ 7^{\,t} \times 3^{\,s+1} & if\ \alpha = 2,\ \beta = 0 \\ 7^{\,t} \times 3^{\,s+2} & if\ \alpha = 2,\ \beta = 1 \\ 7^{\,t+1} \times 3^{\,s+1} & if\ \alpha = 2,\ \beta > 1 \\ 5 \times 7^{\,t} \times 3^{\,s} & if\ \alpha \geq 3,\ \beta = 0 \\ 5 \times 7^{\,t} \times 3^{\,s+1} & if\ \alpha \geq 3,\ \beta = 1 \\ 5 \times 7^{\,t+1} \times 3^{\,s} & if\ \alpha \geq 3,\ \beta > 1 \end{array} \right\}$$

Proof. By Corollary 2.42 [12, see page 104], it is clear that there are exactly 7 solutions if $m_i = p_i^{l_i}$, with $p_i \equiv 1 \pmod 6$ and $p_i's$ are odd primes. Hence, by Chines Remainder Theorem, there are exactly 7^t solutions of the congruence $x^7 \equiv x \pmod{\prod_{i=1}^{t} p_i^{l_i}}$. Again by Corollary 2.42 [12], there must be exactly 3 solutions if $m_i = q_j^{r_j}$, with $q_j \equiv 5 \pmod 6$ and $q_j's$ are odd primes. Hence, by Chines Remainder Theorem, there are exactly 3^s solutions of the congruence $x^7 \equiv x \pmod{\prod_{i=1}^{s} q_j^{r_j}}$. Moreover, we see that the congruence $x^7 \equiv x \pmod{2^{\alpha}}$ has 2, 3 and 5 for $\alpha = 1, 2, 3$ and has 5 solutions for $\alpha \geq 3$. Particularly, these are $0,\ 1,\ 2^{m-1}-1,\ 2^{m-1}+1$, and $m-1$. Similarly, there are three solutions for the congruence $x^7 \equiv x \pmod{3^{\beta}}$ for $\beta = 1$ and has 7 solutions for $\beta \geq 2$. Particularly, these are $0,\ 1,\ 3^{\beta-1}-1,\ 3^{\beta-1}+1,\ 3^{\beta}-3^{\beta-1}-1$, and $3^{\beta}-3^{\beta-1}+1$. Now take $m = 2^{\alpha}3^{\beta}m_1m_2$, where $m_1 = \prod_{i=1}^{t} p_i^{l_i}$ and $m_2 = \prod_{i=1}^{s} q_j^{r_j}$. Finally, we discuss the cases separately and apply Chines Remainder Theorem again to establish our claim. For instance, if $\alpha = 1 = \beta$, then there must be $2 \times 3 \times 7^t \times 3^s = 2 \times 7^t \times 3^{s+1}$ solutions in this case. The rest of the cases can be dealt with a similar technique. □

3. Regularity and Semiregularity

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

Lemma 3.1. *The digraph $G_1(m)$ is regular if and only if $7 \nmid \phi(m)$, where ϕ is the Euler's function.*

Proof. Regularity of $G_1(m)$ yields that the indeg$(u) = 1$ for every vertex u in $G_1(m)$. This means that $x^7 \equiv u \pmod m$ has a unique solution. Without any loss, assume $u \equiv 1 \pmod m$ and let α be the unique solution of the congruence $x^7 \equiv 1 \pmod m$. That is, $\alpha^7 \equiv 1 \pmod m$. Now, if $7 \mid \phi(m)$ then $\phi(m) = 7t$ for some integer t. Note that, $t = 1$ is impossible as $\phi(m)$ is always even. Also by Euler's Theorem, $\alpha^{\phi(m)} \equiv 1 \pmod m$ as

$(\alpha,\ m) = 1$ (by definition of $G_1(m)$). Then, $\alpha^{7t} \equiv 1 \pmod m$ or $(\alpha^t)^7 \equiv 1 \pmod m$. This shows that $\alpha^t,\ t > 1$ is another solution of $x^7 \equiv 1 \pmod m$. This means that $indeg(1) = 2$, a contradiction against the fact that $G_1(m)$ was regular. Therefore $7 \nmid \phi(m)$. Conversely, let $7 \nmid \phi(m)$ and we suppose that $G_1(m)$ is not regular. Then there must be at least one vertex β such that $indeg(\beta) > 1$. For the sake of convenience, take $\beta = 1$ with $indeg(\beta) = 2$. This means that $x^7 \equiv 1 \pmod m$ has two solutions. Let these be β and $\beta^t,\ t > 1$. Then, $\beta^7 \equiv 1 \pmod m$ and $\beta^{7t} \equiv 1 \pmod m$. But, $\beta^{\phi(m)} \equiv 1 \pmod m$. Hence, we deduce that either $\phi(m) = 7$ or $\phi(m) = 7t$. As $\phi(m)$ is always even, so $\phi(m) = 7t$. That is, $7 \mid \phi(m)$, a contradiction. This completes the proof. □

Lemma 3.2. *Let m be a square free positive integer. The digraph $G(m)$ is cyclic if and only if $7 \nmid \phi(m)$.*

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, $G_1(m)$ is cyclic if and only if $7 \nmid \phi(m)$. For $G_2(m)$, suppose $7 \nmid \phi(m)$ and let α be any vertex in $G_2(m)$. Let p be an odd prime such that $p \mid gcd(\alpha, m)$. Then there exists integers r and s such that $\alpha = rp$ and $m = ps$ with $gcd(r, s) = 1$, where gcd stands for greatest common divisor. Now if β is the solution of the congruence $x^7 \equiv \alpha \pmod m$, then $\beta^7 \equiv \alpha \pmod m$ yields that $\beta^7 = \alpha + mt$ for some integer t. But then $\beta^7 = rp + spt$. Consequently, $p \mid \beta$ such that $p \mid gcd(\alpha, m)$. This means that $\beta^7 \equiv \alpha \equiv 0 \pmod p$. Thus we conclude that a number β exists such that it is a solution of $x^7 \equiv \alpha \pmod m$. Next we show that this solution is unique modulo m. Since $7 \nmid \phi(m)$, so $gcd(7, \phi(p)) = 1$. Then the linear congruence $7y \equiv 1 \pmod{p-1}$ has a unique solution in y. Finally, we put $\beta \equiv \alpha^y \pmod p$ to get $\beta^7 \equiv \alpha^{7y} \equiv a \pmod p$. By Chines Reminder Theorem, we get that β is a unique solution of $x^7 \equiv \alpha \pmod m$. Thus, indegree of this arbitrary vertex is one. This certainly implies that every vertex is either a loop (a cycle of length one) or is at some cycle. The converse is a direct consequence of Lemma 1.2. □

For further results on regularity and semi-regularity, we define a function η as,

$$\eta(m) = \begin{cases} s+1, & if\ 7^{\,2} | m \\ s, & if\ 7^{\,2} \nmid m \end{cases}$$

where s is the number distinct prime divisors of m of the type $7m + 1$. In the following theorem, we characterize the semiregularity of $G_1(m)$.

Theorem 3.3. *The digraph $G_1(m)$ is semiregular if and only if $7|\phi(m)$. Also the indegrees in $G_1(m)$ are either $7^{\,\eta(m)}$ or zero.*

Proof. By definition of $G_1(m)$, it is evident that $\alpha^{\phi(m)} \equiv 1 \pmod m$ for each vertex α in $G_1(m)$. This means that the indegrees of the vertices of $G_1(m)$ are same. For sake of convenience, we just count the indegrees of 1. Let p be an odd prime and r be any positive integer. Then we see that, $(7^{r-1} + 1)^7 \equiv 1 \pmod{7^r}$. Likewise, we see that the numbers, $2 \times 7^{r-1} + 1, 3 \times 7^{r-1} + 1, 4 \times 7^{r-1} + 1, 5 \times 7^{r-1} + 1, 6 \times 7^{r-1} + 1, 7 \times 7^{r-1} + 1$ also satisfies the congruence, $x^7 \equiv 1 \pmod{7^r}$. While modulo p^r, there are always 7 solutions whenever $p \equiv 1 \pmod 7$ and there is a trivial solution if $p \not\equiv 1 \pmod 7$ (for detail see [12], page 104). Using the canonical representation of m into odd primes and Chinese Remainder Theorem, simultaneously, we must get that $\alpha^7 \equiv 1 \pmod m$ either have $7^{\,\eta(m)}$

solutions or have no solution for each vertex α in $G_1(m)$. On the other hand, we let $G_1(m)$ is semiregular and indeg $\alpha = 7^{\eta(m)}$ for $\alpha \in G_1(m)$. This means that $\alpha^7 \equiv 1 \pmod{m}$. Using multiplicative order and Euler's Theorem for α, we deduce that $7 \mid \phi(m)$. □

4. Enumeration of Components

The vertices $v_1, v_2,\ v_3,\ \ldots\ v_t$, compose a component $G(p)$ if for each $i, 1 \leq i \leq t$, there exists some $j,\ 1 \leq j \leq t$, such that $v_i^7 \equiv v_j^7 \pmod{p}$, for all $i \neq j$. By [3], it has been established that each component of such digraphs must have exactly one cycle. While the enumeration of components is still under question. From the following results, we discuss and enumerate the number of cycles of different lengths and components up to isomorphism. The following theorem also validates a similar result given in [6] for quadratic congruences.

Theorem 4.1. *There exists a cycle of length s in $G(m),\ m \geq 3$ if and only if s is the least positive integer such that $7^s \equiv 1$ (mod d), where $d \mid \lambda(m)$ and $d > 0$.*

Proof. Suppose there exists a cycle of length s in $G(m)$, for any integer $m \geq 3$. Let v be any vertex on this cycle. Then s is the least positive integer such that $v^{7^s} \equiv v \pmod{m}$. This means that s is the least positive integer for which $v(v^{7^s-1}-1) \equiv 0 \pmod{m}$. Clearly, gcd $(v, v^{7^s} - 1)$. Thus if we let $m_1 = gcd(v, m)$ and $m_2 = \frac{m}{m_1}$, then s would be the least positive integer such that $v \equiv 0 \pmod{m_1}$ and $v^{7^s-1} \equiv 1 \pmod{m_2}$. Applying Chines Reminder Theorem, we must get some integral solution y such that $y \equiv 1 \pmod{m_1}$ and $y \equiv a \pmod{m_2}$. Consequently, s is the least positive integer such that $y^{7^s-1} \equiv 1\ (mod\ m_1)$ and $y^{7^s-1} \equiv 1 \pmod{m_2}$. Both yields that, $y^{7^s-1} \equiv 1 \pmod{m}$. Let $d = ord_y^m$. Then, $y \equiv 1 \pmod{m_1}$ enforce that s is the least positive integer such that $7^s \equiv 1 \pmod{d}$. Also, if $d = ord_m^y$, then $(y, m) = 1$, so by Carmichael's Theorem, it is evident that $d \mid \lambda(m)$.
Conversely, assume that $d > 0$ is divisor of $\lambda(m)$ and let $v = g^{\lambda(m)/d}$. Then $d = ord_m^v$. Since $d/7^s - 1$ but $d \nmid 7^l - 1$ whenever $0 \leq l < s$. We see that s is the least positive integer for which $v^{7^s-1} \equiv 1 \pmod{m}$. Therefore, $v.v^{7^s-1} \equiv v^{7^s} \equiv v \pmod{m}$. □

It is interesting to note that the enumeration of components for every m is much strenuous. As there are many different patterns in its enumerations. For instance, if we take $m = 47k$, where $k \in \{1,\ 2,\ 3,\ 5,\ 6,\ 7,\ 10,\ 13,\ 14,\ 15,\ 17,\ 21\}$, then its digraph has $2k$ cycle of length 22. In particular, take $k = 1$, then there are two cycles. One of such cycle has the vertices 5, 10, 11, 13, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45, because $5^7 \equiv 11 \pmod{47}$, $11^7 \equiv 31 \pmod{47}$, $\ldots$, $39^7 \equiv 35 \pmod{47}$, $35^7 \equiv 5 \pmod{47}$ form a cycle. Similarly, the vertices 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42 form the other cycle as $2^7 \equiv 34 \pmod{47}$, $34^7 \equiv 8 \pmod{47}$, $\ldots$, $21^7 \equiv 37 \pmod{47}$, $37^7 \equiv 2 \pmod{47}$. These are depicted in Fig. 2 given below,

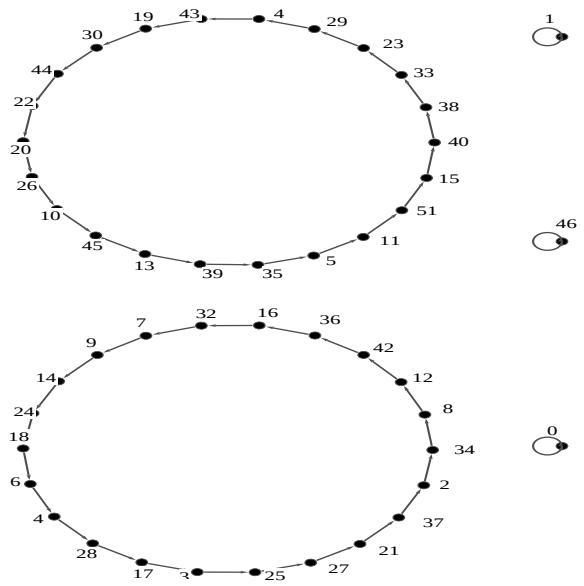

Figure 2. The digraph $G(47)$

For if $k = 2$, the digraph has four cycles of length 22. These are given below: cycles are respectively

a: $4^7 \equiv 28 \pmod{94}$, $28^7 \equiv 64 \pmod{94}$, $64^7 \equiv 50 \pmod{94}$, $50^7 \equiv 72 \pmod{94}$, $72^7 \equiv 74 \pmod{94}$, $74^7 \equiv 68 \pmod{94}$, $68^7 \equiv 84 \pmod{94}$, $84^7 \equiv 2 \pmod{94}$, $2^7 \equiv 34 \pmod{94}$, $34^7 \equiv 8 \pmod{94}$, $8^7 \equiv 12 \pmod{94}$, $12^7 \equiv 42 \pmod{94}$, $42^7 \equiv 36 \pmod{94}$, $36^7 \equiv 16 \pmod{94}$, $16^7 \equiv 32 \pmod{94}$, $32^7 \equiv 54 \pmod{94}$, $54^7 \equiv 56$, $56^7 \equiv 14 \pmod{94}$, $14^7 \equiv 24 \pmod{94}$, $14^7 \equiv 18 \pmod{94}$, $18^7 \equiv 6 \pmod{94}$, $6^7 \equiv 4 \pmod{94}$.

b: $5^7 \equiv 11 \pmod{94}$, $11^7 \equiv 31 \pmod{94}$, $31^7 \equiv 15 \pmod{94}$, $15^7 \equiv 87 \pmod{94}$, $87^7 \equiv 85 \pmod{94}$, $85^7 \equiv 33 \pmod{94}$, $33^7 \equiv 23 \pmod{94}$, $23^7 \equiv 29 \pmod{94}$, $29^7 \equiv 41 \pmod{94}$, $41^7 \equiv 43 \pmod{94}$, $43^7 \equiv 19 \pmod{94}$, $19^7 \equiv 77 \pmod{94}$, $77^7 \equiv 91 \pmod{94}$, $91^7 \equiv 69 \pmod{94}$, $69^7 \equiv 67$, $67^7 \equiv 73 \pmod{94}$, $73^7 \equiv 57 \pmod{94}$, $57^7 \equiv 45 \pmod{94}$, $45^7 \equiv 13 \pmod{94}$, $13^7 \equiv 39 \pmod{94}$, $39^7 \equiv 35 \pmod{94}$, $35^7 \equiv 5 \pmod{94}$.

c: $10^7 \equiv 92 \pmod{94}$, $92^7 \equiv 60 \pmod{94}$, $60^7 \equiv 86 \pmod{94}$, $86^7 \equiv 82 \pmod{94}$, $82^7 \equiv 52 \pmod{94}$, $52^7 \equiv 58 \pmod{94}$, $58^7 \equiv 78 \pmod{94}$, $78^7 \equiv 62 \pmod{94}$, $62^7 \equiv 40 \pmod{94}$, $40^7 \equiv 38 \pmod{94}$, $38^7 \equiv 80 \pmod{94}$, $80^7 \equiv 70 \pmod{94}$, $70^7 \equiv 76$, $88^7 \equiv 90 \pmod{94}$, $90^7 \equiv 66 \pmod{94}$, $66^7 \equiv 30 \pmod{94}$, $30^7 \equiv 44 \pmod{94}$, $44^7 \equiv 22 \pmod{94}$, $22^7 \equiv 20 \pmod{94}$, $20^7 \equiv 26 \pmod{94}$, $26^7 \equiv 10 \pmod{94}$.

d: $3^7 \equiv 25 \pmod{94}$, $25^7 \equiv 27 \pmod{94}$, $27^7 \equiv 21 \pmod{94}$, $21^7 \equiv 37 \pmod{94}$, $37^7 \equiv 49 \pmod{94}$, $49^7 \equiv 81 \pmod{94}$, $81^7 \equiv 55 \pmod{94}$, $55^7 \equiv 59 \pmod{94}$, $59^7 \equiv 89 \pmod{94}$, $89^7 \equiv 83 \pmod{94}$, $83^7 \equiv 63 \pmod{94}$, $63^7 \equiv 79 \pmod{94}$, $79^7 \equiv 7 \pmod{94}$, $7^7 \equiv 9 \pmod{94}$, $9^7 \equiv 61 \pmod{94}$, $61^7 \equiv 71 \pmod{94}$, 71^7

$\equiv 65 \pmod{94}$, $65^7 \equiv 53$, $53^7 \equiv 51 \pmod{94}$, $51^7 \equiv 75 \pmod{94}$, $75^7 \equiv 17 \pmod{94}$ $17^7 \equiv 3 \pmod{94}$.

The above discussion reveals the following remarks,

Remark 4.2. *$G(m)$ has $3k$ fixed point only if $m = 47k$, where $k \in \{1, 2, 3, 6, 7, 14, 21\}$.*

$G(m)$ has exactly $5k$ components only if $m = 47k$, where $k \in \{1, 2, 3, 6, 7, 14, 21\}$.

$G(m)$ has exactly five components only if $m = 8, 23, 47, 71, 83, 179$.

$G(m)$ has exactly 10 components only if $m = 13, 17, 22, 46, 94, 113, 142, 166$.

In view of some particular examples given in the above remark, rather to enumerate components for every integer m, we find integers for which there are a fixed number of components. In the following theorem, we find all integers for which there are seven components.

Theorem 4.3. *The number of components of $G(m)$ is 7 if and only if $m = 9$ or $m = 7^k$ or m is prime of the form $m = 6 \times 7^k + 1$ for some positive integer k.*

Proof. If $m = 9$, then it can easily be seen that there are loops at the vertices 1, 2, 4, 5, 7, and 8, while the vertices 0, 3 and 6 are connected. Thus, there are exactly 7 components. If $m = 7^k$ or m is prime of the form $m = 6 \times 7^k + 1$ then by Theorem 2.1, we have exactly 7 fixed points, and these are either isolated or must be the roots of their respective components. Finally, if m is any number for which we have more than 7 components then by [3] (see lemma 9, page 228), there must be a cycle of length $s > 1$. But then by Theorem 4.1, s is the least positive integer such that $7^s \equiv 1 \pmod{d}$, where $d \mid \lambda(m)$ and $d > 0$. That is, $d \mid 7^s - 1$. But $d \mid \lambda(m) = 6 \times 7^k$ as well. This clearly enforces that $d = 6$. But then $7^k \equiv 1 \pmod{6}$ for each value of k. In particular, if $1 \leq r < s$, then $7^r \equiv 1 \pmod{6}$ as well. This has certainly provided a contradiction against the minimality of s. Thus, this case is not all possible. Consequently, $G(m)$ has 7 components. □

Theorem 4.4. *For any integer $t > 0$, there always exist cycles of length 2^t in the digraph $G_1(2^k)$, $k > 0$ while $G_2(2^k)$ form a tree with root at 0 and have 2^{k-8} branch point. Moreover,*

$$indeg(0) = (2^{k-\lceil \frac{k}{7} \rceil}).$$

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 $G_1(m)$ and $G_2(m)$ contains equal number of vertices namely 2^{k-1}. It can easily be seen that, $1, 2^k, 2^{k-1} \mp 1$ are the only fixed points of $G_1(2^k)$. By Theorem 4.1, there would be a cycle of length s if and only if $s = ord_d^7$, for some divisor d of $\lambda(m) = 2^{k-2}$. Now if there exists such a cycle, then s being order of 7 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 $2^k, k < 8$ mapped onto 0 and if $k > 7$, then again all, even residues of 2^k will be connected by a tree with 2^{k-8} branch points. For instance, if $k = 8$, then $2^7 \not\equiv 0 \pmod{2^8}$. Note that there are two branch points, namely, 0 and $2^7 = 128$. Thus, $(2^{k-\lceil \frac{k}{7} \rceil})$ numbers, namely $2^{\lceil \frac{k}{7} \rceil}$, $2.2^{\lceil \frac{k}{7} \rceil}$, $3.2^{\lceil \frac{k}{7} \rceil}$, $\ldots, 2^{k-\lceil \frac{k}{7} \rceil}.2^{\lceil \frac{k}{7} \rceil}$ are mapped onto 0 while remaining are mapped on to 128. Consequently, $indeg(0) = (2^{k-\lceil \frac{k}{7} \rceil})$. □

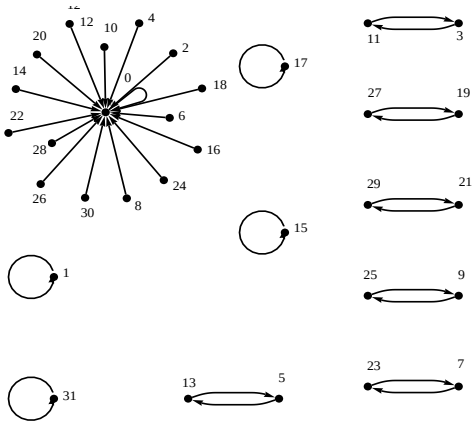

Figure 3. The digraph $G(2^5)$

Theorem 4.5. *Let k be a natural number and $m = 7^k$. Then the digraph $G_1(m)$ consists of six isomorphic trees. Moreover, $G_2(m)$ is a tree with the root in 0 and indeg$(0) = 7^{k-\lceil \frac{k}{7} \rceil}$.*

Proof. Note that the digraph $G(m)$ has exactly 7 components with 7 fixed points [see, Theorem 2.1]. Note that $7^{k-\lceil \frac{k}{7} \rceil}$ elements, namely, $7^{\lceil \frac{k}{7} \rceil}, 2.7^{k-\lceil \frac{k}{7} \rceil}, 3.7^{k-\lceil \frac{k}{7} \rceil}, \ldots,$ $7^{k-\lceil \frac{k}{7} \rceil}.7^{\lceil \frac{k}{7} \rceil}$ are adjacent to 0 in $G_2(m)$. Also, $7|\phi(m) = 6.7^{k-1}$, by Theorem 4.1, we obtain that the digraph $G_1(m)$ is semiregular and every vertex, either has degree 0 or 7. It is clear that this digraph has a tree with root 0. Now consider the set of non-zero fixed points as $\{1, m-1, a, m-a, b, m-b\}$. Define $T_1,\ T_{m-1},\ T_a,\ T_{m-a},\ T_b$ and T_{m-b} trees containing the fixed points $1,\ m-1,\ a,\ m-a,\ b$ and $m-b$, respectively. It can easily deduce that $T_1 \cong T_{m-1}$, $T_a \cong T_{m-a}$ and $T_b \cong T_{m-b}$. Now if we multiply each vertex of the tree T_1 by number a, we have tree T_a. Similarly, if we multiply each vertex of the tree T_1 by number b, we have a tree T_b. This is possible since $(b, m) = 1$ and $(a, m) = 1$. Consequently, we yield that, $T_1 \cong T_b$ and $T_1 \cong T_a$. □

Fig. 3 and Fig. 4 reflects Theorem 4.3 and Theorem 4.4 respectively.

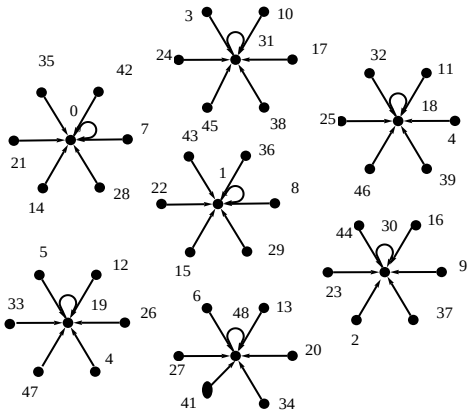

Figure 4. The digraph $G(7^2)$

5. ACKNOWLEDGMENT

We are very thankful to the anonymous referees for sparing their precious time and forwarding useful suggestions/comments. This certainly has made our manuscript more interesting.

REFERENCES

[1] N. Alon, *Combinatorial Nullstellensatz*, Combinatorics, Probability and Computing **8**, No. 1-2 (1999) 7-29.

[2] J. B. Cosgrave and K. Dilcher, *Gauss Factorials, Jacobi Primes, and Generalized Fermat Numbers*, Punjab Univ. j. math. **50**, No. 4 (2018) 1-21.

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

[4] M. K. Mahmood and S. Ali, *A Novel Labeling Algorithm on Several Classes of Graphs*, Punjab Univ. j. math. **49**, No. 2 (2017) 23-35.

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

[6] M. K. Mahmood and F. Ahmad, *A Classification of Cyclic Nodes and Enumerations of Components of a Class of Discrete Graphs*, **9**, No. 1 (2015) 103-112. Doi:10.12785/amis/090115.

[7] M. A. Malik and M. K. Mahmood, *On Simple Graphs Arising from Exponential Congruences*, Hindawi Publishing Corporation, Journal of Applied Mathematics **2012** 10 pages. Doi:10.1155/2012/292895

[8] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley and Sons, Inc. (1991) 1-544.

[9] M. Rahmati, *Some Digraphs Attached With the Congruence $x^5 \equiv y \ (mod \ m)$*, Journal of Mathematical Extension **11**, No. 1 (2017) 47-56.

[10] T. D. Rogers, *The graph of the square mapping on the prime fields*, Discrete Math. **148**, No. 1 (1996) 317-324.

[11] J. Skowronek-Kaziow, *Some digraphs arising from number theory and remarks on the zero-divisor graph of the ring Z_n*, Information Processing Letters **108**, (2008) 165-169.

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

[13] L. Somer and M. Křížek, *The structure of digraph associated with the congurence $x^k \equiv y \ (mod \ m)$*, Czechoslovak Math. J. **61**, No. 136 (2011) 337-358.

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

[15] W. Yangjiang and G. Tang, *The iteration digraphs of finite commutative rings*, Turkish Journal of Mathematics **39**, (2015) 872-883.