Iranian Journal of Mathematical Sciences and Informatics
Vol. 17, No. 2 (2022), pp 307-314
DOI: 10.52547/ijmsi.17.2.307

The Iteration Digraphs of Lambert Map Over the Local Ring $\mathbb{Z}/p^k\mathbb{Z}$: Structures and Enumerations

M. Khalid Mahmood, Lubna Anwar*

Department of Mathematics, University of the Punjab, Lahore, Pakistan

E-mail: khalid.math@pu.edu.pk
E-mail: lubnaanwar30@yahoo.com

Abstract. Let p be prime and $\alpha : x \mapsto xg^x$, the Discrete Lambert Map. For $k \geq 1$, let $V = \{0, 1, 2, ..., p^k - 1\}$. The iteration digraph is a directed graph with V as the vertex set and there is a unique directed edge from u to $\alpha(u)$ for each $u \in V$. We denote this digraph by $G(g, p^k)$, where $g \in (\mathbb{Z}/p^k\mathbb{Z})^*$. In this piece of work, we investigate the structural properties and find new results modulo higher powers of primes. We show that if g is of order $p^d, 1 \leq d \leq k-1$ then $G(g, p^k)$ has $p^{k-\lceil \frac{d}{2} \rceil}$ loops. If $g = tp + 1,\ 1 \leq t \leq p^{k-1} - 1$ then the digraph contains $\frac{p^k+1}{2}$ cycles. Further, if g has order p^{k-1} then $G(g, p^k)$ has $p - 1$ cycles of length p^{k-1} and the digraph is cyclic. We also propose explicit formulas for the enumeration of components.

Keywords: Fixed points, Lambert map, Multiplicative order.

2000 Mathematics subject classification: 05C25, 11E04, 20G15.

1. Introduction

The notion of modular arithmetic is primarily indispensable and imperative in number theory. The study of congruences can be entertained through accustomed examples of integers based on modular arithmetic. In this little piece, we formalize and investigate the structural properties of iteration digraphs via

*Corresponding Author

Received 6 January 2019; Accepted 30 April 2020

[DOI: 10.52547/ijmsi.17.2.307]

Lambert's mapping. We propose new results of such digraphs from modulo a prime p to modulo p^k. We demonstrate certain acquaintances between number theory and graph theory motivated by L. Szalay [6], T. D. Roger [10], B. Wilson [1], L. Somer and M. Křížek [5], Yangjiang Wei and Gaohua Tang [11] and JingJing Chen and Mark Lotts [4]. The digraphs of the exponential congruences and quartic mapping have been discussed in [7] and [8]. We define our digraph as follows.

Let $V = \{0, 1, 2, ..., p^k - 1\}$, $k \geq 1$. Let $G(g, p^k)$ denote the iteration digraph for which V is the set of vertices and with a directed arc between vertices x and y if and only $xg^x \equiv y \ (mod\ p^k)$, where $g \in (\mathbb{Z}/p^k\mathbb{Z})^*$. Thus for each g and $p^k,\ k \geq 1$ there is a fix iteration digraph as given in Fig. 1. Results regarding fixed points, isolated fixed points, cycles and enumeration of components have been proposed. In Fig.1, the iteration digraph has five fixed points and three non-isomorphic components. The vertex 0 is the only isolated fixed pint. This paper follows [2,3,4,9,10] and [11].

Few basic definitions and some previous results are important to make this paper self readable.

Definition 1.1. [2] Let $p \nmid a$, where p is prime. The order of a modulo p^k is the least integer $r > 0$ such that $a^r \equiv 1 \ (mod\ p^k)$. It is labeled as $\mathrm{Ord}_{p^k} a = r$.

Definition 1.2. [2] The function $\phi(n)$ is the number of such residues of n which are prime to n together with $\phi(1) = 1$.

Theorem 1.3. [2] *Let* $(a, m) = 1$, *where* $m \geq 1$, *then* $a^{\phi(m)} \equiv 1 \ (mod\ m)$.

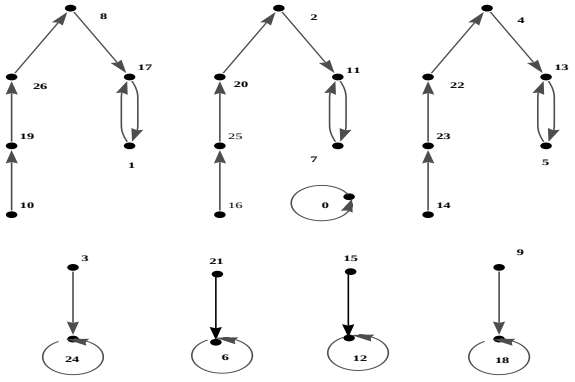

FIGURE 1. $G(17, 3^3)$.

[DOI: 10.52547/ijmsi.17.2.307]

2. Fixed Points of the Map

Recall that a vertex u is said to have a loop on it if $ug^u \equiv u \ (mod\ p^k)$ and it referred to as an isolated fixed point of the graph $G(g, p^k)$ if $ug^u \equiv u \ (mod\ p^k)$ and there does not exist any vertex v such that $ug^u \equiv v \ (mod\ p^k)$. Before proceeding first we state (without proof) few of earlier results regarding fixed points and isolated fixed points.

Theorem 2.1. [9] *If $g \equiv 1 \ (mod\ p^k)$, then all fixed points are isolated.*

Theorem 2.2. [9] *Let $G(g, p^k)$ be a discrete Lambert digraph. Then,*

(i) If $g = tp,\ 1 \leq t \leq p^{k-1} - 1$ then 0 is the only fixed point of G.

(ii) 0 is an isolated fixed point of G if and only if $g \neq tp,\ 1 \leq t \leq p^{k-1} - 1$.

(iii) If $\phi(p^k)$ is a fixed point then $g \neq tp,\ 1 \leq t \leq p^{k-1} - 1$.

Theorem 2.3. [4] *Let q be any prime. Then,*

1. *Let g be a quadratic residue of q, then $\frac{q-1}{2} \equiv \frac{q-1}{2} \ (mod\ q)$.*
2. *A point t is fixed $\Leftrightarrow g^t \equiv 1 \ (mod\ q)$.*
3. *Let $f(t) = tg^t$, then fixed points of f are multiples of order of g.*
4. *If t is odd, then $f(t) = t - 1$, and if t is even, then $f(t) = t$.*

The following lemma is of crucial importance and we prove it as a consequence of Definition 1.1.

Lemma 2.4. $\mathrm{Ord}_{p^k}\ g = p^d$ *if and only if* $g \equiv 1 \ (mod\ p^{k-d}),\ 1 \leq d \leq k-1$.

Proof. Let $\mathrm{ord}_{p^k}\ g = \beta$. Then β is the least positive integer such that $g^\beta \equiv 1 \ (mod\ p^k)$. But then $g^\beta \equiv 1 \ (mod\ p)$ as well. Suppose $g = 1 + tp^{k-d}$ for some integer t where, $(t, p) = 1$. Now

$g^\beta = (1 + tp^{k-d})^\beta = 1 + t\beta p^{k-d} +$ terms involving higher powers of p^{k-d}

Thus $g^\beta \equiv 1(mod\ p^k)$ if and only if $t\beta p^{k-d} \equiv 0(mod\ p^k)$. But $(t, p) = 1$. Hence, we conclude that $g^\beta \equiv 1(mod\ p^k) \Leftrightarrow \beta p^{k-d} \equiv 0(mod\ p^k) \Leftrightarrow \beta = p^d$ for $d = 1, 2, ..., k-1$. □

Theorem 2.5. *Let's denote $N(g, p^k)$ for the number of fixed points in $G(g, p^k)$. Then $N(g, p^k) = p^{k-\lceil \frac{d}{2} \rceil}$ only if* $\mathrm{Ord}_{p^k}\ g = p^d, 1 \leq d \leq k-1$.

Proof. We know that

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

[DOI: 10.52547/ijmsi.17.2.307]

Let $\text{Ord}_{p^k}\ g = p^d, 1 \leq d \leq k-1$. Then by Lemma 2.4, $g = 1 + tp^{k-d}$ for some integer t where, $(t,p) = 1$. Hence by Theorem 2.1, all fixed pints are isolated. Thus we need to find vertices α such that $\alpha(1+tp^{k-d})^\alpha \equiv \alpha(\ mod\ p^k)$ provided $\text{Ord}_{p^k}\ g = p^d, 1 \leq d \leq k-1$. For instance, if $d = 1$ then $\alpha = p, 2p, 3p, ..., p^{k-1}p$ are the $p^{k-1} = p^{k-\lceil \frac{1}{2} \rceil}$ fixed points. Thus the proof can easily be deduced in the light of Lemma 2.4. □

Theorem 2.6. *Let* $\text{Ord}_{p^k}\ g_1 = \text{Ord}_{p^k}\ g_2$. *Then* $N(g_1, p^k) = N(g_2, p^k)$.

Proof. Let $\text{Ord}_{p^k}\ g_1 = \text{Ord}_{p^k}\ g_2 = \beta$. Then β is the least positive integer such that $g_1^\beta = g_2^\beta \equiv 1\ (mod\ p^k)$. Suppose α is a fixed point of $G(g_1, p^k)$. That is, $\alpha g_1^\alpha \equiv \alpha(\ mod\ p^k)$. Then by Theorem 2.3 (2), $g_1^\alpha \equiv 1(\ mod\ p^k)$. But then $\alpha = t\beta$ since β is supposed to be least. Now $\alpha g_2^\alpha = \alpha g_2^{t\beta} = \alpha(g_2^\beta)^t \equiv \alpha(1)^t \equiv \alpha(\ mod\ p^k)$. Thus α is a fixed point of $G(g_2, p^k)$ as well. □

The following theorem is of great importance and can be proved directly using the definition of Lambert Map.

Theorem 2.7. *If* $g = p^k - 1$, *then the number of fixed points in* $G(g, p^k)$ *is*

$$N(g, p^k) = \begin{cases} 2, & \text{if } p = 2,\ k = 1 \\ \frac{p^k}{2}, & \text{if } p = 2,\ k > 1 \\ \frac{p^k+1}{2}, & \text{if } p \text{ is an odd prime} \end{cases}$$

Proof. Let $g = p^k - 1$. First, we note that all even residues of p^k are the fixed points of $G(g, p^k)$ while none of the odd residue of p^k serve as a fixed point of $G(g, p^k)$. For this, we let r be any integer, then we see that

$$\begin{aligned} (2r+1)(p^k-1)^{2r+1} &\equiv (2r+1)(-1)^{2r+1}\ (\ mod\ p^k) \\ &\equiv -(2r+1)\ (\ mod\ p^k) \\ &\not\equiv 2r+1\ (\ mod\ p^k)\ \text{ except } p = 2 \end{aligned}$$

While

$$\begin{aligned} 2r(p^k-1)^{2r} &\equiv 2r(-1)^{2r}\ (\ mod\ p^k) \\ &\equiv 2r\ (\ mod\ p^k) \end{aligned}$$

Finally, it is easy to see that if $p = 2$ and $g = 2 - 1 = 1$, then 0 and 1 are the only fixed points in $G(1, 2)$. And if $k > 1$ with $p = 2$ and $g = 2^k - 1$, then there are $\frac{p^k}{2}$ even numbers. That is, $\frac{p^k}{2}$ fixed points in $G(2^k - 1, 2^k)$. Similarly, if p is an odd prime then there are $\frac{p^k+1}{2}$ even residues of p^k. □

[DOI: 10.52547/ijmsi.17.2.307]

3. Enumeration of Cycles

The vertices $x_1, x_2, ..., x_{r-1}, x_r$ form a cycle of length r if and only if

$$\begin{aligned} x_1 g^{x_1} &\equiv x_2 \ (mod\ p^k) \\ x_2 g^{x_2} &\equiv x_3 \ (mod\ p^k) \\ &\vdots \\ x_r g^{x_r} &\equiv x_1 (mod\ p^k) \end{aligned}$$

In this section, we discuss cyclic vertices, enumeration of cycles of different lengths for the digraph $G(g, p^k)$, where p is any odd prime and $k \geq 1$. These can be entertained in the following theorems.

Proposition 3.1. *Let p be any odd prime and $g \neq 1$ be any integer. Then all cycles in $G(g, p^k), k \geq 1$ are of length at most one if and only if $g^2 \equiv 1\ (mod\ p)$ or $p|g$.*

Proof. Suppose $p \nmid g$ but $g^2 \equiv 1\ (mod\ p)$. Since $g \neq 1$ be any integer, so by Lemma 1 [9], $g = p^k - 1$. Then by Theorem 2.3 (4), if t is odd and $g = p^k - 1$ then $f(t) = p^k - t$ and if t is even then $f(t) = t$. Suppose that there exists a cycle of length 2. Then any odd node x will be sent to some $y \equiv p^k - x$. Now since y is even, so again by Theorem 2.3 (4), $f(y) = y \neq x$, a contradiction against the fact that $G(g, p^k), k \geq 1$ has a cycle of length 2. Conversely, we suppose that for any integer $g \neq 1$, the digraph $G(g, p^k), k \geq 1$ contains only cycles of length at most one. This means that the digraph only contains fixed points or there is no fixed point in case of cycles of length less than one. Combining (i) and (ii) of Theorem 2.2, we must get that either $p|g$ or $g^2 \equiv 1\ (mod\ p)$. □

Corollary 3.2. *If $g = p^k - 1$ then the digraph $G(g, p^k)$ contains $\frac{p^k+1}{2}$ cycles.*

Proof. Let $g = p^k - 1$. By Theorem 2.7, $G(g, p^k)$ contains $\frac{p^k+1}{2}$ fixed points. Also by Lemma 1 [9], $\text{ord}_{p^k}\ g = 2$. Hence by Proposition 3.1, there exists no cycle of length > 1. Thus the only cycles are the fixed points of $G(g, p^k)$. □

Lemma 3.3. *Let $\text{ord}_{p^k}\ g = p^{k-1}$ then the vertices v_i, $1 \leq i \leq r$, such $v_i \equiv j\ (mod\ p)$, where $1 \leq j \leq p-1$ are the cyclic vertices.*

Proof. Let $\text{ord}_{p^k}\ g = p^{k-1}$. By Lemma 2.4, $g \equiv 1\ (mod\ p)$. Then there exist some integers t such that $g = 1 + pt$, provided $\gcd(p, t) = 1$. Also $v_i \equiv j\ (mod\ p)$, so $v_i = j + ps$, where $\gcd(p, s) = 1$. Consider,

$$\begin{aligned} f(v_i) = f(j + sp) &= (j + ps)g^{j+ps} = (j + ps)(1 + pt)^{j+ps} \\ &= (j + ps)(1 + jpt)\ (mod\ p^2) \\ &\equiv j + ps + j^2 pt\ (mod\ p^2) = v_{i+1} \quad \text{(say)} \end{aligned} \tag{3.1}$$

[DOI: 10.52547/ijmsi.17.2.307]

Clearly $v_{i+1} \equiv j \ (mod\ p)$. Now,

$$\begin{aligned} f(v_{i+1}) &= f(j+p(s+j^2t)) = (j+ps+j^2pt)(1+pt)^{j+ps+j^2pt} \\ &\equiv (j+ps+j^2pt)(1+jpt)(mod\ p^2) \\ &\equiv (j+ps+2j^2pt)(mod\ p^2) = v_{i+2} \ \ (\text{say}) \end{aligned} \tag{3.2}$$

Note $v_{i+2} \equiv j \ (mod\ p)$. Similarly,

$$\begin{aligned} f(v_{i+2}) &= f(j+p(s+2j^2t)) = (j+ps+2j^2pt)(1+pt)^{j+ps+j^2pt} \\ &\equiv (j+ps+2j^2pt)(1+jpt)\ (mod\ p^2) \\ &\equiv (j+ps+3j^2pt)\ (mod\ p^2) = v_{i+3} \ \ (\text{say}) \end{aligned} \tag{3.3}$$

Where, $v_{i+3} \equiv j \ (mod\ p)$. Continue in this way, we must arrive at,

$$\begin{aligned} f(v_{i+p-1}) &= f(j+p(s+(p-1)j^2t)) \\ &= (j+ps+(p-1)j^2pt)(1+pt)^{j+ps+(p-1)j^2pt} \\ &\equiv (j+ps+(p-1)j^2pt)(1+jpt)\ (mod\ p^2) \\ &\equiv (r+ps)\ (mod\ p^2) = v_i \end{aligned} \tag{3.4}$$

By equations (3.1) to (3.4), it is clear that the vertices v_i such that $v_i \equiv j \ (mod\ p)$ are the cyclic vertices. By adopting the similar steps, this can be achieved for higher powers of primes as well. □

Theorem 3.4. *If* $\text{ord}_{p^k}\ g = p^{k-1},\ k > 1$ *then the digraph* $G(g, p^k)$ *has* $p-1$ *cycles of length* p^{k-1}.

Proof. Let $\text{ord}_{p^k}\ g = p^{k-1},\ k > 1$. Clearly $g \equiv 1 \ (mod\ p)$. By Lemma 3.3, the vertices congruent to $1, 2, \cdots, p-1$ modulo p^k form cycles. This means that there exist $p-1$ such cycles. Moreover the vertices congruent to $1, 2, \cdots, p-1$ modulo p^k can never be multiple of p. However there exist p^{k-1} vertices which are multiples of p. These are $p, 2p, ..., (p-1)p, p^2, 2p^2, ..., p^{k-1}$, $2p^{k-1}, ..., p^{k-1}p$. Therefore, there exist $p^k - p^{k-1} = p^{k-1}(p-1)$ vertices which are prime to p. Since these vertices form $p-1$ cycles altogether. Hence the length of each cycle is $\frac{p^{k-1}(p-1)}{p-1} = p^{k-1}$. □

Corollary 3.5. *For* $p = 3$*, the length of longest cycle is* $\frac{\phi(p^k)}{2}$.

4. Components

Let p be any odd prime. The digraph $G(g, p^k)$ is said to be connected if for each vertex pair x and y, $xg^x \equiv y \ (mod\ p^k)$. A maximal connected graph is called a component. It is worth mentioning that the discrete Lambert graph is a functional graph. So every vertex contains a unique image under the map. This means that the out degree of every vertex is one. Thus the sequence of images in its graph must terminate at a self loop (a fixed point) or continue until it becomes a part of cycle. Thus every component contains a unique cycle.

[DOI: 10.52547/ijmsi.17.2.307]

Suppose a component C contains no cycle. Then it contains no fixed point, a cycle of length one, in either. Therefore, C must contains at least two vertices. Let $v_1, v_2, ..., v_i$ be vertices in C such that $v_1 \mapsto v_2 \mapsto v_3 \mapsto ... \mapsto v_i$. If this path terminates at v_i then v_i must be a fixed point, contrary to our supposition. Thus v_i continues the path such that there must exist vertices $v_{i+1}, ..., v_j$ such that $v_i \mapsto v_{i+1} \mapsto, ..., v_j \mapsto v_i$, $1 \leq i, j \leq k$. Thus the vertices $v_{i+1}, v_{i+1}, ..., v_j$ form a cycle in C. Since out degree of every vertex is one, so this cycle must be unique. The above discussion leads the following result. In Fig 2, we depict Theorem 3.4 and Lemma 3.3.

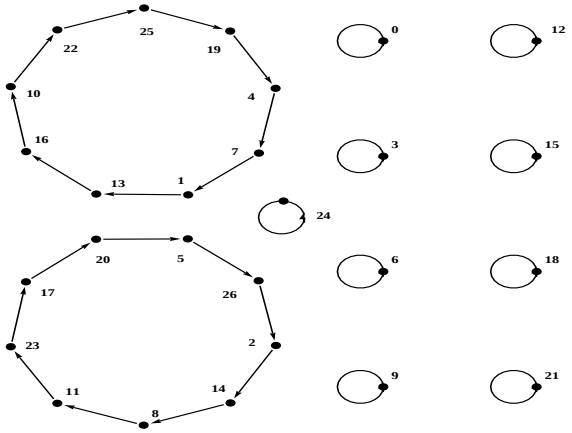

FIGURE 2. $G(13, 3^3)$.

Theorem 4.1. *Every component of the digraph $G(g, p^k)$ contains a unique cycle. Thus the number of cycles in $G(g, p^k)$ precisely enumerate the number of components in $G(g, p^k)$.*

Corollary 4.2. *If $g = p^k - 1$, then there exist $\frac{p^k+1}{2}$ components in $G(g, p^k)$.*

Proof. Let $g = p^k - 1$. Then by Corollary 3.2, the digraph $G(g, p^k)$ contains $\frac{p^k+1}{2}$ cycles. Hence by Theorem 4.1, there exist $\frac{p^k+1}{2}$ components in $G(g, p^k)$. □

Remark 4.3. We referred to a graph as cyclic if each of its component form a cycle. In the following result we find the values of g for which the graph is cyclic. Before this, we prove the following lemma.

Lemma 4.4. *Let $u, v \in \{0, p, \cdots, (p^{k-1} - 1)p\}$ be arbitrary and f be discrete Lambert maps, then $f(u) = v$.*

Proof. Let $u = rp, 1 \leq r \leq p^{k-1} - 1$.

$$\begin{aligned} f(rp) &\equiv (rp)(g)^{rp} \ (mod\ p^k) \\ f(rp) &\equiv r(g)^{rp}p \ (mod\ p^k) \\ f(rp) &\equiv sp \ (mod\ p^k), \text{ where } s = r(g)^{rp} \\ f(rp) &\equiv sp \ (mod\ p^k) \end{aligned}$$

[DOI: 10.52547/ijmsi.17.2.307]

□

Theorem 4.5. *If* $\text{ord}_{p^k}\ g = p^{k-1},\ k > 1$ *then every component is cyclic.*

Proof. By Lemma 2.4, $g \equiv 1(mod\ p)$. Then by Lemma 3.3, the vertices v_i such that $v_i \equiv j\ (mod\ p),\ 1 \leq j \leq p-1$ are the cyclic vertices. That is, the vertices $\equiv 1, 2, \cdots, p-1(mod\ p)$ are cyclic. The remaining vertices must be multiple p. Hence by Lemma 4.4, either all are fixed points or cyclic or form a tree with root at zero. But by Theorem 2.1, all fixed points must be isolated. Hence the third of the possibilities can never ba prevailed. Thus in either case of g provided $\text{ord}_{p^k}\ g = p^{k-1},\ k > 1$, every component must be cyclic. □

5. Acknowledgement

We express our sincere gratitude to the anonymas referees for sending helpful comments. We honestly think that the manuscript has become much better and informative.

References

1. B. Wilson, Power Digraphs Modulo n, *Fibonacci Quart*, **36**, (1998), 229-239.
2. D. M. Burton, *Elementary Number Theory*, Seventh edition, McGraw-Hill, 2007.
3. G. Chartrand, L. Lesnidk, *Graphs and Digraphs*, Third edition, Chapman Hall, London, 1996.
4. JingJing Chen, Mark Lotts, Structure and Randomness of the Discrete Lambert Map, *Rose-Hulman Undergraduate Mathematics Journal*, **13**, (2012), 1-12.
5. L. Somer, M. Křížek, On a Connection of Number Theory with Graph Theory, *Czechoslovak Math. J.,* **54**, (2004), 465-485.
6. L. Szalay, A discrete Iteration in Number Theory, *BDTF Tud. Közl*, **8**, (1992), 71-91.
7. M. Aslam Malik, M. Khalid Mahmood, On Simple Graphs Arising From Exponential Congruences, *Journal of Applied Mathematics*, Volume 2012, Article ID 292895, 10 pages.
8. M. Khalid Mahmood, Farooq Ahmad, A Classification of Cyclic Nodes and Enumerations of Components of a Class of Discrete Graphs, *Applied Mathematics and Information Sciences*, **9**(1), (2015), 103-112.
9. M. Kkalid Mahmood, Lubna Anwar, Loops in Digraphs of Lambert Mapping Modulo Prime Powers: Enumerations and Applications, *Advances in Pure Mathematics*, **6**(08), (2016), 564-570.
10. T. D. Rogers, The Graph of the Square Mapping on the Prime Fields, *Discrete Math.*, **148**, (1996), 317-324.
11. Yangjiang Wei, Gaohua Tang, The Iteration Digraphs of Finite Commutative Rings, *Turkish Journal of Mathematics*, **39**, (2015), 872-883.

[DOI: 10.52547/ijmsi.17.2.307]