Advances in Pure Mathematics, 2016, 6, 564-570
Published Online July 2016 in SciRes. http://www.scirp.org/journal/apm
http://dx.doi.org/10.4236/apm.2016.68045

Loops in Digraphs of Lambert Mapping Modulo Prime Powers: Enumerations and Applications

M. Khalid Mahmood, Lubna Anwar

Department of Mathematics, University of the Punjab, Lahore, Pakistan
Email: khalid.math@pu.edu.pk, lubnaanwar30@yahoo.com

Received 5 February 2016; accepted 25 July 2016; published 28 July 2016

Abstract

For an odd prime number p, and positive integers k and $g \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$, we denote $G\left(g, p^k\right)$, a digraph for which $\left\{0,1,2,\cdots,p^k-1\right\}$ is the set of vertices and there is a directed edge from u to v if $f\left(u\right) \equiv v\left(mod\ p^k\right)$, where $f\left(x\right) = xg^x$. In this work, we study isolated and non-isolated fixed points (or loops) in digraphs arising from Discrete Lambert Mapping. It is shown that if $g \equiv 1\left(mod\ p^{k-i}\right), 1 \le i \le k-1$, then all fixed points in $G\left(g, p^k\right)$ are isolated. It is proved that the digraph $G\left(g, p^k\right)$ has p^{k-1} isolated fixed points only if $g = tp+1, 1 \le t \le p^{k-1}-1$. It has been characterized that $G\left(g, p^k\right)$ has no cycles except fixed points if and only if either g is of order 2 or g is divisible by p. As an application of these loops, the solvability of the exponential congruence $xg^x \equiv x\left(mod\ p^k\right)$ has been discussed.

Keywords

Fixed Points, Lambert Map, Multiplicative Order

1. Introduction

The Lambert W functions are used to find solutions of such equations in which the unknown also appears in exponential (or logarithmic) terms. It is defined as $c = W\left(c\right)e^{W\left(c\right)}$, where c is a complex number. Equivalently,

How to cite this paper: Mahmood, M.K. and Anwar, L. (2016) Loops in Digraphs of Lambert Mapping Modulo Prime Powers: Enumerations and Applications. *Advances in Pure Mathematics*, **6**, 564-570. http://dx.doi.org/10.4236/apm.2016.68045

it can be defined as $f(w) = we^w$. Lambert solved a Diophantine equation $x = x^k + t$ in 1758 (see [1]). Later, the solution is expressed in term of series. In 1980, the Lambert function was stored in MCAS (Maple Computer Algebra System) as a function for the solution of algebraic equations involving exponential (or logarithmic) functions (see [2]). In this work, we discussed solutions of such functions by means of their digraphs using residue theory from number theory.

Let $\mathbb{Z}$ be the ring of residue classes modulo p^k. Define $f : \mathbb{Z} \mapsto \mathbb{Z}$ by $f(x) = xg^x$, the discrete Lambert mapping, where $g \in (\mathbb{Z}/p^k\mathbb{Z})^*$. We investigate this mapping using directed graphs whose vertices are residues modulo p^k with edges from $\underline{u}$ to $\underline{v}$ if and only if $f(\underline{u}) \equiv \underline{v}(mod\ p^k)$. This digraph is denoted by $G(g, p^k)$. We investigate self loops (fixed points) of these digraphs and also lift up the investigations of such digraphs by Jingjing Chen and Mark Lotts in [3] from modulo a prime *p* to modulo p^k. Results regarding fixed points, isolated points followed by astute proofs have been presented. It is important to note that all solutions of congruences of Lambert functions are difficult to find since such mappings are hard to invert and need enormous inversions in any computer algorithm. To understand the terminology and symbols, we follow [3]-[6].

Definition 1. (see [7]). Let *p* be prime and *a* be any integer not divisible by *p*. A least positive integer *r* such that $a^r \equiv 1(mod\ p^k)$ is called order of *a* modulo p^k. It is denoted as $\text{Ord}_{p^k} a = r$.

Theorem 0. (see [3]). Let *q* be any prime and $f(t) = tg^t$. Then,

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

Let's draw a digraph of the Lambert map. Take $g = 13$ and chose a composite modulus *m* as $m = 15 = 3 \times 5$. We see that the digraph (see **Figure 1**) has six loops (fixed points) of which three are non-isolated. The digraph has two non-isomorphic components.

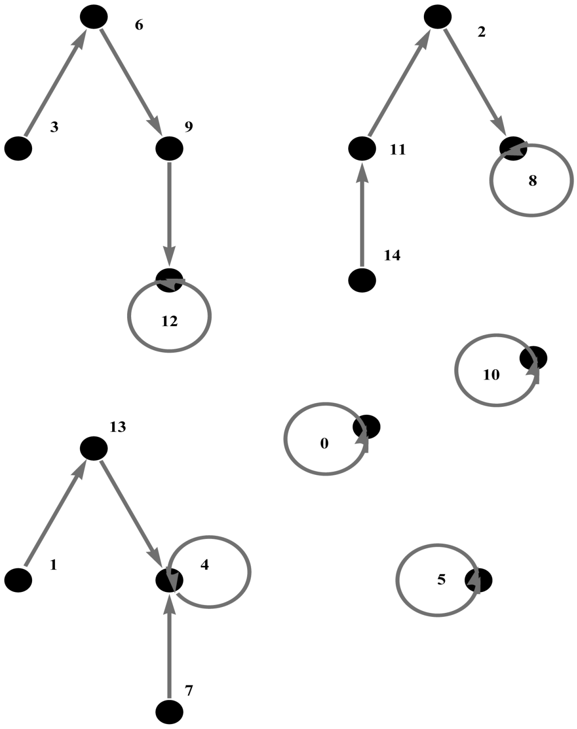

Figure 1. $G(13,15)$.

2. Fixed Points of the Map

Recall that a vertex u is said to have a loop (fixed point) on it if $ug^u \equiv u\left(mod\ p^k\right)$ and it referred to as an isolated fixed point of the graph $G\left(g, p^k\right)$ if $ug^u \equiv u\left(mod\ p^k\right)$ and there does not exist any vertex v such that $ug^u \equiv v\left(mod\ p^k\right)$. In this section, we present some results to find fixed points (or loops) and isolated points of the graph $G\left(g, p^k\right)$.

Lemma 1. *Let p be any prime. Then,* $\operatorname{ord}_{p^k} g = 2$ *if and only if* $g = p^k - 1$ *for any integer g.*

Proof. Let $\operatorname{Ord}_{p^k} g = 2$. Then 2 is the least positive integer such that $g^2 \equiv 1\left(mod\ p^k\right)$. This means that either $g \equiv 1\left(mod\ p^k\right)$ or $g \equiv -1\left(mod\ p^k\right)$. But the first implies that, $\operatorname{Ord}_{p^k} g = 1$. Hence $g \equiv -1 \equiv p^k - 1\left(mod\ p^k\right)$. Since $g \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$. Thus $g = p^k - 1$. Conversely, it is easy to see that $\left(p^k - 1\right)^2 = p^{2k} - 2p^k + 1 \equiv 1\left(mod\ p^k\right)$.

□

The proof of the following theorem is simple and can be established similar to Theorem 0 (4).

Theorem 1. *Let* $g = p^k - 1$ *and f be Discrete Lambert Map. If a is any odd residue of* p^k *then* $a \mapsto -a$ *and if a is an even residue of* p^k *then* $a \mapsto a$ *under f.*

In the following theorem, we find the values of g for which the fixed points of the digraph are necessarily isolated. Before proving the assertion, we give the following important lemmas.

Lemma 2. *If* $g \equiv 1\left(mod\ p\right)$ *then* $tp^{k-1}, 0 \le t \le p^{k-1} - 1, k > 1$ *are the fixed points of the graph* $G\left(g, p^k\right)$. *In particular, the vertices,* $p^{\left\lfloor \frac{k}{2} \right\rfloor}, 2 \cdot p^{\left\lfloor \frac{k}{2} \right\rfloor}, \cdots, \left(p^{\left\lfloor \frac{k}{2} \right\rfloor + 1} - 1\right) p^{\left\lfloor \frac{k}{2} \right\rfloor}$ *when k is odd and* $p^{\left\lfloor \frac{k}{2} \right\rfloor}, 2 \cdot p^{\left\lfloor \frac{k}{2} \right\rfloor}, \cdots, \left(p^{\left\lfloor \frac{k}{2} \right\rfloor} - 1\right) p^{\left\lfloor \frac{k}{2} \right\rfloor}$ *when k is even are always fixed points.*

Proof. Let $g \equiv 1\left(mod\ p\right)$, then $g = 1 + sp$ for some integer s. But then

$$tp^{k-1} g^{tp^{k-1}} = tp^{k-1}\left(1 + sp\right)^{tp^{k-1}} = tp^{k-1}\left(1 + stp^k + \text{terms involving } p^k\right) \equiv tp^{k-1}\left(mod\ p^k\right) \tag{1}$$

For the rest of the proof, we note that $\left\lfloor \frac{k}{2} \right\rfloor + 1 = \frac{k+1}{2}$ when k is odd and $\left\lfloor \frac{k}{2} \right\rfloor = \frac{k}{2}$ when k is even. Therefore,

$$\begin{aligned} p^{\left\lfloor \frac{k}{2} \right\rfloor} g^{p^{\left\lfloor \frac{k}{2} \right\rfloor}} &= p^{\frac{k}{2}}\left(1 + sp\right)^{p^{\frac{k}{2}}} = p^{\frac{k}{2}}\left(1 + sp^{\frac{k}{2}}p\right) + \cdots \\ &= p^{\frac{k}{2}} + sp^{k+1} + \cdots \equiv p^{\frac{k}{2}}\left(mod\ p^k\right) \equiv p^{\left\lfloor \frac{k}{2} \right\rfloor}\left(mod\ p^k\right) \end{aligned}$$

The case when k is odd can be dealt in a similar technique. □

The following Lemma is of crucial importance. However, its proof is simple and can be viewed as a direct consequence of the Definition 1.

Lemma 3. *Let g be a residue of* p^k. *Then* $\operatorname{ord}_{p^k} g = p^i$ *if and only if* $g \equiv 1\left(mod\ p^{k-i}\right), 1 \le i \le k - 1$.

Proof. Let $\operatorname{ord}_{p^k} g = l$. Then l is the least positive integer such that $g^l \equiv 1\left(mod\ p\right)$. Suppose $g \equiv 1\left(mod\ p^{k-i}\right)$, then $g = 1 + sp^{k-i}$ for some integer s such that $\left(s, p\right) = 1$ and $i = 1, 2, \cdots, k - 1$. Now

$$g^l = \left(1 + sp^{k-i}\right)^l = 1 + slp^{k-i} + \text{terms involving higher powers of } p^{k-i}$$

Thus $g^l \equiv 1\left(mod\ p^k\right)$ if and only if $slp^{k-i} \equiv 0\left(mod\ p^k\right)$. But $\left(s, p\right) = 1$. Hence, we conclude that $g^l \equiv 1\left(mod\ p^k\right) \Leftrightarrow lp^{k-i} \equiv 0\left(mod\ p^k\right) \Leftrightarrow l = p^i$ for $i = 1, 2, \cdots, k - 1$. □

Lemma 4. *Let* $\operatorname{ord}_{p^k} g = \alpha$. *If* α *divides v then v is a fixed point of the digraph* $G\left(g, p^k\right)$.

Proof. Let $\operatorname{ord}_{p^k} g = \alpha$. Then α is the least positive integer such that $g^\alpha \equiv 1\left(mod\ p^k\right)$. Now for any vertex *v*, if α divides *v* then $v=\alpha\beta$ for some integer β. But then $f(v)=vg^{v}=\alpha\beta g^{\alpha\beta}=\alpha\beta\left(g^{\alpha}\right)^{\beta}\equiv v\left(\mathrm{mod}\ p^{k}\right)$. □

Theorem 2. *If* $g\equiv 1\left(mod\ p^{k-i}\right),1\le i\le k-1$, *then all fixed points of* $G\left(g,p^{k}\right)$ *are isolated.*

Proof. Let $g\equiv 1\left(mod\ p^{k-i}\right),1\le i\le k-1$. Then by Lemma 3, $\mathrm{ord}_{p^k}g=p^{i}$ for $i=1,2,\cdots,k-1$. This means that possible orders of *g* modulo p^{k} are $p,p^{2},p^{3},\cdots,p^{k-1}$. Hence by Lemma 4, $\lambda p^{i},1\le i\le k-1$, for any integer λ, are the fixed points. We need only to show that these are the possible fixed points and are isolated. Since $p^{k-i}\mid g-1$, so, $g=1+tp^{k-i}$, where $1\le t\le p-1$ and $1\le i\le k-1$. Let *x* be any fixed point in $G\left(g,p^{k}\right)$, then $x=f\left(x\right)\equiv xg^{x}\left(mod\ p^{k}\right)\equiv x\left(1+tp^{k-i}\right)^{x}\left(mod\ p^{k}\right)\equiv x\left(1+tp^{k-i}x+\cdots\right)\left(mod\ p^{k}\right)$. Or $x\left(1+tp^{k-i}x+\cdots-1\right)\equiv 0\left(mod\ p^{k}\right)$. This means that either $p^{k}\mid x$ or $p^{k}\mid tp^{k-i}x+\cdots$. But $x<p^{k}$. Hence $p^{k}\mid tp^{k-i}x+\cdots$. This clearly shows that *x* is p^{i} or multiple of p^{i}. Finally, we show that these are isolated. Let λp^{j} for some $j=1,2,\cdots,k-1$, is adjacent to some $x\ne\lambda p^{j}$. Then $\lambda p^{j}g^{\lambda p^{j}}\equiv x\left(mod\ p^{k}\right)$. But $f\left(\lambda p^{j}\right)\equiv\lambda p^{j}\left(mod\ p^{k}\right)$, so $\lambda p^{j}g^{\lambda p^{j}}\equiv\lambda p^{j}\left(mod\ p^{k}\right)$ implies that $\lambda p^{j}\equiv x\left(mod\ p^{k}\right)$. That is, $p^{k}\mid\lambda p^{j}-x$, which is not possible since $0<p^{j},x<p^{k}$. □

Figure 2 depicts Theorems 2 and 3. In Figure 2, we note that $\mathrm{ord}_{25}11=5$. By Theorem 2, the vertices 5, 10, 15, 20 are the fixed points and are isolated. Also $g=11$ is not a multiple of 5, so by Theorem 3, 0 is also an isolated fixed point. Thus all fixed points are isolated.

Theorem 3. *Let* $G\left(g,p^{k}\right)$ *be a discrete Lambert digraph. Then,*

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

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

iii) *If* $\phi\left(p^{k}\right)$ *is a fixed point then* $g\ne tp,1\le t\le p^{k-1}-1$.

Proof. i) Let $g=tp,1\le t\le p^{k-1}-1$ and *x* be any fixed point of *G*. Then,

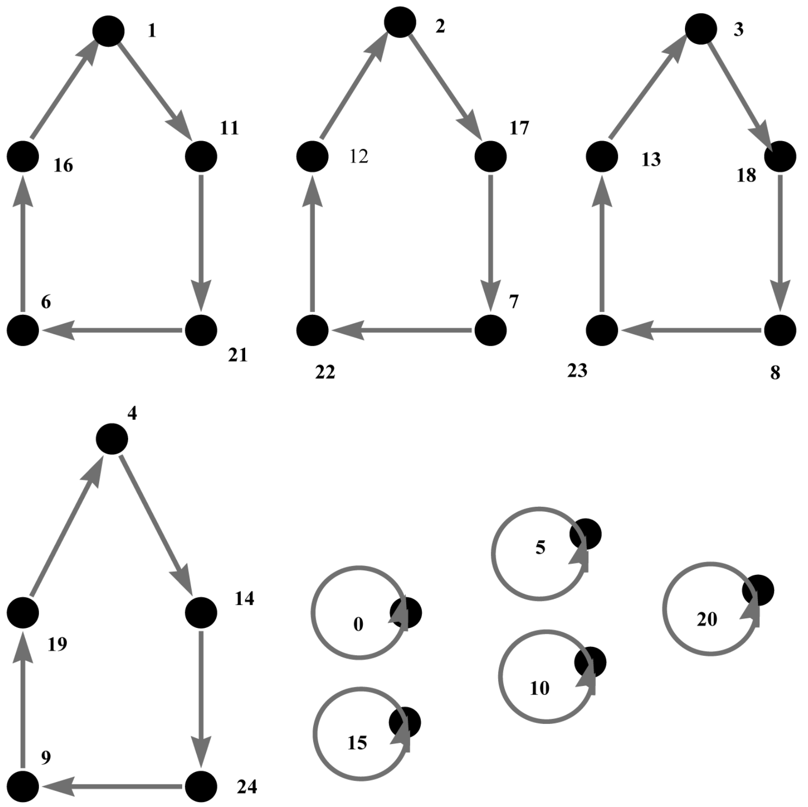

Figure 2. $G(11,25)$.

$$x = f(x) = xg^x \equiv x(tp)^x \left(mod\ p^k\right) \text{ or } x\left(1-(tp)^x\right) \equiv 0\left(mod\ p^k\right) \tag{2}$$

This means that either $p^k \mid x$ or $p^k \mid 1-(tp)^x$. But $x < p^k$, so $p^k \nmid x$. Hence (2) yields that, $(tp)^x \equiv 1\left(mod\ p^k\right)$. This is possible only if $x = 0$.

ii) Let $g \neq tp, t = 0,1,2,\cdots, p^{k-1}-1$. On contrary we suppose that there exist a vertex $x \not\equiv 0$ such that x is adjacent to 0. That is, $f(x) = xg^x \equiv 0\left(mod\ p^k\right)$. This means that $p^k \mid xg^x$. But $x \not\equiv 0\left(mod\ p^k\right)$. Hence, $p^k \mid g^x$. This certainly implies that $p \mid g$. Hence, $g = kp$ for some integer k, a contradiction to supposition that $g \neq tp, t = 0,1,2,\cdots, p^{k-1}-1$. Hence 0 is isolated.

Conversely, suppose 0 is isolated. Let there be any integer k such that $g = kp$ and there exist some x such that $p^k \mid (kp)^x$. Then there must exist some integer $t \not\equiv 0$ such that $t(kp)^t \equiv 0\left(mod\ p^k\right)$. This shows that 0 is not isolated, a contradiction. Therefore $g \neq tp, t = 0,1,2,\cdots, p^{k-1}-1$.

iii) Let $\phi\left(p^k\right)$ be a fixed point together with $g \neq tp, 1 \leq t \leq p^{k-1}-1$. Then,

$$\phi\left(p^k\right)(g)^{\phi\left(p^k\right)} = \phi\left(p^k\right)(tp)^{\phi\left(p^k\right)} \equiv \phi\left(p^k\right)\left(\text{mod } p^k\right)$$

$$\text{so, } (tp)^{\phi\left(p^K\right)} \equiv 1\left(mod\ p^k\right), \text{ since } \left(p^k, \phi\left(p^k\right)\right) = 1$$

This shows that tp is a primitive root of p^k. But $\left(tp, p^k\right) \geq p$. Thus the word primitive root arrive at a contradiction. □

The following corollaries are the simple consequences of above theorem.

Corollary 1. *Let* $V = \{1,2,\cdots, p^k - 1\}$ *be the set of vertices in* $G\left(g, p^k\right)$. *If* $g \in \left\{p, 2p, \cdots, \left(p^{k-1}-1\right)p\right\}$ *then the digraph* $G\left(g, p^k\right)$ *has no fixed point.*

Corollary 2. *If* $g \in \left\{p, 2p, \cdots, \left(p^{k-1}-1\right)p\right\}$ *then* $\phi\left(p^k\right)$ *is not a fixed point.*

Theorem 4. *The digraph* $G\left(g, p^k\right)$ *contains no cycles except fixed points if and only if either g is of order 2 or g is divisible by p.*

Proof. By Lemma 1, $\text{ord}_{p^k} g = 2$ if and only if $g = p^k - 1$ for any integer g. Also by Theorem 1, if $g = p^k - 1$ and x is odd then $f(x) = p^k - x$ otherwise $f(x) = x$. We claim that there exist no cycle of length 2. For otherwise, an odd vertex a must mapped onto $p^k - a \equiv b$ (say), which is of course even and hence b can never adjacent to a since $f(b) \equiv b$, being even, a contradiction. Thus there does not exist any cycle of length > 1. Now if g is a multiple of p then it is trivial that all vertices constitute one component. Also by Theorem 3(i), if g is a multiple of p then 0 is the only fixed point. Thus the digraph must be a tree with root at 0. Consequently $G\left(g, p^k\right)$ contains no cycle of length > 1. □

In **Figure 3**, $g = 15 = 3 \times 5$. By Theorem 4, 0 is the only isolated fixed points.

3. Applications

In recent years, studying graphs through different structural environments like groups, rings, congruences has become much captivating and dominant field of discrete mathematics. These assignments are easy to handle most of the mathematics which is integral based. A variety of graphs have been introduced and characterized regarding their structures through this dynamism. By means of congruences one can inspect numerous enthralling topographies of graphs and digraphs. Thus it becomes interesting to demonstrate that every congruence can generate a graph and hence under certain conditions on these graphs, the nature and solutions of congruences can be discussed. In this section, we discuss the solvability of the congruence and enumerate their solutions using the results given in previous section. The non-trivial (other than $x = 0$) solution of the congruence modulo a single prime p is easy to discuss since every $x < p$ is prime to p. So the congruence $xg^x \equiv x(mod\ p)$ is solvable if and only if $g^x \equiv 1(mod\ p)$ as given in Theorem 0 (4). Hence by Fermat's Little Theorem, the number $p-1$ becomes a solution of $g^x \equiv 1(mod\ p)$. Now if we lift up the modulo from p to its higher powers $p^k, k > 1$, then the vertices which are not prime to p must not follow the fashion as for $k = 1$.

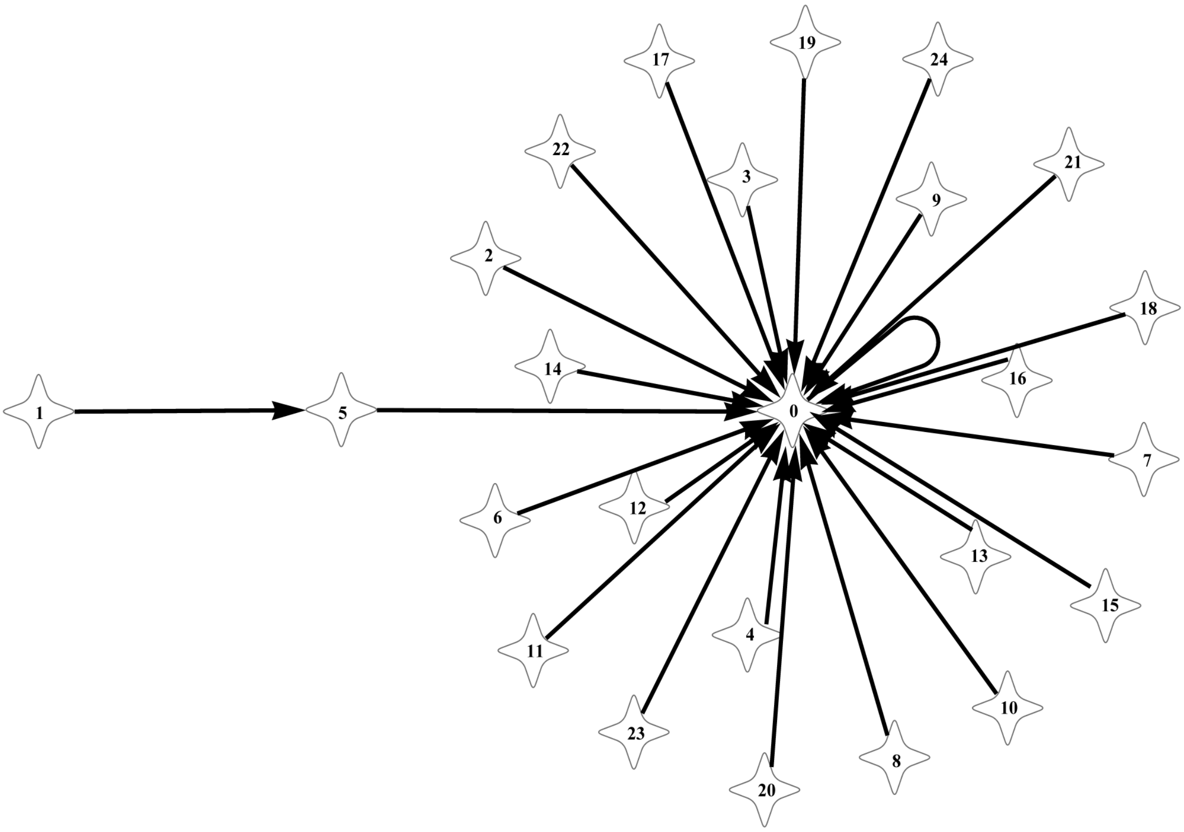

Figure 3. $G(15,25)$.

The following result tackle this case and enumerate the solutions as well. Note that the vertex $x = 0$ is the trivial solution in either case. The proof of the following theorem is simple and can be established using results given in Section 2.

Theorem 5. *Let p be an odd prime and* $k > 1$. *Then the following hold*:

1. If $g \equiv 1(mod\ p)$ then the congruence $xg^x \equiv x\left(mod\ p^k\right)$ is solvable.

2. Let $b \neq 0$ be any integer. If $\text{ord}_{p^k} g = b$ then the congruence $xg^x \equiv x\left(mod\ p^k\right)$ is solvable. In particular, $b, 2b, 3b, \cdots, b\left\lfloor \frac{p^k}{b} \right\rfloor$ all are its $\left\lfloor \frac{p^k}{b} \right\rfloor$ solutions.

3. If *g* is a primitive root of p^k then congruence $xg^x \equiv x\left(mod\ p^k\right)$ has a unique non-trivial solution. Thus, 0 and $p^{k-1}(p-1)$ are the only solutions of $xg^x \equiv x\left(mod\ p^k\right)$.

4. If $g \in \left\{p, 2p, \cdots, \left(p^{k-1} - 1\right)p\right\}$, then the congruence $xg^x \equiv x\left(mod\ p^k\right)$ has no non-trivial solution.

Acknowledgements

We are very thankful to the editor and the reviewers for specially sparing their precious time and forwarding useful comments. We sincerely believe that this has made the manuscript more interesting and informative.

References

[1] Lambert, J.H. (1758) Observationes Variae in Mathesin Puram. *Acta Helvetica Physico-Mathematico-Anatomico-Botanico-Medica*, **3**, 128-168.

[2] Corless, R.M., Gonnet, G.H., Hare, D.E.G. and Jeffrey, D.J. (1993) Lambert's W Function in Maple. *The Maple Technical Newsletter* (*MapleTech*), **9**, 12-22.

[3] Chen, J. and Lotts, M. (2012) Structure and Randomness of the Discrete Lambert Map. *Rose-Hulman Undergraduate Mathematics Journal*, **13**, 63-99.

[4] Corless, R.M., Gonnet, G.H., Hare, D.E.G., Jeffrey, D.J. and Knuth, D.E. (1996) On the Lambert *W* Function. *Advances in Computational Mathematics*, **5**, 329-359. http://dx.doi.org/10.1007/BF02124750

[5] Khalid Mahmood, M. and Ahmad, F. (2015) A Classification of Cyclic Nodes and Enumerations of Components of a Class of Discrete Graphs. *Applied Mathematics and Information Sciences*, **9**, 103-112. http://dx.doi.org/10.12785/amis/090115

[6] Aslam Malik, M. and Khalid Mahmood, M. (2012) On Simple Graphs Arising from Exponential Congruences. *Journal of Applied Mathematics*, Article ID: 292895. http://dx.doi.org/10.1155/2012/292895

[7] Burton, D.M. (2007) Elementary Number Theory. McGraw-Hill.