



**Definition 2.** Digraph A graph in which edges have direction is called directed graphs or digraphs.

## 2 Special Images

: A number  $\beta$  is said to be fixed point of DLTM iff  $\beta^2 g^\beta \equiv \beta \pmod{m}$  for a positive integer  $m$ . The following results are elaborating fixed points and image structures for specific numbers.

**Theorem 1.** Let  $f$  be a DLTM and  $s$  be any odd prime. If  $s$  is any odd prime, and  $h = 2$  then  $t = s - 2$  always map on  $2 \pmod{s}$ .

*Proof.* Suppose

$$\begin{aligned} f(t) &= t^2 h^t \\ \text{then, } f(s-2) &\equiv (s-2)^2 (2)^{s-2} \pmod{s} \\ &\equiv (s-2)^2 2^{s-2} \pmod{s} \end{aligned}$$

Using Euler's formula, we have

$$\begin{aligned} f(s-2) &\equiv ((s-2)^2 2^{-1}) \pmod{s} \\ &\equiv ((-2)^2 2^{-1}) \pmod{s} \\ &\equiv 2 \pmod{s}. \end{aligned}$$

□

**Proposition 1.** Let  $f$  be a DLTM and  $h = s - 1$ . If  $t$  is odd then  $f(t) = s - t^2$  and if  $t$  is even then  $f(t) \equiv t^2 \pmod{s}$ .

*Proof.* Let  $t$  be any odd integer. then

$$t = 2k + 1 \tag{1}$$

As  $h = s - 1$ , we see that

$$f(2k + 1) = (2k + 1)^2 (s - 1)^{2k + 1},$$

Now since  $(s - 1)^2 \equiv 1 \pmod{s}$

$$\begin{aligned} &\equiv ((2k + 1)^2 (s - 1)^{2k} (s - 1)) \pmod{s} \\ &\equiv ((2k + 1)^2 (s - 1)) \pmod{s} \\ &\equiv ((4k^2 + 1 + 4k)(s - 1)) \pmod{s} \\ &\equiv -(2k + 1)^2 \\ &\equiv -t^2 \\ &\equiv s - t^2 \pmod{s}, \end{aligned}$$

Also, if  $t$  is even then it is of the form

$$\begin{aligned} t &= 2k \\ f(t) &= t^2 h^t \\ &\equiv (2k)^2 (s - 1)^{2k} \pmod{s} \\ &\equiv (2k)^2 \\ &\equiv t^2 \pmod{s}. \end{aligned}$$

□

### 3 Power Residue

Recall that an integer  $\alpha$  is a power  $p$ th residue of any prime  $s$  if the congruence  $t^p \equiv \alpha \pmod{s}$  admits a solution in  $t$  modulo  $s$ . In the following result, we discuss the power residues of the map DLTM.

**Theorem 2.** Let  $h$  be an  $n$ th power residue of  $s$ . Then,  $t^2$  is an  $n$ th power residue of  $s$  if and only if  $t^2 h^t$  is an  $n$ th power residue of  $s$ .

*Proof.* Assume first that  $t^2$  is an  $n$ th power residue of  $s$  then there must exist some integer  $b$  such that it satisfies

$$y^n \equiv s^2 \pmod{s}, \quad (2)$$

Equivalently,

$$b^n \equiv t^2 \pmod{s} \quad (3)$$

now since  $h$  is an  $n$ th power residue of  $s$  so we will find some integer for  $u$  such that

$$u^n \equiv h \pmod{s}, \quad (4)$$

This means that

$$t^2 h^t \equiv b^n (u^n)^t \quad (5)$$

$$\equiv (bu^t)^n. \quad (6)$$

this clearly shows that  $t^2 h^t$  is an  $n$ th power residue of  $s$

Conversely, suppose  $t^2 h^t \pmod{s}$  is an  $n$ th power residue. Then we can write

$$t^2 h^t \equiv z^n \pmod{s} \quad \text{for some value of } z \in (\mathbb{Z}/s\mathbb{Z})^*, \quad (7)$$

$h$  is an  $n$ th power residue

$$h = y^n \pmod{s} \quad \text{for some } y \in (\mathbb{Z}/s\mathbb{Z})^*, \quad (8)$$

$$t^2 h^t \equiv z^n \quad (9)$$

$$t^2 h^t h^{-t} \equiv z^n h^{-t} \quad (10)$$

$$\equiv z^n (y^n)^{-t} \quad (11)$$

$$t^2 \equiv z^n (y^{-t})^n \quad (12)$$

$$\equiv (zy^{-t})^n \pmod{s}, \quad (13)$$

$t^2$  is an  $n$ th power residue. □

The following result is easy to prove.

**Corollary 1.** If  $h$  is quadratic residue then  $\frac{s-1}{2} \rightarrow (\frac{s-1}{2})^2 \pmod{s}$ .

**Theorem 3.** If  $s$  is quadratic residue then  $s - 1 \rightarrow 1$ .

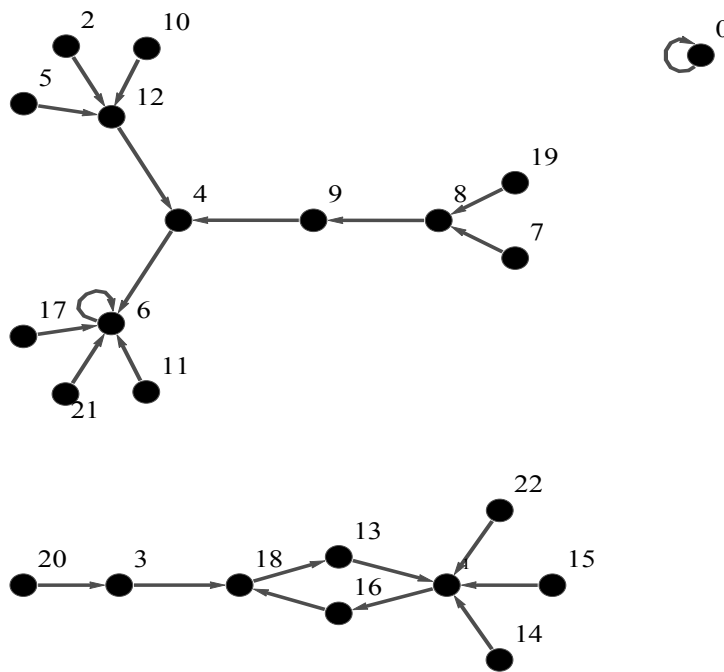


Figure 1. Shows the diagraph  $G(16, 23)$

Proof. Let  $f(t) = t^2h^t$  be a DLTM, then

$$f(s - 1) = (s - 1)^2h^{s-1}, \tag{14}$$

$$Asq^{s-1} \equiv 1 \pmod{s}$$

$$\therefore, h^{s-1} \equiv 1 \pmod{s}, \text{ an hence, } (s - 1)^2 \equiv 1 \pmod{s}.$$

$$\text{Or } f(s - 1) \equiv 1 \pmod{s}. \tag{□}$$

## 4 Continuity of the Map

In this section, we discuss uniformly continuity and continuity of the map for references.

**Theorem 4.** If  $q$  is an odd prime  $d \in \mathbb{Z}_q$  is fixed, and  $h \in 1 + q\mathbb{Z}_q$ , then  $f(t) = t^2h^t - d$  is uniformly continuous for  $t \in \mathbb{Z}$ .

Proof. Suppose  $h = 1 + qA$  where  $A \in \mathbb{Z}_q$ . We're aware of that for any  $\varepsilon > 0$ , there exist an  $N$  such that  $q^{-N} < \varepsilon$ .

Let  $l, m \in \mathbb{Z}$  s.t

$$|l - m|_q \leq q^{-N} < q^{-(N-1)} = \delta \tag{15}$$

or  $(l - m) \in q^N\mathbb{Z}_q$ , and  $l = m + bq^N$  where  $b \in \mathbb{Z}$ , then we must demonstrate that

$$|l^2h^l - d - (m^2h^m - d)|_q < \varepsilon \tag{16}$$

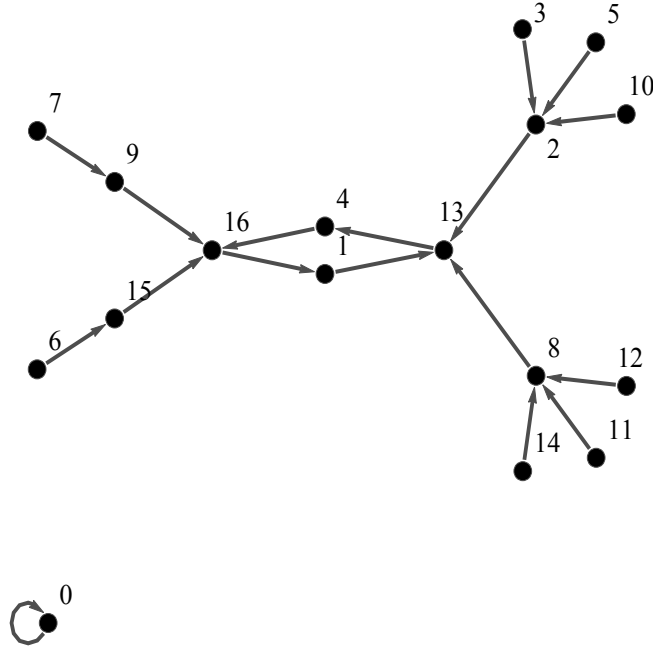


Figure 2. Shows the diagraph  $G(13, 17)$

Note that

$$h^{bq^N} = (1 + qA)^{bq^N} \tag{17}$$

$$= 1 + bq^N qA + \dots + (qA)^{bq^N} \tag{18}$$

$$\in 1 + q^N Z_q. \tag{19}$$

So we know that  $h^{bq^N} - 1 \in q^N Z_q$ , or  $|h^{bq^N} - 1|_q \leq q^{-N}$ . Moreover, since  $m \in Z$ ,  $|m|_q \leq 1$ . Notice that  $|bq^N h^{bq^N}|_q \leq q^{-N}$ . Now, consider

$$|l^2 h^l - m^2 h^m| = |(m + bq^N)^2 h^{m+bq^N} - m^2 h^m|_q \tag{20}$$

$$= |(m^2 + b^2 q^{2N} + 2mbq^N) h^{m+bq^N} - m^2 h^m|_q \tag{21}$$

$$= |m^2 h^{m+bq^N} + b^2 q^{2N} h^{m+bq^N} + 2mbq^N h^{m+bq^N} - m^2 h^m|_q \tag{22}$$

$$= |h^m|_q |m^2 h^{bq^N} + b^2 q^{2N} h^{bq^N} + 2mbq^N h^{bq^N} - m^2|_q. \tag{23}$$

Since  $h \in 1 + qZ_q$ ,  $|h^m|_q = 1$ ,

$$= |m^2 h^{bq^N} + b^2 q^{2N} h^{bq^N} + 2mbq^N h^{bq^N} - m^2|_q \tag{24}$$

$$= |m^2 (h^{bq^N} - 1) + bq^N h^{bq^N} (bq^N + 2m)|_q, \tag{25}$$

$\therefore \alpha = bq^N + 2m$ ,

$$\leq \max(|h^{bq^N} - 1| |h|_q, |\alpha bq^N h^{bq^N}|_q) \tag{26}$$

$$\leq q^N. \tag{27}$$

□

## 5 Special solutions of the Map

Its a converse back way to write solutions of the DLTM type congruences modulo prime number using digraphs. As we are interested to tell after observing the digraphs that which type of congruences are satisfying some special solution and whats such solutions count. The following theorem is an attempt to incorporate the idea behind.

**Theorem 5.** Let  $r$  be an odd prime. For a fixed  $m \in \{1, \dots, r^e\}$  and for  $r \nmid h$  and  $d \in \{1 \dots r^{e-1}(r-1)\}$ , if we consider  $m^2 h^m \equiv d \pmod{r^e}$  and let  $m^2 (h^{-1})^m \equiv \acute{d} \pmod{r^e}$ , then  $d \cdot \acute{d} \equiv m^4 \pmod{r^e}$ . Moreover, if we let  $m^2 (-h)^m \equiv \dot{d} \pmod{r^e}$  then  $\dot{d} \equiv (-1)^m d \pmod{r^e}$ .

*Proof.* We show that  $d \cdot \acute{d} \equiv m^4 \pmod{r^e}$ . Since  $m^2 h^m \equiv d \pmod{r^e}$  and  $m^2 (h^{-1})^m \equiv \acute{d} \pmod{r^e}$ , We could say that

$$d \cdot \acute{d} \equiv (m^2 h^m)(m^2 (h^{-1})^m) \pmod{r^e} \quad (28)$$

$$\equiv m^4 (h^m)(h^{-m}) \pmod{r^e} \quad (29)$$

$$\equiv m^4 \pmod{r^e}. \quad (30)$$

Hence,  $d \cdot \acute{d} \equiv m^4 \pmod{r^e}$ . Now we must demonstrate that  $\dot{d} \equiv (-1)^m d \pmod{r^e}$ ,

$$\dot{d} \equiv m^2 (-h)^m \pmod{r^e} \quad (31)$$

$$\equiv m^2 (-1)^m h^m \pmod{r^e} \quad (32)$$

$$\equiv (-1)^m m^2 h^m \pmod{r^e} \quad (33)$$

$$\equiv (-1)^m d \pmod{r^e}. \quad (34)$$

Thus

$$\dot{d} \equiv (-1)^m d \pmod{r^e}.$$

□

**Proposition 2.** Let  $r$  be an odd prime and  $h$  be a generator modulo  $r^e$ . If  $d = \frac{r^e + r^{e-1} + 1}{4}$  and  $r^e - 1$  is the only element of order 2 in the multiplicative group of  $Z/r^e Z$ , Then  $m = \frac{r^e - r^{e-1}}{2}$  is one of the solution to

$$m^2 h^m \equiv d \pmod{r^e}. \quad (35)$$

*Proof.* We can see that by hypothesis

$$m^2 h^m - d = \left(\frac{r^e - r^{e-1}}{2}\right)^2 h^{\frac{r^e - r^{e-1}}{2}} - \frac{r^e + r^{e+1}}{4} \quad (36)$$

$$\equiv \left(\frac{r^e - r^{e-1}}{2}\right)^2 (r^e - 1) - \frac{r^e + r^{e+1}}{4} \pmod{r^e} \quad (37)$$

$$= \frac{(r^{2e} - r^{2e-2} - 2r^{e+e-1})(r^e - 1) - r^e + r^{e+1}}{4} \pmod{r^e} \quad (38)$$

$$= \frac{r^e(r^e - r^{e-2} - 2r^{e-1})(r^e - 1) - r^e + r^{e+1}}{4} \pmod{r^e} \quad (39)$$

$$= \frac{r^e(r^e - r^{e-2} - 2r^{e-1})(r^e - 1) - r^e - r^{e+1}}{4} \pmod{r^e} \quad (40)$$

$$= \frac{r^e(r^e - r^{e-2} - 2r^{e-1})(r^e - 1) - r^e(1 + r)}{4} \pmod{r^e} \quad (41)$$

$$= \frac{r^e[(r^e - r^{e-2} - 2r^{e-1})(r^e - 1) - (1 + r)]}{4} \pmod{r^e} \quad (42)$$

$$\equiv 0 \pmod{r^e}. \quad (43)$$

□

## 6 Cycles

Recall that the vertices  $v_1, v_2, \dots, v_{k-1}, v_k$  forms a  $k$  length cycle if and only if

$$v_1^2 h^{v_1} \equiv v_2 \pmod{m}$$

$$v_2^2 h^{v_2} \equiv v_3 \pmod{m}$$

⋮

$$v_k^2 h^{v_k} \equiv v_1 \pmod{m},$$

The following theorem illustrate the cyclic behaviour of the map DLTM, Let  $f^n(t)$  denote the function  $f(t) = t^2 h^t \pmod{s}$  applied  $n + 1$  times (e.g.  $f^2(t) = f(f(t))$ ). Then

$$f^n(t) = (f^{n-1}(t))^2 h^{f^{n-1}(t)} \quad (44)$$

$$f^{n+1}(t) = (f^n(t))^2 h^{f^n(t)}. \quad (45)$$

*Proof.* we prove it by induction.

Let

$$f^0(t) = t \quad (46)$$

$$f^1(t) = f(t) = t^2 h^t, \quad (47)$$

suppose  $n = k$

$$(f^n(t)) = (f^{n-1}(t))^2 h^{f^{n-1}(t)} \pmod{s}. \quad (48)$$

Then  $n = k + 1$

$$f(f^n(t)) = f((f^{n-1}(t))^2 h^{f^{n-1}(t)}) \tag{49}$$

$$= ((f^{n-1}(t))^2 h^{f^{n-1}(t)})^2 h^{(f^{n-1}(t))^2 h^{f^{n-1}(t)}} \tag{50}$$

$$= (f^{n-1}(t))^4 h^{2f^{n-1}(t)} (f^{n-1}(t))^2 h^{f^{n-1}(t)} \tag{51}$$

$$= (f^{n-1}(t))^2 h^{f^{n-1}(t)} (f^{n-1}(t))^2 h^{f^{n-1}(t)} (f^{n-1}(t))^2 h^{f^{n-1}(t)} \tag{52}$$

$$= f(n)f(n)h^{f^n(t)} \tag{53}$$

$$f^{n+1}(t) = (f(n))^2 h^{f^n(t)}. \tag{54}$$

□

The following are the few results without proof regarding cycles and components

**Theorem 6.** The Functional graphs of  $t \mapsto t^2 h^t \pmod s$ ,  $h = s - 1$  and  $s \equiv 3 \pmod 4$  are the union of disjoint cycle, here  $s$  is prime.

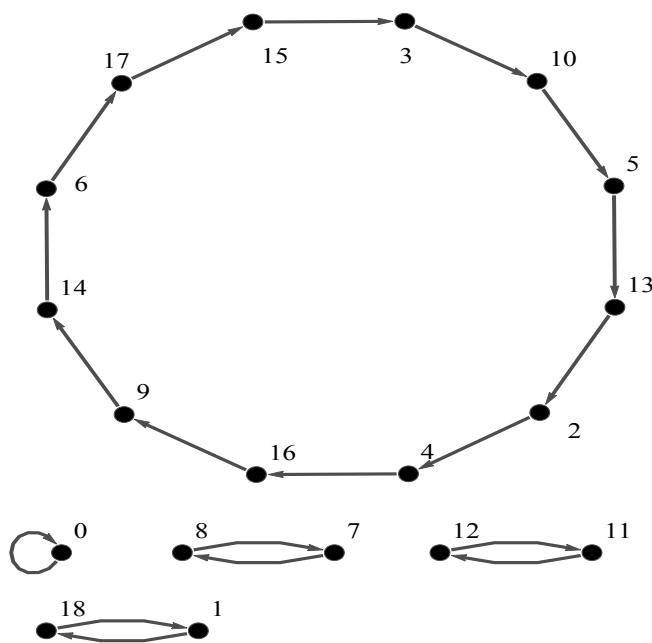


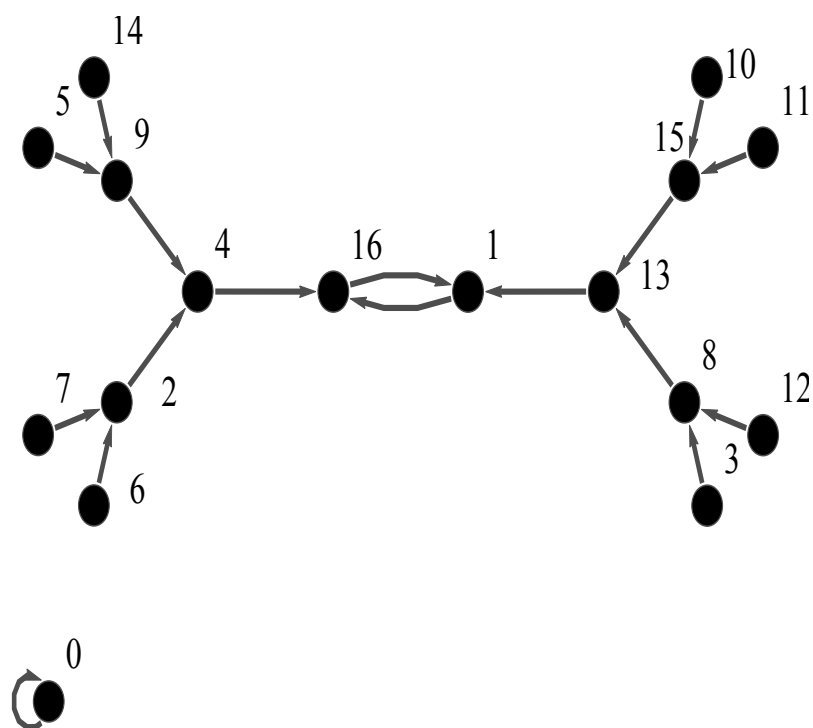
Figure 3. Shows the diagraph  $G(18, 19)$

**Theorem 7.** Let  $f$  be DLTM. Let  $s$  be an odd prime. if  $h = s - 1$  there exist a cycle of length two between 1 and  $s - 1$ .

**Theorem 8.** Every component contains a cycle.

**Theorem 9.** Let  $f$  be DLTM. There exists a cycle of length  $w > 1$  in  $G(n)$  under DLTM,  $f(t) = t^2 h^t$  with  $\text{ord}_n^h \mid t$  if and only if  $w$  is the least positive integer such that  $2^w \equiv 1 \pmod s$ , where  $s$  is odd positive divisor of  $\lambda(n)$ , and  $\lambda(n)$  is the Charmical Lambda





**Figure 4.** Shows the digraph  $G(16, 17)$

## References

- [1] Lambert, J.H. (1758) *Observationes Variæ 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] Scott, TC; Babb, JF; Dalgarno, A; Morgan, John D (Aug 15, 1993). "The calculation of exchange forces: General results and specific models". *J. Chem. Phys. American Institute of Physics*. 99 (4): 2841-2854.
- [4] M. Khalid Mahmood, Lubna Anwar(2016). *Loops in Digraphs of Lambert Mapping Modulo Prime Powers: Enumerations and Applications. Advances in Pure Mathematics*, 6, 564-570.