PROBLEMS MOTIVATED BY CRYPTOLOGY: COUNTING FIXED POINTS AND TWO-CYCLES OF THE DISCRETE LAMBERT MAP

DARA ZIRLIN

A THESIS PRESENTED TO THE FACULTY OF MOUNT HOLYOKE COLLEGE IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF BACHELOR OF ARTS WITH HONORS.

DEPARTMENT OF MATHEMATICS AND STATISTICS

SOUTH HADLEY, MASSACHUSETTS

MAY 2015

Acknowledgements

I would like to thank my advisor, Professor Margaret Robinson, for her guidance and support throughout this project. Thanks to Professors Harriet Pollatsek and Samuel Mitchell for serving on my thesis defense panel. Thank you to the Mount Holyoke College Mathematics and Statistics Department for their support. In addition, I would like to thank my friends and family for their encouragement.

Abstract

In this thesis, we begin with a brief introduction to some relevant number theory and to digital signature schemes (DSS). We explain how information about the discrete Lambert map (DLM) [2] relates to DSS security. Next we introduce results from p-adic analysis. We summarize the results from previous work on the DLM and extend these results to $p = 2$. In the main part of this thesis we explain our results counting fixed points and two-cycles of the DLM. That is, for a fixed prime p and a nonzero integer g where $p \nmid g$ and e is a positive integer, we will count the number of fixed points or solutions to $xg^x \equiv x \pmod{p^e}$ and the number of two cycles or simultaneous solutions to $xg^x \equiv y \pmod{p^e}$ and $yg^y \equiv x \pmod{p^e}$ where x and y range through appropriate sets of integers. This work is a continuation of work started by Holden and Robinson in [7] and their students from the 2014 Mount Holyoke summer REU program: Anne Waldo and Caiyun Zhu [10], Yu Liu [8], and Abigail Mann and Adelyn Yeoh [9].

Contents

Introduction

The goal of this thesis is to investigate the number of solutions to the congruence $xg^x \equiv x \pmod{p^e}$ and also simultaneous solutions to the congruences $xg^x \equiv y \pmod{p^e}$ and $yg^y \equiv x \pmod{p^e}$, where p is a fixed prime, g and e are fixed integers greater than zero, $p \nmid g$, $m = \mathrm{ord}_p(g)$, and $1 \leq x, y \leq p^e m$. However, before we discuss the answers and their proofs, we must introduce some important number theoretical results, discuss the motivation for the problem, introduce p-adic analysis, and review previous results.

In section 1, we present the number theory results that are needed to prove the main theorems in this thesis. In section 2, we introduce the ElGamal digital signature scheme as the motivation for analyzing the solutions to the discrete Lambert map and, hence, as motivation for the main problems which we solve in this thesis. In section 3, we will introduce p-adic numbers and Hensel's Lemma as well as the $(p-1)$st roots of unity in $\mathbb{Z}_p$ and some key notation for our theorems. In section 4, we recall Anne Waldo and Caiyun Zhu's solution to counting solutions to $xg^x \equiv c \pmod{p^e}$ [10] and Yu Lui's solution to counting collisions of the discrete Lambert map, $xg^x \equiv yg^y \pmod{p^e}$ [8]. We note that both these results were for odd primes only and we extend these theorems to the case where $p = 2$. In section 5, we discuss our solution to the problem of counting the fixed points and two cycles of the discrete Lambert map for all primes p. Finally, we conclude with a discussion of questions for further research in this area.

1. Some important basic theorems in number theory

We begin with the basic definitions, propositions, lemmas, and theorems from number theory which will be needed later in this thesis. All the proofs are very straightforward, and so we only include a few of them.

Definition 1.1 (Primes)**.** A prime is a positive number greater than 1 that only has positive integer divisors that are 1 and itself.

For example, 2, 3 and 17 would be primes. However, -3, 1, $6 = 3 \cdot 2$, and 3.1 are not primes.

Definition 1.2 (Integer division)**.** Let a and b be any integers. We say that b divides a and write that $b \mid a$, if there exists an integer c such that $a = bc$.

Example 1.3. Let $a = 6$ and $b = -2$. We say that b divides a, or $b \mid a$, because $c = -3$ exists such that $a = bc$.

Example 1.4. Let $a = 0$ and $b = -6$. We say that b divides a, or $b \mid a$, because $c = 0$ exists such that $a = bc$. Thus we see that any integer divides 0. However, 0 does not divide any nonzero integer since the equation $a = 0c$ has no integer solution for c when a is nonzero.

Proposition 1.5. *Let $m, a, b \in \mathbb{Z}$. If $m \mid a$ and $m \mid b$, then $m \mid a + b$.*

Proof. Since $m \mid a$ and $m \mid b$, then there exist $k, l \in \mathbb{Z}$ such that $a = m \cdot k$ and $b = m \cdot l$. Thus, $a + b = m \cdot k + m \cdot l = m(k + l)$. So, by the definition of integer division, since $k + l \in \mathbb{Z}$, then $m \mid a + b$. □

Definition 1.6 (Integer congruence)**.** Let m be a positive integer. Let $a, b \in \mathbb{Z}$. We say that a is congruent to b modulo m, if m divides $a - b$, that is if $m \mid a - b$. We write this relation between a and b more concisely as $a \equiv b \pmod{m}$.

Following are six basic propositions whose proofs use the definition of congruence modulo m.

Proposition 1.7 (Congruence is an equivalence relation)**.** *Let m be a positive integer. Let $a, b, c \in \mathbb{Z}$. Then, $a \equiv a \pmod{m}$. If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.*

Proof. The first two parts can be easily shown, so we will only show the third.

If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then, by definition, $m \mid a - b$ and $m \mid b - c$. Thus, $m \mid a - b + b - c = a - c$, by Proposition 1.5. So, by definition, $a \equiv c \pmod{m}$. □

Proposition 1.8. *Let m be a positive integer. Let $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.*

Proposition 1.9. *Let m be a positive integer. Let $a, b, c \in \mathbb{Z}$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$.*

Proof. Note if $a \equiv b \pmod{m}$, then $m \mid a - b$. Note that $m \mid (a - b)c = ac - bc$. Thus, $ac \equiv bc \pmod{m}$. Similarly one can show $bc \equiv bd \pmod{m}$. Thus, using Proposition 1.7, $ac \equiv bd \pmod{m}$. □

Proposition 1.10. *Let m be a positive integer. Let $a, b \in \mathbb{Z}$. Let d be a positive integer such that $d \mid m$. If $a \equiv b \pmod{m}$, then $a \equiv b \pmod{d}$.*

Proof. If $a \equiv b \pmod{m}$, then $m \mid a - b$, meaning there exists $c \in \mathbb{Z}$ such that $a - b = m \cdot c$. Since $d \mid m$, there exists $e \in \mathbb{Z}$ such that $m = d \cdot e$. Therefore, $a - b = m \cdot c = d \cdot e \cdot c = d(e \cdot c)$, where $e \cdot c \in \mathbb{Z}$. Therefore, by definition of Integer Division, $d \mid a - b$. Thus, $a \equiv b \pmod{d}$, by definition of Integer Congruence. □

Proposition 1.11. *Let m be a positive integer. Let $a, b \in \mathbb{Z}$. Let c be a positive integer. If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$*

Following are some less basic and still very important properties pertaining to congruences.

Lemma 1.12. *Let m be a positive integer. Let $a, b \in \mathbb{Z}$. Let c be a positive integer. If $a \equiv b \pmod{m}$, then $a^c \equiv b^c \pmod{m}$.*

Proof. If $a \equiv b \pmod{m}$, then $m \mid a - b$. Note that

$$a^c - b^c = (a-b)(a^{c-1} + a^{c-2}b + \cdots + ab^{c-2} + b^{c-1}).$$

Thus, $m \mid a^c - b^c$. Therefore, $a^c \equiv b^c \pmod{m}$. □

Definition 1.13 (Greatest Common Divisor)**.** Note that $\gcd(a, b)$ stands for the greatest common divisor of a and b, that is c such that $c \mid a, b$ and if $d \mid a, b$, then $d \mid c$. Note we will always define the greatest common divisor to be positive.

Lemma 1.14 (Bezout's Lemma)**.** *Let $a, b \in \mathbb{Z}$ such that a and b are not both zero. Then there exists integers m, n such that $ma + nb = \gcd(a, b)$. Moreover, if there exists m, n such that $ma + nb = c$ for some integer c, then $\gcd(a, b) \mid c$.*

Proof. See section 3.3 of [12] for more. □

Example 1.15. Consider $\gcd(12, 18)$. Note $6 \mid 12$ and $6 \mid 18$. The only other numbers which divide 12 and 18 are $1, -1, 2, -2, 3, -3, -6$, which all divide 6. Thus, $\gcd(12, 18) = 6$. Note, $\gcd(12, 18) \neq -6$, since we define the greatest common divisor to be positive.

Lemma 1.16. *Let m be a positive integer. Let $a \in \mathbb{Z}$. Let $c = \gcd(a, m)$. Then $\gcd(\frac{a}{c}, \frac{m}{c}) = 1$.*

Proof. By definition of c, $c \mid a$ and $c \mid m$. By Bezout's Lemma, there exists integers x, y such that $c = ax + my$. Thus, $1 = \frac{a}{c}x + \frac{m}{c}y$, where $\frac{a}{c}$ and $\frac{m}{c}$ are integers. So, by Bezout's Lemma, $\gcd(\frac{a}{c}, \frac{m}{c}) = 1$. □

Lemma 1.17. *Let m be a positive integer. Let $a, x, y \in \mathbb{Z}$. Then $ax \equiv ay \pmod{m}$ if and only if $x \equiv y \pmod{\frac{m}{\gcd(m,a)}}$.*

Proof. Note that by definition $\gcd(m, a)$ divides both a and m. So we know that there exist integers b, n such that $m = n \cdot \gcd(m, a)$ and $a = b \cdot \gcd(m, a)$. Note, by Proposition 1.16, $\gcd(n, b) = 1$.

To show sufficiency we assume that $x \equiv y \pmod{n}$, so that $n \mid x - y$ or $x - y = nk$ for some $k \in \mathbb{Z}$. Now, $\gcd(m, a)(x-y) = \gcd(m, a)nk = mk$ by the definition of n. So $b \cdot gcd(m, a)(x - y) = bmk$. By definition of b, this means $a(x - y) = bmk$. Thus, $m \mid a(x - y) = ax - ay$. Thus, $ax \equiv ay \pmod{m}$.

Now, consider $ax \equiv ay \pmod{m}$. Then, $m \mid ax - ay$ or $ax - ay = mk$ for $k \in \mathbb{Z}$. Thus, $b \gcd(m, a)(x - y) = a(x - y) = mk$. So, by the definition of n, $b \gcd(m, a)(x - y) = n \gcd(m, a)k$. Thus, $b(x - y) = nk$. Since, $\gcd(n, b) = 1$ this means $n \mid (x - y)$. Therefore, $x \equiv y \pmod{\frac{m}{\gcd(m,a)}}$. □

Before we introduce more helpful properties, we make a remark and give two more definitions.

Remark 1.18. Note that if $\gcd(m, a) = 1$ then an inverse of a modulo m exists. That is an x such that $ax \equiv 1 \pmod{m}$. This follows from Bezout's Lemma. We denote the inverse as a^{-1}. The inverse of a^l can be denoted as a^{-l}. Thus negative exponents are defined. For more information please see [13], the section on cyclic groups.

Example 1.19. Consider 2 modulo 5. Note $\gcd(2, 5) = 1$. Also $2 \cdot 3 + 5 \cdot (-1) = 1$. Thus, $2 \cdot 3 \equiv 1 \pmod{5}$ and 3 is the inverse of 2 modulo 5, so that $2^{-1} \equiv 3 \pmod{5}$.

Definition 1.20 (Order of an integer modulo m)**.** Let m and a be integers such that $\gcd(m, a) = 1$ and m is positive. The **order of a modulo m** is the smallest positive integer, n, such that such that $a^n \equiv 1 \pmod{m}$. We write

the order of a modulo m concisely as $n = \text{ord}_m(a)$. Note that such an n will always exist. See section 9.1 and 6.3 of [12] for more detail.

Example 1.21. Consider 2 modulo 5. Note $\gcd(2, 5) = 1$. We see that $2^1 \equiv 2 \pmod 5$, $2^2 \equiv 4 \pmod 5$, $2^3 \equiv 3 \pmod 5$, and $2^4 \equiv 1 \pmod 5$. Thus, the order of 2 modulo 5 is 4 or $\text{ord}_5(2) = 4$.

Now, consider 3 modulo 8. Note $\gcd(3, 8) = 1$. We see that $3^1 \equiv 3 \pmod 8$ and $3^2 \equiv 1 \pmod 8$. Hence the order of 3 modulo 8 is 2 or $\text{ord}_8(3) = 2$.

Remark 1.22. Note that for $a \not\equiv 1 \pmod m$ then $\text{ord}_m(a) > 1$ and since $a \cdot a^{\text{ord}_m(a)-1} \equiv a^{\text{ord}_m(a)} \equiv 1 \pmod m$, the inverse of a modulo m will be $a^{\text{ord}_m(a)-1}$.

The following is a result pertaining to the order of an integer a modulo m.

Proposition 1.23. *Let m and a be integers such that $m > 0$ and $\gcd(m, a) = 1$. If $a^t \equiv 1 \pmod m$ for some $t \in \mathbb{Z}$ then $\text{ord}_m(a) \mid t$.*

Proof. Note that by dividing by $\text{ord}_m(a)$ we can find a quotient k and remainder c such that $t = c + k \cdot \text{ord}_m(a)$ for $0 \leq c < \text{ord}_m(a)$ and $c, k \in \mathbb{Z}$. Then $1 \equiv a^t \equiv a^{c+k\cdot\text{ord}_m(a)} \equiv a^c a^{k\cdot\text{ord}_m(a)} \equiv a^c \pmod m$. Since $0 \leq c < \text{ord}_m(a)$ and $a^c \equiv 1 \pmod m$, by the definition of order $c = 0$. Thus, $\text{ord}_m(a) \mid t$. □

For the next definition, lemma, and theorem, we will be focusing on the case when $m = p$, where p is a prime, for the sake of simplicity. While there are similar results for m not a prime, for this paper the case when m is a prime will suffice.

Definition 1.24 (Generators modulo p)**.** Let p be a prime integer and a be an integer such that $\gcd(p, a) = 1$. Then we say that a is a generator modulo p if $ord_p(a) = p - 1$.

Remark 1.25. Note, this that a being a generator modulo p is equivalent to saying that for every integer g such that $g \not\equiv 0 \pmod{p}$ there exists a $t \in \mathbb{Z}$ such that $a^t \equiv g \pmod{p}$. See section 9.1 of [12] for more detail.

Example 1.26. Note that 2 is a generator modulo 5 because $2^1 \equiv 2 \pmod{5}$, $2^2 \equiv 4 \pmod{5}$, $2^3 \equiv 3 \pmod{5}$, and $2^4 \equiv 1 \pmod{5}$. Thus, 2 is a generator modulo 5 because $\mathrm{ord}_5(2) = 4$ and $\{2^t \text{ for } t \in \mathbb{Z}\} = \{1, 2, 3, 4\}$.

Theorem 1.27. *Let p be a prime. Then there is always a generator modulo p.*

Proof. Please see [12] Corollary 9.8.1 in the section on primitive roots. □

The following results are some properties pertaining to the order of an element and generators modulo p.

Lemma 1.28. *Let p be a prime and a be an integer such that $\gcd(p, a) = 1$. Suppose a is a generator modulo p. Then $s \equiv t \pmod{p-1}$ if and only if $a^s \equiv a^t \pmod{p}$.*

Proof. First, suppose $a^s \equiv a^t \pmod{p}$. Then $a^{s-t} \equiv 1 \pmod{p}$. By Proposition 1.23, $\mathrm{ord}_p(a) \mid s - t$. Since $\mathrm{ord}_p(a) = p - 1$, $s \equiv t \pmod{p-1}$.

Now, suppose $s \equiv t \pmod{p-1}$. Note $p - 1 = \mathrm{ord}_p(a)$ and $\mathrm{ord}_p(a) \mid s - t$. Thus, $p - 1 \mid s - t$. Therefore, $a^{s-t} \equiv 1 \pmod{p}$ implying $a^{s-t}a^t \equiv 1 \cdot a^t \pmod{p}$ and $a^s \equiv a^t \pmod{p}$. □

Theorem 1.29 (Fermat's Little Theorem)**.** *Let p be a prime and a be an integer such that $\gcd(a, p) = 1$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Note that by Theorem 1.27, there exists g, an integer modulo p, such that g is a generator modulo p. Thus, there exists positive k such that $a \equiv g^k \pmod{p}$. So $a^{p-1} \equiv (g^k)^{p-1} \equiv (g^{p-1})^k \equiv 1 \pmod{p}$, by Definition 1.24. So $a^{p-1} \equiv 1 \pmod{p}$ □

Here is a generalization of Fermat's Little Theorem.

Theorem 1.30 (Euler's Theorem)**.** *Consider integers a and n such that $n > 0$ Let $\phi(n) = |\{d > 0$ such that $\gcd(d, n) = 1\}|$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Proof. Please see Section 6.2 of [12]. □

Now we will present one last and very important theorem, the Chinese Remainder Theorem.

Theorem 1.31 (Chinese Remainder Theorem)**.** *Let $m_1, \ldots, m_r$ be positive integers such that $\gcd(m_i, m_j) = 1$ for all $i \neq j$. Consider the system of congruences*

$$x \equiv a_1 \pmod{m_1}, \cdots, x \equiv a_r \pmod{m_r}.$$

Then there will be one unique solution x to this system such that $0 \leq x < M$, where $M = m_1 m_2 \cdots m_r$.

Proof. First, let us construct a solution to this system to show there is one. Let $M_k = \frac{M}{m_k}$. Note that $\gcd(M_k, m_k) = 1$. Thus, by Remark 1.18, M_k has a multiplicative inverse modulo m_k. We will call this inverse y_k. Thus, $M_k y_k \equiv 1 \pmod{m_k}$.

Then, construct the integer x so that

$$x = a_1 y_1 M_1 + \cdots + a_r y_r M_r.$$

For any fixed i and j where $i \neq j$ we see that $a_i y_i M_i \equiv 0 \pmod{m_j}$ since $m_j \mid M_i$. Thus,

$$x \equiv a_j y_j M_j \pmod{m_j}$$

$$x \equiv a_j \pmod{m_j}.$$

Therefore, the x that we constructed is an integer solution to the system of congruences.

Now, let us show that x can be taken uniquely such that $0 \leq x < M$. Suppose x and x' are two integers that both satisfy the system of congruences. We see that $x \equiv x' \equiv a_i \pmod{m_i}$. So $m_i \mid x - x'$ for all $1 \leq i \leq r$.

Since $\gcd(m_i, m_j) = 1$ for all $i \neq j$, $\frac{x-x'}{m_1 m_2}$ is an integer. Continuing $\gcd(m_1 m_2, m_3) = 1$, so $\frac{x-x'}{m_1 m_2 m_3}$ is an integer. Following in the same manner $\frac{x-x'}{m_1 \cdots m_r} = \frac{x-x'}{M}$ is an integer. So $M \mid x - x'$. Thus, $x \equiv x' \pmod{M}$. Thus, there is a unique solution x to the system of congruences such that $0 \leq x < M$. □

2. The ElGamal digital signature scheme and its connection to the discrete Lambert map

Before we begin, note that the discrete Lambert map is the map $x \to xg^x$.

Our analysis of the discrete Lambert function is motivated by the need to test the security of digital signature schemes. Think of the signature card you sign at your bank. A teller can compare it with your checks to verify that you really signed a check. The idea of a digital signature is very similar, except it is a number that verifies your identity and can be exchanged over the Internet. Thus, like a real signature, a digital signature must be identifiable as yours, without others being able to replicate it.

Thus, if Alice wanted to send a message to Bob, then the message must have two parts, the actual message and the digital signature that verifies that Alice is the person actually sending a specific message. Bob then must have some method for verifying that the signature really is Alice's. Suppose Frank wanted to forge a message from Alice. We must make sure that the system we create is such that Bob will be able to tell the message is not from Alice. Note we will not be able to tell who sent it, just that Alice did not.

Before we introduce the ElGamal digital signature scheme, we must discuss the message itself. For the message to be sent it must be in number form.

There are many ways to create a number from a series of characters. One way is to identify each character with a 2 digit number. For example "a" could be identified with "01", "b" with 02, and so on. The only problem with this system is that if a letter that identifies with a number whose first digit is 0 is at the beginning, then the zero will be dropped off. For example, if our word was "ape", then it would technically be turned into the number 011605, which would usually be represented as the number 11605. So if we try to translate back into English going from left to right, we do not know if the first letter corresponds to 01 or to 11. Thus, when converting back into English we start with the last two digits of the number-message and move from right to left. So we know the last letter corresponds to 05 and must be "e". The second to last letter corresponds to 16 and must be "p". Thus the first letter must correspond to 1, which means it really was 01 and must be "a".

From now on we will think of a message as a number instead of a list of letters.

Returning to digital signature schemes, we will now discuss one such scheme, the ElGamal digital signature scheme. Alice picks a large prime p. This prime is assigned to her and will be public knowledge. She might use the same prime for many messages. In addition, Alice picks a number g such that $1 \leq g \leq p-2$ and $g^a \not\equiv 1 \pmod{p}$ for all $0 < a < p-1$. Thus we know that g is a generator modulo p and $\text{ord}_p(g) = p-1$. Alice will make public the p and g that she has chosen.

Now, Alice must choose a fixed x such that $1 \leq x \leq p-2$. Alice must not share what x is with anyone. However, she should compute h such that $g^x \equiv h \pmod{p}$ and make h public along with p and g.

Now, Alice's message must be turned into a number, M, such that $1 \leq M \leq p-1$ and $\gcd(M, p-1) = 1$. If M is larger than $p-1$, it can be split into multiple message blocks. Her message M can also be made public.

Next, Alice must randomly choose a number y such that $1 \leq y \leq p-2$ and $\gcd(y, p-1) = 1$. Now, it is important to note that with every new message y should change. In addition, y should be kept private.

Now, Alice should compute s_1 and s_2 where

$$s_1 = g^y \pmod{p}$$

and

$$s_2 = \frac{M - xs_1}{y} \pmod{p-1}.$$

Alice's signature will be (s_1, s_2), which she should make public.

It is important to note that since $\gcd(y, p-1) = 1$, y has a multiplicative inverse modulo p, so s_2 is well defined.

To verify that M was really written by Alice, Bob should compute v_1 and v_2 such that

$$v_1 = h^{s_1} s_1^{s_2} \pmod{p}$$

and

$$v_2 = g^M \pmod{p}.$$

If Alice really created the message, then $v_1 = v_2$. To see that v_1 should equal v_2 we give the following illustrative computation modulo p.

$$\begin{aligned} v_1 &\equiv h^{s_1} {s_1}^{s_2} \pmod{p} \\ &\equiv (g^x)^{s_1} (g^y)^{s_2} \pmod{p} \\ &\equiv g^{xs_1} g^{ys_2} \pmod{p} \\ &\equiv g^{xs_1} g^{y\frac{M-xs_1}{y}} \pmod{p} \\ &\equiv g^{xs_1} g^{M-xs_1} \pmod{p} \\ &\equiv g^M \pmod{p}. \end{aligned}$$

This calculation gives the flavor of why v_1 should equal v_2 if s_1 and s_2 were calculated correctly.

In this way, if Alice sent the message, then Bob will believe she sent the message. However, can Frank create a message with a signature that tricks Bob into thinking Alice sent the message? One way to forge a message, would be to create our own M, to fix s_2, and solve for s_1 such that

$$h^{s_1}{s_1}^{s_2} \equiv g^M \pmod{p}$$

holds for your M and s_2 and Alice's g and p. Then Bob would find that $v_1 = v_2$ and assume incorrectly that Alice sent the message.

Note that solving $h^{s_1}{s_1}^{s_2} \equiv g^M \pmod{p}$ is equivalent to solving

$$h^{s_1{s_2}^{-1}}s_1 \equiv g^{M{s_2}^{-1}} \pmod{p},$$

which is

$$s_1(h^{{s_2}^{-1}})^{s_1} \equiv g^{M{s_2}^{-1}} \pmod{p}.$$

Setting $a = h^{{s_2}^{-1}}$ and $b = g^{M{s_2}^{-1}}$, Carl must solve $s_1 a^{s_1} \equiv b \pmod{p}$.

Here we see the motivation for studying the discrete Lambert map. We want to analyze the behavior of the discrete Lambert map so we will have a more complete understanding of how easy it might be to forge a signature.

Now, you may be asking yourself about the p^e we discussed before instead of the p. It turns out there is a generalized ElGamal digital signature scheme where Alice selects a number n instead of a prime p. So we would be interested in $s_1 a^{s_1} \equiv b \pmod{n}$. However, due to the Chinese Remainder Theorem, we can solve a problem modulo n by breaking it up into the smaller problem of solving the congruence modulo p^e for all factors p^e in the prime factorization of n.

In [2] Chen and Lotts investigated $xg^x \equiv y \pmod{p}$. In [10] Waldo and Zhu investigated $xg^x \equiv y \pmod{p^e}$. In [3], Holden and Moree investigated

two-cycles and fixed points of $x \to g^x$. We wanted to compare their solutions with ours. Our primary goal is to count simultaneous solutions to $xg^x \equiv y \pmod{p^e}$ and $yg^y \equiv x \pmod{p^e}$ or two cycles of the discrete Lambert map. To accomplish this goal we also need to count solutions to $xg^x \equiv x \pmod{p^e}$ or fixed points of the discrete Lambert map.

3. A brief introduction to p-adic analysis

In this chapter we will introduce the p-adic numbers and prove Hensel's Lemma, a crucial tool in p-adic analysis. The p-adic numbers will provide us with a way to use the continuous ideas of calculus to solve discrete problems involving solutions modulo p^e.

The p-adic numbers are analogous to the real numbers. Indeed they arise from the rational numbers in just the same way the real numbers arise.

In order to define both the real numbers and the p-adic numbers, we must begin with an absolute value on the rational numbers.

Definition 3.1. An absolute value is a map from $\mathbb{Q}$ to the nonnegative rational numbers with the following properties. For all $a, b \in \mathbb{Q}$

(1) $\mid a \mid \geq 0$ and $\mid a \mid = 0$ if and only if $a = 0$
(2) $\mid a \cdot b \mid = \mid a \mid \cdot \mid b \mid$
(3) $\mid a + b \mid \leq \mid a \mid + \mid b \mid$

Definition 3.2. The usual absolute value on $\mathbb{Q}$, which we will denote by $\mid \cdot \mid_\infty$, is defined as follows for $a \in \mathbb{Q}$:

$$\mid a \mid_\infty = \begin{cases} a & \text{for } a \geq 0 \\ -a & \text{for } a < 0, \end{cases}$$

It can be verified that the usual absolute value has properties (1), (2), and (3) above.

The real numbers can be constructed from the rational numbers using the usual absolute value and Cauchy sequences of the rational numbers.

Definition 3.3. A sequence of rational numbers $\{a_n\}$ is a *Cauchy sequence* with respect to some absolute value $|\cdot|$ if for any $\epsilon > 0$ there exists a positive integer N such that $|\, a_i - a_j \,| < \epsilon$ for all $i, j > N$.

Please note that every Cauchy sequence converges. See Theorem 10.11 of [14] for more detail.

We will define an equivalence relation on Cauchy sequences below. When we use the absolute value $|\cdot|_\infty$, the equivalence classes will give us the real numbers. The following example shows why we need equivalence classes.

We can define the real number π to be the limit of the sequence

$$\{3, 3.1, 3.14, 3.141, 3.1415, \dots\}.$$

Since we have methods for computing the next rational number in the sequences we also know that

$$\{3.1, 3.11, 3.141, 3.1411, 3.14151, \dots\}$$

also converges to the real number π. So when we write $\pi = 3.1415\dots$ we really mean that we are taking 3.1415... to represent all Cauchy sequences that are equivalent to $\{3, 3.1, 3.14, 3.141, 3.1415, \dots\}$.

Definition 3.4. Two Cauchy sequences, $\{a_n\}$ and $\{b_n\}$ are said to be equivalent if the sequence $|\, a_n - b_n \,|$, with respect to the given absolute value, converges to 0 as $n \to \infty$. For any absolute value, this creates an equivalence relation on Cauchy sequences of rational numbers.

Remark 3.5. Since this relation is an equivalence relation, the Cauchy sequences of rational numbers will be partitioned into distinct non-overlapping classes of equivalent sequences.

Example 3.6. Consider the Cauchy sequences $\{a_n\} = \{\frac{1}{10^n}\}$ and $\{b_n\} = \{0\}$. These are equivalent with respect to $|\cdot|_\infty$ because $\lim_{n\to\infty} |\frac{1}{10^n} - 0|_\infty = \lim_{n\to\infty} \frac{1}{10^n} = 0$.

The real numbers are the equivalence classes of Cauchy sequences defined using the usual absolute value. We usually use the decimal expansion to stand for the whole equivalence class.

Just as we use the usual absolute value to construct the real numbers, we will construct the p-adic numbers using Cauchy sequences of rational numbers, but using the p-adic absolute value. In the p-adic case we will also find a representative for each equivalence class.

To start we must define the p-adic valuation of a rational number.

Definition 3.7 (The p-adic valuation of an integer and of a rational number)**.** Let p be a prime number. Let a be an integer. Then $v_p(a)$, the p-adic valuation of a is the highest power of p dividing a. Another way to state this is $a = p^{v_p(a)}b$ where $p \nmid b$. By convention $v_p(0) = \infty$.

Let c be a rational number. We can write $c = p^n \frac{a}{b}$ where $a, b, n \in \mathbb{Z}$ and $p \nmid a, b$. Then $v_p(c) = n$. Note another way to define the p-adic valuation of a rational number would be to write $c = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and then use the definition of the valuation of an integer to say that $v_p(c) = v_p(a) - v_p(b)$.

Let us consider a few examples:

$$v_5(100) = v_5(5^2 \cdot 4) = 2,$$
$$v_3(5) = v_3(3^0 \cdot 5) = 0,$$
$$v_7(\frac{21}{98}) = v_7(7^{-1}\frac{3}{2}) = -1.$$

Using the definition of p-adic valuation, we define p-adic absolute value as follows.

Definition 3.8. The *p-adic absolute value* for $a \in \mathbb{Q}$ is defined as follows:

$$| a |_p = \begin{cases} \frac{1}{p^{v_p(a)}} & : a \neq 0 \\ 0 & : a = 0. \end{cases}$$

Examples:

$$| 100 |_5 = \frac{1}{5^2},$$
$$| 5 |_3 = \frac{1}{3^0} = 1,$$
$$| \frac{21}{98} |_7 = \frac{1}{7^{-1}} = 7.$$

Using the definition, we can easily show that $| \cdot |_p$ is an absolute value. In fact, $| \cdot |_p$ is what we call a non-archimedean absolute value because in addition to the triangle property (3) of the absolute value holding, something stronger is true for $| \cdot |_p$ and $x, y \in \mathbb{Q}$: $| x + y |_p \leq max(| x |_p, | y |_p)$.

We can now define p-adic numbers in the same way we defined real numbers, except that we use the absolute value $| \cdot |_p$. Thus p-adic numbers $\mathbb{Q}_p$ are equivalence classes of p-adic Cauchy sequences: Cauchy sequences of rational numbers defined using the absolute value $| \cdot |_p$.

Note, as we use $\mathbb{R}$ to denote the real numbers, $\mathbb{Q}$ to denote the rational numbers, and $\mathbb{Z}$ to denote the integers, we will use $\mathbb{Q}_p$ to denote the p-adic numbers. and $\mathbb{Z}_p$ to denote the p-adic integers.

Now, this is a very abstract definition and we need an explicit representation for each equivalence class. After all, we can operate in $\mathbb{R}$ just thinking of each real number as being represented by its decimal expansion. For example $\pi = 3.1415926\ldots$, $1 = 1.00\overline{0}$, and $1 = 0.99\overline{9}$. Similarly there is an explicit representation of each Cauchy sequence that we can use to visualize the elements in $\mathbb{Q}_p$. This representation is called the p-adic expansion of a p-adic number. For $\alpha \in \mathbb{Q}_p$ with $v_p(\alpha) = -n$

$$\alpha = a_{-n}p^{-n} + a_{-n+1}p^{-n+1} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + \cdots,$$

where $a_{-n} \neq 0$ and $a_i \in \{0, 1, 2, \ldots, p-1\}$.

We can see that a p-adic Cauchy sequence of rational numbers of the form $\{a_{-n}p^{-n}, a_{-n}p^{-n}+a_{-n+1}p^{-n+1}, \ldots, a_{-n}p^{-n}+\cdots+a_{-1}p^{-1}, a_{-n}p^{-n}+\cdots+a_{-1}p^{-1}+a_0, a_{-n}p^{-n}+\cdots+a_{-1}p^{-1}+a_0+a_1p, \ldots\}$ where $a_{-n} \neq 0$ and $a_i \in \{0, 1, 2, \ldots, p-1\}$ must converge to some p-adic number since it is clearly a p-adic Cauchy sequence of rational numbers. We can represent this Cauchy sequence as the infinite sum

$$\alpha = a_{-n}p_{-n} + a_{-n+1}p^{-n+1} + \cdots + a_{-1}p^{-1} + a_0 + a_1p + \cdots,$$

where $a_{-n} \neq 0$ and $a_i \in \{0, 1, 2, \ldots, p-1\}$. This infinite sum is called the p-adic representation of α. If $v_p(a) \geq 0$ then its p-adic representation is of the form

$$a_0 + a_1p + a_2p^2 + \cdots,$$

where $a_i \in \{0, 1, 2, \ldots, p-1\}$. It is true that all p-adic Cauchy sequences are equivalent to exactly one p-adic Cauchy sequence of this form (See Theorem 1.30 of [5] for more detail). So $p^{-n}(a_{-n} + a_{-n+1}p + \cdots)$ for $v_p(a) < 0$ or $a_0 + a_1p + a_2p^2 + \cdots$ for $v_p(a) \geq 0$ will be our explicit p-adic representative for every p-adic number.

Let us consider a few p-adic expansions for some sample rational numbers.

Example 3.9.

The 5-adic expansion of 620: $4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 = .444_5$

The 3-adic expansion of 73: $1 \cdot 3^0 + 0 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^2 = 1.022_3$

The 2-adic expansion of $\frac{25}{16}$*:* $1 \cdot 2^{-4} + 0 \cdot 2^{-3} + 0 \cdot 2^{-2} + 3 \cdot 2^{-1} + 1 \cdot 2^0 = 10011.0_2$

Note: we have used a decimal-like short hand to represent these expansions.

Definition 3.10. We will define the ring of p-adic integers to be those p-adic numbers such that their p-adic expansion is of the form

$$a_0 + a_1 p + a_2 p^2 \cdots .$$

We will denote the p-adic integers as $\mathbb{Z}_p$. Note $\mathbb{Z} \subset \mathbb{Z}_p$ and $\mathbb{Z}_p$ is an integral domain. See Proposition 1.44 of [5] for more detail.

One last thing we will want to consider is polynomials over $\mathbb{Q}_p$. Suppose we have a polynomial, say $f(x) = x^2 + 2$, and we want to know if it has roots in $\mathbb{Q}_p$. We have a very helpful lemma to help us answer this question in an important special case.

Lemma 3.11 (Hensel's Lemma)**.** *Let $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$ be a polynomial with coefficients in $\mathbb{Z}_p$ and let $f'(x) = c_1 + 2c_2 x + \cdots + n c_n x^{n-1}$ be the formal derivative of $f(x)$. If there exists $a \in \mathbb{Z}_p$ such that $f(a) \equiv 0 \pmod{p}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there exists a unique $b \in \mathbb{Z}_p$ such that $f(b) = 0$ in $\mathbb{Z}_p$ and $b \equiv a \pmod{p}$.*

Proof. We will proceed by constructing a root in $\mathbb{Z}_p$ of the polynomial $f(x)$ which we call b. We construct its p-adic expansion so that $b = b_0 + b_1 p + b_2 p^2 + \cdots$ for $b_i \in \{0, 1, \ldots, p-1\}$. We will construct b by inductively finding each b_i. At the k-th step we will have constructed a $\beta_k = b_0 + b_1 p + b_2 p^2 + \cdots + b_k p^k$ such that $f(\beta_k) \equiv 0 \pmod{p^{k+1}}$ and $\beta_k \equiv a \pmod{p}$. Since we can do this for all k, we have produced a $b = b_0 + \cdots + b_k p^k + \cdots$ such that $f(b) \equiv 0 \pmod{p^k}$ for all k.

For our base case when $k = 0$, we let $\beta_0 = a \pmod{p}$. Then $f(\beta_0) \equiv f(a) \equiv 0 \pmod{p}$ and $\beta_0 = b_0 \equiv a \pmod{p}$.

Now suppose there exists $\beta_{k-1} = b_0 + b_1 p + b_2 p^2 + \cdots + b_{k-1} p^{k-1}$ such that $f(\beta_{k-1}) \equiv 0 \pmod{p^k}$ and $\beta_{k-1} \equiv b_0 \equiv a \pmod{p}$.

Consider the k-th case. First, note that $f(\beta_{k-1}) \equiv 0 \pmod{p^k}$, so $p^k \mid f(\beta_{k-1})$. So, if $\gamma_k = \frac{f(\beta_{k-1})}{p^k}$ then $\gamma_k \in \mathbb{Z}$. Also note that $p \nmid f'(\beta_{k-1})$ since $f'(\beta_{k-1}) \equiv f'(a) \pmod{p}$ and by hypothesis $f'(a) \not\equiv 0 \pmod{p}$. Thus, by Remark 1.18 , $(f'(\beta_{k-1}))^{-1}$ is well defined modulo p.

Now, let $b_k = -\gamma_k \cdot (f'(\beta_{k-1}))^{-1} \pmod{p}$, which is well-defined. We can let $\beta_k = b_0 + b_1 p + b_2 p^2 + \cdots + b_{k-1}p^{k-1} + b_k p^k$ which will be the unique solution to $f(\beta_k) \equiv 0 \pmod{p^{k+1}}$ where $\beta_k \equiv \beta_{k-1} \equiv a \pmod{p}$.

Finally, we verify our solution as follows

$$
\begin{aligned}
(1) \qquad f(\beta_k) &= f(\beta_{k-1} + b_k p^k) \\
(2) \qquad &= \sum_{i=0}^{n} c_i (\beta_{k-1} + b_k p^k)^i \\
(3) \qquad &= c_0 + \sum_{i=1}^{n} c_i (\beta_{k-1}^i + i\beta_{k-1}^{i-1} b_k p^k + \text{terms divisible by } p^{k+1}) \\
(4) \qquad &\equiv \sum_{i=0}^{n} c_i \beta_{k-1}^i + b_k p^k \sum_{i=0}^{n} i\beta_{k-1}^{i-1} \pmod{p^{k+1}} \\
(5) \qquad &\equiv f(\beta_{k-1}) + b_k p^k f'(\beta_{k-1}) \pmod{p^{k+1}} \\
(6) \qquad &\equiv f(\beta_{k-1}) - \gamma_k (f'(\beta_{k-1}))^{-1} p^k f'(\beta_{k-1}) \pmod{p^{k+1}} \\
(7) \qquad &\equiv f(\beta_{k-1}) - \gamma_k p^k \pmod{p^{k+1}} \\
(8) \qquad &\equiv f(\beta_{k-1}) - \frac{f(\beta_{k-1})}{p^k} p^k \pmod{p^{k+1}} \\
(9) \qquad &\equiv 0 \pmod{p^{k+1}},
\end{aligned}
$$

and see that $f(\beta_k) \equiv 0 \pmod{p^{k+1}}$ and $\beta_k \equiv \beta_{k-1} \equiv a \pmod{p}$. Thus, our induction step is complete and we have shown that $b = b_0 + \cdots + b_k p^k + \cdots$ will exist such that $f(b) = 0$ in $\mathbb{Z}_p$ and $b \equiv a \pmod{p}$.

The only thing left to show is that b is unique. Suppose it is not, then suppose b and b' satisfy the conditions such that $b \neq b'$. They both have p-adic representations $b = b_0 + b_1p + b_2p^2 + \cdots$ and $b' = b'_0 + b'_1p + b'_2p^2 + \cdots$. Let the first coefficient they differ in be the k-th. That is $b_i = b'_i$ for $i < k$, but $b_k \neq b'_k$. Let $\beta_{k-1} = b_0 + b_1p + \cdots + b_{k-1}p^{k-1} = b'_0 + b'_1p + \cdots + b'_{k-1}p^{k-1}$.

Then we know we need $f(\beta_{k-1} + b_kp^k) \equiv f(\beta_{k-1} + b_kp^k) \equiv 0 \pmod{p^{k+1}}$. From (5) above, this means $f(\beta_{k-1}) + b_kp^kf'(\beta_{k-1}) \equiv f(\beta_{k-1}) + b'_kp^kf'(\beta_{k-1}) \pmod{p^{k+1}}$, which implies $b_kp^kf'(\beta_{k-1}) \equiv b'_kp^kf'(\beta_{k-1}) \pmod{p^{k+1}}$. Thus, $b_kp^k \equiv b_kp^k \pmod{p^{k+1}}$. Therefore $p^{k+1} \mid p^k(b_k - b'_k)$. Thus, $p \mid b_k - b'_k$ and $b_k \equiv b'_k \pmod{p}$. However $0 \leq b_k, b'_k < p$, so $b_k = b'_k$, which is a contradiction. Thus, $b = b'$ and our solution must be unique. □

Now, we will use this lemma to introduce p-adic notation that is very important for our results.

We will show that in each ring of p-adic integers $\mathbb{Z}_p$ there are $(p-1)$ distinct p-adic numbers x such that $x^{p-1} - 1 = 0$. These p-adic integers are called the $(p-1)$st roots of unity. In each $\mathbb{Z}_p$ one of those roots will always be 1. In fact, these roots form a multiplicative group.

For example in $\mathbb{Z}_2$ there will just be one 2-adic integer such that $x-1 = 0$ and it is $x_1 = 1$. In $\mathbb{Z}_3$ there will two quadratic roots of one and they will be the 3-adic integers $x_1 = 1$ and $x_2 = 2+2\cdot3+2\cdot3^3+\cdots$ satisfying $x^2-1 = 0$. Note that $2+2\cdot3+2\cdot3^2+\cdots = -1$ in $\mathbb{Z}_3$. In $\mathbb{Z}_5$ there will four 4th roots of one, the 5-adic integers satisfying $x^4-1 = 0$, and they are $x_1 = 1$, $x_2 = 2+1\cdot5+2\cdot5^2+1\cdot5^3+\cdots$, $x_3 = 3 + 3\cdot5 + 2\cdot5^2 + 3\cdot5^3 + 1\cdot5^4 + \cdots$, and $x_4 = 4 + 4\cdot5 + 4\cdot5^2 + \cdots$. Note in general that $(p-1) + (p-1)\cdot p + (p-1)\cdot p^2 + \cdots = -1$ in $\mathbb{Z}_p$ since $1 + ((p-1) + (p-1)\cdot p + (p-1)\cdot p^2 + \cdots) = 0$.

Now, why are there $(p-1)$ distinct p-adic numbers x such that $x^{p-1} - 1 = 0$? Consider the polynomial $f(x) = x^{p-1} - 1$. Note that by Fermat's Little

Theorem, for any integer g modulo p such that $p \nmid g$, $f(g) = g^{p-1} - 1 \equiv 1 - 1 \equiv 0 \pmod{p}$. In addition $f'(g) = (p-1)g^{p-2} \not\equiv 0 \pmod{p}$ because $p \nmid p-1, g$. Thus, by Hensel's Lemma for each g where $1 \leq g \leq p-1$ there exists a unique $a \in \mathbb{Z}_p$ such that $f(a) = 0$ and $g \equiv a \pmod{p}$. That is, $a^{p-1} = 1$ and $g \equiv a \pmod{p}$. For any g not divisible by p there is a corresponding $(p-1)$st root of unity. This means that there are at least $p-1$ such roots, one for each remainder class of g modulo p. By Hensel's Lemma for each g its corresponding $(p-1)$st root of unity is unique. Since there are exactly $p-1$ non-zero remainder classes modulo p, there are exactly $p-1$ of these roots of unity in $\mathbb{Z}_p$.

Definition 3.12 (The notation $\omega(g)$ and $< g >$)**.** For odd primes p and for $g \in \mathbb{Z}$ such that $p \nmid g$, we will let $\omega(g)$ be the $(p-1)$st root of unity in $\mathbb{Z}_p$ such that $g \equiv \omega(g) \pmod{p}$. This means that $\omega(g)^{p-1} = 1$ in $\mathbb{Z}_p$. Note we will let $\text{ord}(\omega(g))$ be the order of $\omega(g)$ as an element in the finite group of $(p-1)$st roots of unity in $\mathbb{Z}_p$

When $p = 2$ we define $\omega(g)$ differently. For $p = 2$ and $g \in \mathbb{Z}$ such that $p \nmid g$, we will let $\omega(g)$ be the quadratic root of unity in $1 + 2\mathbb{Z}_2$ such that $g \equiv \omega(g) \pmod{4}$. This means

$$\omega(g) = \begin{cases} 1 & g \equiv 1 \pmod{4} \\ -1 & g \equiv 3 \pmod{4} \end{cases}$$

Thus, $\omega(g)^2 = 1$ in $1 + 2\mathbb{Z}_2$, and $g \equiv \omega(g) \pmod{4}$. Note we will let $\text{ord}(\omega(g))$ be the order of $\omega(g)$ in the multiplicative group $\{1, -1\}$ of order 2

Example 3.13. Let $p = 5$ and $g = 24$. Then $\omega(24) = 4 + 4 \cdot 5 + 4 \cdot 5^2 + \cdots$. This is because $g \equiv 4 \equiv \omega(24) \pmod{5}$. Also, $\omega(24) + 1 = 0$ in $\mathbb{Z}_p$ so $\omega(24)^4 = (-1)^4 = 1$.

Let $p = 5$ and $g = 7$. Then $\omega(7) = 2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \cdots$. This is because $g \equiv 2 \equiv \omega(7) \pmod{5}$. Also

$$\omega(7)^4 \equiv (2)^4 \equiv 1 \pmod 5$$

$$\omega(7)^4 \equiv (2 + 1 \cdot 5)^4 \equiv 1 \pmod{5^2}$$

$$\omega(7)^4 \equiv (2 + 1 \cdot 5 + 2 \cdot 5^2)^4 \equiv 1 \pmod{5^3}$$

$$\omega(7)^4 \equiv (2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3)^4 \equiv 1 \pmod{5^4}$$

$$\omega(7)^4 \equiv (2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4)^4 \equiv 1 \pmod{5^5}$$

$$\vdots$$

Thus, $\omega(7) \equiv 1 \pmod{p^e}$ for all positive integers e. Thus, $\omega(7) = 1$ in $\mathbb{Z}_p$.

Lemma 3.14. *For odd primes p and for $g \in \mathbb{Z}$ such that $p \nmid g$, let $m = \mathrm{ord}_p(g)$. Then,* $\mathrm{ord}(\omega(g)) = m$.

Proof. Suppose $\mathrm{ord}(\omega(g)) = n$. We must show $m = n$. Recall that $g \equiv \omega(g) \pmod p$. Thus, $g^x \equiv \omega(g)^x \pmod p$ for any integer x. Therefore, $\omega(g)^m \equiv g^m \equiv 1 \pmod p$. So $n \leq m$. In addition, $g^n \equiv \omega(g)^n \equiv 1 \pmod p$. So $m \leq n$. Thus, $m = n$. □

Lemma 3.15. *For $p = 2$ and for $g \in \mathbb{Z}$ such that $p \nmid g$, let $m = \mathrm{ord}_4(g)$. Then* $\mathrm{ord}(\omega(g)) = m$.

Proof. This proof is similar to the proof of Lemma 3.14. □

Note that for $p = 2$, $\mathrm{ord}(\omega(g)) = 1$ or 2 depending on whether $\omega(g) = 1$ or -1 respectively.

4. Previous results from the 2014 Mount Holyoke REU and their extension to the case where $p = 2$

Recall that the map that sparked our interest because of its relation to the ElGamal DDS for a fixed integer g where $p \nmid g$

$$x \to xg^x \pmod{p}$$

was called the discrete Lambert map (DLM).

There are a few previous results related concerning the DLM. In [8], Liu proves the following result.

Theorem 4.1. *For an odd prime p and a positive integer g such that $p \nmid g$, let $m = \mathrm{ord}_p(g)$. Then the number of collisions that are solutions to*

$$xg^x \equiv yg^y \pmod{p^e}$$

is equal to

$$\frac{m(m+1)(p-1)}{2}p^{e-1}$$

for x and $y \in \{1, 2, 3, ..., p^e m\}$, $p \nmid x$ and $p \nmid y$.

Next we have the analogous theorem to Theorem 4.1 for $p = 2$.

Theorem 4.2. *Let $p = 2$ and let g be a positive integer such that $p \nmid g$. Then the number of collisions that are solutions to*

$$xg^x \equiv yg^y \pmod{p^e}$$

is equal to p^{e-1} for x and $y \in \{1, 2, 3, ..., p^e\}$, $p \nmid x$ and $p \nmid y$. If $x \neq y$ the number of solutions to

$$xg^x \equiv yg^y \pmod{p^e}$$

is equal to 0.

Proof. *Case* 1 : Let $x = y$. Then $xg^x = yg^y$ so $xg^x \equiv yg^y \pmod{p^e}$. Note that there are p^{e-1} values x and y can take such that $x = y$ to solve the congruence, because any odd value in $\{1, 2, \ldots, p^e\}$ will work.

Case 2 : Let $x \neq y$. Suppose there is a solution (a, b) to the congruence. That is $ag^a \equiv bg^b \pmod{2^e}$. This congruence is equivalent to $ag^{a-b} \equiv b \pmod{2^e}$. Thus, $ag^{a-b} \equiv b \pmod{2^i}$ for all $i \leq e$. This means $ag^{a-b} \equiv b \pmod{2^1}$. Since $2 \nmid g$, then $g \equiv 1 \pmod 2$ and $a \equiv b \pmod 2$. So $2 \mid a - b$. Since $\phi(2^2) = 2$, by Euler's Theorem, $g^{a-b} \equiv 1 \pmod{2^2}$. Thus, $a \equiv b \pmod{2^2}$. Since $\phi(2^3) = 2^2$, this implies $g^{a-b} \equiv 1 \pmod{2^3}$. Again we find $a \equiv b \pmod{2^3}$. Following in this manner, we find that $a \equiv b \pmod{2^e}$. Thus, since $a, b \in \{1, \ldots, 2^e\}$, $a = b$. This is a contradiction. Thus, there are no solutions in this case.

□

In [10] Waldo and Zhu prove the following result.

Theorem 4.3. *Let p be an odd prime. Let g and c be integers such that $p \nmid g$ and $p \nmid c$. Let $m = \mathrm{ord}_p(g)$. Let $x \in \{1, \ldots, p^e m \mid x \not\equiv 0 \pmod p\}$. Then the number of solutions to*

$$xg^x \equiv c \pmod{p^e}$$

is m.

Next we have the analogous theorem to Theorem 4.3 for $p = 2$.

Theorem 4.4. *Let $p = 2$. Let g and c be integers such that $p \nmid g$ and $p \nmid c$. Let $x \in \{1, \ldots, p^e \mid x \not\equiv 0 \pmod p\}$. Then the number of solutions to*

$$xg^x \equiv c \pmod{p^e}$$

is 1.

Proof. First suppose that both $xg^x \equiv c \pmod{p^e}$ and $yg^y \equiv c \pmod{p^e}$ for a fixed c. This means $xg^x \equiv yg^y \pmod{p^e}$. By Theorem 4.2, there are no solutions to this congruence unless $x = y$. Thus, if there exists x such that $xg^x \equiv c \pmod{p^e}$, then x is unique in the given set.

Now, let us show that if $p \nmid c$ then there is at least one x such that $xg^x \equiv c \pmod{p^e}$. By hypothesis, we need only consider odd $x \in \{1, 3, \ldots, p^e - 1\}$. Note that for $c > p^e - 1$ then there exists c' such that $c \equiv c' \pmod{p^e}$. Thus, if $xg^x \equiv c' \pmod{p^e}$, then $xg^x \equiv c \pmod{p^e}$.

So we only consider odd $c \in \{1, 3, \ldots, p^e - 1\}$. Note that there are only p^{e-1} elements in $\{1, 3, \ldots, p^e - 1\}$.

Consider any x in $\{1, \ldots, p^e \mid x \not\equiv 0 \pmod{p}\}$. There are p^{e-1} such x. For each x there exists some odd c in $\{1, 3, \ldots, p^e - 1\}$ such that $xg^x \equiv c \pmod{p^e}$.

Since the sets of c and x are in one-to-one correspondence, for each c there exists an x such that $xg^x \equiv c \pmod{p^e}$.

Thus, for each c there is exactly one x such that $xg^x \equiv c \pmod{p^e}$.

□

5. Counting fixed points and two-cycles of the discrete Lambert map

In this section we want to count the number of fixed points and two cycles of the discrete Lambert map.

Below is the definition of a fixed point.

Definition 5.1 (Fixed Points of the discrete Lambert map)**.** Let p be a fixed prime and g and e fixed positive integers such that $p \nmid g$. A fixed point is a solution, x, to

$$xg^x \equiv x \pmod{p^e}$$

such that $1 \leq x \leq p^{e-1}(p-1)$ and $p \nmid x$.

The definition of a two-cycle is given below.

Definition 5.2 (Two-Cycles of the discrete Lambert map)**.** Let p be a fixed prime and g and e be fixed positive integers such that $p \nmid g$. A two-cycle is a simultaneous solution, (x, y), to

$$xg^x \equiv y \pmod{p^e}$$

$$yg^y \equiv x \pmod{p^e}$$

such that $1 \leq x, y \leq p^e m$, $x \not\equiv y \pmod{p^e}$, $m = \text{ord}_p(g)$, and $p \nmid x, y$.

To count the number of fixed points and two cycles for odd primes, we first give some preliminary propositions that will help us count the number of solutions to $g^x \equiv 1 \pmod{p^e}$. This in turn will help us count the number of fixed points. Then we will count the number of fixed points for an extended range of x values. This will help us count the number of two cycles. Along the way we will present an interesting result about order modulo p^e.

We then repeat this process for $p = 2$.

Before we proceed we recall the formula for the number of k-combinations or the number of ways to choose k unordered objects from n distinct objects, where $0 \leq k \leq n$. We will use the notation $\binom{n}{k}$ for this quantity and recall that it has the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Proposition 5.3. *For any positive integer n, $v_p(n!) = \frac{n-s_n}{p-1}$, where, to define the integer s_n, we write n in its p-adic expansion as $a_0+a_1p+\cdots+a_{t-1}p^{t-1}+a_tp^t$ and then we can define $s_n = a_0 + a_1 + \cdots + a_t$.*

Proof. Please see Lemma 3.1 in [1]. □

For example, for $n = 100$, $v_5(100!) = \frac{100-s_{100}}{5-1}$. Since $100 = 0 + 0 \cdot 5 + 4 \cdot 5^2$, $s_{100} = 4$ and $v_5(100!) = \frac{100-4}{4} = 24$. So we have that $5^{24} \mid 100!$, but $5^{25} \nmid 100!$

Next, we present a result that will help us count the number of solutions to $g^x \equiv 1 \pmod{p^e}$.

Proposition 5.4. *Fix a prime p and a positive integer e. Let n and k be integers such that $k > 0$ and $1 \leq n \leq p^{e-1}(p-1)$, then for $1 < i \leq n$, $v_p(np^k) < v_p\left(\binom{n}{i}p^{ki}\right)$ if p is an odd prime or if $p = 2$ and $k > 1$.*

Proof. Let r be the largest integer such that $p^r \mid n$. Then the p-adic expansion of n is $n = a_r p^r + \cdots + a_{e-1}p^{e-1}$ where $a_r > 0$ since $p^r \mid n$ and $0 \leq a_i < p$ for all indices i. We can note that $v_p(np^k) = r + k$. So we need to examine $v_p\left(\binom{n}{i}p^{ki}\right)$ for $1 < i \leq n$.

Now we consider three cases.

Case 1 : Let $r = 0$. Then $v_p(np^k) = k$ and $v_p\left(\binom{n}{i}p^{ki}\right) \geq ki$. Since $i > 1$ we have $k = v_p(np^k) < ki \leq v_p\left(\binom{n}{i}p^{ki}\right)$.

Case 2 : Let $i \geq p^r$ and $r \geq 1$. So $1 < p^r \leq i \leq n$. Then $v_p\left(\binom{n}{i}p^{ki}\right) \geq ki \geq kp^r$ and $v_p(np^k) = r + k$. So if we show $r + k < kp^r$ then this case is proven.

Consider the continuous functions $f(r) = r + k$ and $g(r) = kp^r$ of r. For $r = 1$ clearly $f(1) < g(1)$ since, by hypothesis, either $k \geq 1$ and $p > 2$ or $k \geq 2$ and $p = 2$. Now note that $1 = f'(r)$ and $g'(r) = krp^{r-1}$. Thus $f'(r) < g'(r)$ for $r > 1$. Thus $g(r)$ increases more quickly than $f(r)$. So $f(r) < g(r)$ for $r \geq 1$ by essentially the mean value theorem. Thus, $v_p(np^k) < v_p\left(\binom{n}{i}p^{ki}\right)$.

Case 3 : Let $i < p^r$ and $r \geq 1$. So $1 < i \leq p^r \leq n$. Then i has a p-adic expansion of $i = c_j p^j + \cdots + c_{r-1}p^{r-1}$ where $0 \neq c_j$, $0 \leq j < r$, and $0 \leq c_t \leq p - 1$ for all indices t.

Note that

$$\begin{aligned} n-i &= a_r p^r + \cdots + a_{e-1}p^{e-1} - c_j p^j - \cdots - c_{r-1}p^{r-1} \\ &= -c_j p^j - \cdots - c_{r-1}p^{r-1} + a_r p^r + \cdots + a_{e-1}p^{e-1} \\ &= (p-c_j)p^j + (p-1-c_{j+1})p^{j+1} + \cdots + (p-1-c_{r-1})p^{r-1} \\ &+ (a_r - 1)p^r + a_{r+1}p^{r+1} + \cdots + a_{e-1}p^{e-1}. \end{aligned}$$

Note for all indices s that $0 \leq a_s \leq p-1$ for $r+1 \leq s \leq e-1$ and $1 \leq a_r \leq p-1$ so $0 \leq a_r - 1 < p-1$. In addition, $0 \leq c_s \leq p-1$ for $j+1 \leq s \leq r-1$ so $0 \leq p-1-c_s \leq p-1$. Lastly, $1 \leq c_j \leq p-1$ so $1 \leq p-c_j \leq p-1$. Thus, the expression for $n-i$ above is a valid p-adic expansion.

Thus,

$$v_p(n!) = \frac{n - a_{e-1} - \cdots - a_r}{p-1}$$

$$v_p(i!) = \frac{i - c_{r-1} - \cdots - c_j}{p-1}$$

$$v_p((n-i)!) = \frac{n - i - a_{e-1} - \cdots - a_r + 1 - (p-1)(r-j-1) + c_{r-1} + \cdots + c_j - p}{p-1}.$$

Therefore, by simplification we see that

$$\begin{aligned} v_p(\binom{n}{i}) = v_p(\frac{n!}{i!(n-i)!}) &= v_p(n!) - v_p(i!) - v_p((n-i)!) \\ &= \frac{(p-1)(r-1-j)+p-1}{p-1} \\ &= r-1-j+1 \\ &= r-j \end{aligned}$$

So in this case where $i < p^r$ we have that $v_p\left(\binom{n}{i}p^{ki}\right) = r-j+ki$ when $v_p(i) = j$ and $v_p(n) = r$.

Note that $kp^j - j \leq ki - j$ since $i \geq p^j$. Note as in Case 2, if $j \geq 1$, then $k + j < kp^j$. Thus, $k < kp^j - j \leq ki - j$. If $j = 0$, then, since $i > 1$, we have that $k < ki = ki - j$. Thus, $k + r < ki - j + r$. Thus, $v_p(np^k) < v_p\left(\binom{n}{i}p^{ki}\right)$.

□

In the next theorem we use Proposition 5.4 to count the number of solutions to $g^x \equiv 1 \pmod{p^e}$. The proof will help us to count the number of fixed points.

Before we continue, note that we will define $N = \frac{p-1}{m}$. This is an integer because $m \mid p-1$ by Fermat's Little Theorem and Proposition 1.23.

Theorem 5.5. *Let p be an odd prime. Let g be fixed such that $p \nmid g$. Take e to be a positive integer. Further, we let $m = \mathrm{ord}_p(g)$ and take $N = \frac{p-1}{m}$. In this situation we can count the number of solutions to $g^x \equiv 1 \pmod{p^e}$ for $x \in \{1, \ldots, p^{e-1}(p-1)\}$.*

If $g \equiv \omega(g) \pmod{p^e}$ then there will be $p^{e-1}N$ solutions to $g^x \equiv 1 \pmod{p^e}$.

Otherwise, let k be the positive integer $1 \leq k < e$ such that $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$. Then $g^x \equiv 1 \pmod{p^e}$ will have $p^{k-1}N$ solutions.

Proof. Case 1 : Suppose $g \equiv \omega(g) \pmod{p^e}$. In this case, $g^x \equiv (\omega(g))^x \pmod{p^e}$. Thus, we only need to count the number of x in $\{1, \ldots, p^{e-1}(p-1)\}$ such that $(\omega(g))^x \equiv 1 \pmod{p^e}$.

For x to be a solution of the equation modulo p^e, we need $(\omega(g))^x \equiv 1 \pmod{p}$. This is by Proposition 1.10.

Since $g \equiv \omega(g) \pmod{p}$ and $\mathrm{ord}(\omega(g))$ is m, we know that for x to be a solution $m \mid x$.

Now for x such that $m \mid x$, $(\omega(g))^x \equiv 1 \pmod{p^e}$ by definition of $\omega(g)$. Thus, in this case, $g^x \equiv (\omega(g))^x \equiv 1 \pmod{p^e}$ if and only if $x \equiv 0 \pmod{m}$. Thus, there are $\frac{p^{e-1}(p-1)}{m} = p^{e-1}N$ values for x where $1 \leq x \leq p^{e-1}(p-1)$ for which $g^x \equiv 1 \pmod{p^e}$.

Case 2 : We have $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$. Rewriting g^x we have $g^x = (\omega(g))^x \left(\frac{g}{\omega(g)}\right)^x$. We have the p-adic expansion for the integer

g and the p-adic value $\omega(g)$ where $1 \leq k < e$, $g = a_0 + a_1p + a_2p^2 + \cdots + a_{k-1}p^{k-1} + a_kp^k + \cdots + a_lp^l$ and $\omega(g) = a_0 + a_1p + a_2p^2 + \cdots + a_{k-1}p^{k-1} + b_kp^k + \cdots$ such that $a_k \neq b_k$ and $0 \leq a_k, b_k \leq p-1$.

Thus, dividing g by $\omega(g)$ we get a p-adic integer in $1 + p\mathbb{Z}_p$

$$\begin{aligned}\frac{g}{\omega(g)} &= \frac{a_0 + a_1p + a_2p^2 + \cdots + a_{k-1}p^{k-1} + a_kp^k + \cdots + a_lp^l}{a_0 + a_1p + a_2p^2 + \cdots + a_{k-1}p^{k-1} + b_kp^k + \cdots} \\ &= (1 + c_kp^k + \cdots),\end{aligned}$$

where $p \nmid c_k$.

Therefore,

$$\begin{aligned}g^x &= \omega(g)^x \left(\frac{g}{\omega(g)}\right)^x \\ &= \omega(g)^x(1 + c_kp^k + \cdots)^x \\ &= \omega(g)^x(1 + \left(c_kp^k + \cdots\right))^x \\ &= \omega(g)^x(1 + \binom{x}{1}(c_kp^k + \cdots) + \cdots + \binom{x}{x}(c_kp^k + \cdots)^x).\end{aligned}$$

Note that in $1 + c_kp^k + \cdots$ all the terms after c_kp^k have larger powers of p in them.

Thus, to have solutions to $g^x \equiv 1 \pmod{p^e}$, we start with $g^x \equiv 1 \pmod{p}$. Since $g^x \equiv \omega(g)^x \pmod{p}$, by definition of $\omega(g)$ since $p \nmid g$, we want x such that $\omega(g)^x \equiv 1 \pmod{p}$, which only happens when $m \mid x$. Again, if $m \mid x$, we know that $\omega(g)^x \equiv 1 \pmod{p^e}$, by definition.

Therefore, when $m \mid x$ we have by the binomial expansion, since x is a positive integer, that

$$\begin{aligned}g^x &\equiv (1 + (c_kp^k + \cdots) + \cdots + (c_kp^k + \cdots)^x) \pmod{p^e} \\ &\equiv (1 + p^k(c_k + \cdots) + \cdots + p^{kx}(c_k + \cdots)^x) \pmod{p^e}\end{aligned}$$

Note that $(c_k + \cdots)$ is not divisible by p since c_k is not divisible p, and all other terms are.

Thus, by Proposition 5.4, $v_p(\binom{x}{1}p^k(c_k + \cdots)) = v_p(xp^k) < v_p(\binom{x}{i}p^{ki}) = v_p(\binom{x}{i}p^{ki}(c_k + \cdots))$ for all $i > 1$.

So for $g^x \equiv 1 \pmod{p^e}$, we need $p^e \mid xp^k(c_k + \cdots)$ which implies that we need $p^{e-k} \mid x$.

Thus we need to count all the $1 \leq x \leq p^{e-1}(p-1)$ such that $x \equiv 0 \pmod{p^{e-k}}$ and $x \equiv 0 \pmod{m}$. Thus, since $\gcd(m, p) = 1$, we need $x \equiv 0 \pmod{p^{e-k}m}$. So there will be $\frac{p^{e-1}(p-1)}{p^{e-k}m} = p^{k-1}N$ solutions to $g^x \equiv 1 \pmod{p^e}$ where $1 \leq x \leq p^{e-1}(p-1)$.

□

Here is an example to illustrate Theorem 5.5.

Example 5.6. Let $p = 5$ and $g = 24$. Note that $g = 24 = 4 + 4 \cdot 5$ and $\omega(g) = 4 + 4 \cdot 5 + 4 \cdot 5^2 + \cdots$. Also note that $\mathrm{ord}_p(g) = 2$ because $g \not\equiv 1 \pmod 5$ but $g^2 \equiv 24^2 \equiv 4^2 \equiv 1 \pmod 5$. If $e = 1, 2$ then $g \equiv \omega(g) \pmod{p^e}$. If $e > 2$, then $g \not\equiv \omega(g) \pmod{p^e}$ but $g \equiv \omega(g) \pmod{p^2}$.

Now, consider the number of solutions to $(24)^x \equiv 1 \pmod{5^e}$ for $1 \leq x \leq 5^{e-1}(5-1) = 5^{e-1}4$.

By Theorem 5.5, if $e = 1$ then there are $5^{e-1} \cdot \frac{5-1}{2} = \frac{4}{2} = 2$ solutions for $1 \leq x \leq 4$. The solutions are $x = 2, 4$ since $24^2 \equiv 1 \equiv 24^4 \pmod 5$.

If $e = 2$, there are $5^{e-1} \cdot \frac{5-1}{2} = 5 \cdot \frac{4}{2} = 10$ solutions for $1 \leq x \leq 20$. The solutions are $x = 2, 4, 6, 8, 10, 12, 14, 16, 18, 20$.

If $e > 2$, then there are $5^{k-1}\frac{5-1}{2} = 5^1\frac{4}{2} = 10$ solutions for $1 \leq x \leq 5^{e-1} \cdot 4$.

Next we will present a corollary of Theorem 5.5 that gives a formula for $\mathrm{ord}_{p^e}(g)$. It will be used throughout the proofs on counting the number of fixed points and two cycles.

Corollary 5.7. *Let p be an odd prime. Let g be fixed such that $p \nmid g$ and consider a positive integer e. Let $m = \mathrm{ord}_p(g)$.*

If there exists k such that $1 \leq k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$ then $\mathrm{ord}_{p^e}(g) = p^{e-k}m$.

If $g \equiv \omega(g) \pmod{p^e}$ then $\mathrm{ord}_{p^e}(g) = m$.

Proof. If there exists k such that $1 \leq k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$ then the order of g modulo p^e will be the smallest x such that $g^x \equiv 1 \pmod{p^e}$. From the proof above, note that we said for there to be a solution, we only need $x \equiv 0 \pmod{p^{e-k}}$ and $x \equiv 0 \pmod{m}$. Thus, since $\gcd(m, p^{e-k}) = 1$ there will be a solution if and only if $p^{e-k}m \mid x$. Thus, $\mathrm{ord}_{p^e}(g) = p^{e-k}m$.

If $g \equiv \omega(g) \pmod{p^e}$ then the order of g modulo p^e will be the same as the order of $\omega(g)$ modulo p^e and, by the definition of the order of $\omega(g)$ in the ring of $(p-1)$st roots of unity, the order of $\omega(g)$ is equal to m. Note that, from the proof of Theorem 5.5, $\omega(g)^x \equiv 1 \pmod{p^e}$ if and only if $m \mid x$. Thus, $\mathrm{ord}_{p^e}(g) = m$. □

Below is an example to illustrate Corollary 5.7.

Example 5.8. Let $p = 5$ and $g = 24$. We know that $\mathrm{ord}_p(g) = 2$. Since $g \equiv \omega(g) \pmod{p^e}$ for $e = 1, 2$, then $\mathrm{ord}_p(g) = 2$ and $\mathrm{ord}_{p^2}(g) = 2$.

Since $g \not\equiv \omega(g) \pmod{p^3}$, for $e > 2$ $\mathrm{ord}_{p^e}(24) = p^{e-2}2$.

In the next theorem we use Theorem 5.5 to help us count fixed points, which are defined in Definition 5.1. This will be useful for counting the number of two cycles.

Theorem 5.9. *Let p be an odd prime. Let g be fixed such that $p \nmid g$ and consider a positive integer e. Let $x \in \{1, \ldots, p^{e-1}(p-1)\}$ such that $p \nmid x$. Let $m = \mathrm{ord}_p(g)$ and $N = \frac{p-1}{m}$. Consider the congruence $xg^x \equiv x \pmod{p^e}$.*

If $e = 1$ there will be N solutions.

If there exists a positive integer k such that $1 \leq k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$ then there will be no solutions to the congruence $xg^x \equiv x \pmod{p^e}$.

If $g \equiv \omega(g) \pmod{p^e}$ and $e > 1$ then there will be $p^{e-2}N(p-1)$ solutions to the congruence.

Proof. Since $p \nmid x$, counting the solutions to our congruence reduces to counting the solutions to $g^x \equiv 1 \pmod{p^e}$. Now, this is not the same problem as in Theorem 5.5, because here p cannot divide x.

If $e = 1$, we will never have $p \mid x$, since $1 \leq x \leq p-1$. Thus, we will have the same number of solutions as in Theorem 5.5, which is N.

In the case where there exists k such that $k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$, then from Theorem 5.5, for a solution x we needed $p^{e-k} \mid x$. Thus, in this case there will be no solutions to our current congruence.

Now, in the case where $g \equiv \omega(g) \pmod{p^e}$ and $e > 1$, there were $p^{e-1}N$ solutions to $g^x \equiv 1 \pmod{p^e}$ where we allowed $p \mid x$. So now we take out all the solutions where $p \mid x$. We saw that we needed $m \mid x$. Now, by the Chinese Remainder Theorem, when $x \equiv 0 \pmod{m}$ and $x \equiv 0 \pmod{p}$, there is one solution to $x \equiv 0 \pmod{pm}$. So there are $\frac{p^{e-1}(p-1)}{pm} = p^{e-2}N$ solutions where $p \mid x$. Thus, there are $p^{e-1}N - p^{e-2}N = p^{e-2}N(p-1)$ solutions when $p \nmid x$.

□

Here is an example to illustrate Theorem 5.9.

Example 5.10. Let $p = 5$ and $g = 24$. Consider the number of solutions to $x24^x \equiv x \pmod{5^e}$ for $1 \leq x \leq 5^{e-1}(5-1) = 5^{e-1}4$ such that $5 \nmid x$.

By Theorem 5.9, if $e = 1$ there are $\frac{5-1}{m} = \frac{4}{2} = 2$ solutions for $1 \leq x \leq 4$. These are $x = 2, 4$. Note that $2 \cdot 24^2 \equiv 2 \pmod{5}$ and $4 \cdot 24^4 \equiv 4 \pmod{5}$.

If $e = 2$, there are $5^{e-2}(5-1) \cdot \frac{5-1}{m} = 5^0(4) \cdot \frac{4}{2} = 4 \cdot 2 = 8$ solutions for $1 \leq x \leq 20$. They are $x = 2, 4, 6, 8, 12, 14, 16, 18$.

If $e > 2$, there are no solutions for $1 \leq x \leq 5^{e-1}4$.

In the lemma below we count the number of fixed points for an extended range of x values from $1 \leq x \leq p^{e-1}(p-1)$ to $1 \leq x \leq p^e m$. This will help us prove our result about two cycles.

Lemma 5.11. *Let p be an odd prime. Let g be fixed such that $p \nmid g$. Let e be a positive integer. Let $x \in \{1, \ldots, p^e m\}$ such that $p \nmid x$. Let $m = ord_p(g)$. Consider $xg^x \equiv x \pmod{p^e}$.*

If $g \equiv \omega(g) \pmod{p^e}$ then there will be $p^{e-1}(p-1)$ solutions to $xg^x \equiv x \pmod{p^e}$.

If there exists k such that $1 \leq k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$ then there will be no solutions to the congruence.

Proof. Case 1 : Let $g \equiv \omega(g) \pmod{p^e}$.

Note, since $p \nmid x$, our congruence reduces to $g^x \equiv 1 \pmod{p^e}$.

We want $g^x \equiv 1 \pmod{p^e}$, thus $g^x \equiv 1 \pmod{p}$. Therefore, $m \mid x$. In fact, if $m \mid x$ then

$$\begin{aligned} g^x &\equiv \omega(g)^x \pmod{p^e} \\ &\equiv 1, \end{aligned}$$

by definition.

Hence, all we need is $m \mid x$. However, we have accidentally counted in solutions such that $p \mid x$. Note that since $\gcd(m, p) = 1$, the only time both m and p divide x is when $pm \mid x$. So between 1 and $p^e m$ there are $\frac{p^e m}{pm} = p^{e-1}$ solutions x such that both m and p divide x.

Thus, there are $p^e - p^{e-1} = p^{e-1}(p-1)$ solutions such that $p \nmid x$.

Case 2 : Let there exists k such that $1 \leq k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$.

By Theorem 5.5, for a solution x we needed $p^{e-k} \mid x$. Thus, in this case there will be no solutions to our current congruence. □

Below is an example illustrating Lemma 5.11.

Example 5.12. Let $p = 5$ and $g = 24$.

Consider the number of solutions to $xg^x \equiv x \pmod{p^e}$ for $1 \leq x \leq 5^e \cdot 2$ such that $5 \nmid x$.

By Lemma 5.11, if $e = 1$ there are $5^{e-1}(5-1) = 4$ solutions for $1 \leq x \leq 10$. These are $x = 2, 4, 6, 8$.

If $e = 2$, there are $5^{e-1}(5-1) = 5(4) = 20$ solutions for $1 \leq x \leq 50$. They are $x = 2, 4, 6, 8, 12, 14, 16, 18, 22, 24, 26, 28, 32, 34, 36, 38, 42, 44, 46, 48$.

If $e > 2$, there are no solutions for $1 \leq x \leq 5^e \cdot 2$.

Next is a small lemma we need to help us prove our result about two cycles.

Lemma 5.13. *Let p be an odd prime. Let e be a positive integer. Let g be a positive integer such that $p \nmid g$ and $g \equiv \omega(g) \pmod{p^e}$. Let $ord_p(g) = m$. If $m \nmid y$ and $m \mid 2y$, then $g^y \equiv -1 \pmod{p^e}$.*

Proof. Note that $g^y \equiv \omega(g)^y \not\equiv 1 \pmod{p^e}$. So $\omega(g)^{2y} \equiv 1 \pmod{p^e}$ and $\omega(g)^y \not\equiv 1 \pmod{p^e}$. Since $\omega(g)$ is a root of unity, so is $\omega(g)^y$, since y is an integer. Now, since $m \mid 2y$, $\omega(g)^{2y} \equiv 1 \pmod{p^e}$. Thus, $\omega(g)^y$ is a root of order 2, so $\omega(g)^y \equiv -1 \pmod{p^e}$. Thus, $g^y \equiv -1 \pmod{p^e}$. □

We will now use Lemmas 5.11 and 5.13 to count the number of two cycles of the discrete Lambert map, defined in Definition 5.2.

Theorem 5.14. *Let p be an odd prime. Let g be a positive integer such that $p \nmid g$. Let e be a positive integer. Let $m = ord_p(g)$. Consider the number of simultaneous solutions, or two cycles, of the congruences $xg^x \equiv y \pmod{p^e}$*

and $yg^y \equiv x \pmod{p^e}$*, such that* $x, y \in \{1, \ldots, p^e m\}$*,* $x \not\equiv y \pmod{p^e}$*, and* $p \nmid x, y$*.*

If $g \equiv \omega(g) \pmod{p^e}$*, then there are* $\frac{p^{e-1}(p-1)(m-1)}{2}$ *such solutions.*

If $g \not\equiv \omega(g) \pmod{p^e}$ *then will exist a* k *such that* $g \equiv \omega(g) \pmod{p^k}$ *but* $g \not\equiv \omega(g) \pmod{p^{k+1}}$ *for* $1 \leq k < e$*.*

When $2 \mid m$ *and* $e \leq 2k$ *there are* $\frac{p^{e-1}(p-1)}{2}$ *two cycles.*

In all other cases (for $e > 2k$ *or for odd* m*) there are no two cycles.*

Proof. First, suppose there is a solution (x, y) that is a two cycle. Since, $xg^x \equiv y \pmod{p^e}$ and $yg^y \equiv x \pmod{p^e}$, we see that

$$xg^x g^y \equiv x \pmod{p^e}$$

so that we have

$$xg^{x+y} \equiv x \pmod{p^e}.$$

Since $p \nmid x$, x must be invertible modulo p^e by Remark 1.18 so we see that

$$(*) \qquad g^{x+y} \equiv 1 \pmod{p^e}.$$

Case 1 : We will first consider $g \equiv \omega(g) \pmod{p^e}$.

Note by Corollary 5.7, $\mathrm{ord}_{p^e}(g) = m$. Thus, by $(*)$ it must be that $m \mid x+y$. This implies $x \equiv -y \pmod{m}$.

Now, suppose we fix a y, such that $p \nmid y$ and $1 \leq y \leq p^e m$. To be a two cycle we must consider all x such that $x \equiv yg^y \pmod{p^e}$ and $x \equiv -y \pmod{m}$. By the Chinese Remainder Theorem, there is one solution, x, modulo $p^e m$ such that $x \equiv yg^y \pmod{p^e}$ and $x \equiv -y \pmod{m}$ are satisfied. Now we must show that this value for x will pair with our y to form a two cycle.

Note that for this x, when $e > 0$, $p^e \mid x - yg^y$ so $p \mid x - yg^y$. So if p were to divide x then p would divide yg^y, but since $p \nmid g$, that would mean $p \mid y$ which would contradict our choice of y. Thus $p \nmid x$.

In addition, if we have found such an x, then

$$\begin{aligned} xg^x &\equiv yg^y g^x \pmod{p^e} \\ &\equiv yg^{x+y} \pmod{p^e} \\ &\equiv y \pmod{p^e}. \end{aligned}$$

Thus, (x, y) really does form a simultaneous solution to the two congruences.

Since, there is one x for each y, there are $p^e m - p^{e-1}m = p^{e-1}(p-1)m$ simultaneous solutions to the two congruences. However, this includes fixed points, where $x \equiv y \pmod{p^e}$, and also we are still counting solution (x, y) and (y, x) as different solutions.

Since, we do not want to count fixed points, let us find out how many there are and subtract them. That is, we want to count values for y such that $yg^y \equiv y \pmod{p^e}$. By Lemma 5.11, there are $p^{e-1}(p-1)$ such fixed points. Thus, there are $p^{e-1}(p-1)m - p^{e-1}(p-1) = p^{e-1}(p-1)(m-1)$ two cycles where $x \not\equiv y \pmod{p^e}$ and x, y are in the required range of values.

However, we have counted x, y and y, x as different solutions. Thus, we must divide by 2 to get the actual number of two cycles. So there are $\frac{p^{e-1}(p-1)(m-1)}{2}$ two cycles in the case where $g \equiv \omega(g) \pmod{p^e}$.

Case 2 : Now if $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$, where $1 \leq k < e$.

For (x, y) to be a two cycle, we must still require $g^{x+y} \equiv 1 \pmod{p^e}$, but now $\mathrm{ord}_{p^e}(g) = p^{e-k}m$ by Corollary 5.7. Thus, it must be true that $p^{e-k}m \mid x + y$.

Now suppose we choose a y such that $p \nmid y$ and $1 \leq y \leq p^e m$.

We must consider all x such that $x \equiv -y \pmod{p^{e-k}m}$ and $x \equiv yg^y \pmod{p^e}$. Since $e-k < e$, we have that $yg^y \equiv x \equiv -y \pmod{p^{e-k}}$. Now, since $p \nmid y$ and y is invertible modulo p^{e-k}, we deduce that $g^y \equiv -1 \pmod{p^{e-k}}$.

Therefore, since $e-k \geq 1$, then $g^y \equiv -1 \pmod{p}$. Thus, $m \nmid y$, but $m \mid 2y$. Thus, m must be even since $1 \leq e-k$ and p is odd.

Case 2*a* : If m is odd, there cannot be any solutions since $m \nmid y$, but $m \mid 2y$ must hold for there to be a solution.

Case 2*b* : Note that if $e \geq 2k+1$ then $g^y \equiv -1 \pmod{p^{e-k}}$ implies that $-1 \equiv g^y \pmod{p^{k+1}}$ since $e-k \leq k+1$. Thus, the order of g modulo p^{k+1} will not divide y, but the order of g modulo p^{k+1} will divide $2y$. By Corollary 5.7, the order of g modulo p^{k+1} is pm. Thus, $pm \mid 2y$. Since $p \neq 2$, we have that $p \mid y$, which contradicts our assumption that $p \nmid y$. Thus, there are no solutions when $e \geq 2k+1$.

Case 2*c* : Now, suppose $2 \mid m$ and $e \leq 2k$. We know that we must count the solutions y where $m \nmid y$, but $m \mid 2y$. So, fix such a y. This implies that $g^y \equiv -1 \pmod{p^{e-k}}$, by Lemma 5.13.

We know we also need $x \equiv -y \pmod{p^{e-k}m}$ and $x \equiv yg^y \pmod{p^e}$. If that is the case, then $x \equiv -y \pmod{m}$ and $x \equiv yg^y \pmod{p^e}$. By the Chinese Remainder Theorem there is one x such that $1 \leq x \leq p^e m$ and such that for a given y, $x \equiv -y \pmod{m}$ and $x \equiv yg^y \pmod{p^e}$.

If $x \equiv -y \pmod{m}$ and $x \equiv yg^y \pmod{p^e}$, then $x \equiv -y \pmod{m}$ and $x \equiv yg^y \pmod{p^{e-k}}$. Since $g^y \equiv -1 \pmod{p^{e-k}}$, this implies that $x \equiv y(-1) \equiv -y \pmod{p^{e-k}}$.

Thus, since $\gcd(m, p^{e-k}) = 1$, we have $p^{e-k}m \mid x+y$. Thus, there is one solution to $x \equiv -y \pmod{p^{e-k}m}$ and $x \equiv yg^y \pmod{p^e}$ where $1 \leq x \leq p^e m$.

If $x \equiv -y \pmod{p^{e-k}m}$, then $g^{x+y} \equiv 1 \pmod{p^e}$. Thus, for this pair (x, y)

$$xg^x \equiv yg^y g^x \equiv yg^{x+y} \equiv y \pmod{p^e}.$$

Therefore, if $k < e \leq 2k$ and $2 \mid m$, there will be a two cycle (x, y) if and only if $m \nmid y$ and $m \mid 2y$. So, let us count how many y there are such that $m \nmid y$ and $m \mid 2y$.

First, let us count how many y there are such that $m \mid 2y$. Since m is even, we have that $\frac{m}{2} \mid y$. Thus, there are $\frac{2}{m}p^e m - \frac{2}{m}p^{e-1}m = 2p^{e-1}(p-1)$ such y since we are subtracting out those y such that $p \mid y$. Similarly, there are $\frac{1}{m}p^e m - \frac{1}{m}p^{e-1}m = p^{e-1}(p-1)$ such y such that $m \mid y$. Thus, there are $2p^{e-1}(p-1) - p^{e-1}(p-1) = p^{e-1}(p-1)$, y such that $m \nmid y$, but $m \mid 2y$ and $p \nmid y$. For each y there will be exactly one x.

Now, we have counted all of the simultaneous solutions to $(*)$, and note by Lemma 5.11, none of these will be fixed points.

Lastly, we have double counted, since we counted (x, y) and (y, x) as different solutions. Thus, there are $\frac{p^{e-1}(p-1)}{2}$ total two cycles in this case.

□

Here is an example to illustrate Theorem 5.14.

Example 5.15. Let $p = 5$ and $g = 24$. So $m = \text{ord}_5(24) = 2$.

Now, consider the number of simultaneous solutions, or two cycles, to the equations $x24^x \equiv y \pmod{5^e}$ and $y24^y \equiv x \pmod{5^e}$, such that $0 \leq x, y \leq 5^e \cdot 2$, $x \not\equiv y \pmod{5^e}$, and $5 \nmid x, y$.

If $e = 1$, by Theorem 5.14, there are $\frac{5^{e-1}(5-1)(2-1)}{2} = \frac{4}{2} = 2$ solutions for $0 \leq x, y \leq 10$. One solution is $(x, y) = (3, 7)$ because $7 \cdot 24^7 \equiv 7 \cdot 4 \equiv 3 \pmod{5}$ and $3 \cdot 24^3 \equiv 2 \cdot 4 \equiv 2 \equiv 7 \pmod{5}$. The other solution is $(x, y) = (1, 9)$ because $1 \cdot 24^1 \equiv 1 \cdot 4 \equiv 4 \pmod{5}$ and $9 \cdot 24^9 \equiv 4 \cdot 4 \equiv 1 \pmod{5}$.

If $e = 2$, there are $\frac{5^{e-1}(5-1)(2-1)}{2} = \frac{5 \cdot 4}{2} = 10$ solutions for $0 \leq x, y \leq 50$. The solutions are $(x, y) \in$

$\{(1, 49), (3, 47), (7, 43), (9, 41), (11, 39), (13, 37), (17, 33), (19, 31), (21, 29), (23, 27)\}$.

If $e = 3$, there are $\frac{5^{e-1}(5-1)}{2} = \frac{5^2 \cdot 4}{2} = 50$ solutions for $0 \leq x, y \leq 250$. One solution is $(x, y) = (1, 149)$.

If $e = 4$, there are $\frac{5^{e-1}(5-1)}{2} = \frac{5^3 \cdot 4}{2} = 250$ solutions for $0 \leq x, y \leq 1250$. One solution is $(x, y) = (1, 649)$.

If $e > 4$, there are no solutions for $0 \leq x, y \leq 5^e \cdot 2$.

Next we consider the case where $p = 2$ and try to count two cycles modulo 2^e. From this point on g will be an odd number and m the order of g modulo 4. Note that for all such g either $m = 1$ for $g \equiv 1 \pmod 4$ or $m = 2$ for $g \equiv 3 \pmod 4$. In addition, $\omega(g) = 1$ if $g \equiv 1 \pmod 4$ and $\omega(g) = -1$ if $g \equiv 3 \pmod 4$. Note that by $\text{ord}(\omega(g))$ we mean the order of $\omega(g)$ in the multiplicative group $\{1, -1\}$.

In the next theorem we use Proposition 5.4 to count the number of solutions to $g^x \equiv 1 \pmod{p^e}$ for $p = 2$. The proof will help us count the number of fixed points. This is analogous to Theorem 5.5.

Theorem 5.16. *Let $p = 2$. Let g and $e > 1$ be fixed integers such that $p \nmid g$. Let $1 \leq x \leq p^{e-1}$. Let $m = \text{ord}_4(g)$. In this situation we count the number of solutions to $g^x \equiv 1 \pmod{p^e}$.*

If $g \equiv \omega(g) \pmod{p^e}$ then there will be $\frac{p^{e-1}}{m}$ solutions to $g^x \equiv 1 \pmod{p^e}$.

Otherwise there exists a positive integer k such that $2 \leq k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$ and there will be p^{k-1} solutions to $g^x \equiv 1 \pmod{p^e}$.

Proof. Case 1 : Suppose $g \equiv \omega(g) \pmod{p^e}$. In this case, $g^x \equiv (\omega(g))^x \pmod{p^e}$. Thus, we only need to count the solutions to $(\omega(g))^x \equiv 1 \pmod{p^e}$ for $1 \leq x \leq p^e$.

If $\omega(g)^x \equiv 1 \pmod{p^e}$ for $e > 1$, then $(\omega(g))^x \equiv 1 \pmod{p^2}$. This is by Proposition 1.10.

Since $g \equiv \omega(g) \pmod{p^2}$, $(\omega(g))^x \equiv 1 \pmod{p^2}$. Since $\text{ord}_4(g) = \text{ord}(\omega(g)) = m$, $m \mid x$.

Then note that for x such that $m \mid x$, $(\omega(g))^x \equiv 1 \pmod{p^e}$ by definition. Thus, $g^x \equiv (\omega(g))^x \equiv 1 \pmod{p^e}$ if and only if $x \equiv 0 \pmod m$. Thus, there are $\frac{p^{e-1}}{m}$ solutions for $1 \leq x \leq p^{e-1}$ when $g \equiv \omega(g) \pmod{p^e}$.

Case 2 : We have $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$. So $g^x = (\omega(g))^x \left(\frac{g}{\omega(g)}\right)^x$ where $g = a_0 + a_1p + a_2p^2 + \cdots + a_{k-1}p^{k-1} + a_kp^k + \cdots + a_lp^l$ and $\omega(g) = a_0 + a_1p + a_2p^2 + \cdots + a_{k-1}p^{k-1} + b_kp^k + \cdots$ such that $a_k \neq b_k$. Keep in mind that $\omega(g) = 1$ or $\omega(g) = -1$.

Thus, when dividing g by $\omega(g)$ we get

$$\begin{aligned}\frac{g}{\omega(g)} &= \frac{a_0 + a_1p + a_2p^2 + \cdots + a_{k-1}p^{k-1} + a_kp^k + \cdots + a_lp^l}{a_0 + a_1p + a_2p^2 + \cdots + a_{k-1}p^{k-1} + b_kp^k + \cdots} \\ &= (1 + c_kp^k + \cdots),\end{aligned}$$

where $p \nmid c_k$, so that $c_k = 1$ since $p = 2$.

Therefore, for an integer x where $1 \leq x \leq p^{e-1}$

$$\begin{aligned}g^x &= \omega(g)^x \left(\frac{g}{\omega(g)}\right)^x \\ &= \omega(g)^x(1 + p^k + \cdots)^x \\ &= \omega(g)^x(1 + \left(p^k + \cdots\right))^x \\ &= \omega(g)^x(1 + \binom{x}{1}(p^k + \cdots) + \cdots + \binom{x}{x}(p^k + \cdots)^x).\end{aligned}$$

Note that in $p^k + \cdots$ all the terms after p^k have larger powers of p in them.

Thus, to have solutions to $g^x \equiv 1 \pmod{p^e}$, we start with $g^x \equiv 1 \pmod{p^2}$. Since $g^x \equiv \omega(g)^x \pmod{p^2}$, by definition of $\omega(g)$ since $p \nmid g$, we want x such that $\omega(g)^x \equiv 1 \pmod{p^2}$, which only happens when $m \mid x$. Again, if $m \mid x$, we know that $\omega(g)^x \equiv 1 \pmod{p^e}$, by definition.

Therefore, when $m \mid x$ we have that

$$\begin{aligned}g^x &\equiv (1 + \binom{x}{1}(p^k + \cdots) + \cdots + \binom{x}{x}(p^k + \cdots)^x) \pmod{p^e} \\ &\equiv (1 + \binom{x}{1}p^k(1 + \cdots) + \cdots + \binom{x}{x}p^{kx}(1 + \cdots)^x) \pmod{p^e}\end{aligned}$$

Note that $(1 + \cdots)$ is not divisible by p since 1 is not divisible p, and all other terms are.

Thus, by Proposition 5.4, $v_p(\binom{x}{1}p^k(1+\cdots)) < v_p(\binom{x}{i}p^{ki}(1+\cdots))$ for all $i > 1$.

So for $g^x \equiv 1 \pmod{p^e}$, we need $p^e \mid xp^k(1+\cdots)$ which implies we need $p^{e-k} \mid x$.

Thus we need to count all the $1 \leq x \leq p^{e-1}$ such that $x \equiv 0 \pmod{p^{e-k}}$ and $x \equiv 0 \pmod{m}$. Thus, since $m = 1$ or $m = 2$ and $2 \leq k < e$, we see that $m \mid p^{e-k}$. Thus, all we need is $x \equiv 0 \pmod{p^{e-k}}$. So there will be $\frac{p^{e-1}}{p^{e-k}} = p^{k-1}$ solutions to $g^x \equiv 1 \pmod{p^e}$ where $1 \leq x \leq p^{e-1}$.

□

Next we will present a corollary of Theorem 5.16 that gives a formula for $\text{ord}_{p^e}(g)$ for $p = 2$. It will be used throughout the proofs on counting the number of fixed points and two cycles.

Corollary 5.17. *Let $p = 2$. Let g be fixed such that $p \nmid g$ and consider an integer $e > 1$. Let $m = \text{ord}_4(g)$.*

If there exists k such that $2 \leq k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$ then $\text{ord}_{p^e}(g) = p^{e-k}$.

If $g \equiv \omega(g) \pmod{p^e}$ then $\text{ord}_{p^e}(g) = m$.

Proof. If there exists k such that $2 \leq k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$ then the order of g modulo p^e will be the smallest x such that $g^x \equiv 1 \pmod{p^e}$. From the proof above, note that we said for there to be a solution, we only need $x \equiv 0 \pmod{p^{e-k}}$. Thus, $\text{ord}_{p^e}(g) = p^{e-k}$.

If $g \equiv \omega(g) \pmod{p^e}$ then the order of g modulo p^e will be the same as the order of $\omega(g)$ in the multiplicative group $\{1, -1\}$, which is either 1 or 2. Note that, by looking at the proof from Theorem 5.5, $\omega(g)^x \equiv 1 \pmod{p^e}$ if and only if $m \mid x$. Thus, $\text{ord}_{p^e}(g) = m$. □

In the next theorem we use Theorem 5.16 to help us count fixed points, which are defined in Definition 5.1, for $p = 2$. This will be useful for counting the number of two cycles for $p = 2$.

Theorem 5.18. *Let $p = 2$. Let g be fixed such that $p \nmid g$ and consider an integer $e > 1$. Let $x \in \{1, \ldots, p^{e-1}\}$ such that $p \nmid x$. Let $m = ord_4(g)$. Consider the $xg^x \equiv x \pmod{p^e}$.*

If there exists a positive integer k such that $2 \leq k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$ then there will be no solutions to the congruence $xg^x \equiv x \pmod{p^e}$.

If $g \equiv \omega(g) \pmod{p^e}$, $e > 1$, and $m = 1$ (so that $g \equiv 1 \pmod 4$) then there will be p^{e-2} solutions to the congruence.

If $g \equiv \omega(g) \pmod{p^e}$, $e > 1$, and $m = 2$ (so that $g \equiv 3 \pmod 4$) then there will be no solutions to the congruence.

Proof. Since $p \nmid x$, x is an invertible element modulo p^e. Thus, counting the solutions to our congruence reduces to counting the solutions to $g^x \equiv 1 \pmod{p^e}$. Now, this is not the same problem as in Theorem 5.16, because here p cannot divide x.

In the case where there exists k such that $2 \leq k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$, then from Theorem 5.16, for a solution x we needed $p^{e-k} \mid x$. Thus, in this case there will be no solutions to our current congruence.

Now, in the case where $g \equiv \omega(g) \pmod{p^e}$, there were $\frac{p^{e-1}}{m}$ solutions to $g^x \equiv 1 \pmod{p^e}$ where we allowed $p \mid x$. So now we take out all the solutions where $p \mid x$. We saw that we needed $m \mid x$. Now, if $p \mid x$ then $m \mid x$ since $m = 1$ or $m = 2$. So there are $\frac{p^{e-1}}{p} = p^{e-2}$ solutions where $p \mid x$. Thus, there are $\frac{p^{e-1}}{m} - p^{e-2}$ solutions. Note that this is equal to p^{e-2} when $m = 1$ and 0 when $m = 2$. So there are p^{e-2} solutions when $p \nmid x$ and $m = 1$. There are no solutions when $p \nmid x$ $m = 2$.

□

In the lemma below we count the number of fixed points, for $p = 2$, for an extended range of x values from $1 \leq x \leq p^{e-1}$ to $1 \leq x \leq p^e$. This will help us prove our result about two cycles.

Lemma 5.19. *Let $p = 2$. Let g be fixed such that $p \nmid g$. Let $e > 1$ be an integer. Let $x \in \{1, \ldots, p^e\}$ such that $p \nmid x$. Let $m = ord_4(g)$. Consider $xg^x \equiv x \pmod{p^e}$.*

If $g \equiv \omega(g) \pmod{p^e}$ and $m = 1$ then there will be p^{e-1} solutions to $xg^x \equiv x \pmod{p^e}$.

If $g \equiv \omega(g) \pmod{p^e}$ and $m = 2$ then there will be no solutions to $xg^x \equiv x \pmod{p^e}$.

If there exists k such that $2 \leq k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $\not\equiv \omega(g) \pmod{p^{k+1}}$ then there will be no solutions to $xg^x \equiv x \pmod{p^e}$.

Proof. Case 1 : Let $g \equiv \omega(g) \pmod{p^e}$ and $m = 1$.

Since $p \nmid x$, x is invertible modulo p and our congruence reduces to counting solutions to $g^x \equiv 1 \pmod{p^e}$ for odd x such that $1 \leq x \leq p^e$.

We want $g^x \equiv 1 \pmod{p^e}$ where $e > 1$, so we know that $g^x \equiv 1 \pmod 4$. Therefore, $m \mid x$. In fact, if $m \mid x$ then

$$\begin{aligned} g^x &\equiv \omega(g)^x \pmod{p^e} \\ &\equiv 1, \end{aligned}$$

by definition.

Hence, all we need is $m \mid x$. So since $m = 1$ all x work. However, we have accidentally counted in values for x where $p \mid x$. So modulo p^e there are $\frac{p^e}{p} = p^{e-1}$ solutions such that $p \mid x$ (these are even x values).

Thus, there are $p^e - p^{e-1} = p^{e-1}$ solutions such that $p \nmid x$ (these are odd x values).

Case 2 : Let $g \equiv \omega(g) \pmod{p^e}$ and $m = 2$.

By Theorem 5.16, we needed $m \mid x$ for there to be solutions to the congruence. However, since $p \nmid x$ and $p = 2$, $m \nmid x$. Thus, there are no solutions to the congruence for this case.

Case 3 : Let there exists k such that $2 \leq k < e$ and $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$.

By Theorem 5.16, for a solution x we needed $p^{e-k} \mid x$. Thus, in this case there will be no solutions to our current congruence. □

Next is a small lemma we need to help us prove our result about two cycles.

Lemma 5.20. *Let $p = 2$. Let $e > 1$ be an integer. Let g be a positive integer such that $p \nmid g$ and $g \equiv \omega(g) \pmod{p^e}$. Let $m = ord_4(g)$. If $m \nmid y$ and $m \mid 2y$, then $g^y \equiv -1 \pmod{p^e}$.*

Proof. Note that $g^y \equiv \omega(g)^y \pmod{p^e}$. Clearly $\omega(g)^{2y} \equiv 1 \pmod{p^e}$ and $\omega(g)^y \not\equiv 1 \pmod{p^e}$. Since $\omega(g)$ is ± 1, so is $\omega(g)^y$, which clearly has order 2. Thus, it must be that $\omega(g)^y \equiv -1 \pmod{p^e}$. Thus, $g^y \equiv -1 \pmod{p^e}$. □

We will now use Lemmas 5.19 and 5.20 to count the number of two cycles of the discrete Lambert map, defined in Definition 5.2, for $p = 2$.

Theorem 5.21. *Let $p = 2$. Let g be a positive integer such that $p \nmid g$. Let $e \geq 2$ be an integer. Let $m = \mathrm{ord}_4(g)$. Consider the number of simultaneous solutions, or two cycles, to the congruences*

$$xg^x \equiv y \pmod{p^e}$$

and

$$yg^y \equiv x \pmod{p^e}$$

, such that $x, y \in \{1, \ldots, p^e\}$, $x \not\equiv y \pmod{p^e}$, and $p \nmid x, y$.

If $g \equiv \omega(g) \pmod{p^e}$ and $m = 1$, then there are no two cycles.

If $g \equiv \omega(g) \pmod{p^e}$ *and* $m = 2$*, then there are* p^{e-2} *two cycles.*

In the next case let k *be the integer* $2 \leq k < e$ *such that* $g \equiv \omega(g) \pmod{p^k}$ *but* $g \not\equiv \omega(g) \pmod{p^{k+1}}$.

If $m = 1$*, then if* $e = k + 1$ *there are* p^{e-2} *two cycles.*

If $m = 1$ *and* $e \neq k + 1$ *there are no two cycles.*

If $m = 2$ *and* $k \leq e \leq 2k$ *there are* p^{e-2} *two cycles.*

If $m = 2$ *and* $e \geq 2k + 1$ *there are no two cycles.*

Proof. First, suppose there is a solution x, y. Since, $xg^x \equiv y \pmod{p^e}$ and $yg^y \equiv x \pmod{p^e}$, we see that

$$xg^x g^y \equiv x \pmod{p^e}$$

$$xg^{x+y} \equiv x \pmod{p^e}.$$

Since $p \nmid x$, x will be invertible modulo p^e and so $g^{x+y} \equiv 1 \pmod{p^e}$. Thus, the order of g modulo p^e must divide $x + y$.

Case 1 : We first consider the case where $g \equiv \omega(g) \pmod{p^e}$.

By Corollary 5.17, in this case $\text{ord}_{p^e}(g) = m$. Thus, we need $m \mid x + y$ so that we have $g^{x+y} \equiv 1 \pmod{p^e}$.

Now, suppose we fix a y such that $p \nmid y$ and $1 \leq y \leq p^e$. Then, we need an x such that $x \equiv yg^y \pmod{p^e}$ and $x \equiv -y \pmod{m}$. Note that if $x \equiv yg^y \pmod{p^e}$ and $m = 2$, then we see that $x \equiv y \pmod{2}$ since $g \equiv 1 \pmod{2}$. Since $2x \equiv 0 \pmod{2}$, we see that $x \equiv -x \equiv -y \pmod{2}$. Thus, if $x \equiv yg^y \pmod{p^e}$ and $m = 2$, then $x \equiv -y \pmod{m}$ is automatically satisfied. In addition, we see that if $m = 1$ then $x \equiv -y \pmod{m}$ is automatically satisfied. Thus, we only need consider x such that $x \equiv yg^y \pmod{p^e}$.

Note that for such an x, $p^e \mid x - yg^y$ and so $p \mid x - yg^y$. So, if $p \mid x$, then $p \mid yg^y$ and since $p \nmid g$, then $p \mid y$. Since this goes against how we chose y, $p \nmid x$.

In addition, if we have found such an x, then

$$\begin{aligned} xg^x &\equiv yg^y g^x \pmod{p^e} \\ &\equiv yg^{x+y} \pmod{p^e} \\ &\equiv y \pmod{p^e}. \end{aligned}$$

Thus, both congruences are satisfied.

Since there is one solution, x, for each y where $p \nmid y$, then there are $p^e - p^{e-1} = p^{e-1}$ solutions to $x \equiv yg^y \pmod{p^e}$ including fixed points. We are also currently counting x, y and y, x as different solutions.

Since, we don't want to count fixed points, let's find out how many there are and subtract them. That is, we want to count $yg^y \equiv y \pmod{p^e}$.

Case 1*a* : Let $m = 1$. By Lemma 5.19, there are p^{e-1} fixed points. Thus, there are $p^{e-1} - p^{e-1} = 0$ two cycles.

Case 1*b* : Let $m = 2$. By Lemma 5.19, there are no fixed points. Thus, there are $p^{e-1} - 0 = p^{e-1}$ solutions to $xg^x \equiv y \pmod{p^e}$ and $yg^y \equiv x \pmod{p^e}$ However, we have counted x, y and y, x as different solutions. Thus, we must divide by 2 to get the actual number of solutions. So there are $\frac{p^{e-1}}{2} = p^{e-2}$ two cycles.

Case 2 : Now consider the case where $g \equiv \omega(g) \pmod{p^k}$ but $g \not\equiv \omega(g) \pmod{p^{k+1}}$ for $2 \leq k < e$.

We have already established that if there is a solution then the order of g modulo p^e must divide $x+y$. Thus, by Corollary 5.17, $p^{e-k} \mid x+y$. This means $x \equiv -y \pmod{p^{e-k}}$. In addition, $x \equiv yg^y \pmod{p^e}$. These two congruences

together imply the following:

$$x \equiv yg^y \pmod{p^{e-k}} \tag{10}$$

$$-y \equiv yg^y \pmod{p^{e-k}} \tag{11}$$

$$-1 \equiv g^y \pmod{p^{e-k}} \tag{12}$$

This means we have that $m \nmid y$ and $m \mid 2y$. For reference later, we call this condition $(\star)$.

Case $2a$: Suppose $m = 1$ and $e > k + 1$

By (12), $e > k + 1$ implies $g^y \equiv -1 \pmod{p^2}$. Thus, $m \neq 1$. Thus, there are no two cycles when $m = 1$ and $e > k + 1$.

Case $2b$: Suppose $m = 1$ and $e = k + 1$.

We have already established that if there is a solution then the order of g modulo p^e must divide $x+y$. Thus, by Corollary 5.17, $p = p^{e-k} \mid x+y$ meaning $x \equiv -y \pmod{p}$. In addition we need $x \equiv yg^y \pmod{p^e}$. However, if $x \equiv yg^y \pmod{p^e}$, then we see that $x \equiv y \pmod{p}$ since $g \equiv 1 \pmod{p}$. Since $2x \equiv 0 \pmod{p}$, we see that $x \equiv -x \equiv -y \pmod{p}$. Thus, if $x \equiv yg^y \pmod{p^e}$ then $x \equiv -y \pmod{p}$ is automatically satisfied. Thus, for a fixed y we only need consider x such that $x \equiv yg^y \pmod{p^e}$.

Note that for such an x, $p^e \mid x - yg^y$ and so $p \mid x - yg^y$. So, if $p \mid x$, then $p \mid yg^y$ and since $p \nmid g$, then $p \mid y$. Since this contradicts our choice of y, we have that $p \nmid x$.

In addition, if we have found such an x, then

$$\begin{aligned} xg^x &\equiv yg^y g^x \pmod{p^e} \\ &\equiv yg^{x+y} \pmod{p^e} \\ &\equiv y \pmod{p^e}. \end{aligned}$$

Thus, both congruences are satisfied.

Since, there is one solution for each y such that $p \nmid y$, then there are $p^e - p^{e-1} = p^{e-1}$ solutions to $x \equiv yg^y \pmod{p^e}$ including fixed points. We are also currently counting x, y and y, x as different solutions.

Since, we do not want to count fixed points, let us find out how many there are and subtract them. That is, we want to count $yg^y \equiv y \pmod{p^e}$. By Lemma 5.19, there are no such fixed points in this case. Thus, there are $p^{e-1} - 0 = p^{e-1}$ two cycles in this case.

However, we have counted x, y and y, x as different solutions. Thus, we must divide by 2 to get the actual number of solutions. So there are $\frac{p^{e-1}}{2} = p^{e-2}$ two cycles.

Case 2*c* : Suppose $m = 2$ and $e > 2k + 1$.

By (12), $g^y \equiv -1 \pmod{p^{e-k}}$. If $e > 2k + 1$, then the order of g modulo p^{e-k} is p^{e-2k}. Thus, $p^{e-2k} \nmid y$, but $p^{e-2k} \mid 2y$. Thus, since $e > 2k + 1$, $p^2 \mid 2y$. This implies that $2 \mid y$. Thus, if $m = 2$ and $e > 2k+1$, there are no two cycles.

Case 2*d* : Suppose $m = 2$ and $e = 2k + 1$.

By (12), $g^y \equiv -1 \pmod{p^{e-k}}$. If $e = 2k + 1$ then the order of g modulo p^{k+1} is p. We know that $p \nmid y$, so y is odd. This means $y = 2 \cdot s + 1$ for some integer s. Thus, $g^y \equiv g^{2s+1} \equiv g^{2s}g \equiv g \not\equiv \omega(g) \pmod{p^{k+1}}$. Since $g \not\equiv \omega(g) \pmod{p^{k+1}}$ and $\omega(g) = -1$ since $g \equiv 3 \pmod 4$, $g \not\equiv -1 \pmod{p^{k+1}}$. Thus, $g^y \not\equiv -1 \pmod{p^{k+1}}$ and we have a contradiction. Thus, there are no two cycles.

Case 2*e* : Suppose $m = 2$ and $2 < k < e < 2k + 1$.

We saw in $(\star)$ that it is necessary that $m \nmid y$, but $m \mid 2y$. So assume we have a fixed such y. Then, by Lemma 5.20, $g^y \equiv -1 \pmod{p^{e-k}}$.

There is one x such that $x \equiv yg^y \pmod{p^e}$ because $1 \leq x \leq p^e$. This implies

$$\begin{aligned} x &\equiv yg^y \pmod{p^{e-k}} \\ x &\equiv y(-1) \pmod{p^{e-k}} \\ x &\equiv -y \pmod{p^{e-k}} \end{aligned}$$

Thus, by Corollary 5.17, $g^{x+y} \equiv 1 \pmod{p^e}$. Therefore, if we have found such an x, then

$$\begin{aligned} xg^x &\equiv yg^yg^x \pmod{p^e} \\ &\equiv yg^{x+y} \pmod{p^e} \\ &\equiv y \pmod{p^e}. \end{aligned}$$

Thus, both two-cycle congruences are satisfied for such a y. Thus, there is one two-cycle for y such that $m \nmid y$ and $m \mid 2y$, and there are two-cycles for only these such y. Since $m = 2$, $m \mid 2y$ for all y. Thus, we only need concern ourselves with $m \nmid y$. Since there are $p^e - p^{e-1}$ such odd y there are just that many solutions. However, we over-counted by counting x, y and y, x as different solutions. Thus, there are really $\frac{p^{e-1}}{2} = p^{e-2}$ two cycles in this case. □

6. Conclusion

In this thesis, we were able to count the number of fixed points and two cycles of the discrete Lambert map.

Now, let us consider what our theorems on fixed points and two cycles might mean for the security of the ElGamal digital signature scheme. Consider a given prime p and integer $g > 0$ such that $p \nmid g$. Our theorems on fixed points

and two cycles prove that for large enough e and $g \neq 1$ the discrete Lambert map will have no fixed points and no two-cycles.

We briefly review what is known from [7] about the discrete logarithm map. If p is an odd prime, $g \in \mathbb{Z}$ such that $p \nmid g$, and $m = \mathrm{ord}_p(g)$, then the number of fixed points or solutions to $g^x \equiv x \pmod{p^e}$ is m for $x \in \{1, \ldots, p^e m\}$. The number of two cycles or simultaneous solutions to $g^x \equiv y \pmod{p^e}$ and $g^y \equiv x \pmod{p^e}$ is $\frac{m^2-m}{2}$, for $x, y \in \{1, \ldots, p^e m\}$ such that $p \nmid x, y$ and $x \not\equiv y \pmod{p^e}$.

These results indicate that the discrete Lambert map has a certain amount of regularity that the discrete logarithm map does not have. See [7] for results on the discrete logarithm map. Our results suggest that an attack on the ElGamal digital signature scheme might be easier via the discrete Lambert map than via the discrete logarithm map.

The function $x \to xg^x$ is not the only one that people would like to understand. Other congruences that relate to cryptological problems are:

$$\begin{aligned}
x^x &\equiv x \pmod{n} \\
g^{x^2} &\equiv x \pmod{n} \\
xg^{x^2} &\equiv x \pmod{n} \\
xg^x &\equiv x^{-1} \pmod{n} \\
a^x + b^x &\equiv 1 \pmod{n} \\
g^{x^2} &\equiv c \pmod{n} \\
x^2 g^{x^2} &\equiv x \pmod{n}.
\end{aligned}$$

7. Appendix

The following are the tables I used to formulate the conjectures that led to the main results.

Let p, e, m and g be defined as in Theorem 5.14.

For $p = 3$:

g	p	e	m	fixed points	two cycles
2	3	1	2	2	1
2	3	2	2	0	3
2	3	3	2	0	0
2	3	4	2	0	0
2	3	5	2	0	0
2	3	6	2	0	0
4	3	1	1	2	0
4	3	2	1	0	0
4	3	3	1	0	0
4	3	4	1	0	0
4	3	5	1	0	0
4	3	6	1	0	0
5	3	1	2	2	1
5	3	2	2	0	3
5	3	4	2	0	0
5	3	3	2	0	0
5	3	5	2	0	0
5	3	6	2	0	0
7	3	1	1	0	0
7	3	2	1	0	0
7	3	3	1	0	0
7	3	4	1	0	0
7	3	5	1	0	0
7	3	6	1	0	0
8	3	1	2	2	1
8	3	2	2	6	3
8	3	3	2	0	9
8	3	4	2	0	27
8	3	5	2	0	0
8	3	6	2	0	0
10	3	1	1	2	0
10	3	2	1	6	0
10	3	3	1	0	0
10	3	4	1	0	0
10	3	5	1	0	0
10	3	6	1	0	0

For $p = 5$:

g	p	e	m	fixed points	two cycles
2	5	1	4	4	6
2	5	2	4	0	10
2	5	3	4	0	0
2	5	4	4	0	0
2	5	5	4	0	0
2	5	6	4	0	0
3	5	1	4	4	6
3	5	2	4	0	10
3	5	3	4	0	0
3	5	4	4	0	0
3	5	5	4	0	0
3	5	6	4	0	0
4	5	1	2	4	2
4	5	2	2	0	10
4	5	4	2	0	0
4	5	3	2	0	0
4	5	5	2	0	0
4	5	6	2	0	0
6	5	1	1	4	0
6	5	2	1	0	0
6	5	3	1	0	0
6	5	4	1	0	0
6	5	5	1	0	0
6	5	6	1	0	0
7	5	1	4	4	6
7	5	2	4	20	30
7	5	3	4	0	50
7	5	4	4	0	250
7	5	5	4	0	0
7	5	6	4	0	0
8	5	1	4	4	6
8	5	2	4	0	10
8	5	3	4	0	0
8	5	4	4	0	0
8	5	5	4	0	0
8	5	6	4	0	0
9	5	1	2	4	2
9	5	2	2	0	10
9	5	3	2	0	0
9	5	4	2	0	0
9	5	5	2	0	0
9	5	6	2	0	0
11	5	1	1	4	0
11	5	2	1	0	0
11	5	3	1	0	0
11	5	4	1	0	0
11	5	5	1	0	0
11	5	6	1	0	0

For $p = 7$:

g	p	e	m	fixed points	two cycles
2	7	1	3	6	6
2	7	2	3	0	0
2	7	3	3	0	0
2	7	4	3	0	0
2	7	5	3	0	0
3	7	1	6	6	15
3	7	2	6	0	21
3	7	3	6	0	0
3	7	4	6	0	0
3	7	5	6	0	0
4	7	1	3	6	6
4	7	2	3	0	0
4	7	3	3	0	0
4	7	4	3	0	0
4	7	5	3	0	0
5	7	1	6	6	15
5	7	2	6	0	21
5	7	3	6	0	0
5	7	4	6	0	0
5	7	5	6	0	0
6	7	1	2	6	3
6	7	2	2	0	21
6	7	3	2	0	0
6	7	4	2	0	0
6	7	5	2	0	0
8	7	1	1	6	0
8	7	2	1	0	0
8	7	3	1	0	0
8	7	4	1	0	0
8	7	5	1	0	0
9	7	1	3	6	6
9	7	2	3	0	0
9	7	3	3	0	0
9	7	4	3	0	0
9	7	5	3	0	0
10	7	1	6	6	15
10	7	2	6	0	21
10	7	3	6	0	0
10	7	4	6	0	0
10	7	5	6	0	0
11	7	1	3	6	6
11	7	2	3	0	0
11	7	3	3	0	0
11	7	4	3	0	0
11	7	5	3	0	0

For $p = 11$:

g	p	e	m	fixed points	two cycles
2	11	1	10	10	45
2	11	2	10	0	55
2	11	3	10	0	0
2	11	4	10	0	0
3	11	1	5	10	20
3	11	2	5	110	220
3	11	3	5	0	0
3	11	4	5	0	0
4	11	1	5	10	20
4	11	2	5	0	0
4	11	3	5	0	0
4	11	4	5	0	0
5	11	1	5	10	20
5	11	2	5	0	0
5	11	3	5	0	0
5	11	4	5	0	0
6	11	1	10	10	45
6	11	2	10	0	55
6	11	3	10	0	0
6	11	4	10	0	0
7	11	1	10	10	45
7	11	2	10	0	55
7	11	3	10	0	0
7	11	4	10	0	0
8	11	1	10	10	45
8	11	2	10	0	55
8	11	3	10	0	0
8	11	4	10	0	0
9	11	1	5	10	20
9	11	2	5	110	220
9	11	3	5	0	0
9	11	4	5	0	0
10	11	1	2	10	5
10	11	2	2	0	55
10	11	3	2	0	0
10	11	4	2	6	0

For $p = 2$, let p, e, m and g be defined as in Theorem 5.21.

Our table is

g	p	e	m	fixed points	two cycles
3	2	1	2	1	0
3	2	2	2	0	1
3	2	3	2	0	2
3	2	4	2	0	4
3	2	5	2	0	0
3	2	6	2	0	0
3	2	7	2	0	0
5	2	1	1	1	0
5	2	2	1	2	0
5	2	3	1	0	2
5	2	4	1	0	0
5	2	5	1	0	0
5	2	6	1	0	0
5	2	7	1	0	0
7	2	1	2	1	0
7	2	2	2	0	1
7	2	3	2	0	2
7	2	4	2	0	4
7	2	5	2	0	8
7	2	6	2	0	16
7	2	7	2	0	0
9	2	1	1	1	0
9	2	2	1	2	0
9	2	3	1	4	0
9	2	4	1	0	4
9	2	5	1	0	0
9	2	6	1	0	0
9	2	7	1	0	0
11	2	1	2	1	0
11	2	2	2	0	1
11	2	3	2	0	2
11	2	4	2	0	4
11	2	5	2	0	0
11	2	6	2	0	0
11	2	7	2	0	0
13	2	1	1	1	0
13	2	2	1	2	0
13	2	3	1	0	2
13	2	4	1	0	0
13	2	5	1	0	0
13	2	6	1	0	0
13	2	7	1	0	0

References

[1] George Bachman, *Introduction to p-adic Numbers and Valuation Theory*, Academic Press Inc., 1964.

[2] J. Chen and M. Lotts, *Structure and Randomness of the Discrete Lambert Map*, Rose-Hulman Undergraduate Mathematics Journal **13** (Spring 2012), no. 1, 64–99.

[3] J. Holden and P. Moree, *Some Heuristics and Results for Small Cycles of the Discrete Logarithm*, Math. Comp. (2006).

[4] Fernando Quadros Gouvea, *p-adic Numbers: An Introduction*, 2nd ed., Springer, 1997.

[5] Svetlana Katok, *p-adic Analysis Compared with Real*, Vol. 37, American Mathematical Society, 2007.

[6] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Graduate Texts in Mathematics, Springer, 1984.

[7] Joshua Holden and Margaret M. Robinson, *Counting Fixed Points, Two-Cycles, and Collisions of the Discrete Exponential Function Using p-adic Methods*, Journal of the Australian Mathematical Society **92** (2012), no. 2, 163–178, DOI 10.1017/S1446788712000262.

[8] Y. Liu, *Collisions of the Discrete Lambert Map*, preprint (July 2014), 1-10.

[9] A. Mann and A. Yeoh, *Deconstructing the Welch Equation Using p-adic Methods*, preprint (July 2014), 1-18.

[10] A. Waldo and C. Zhu, *The Discrete Lambert Map*, preprint (July 2014), 1-12.

[11] Joseph Gallian, *Contemporary Abstract Algebra*, 2nd ed., Cengage Learning, 2004.

[12] Kenneth Rosen, *Elementary Number Theory*, 6th ed., Pearson, 2010.

[13] Birkhoff MacLane, *Algebra*, 2nd ed., Macmillan Publishing Co., 1979.

[14] Kenneth Ross, *Elementary Analysis: The Theory of Calculus*, Springer, 2010.