Rose-
Hulman
Undergraduate
Mathematics
Journal

THE DISCRETE LAMBERT MAP

Caiyun Zhu [a] Anne Waldo [b]

Volume 16, No. 2, Fall 2015

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]Mount Holyoke College, Department of Mathematics and Statistics
[b]Mount Holyoke College, Department of Mathematics and Statistics

Rose-Hulman Undergraduate Mathematics Journal
Volume 16, No. 2, Fall 2015

THE DISCRETE LAMBERT MAP

Caiyun Zhu Anne Waldo

Abstract. The goal of this paper is to analyze the discrete Lambert problem (DWP) which is important for security and verification of the ElGamal digital signature scheme. We use p-adic methods (p-adic interpolation and Hensel's Lemma) to count the number of solutions of the DWP modulo powers of a prime. At the same time, we discover special patterns in the solutions.

Acknowledgements:
We would like to thank Professor Joshua Holden and Professor Margaret Robinson for their guidance and support throughout our project during the summer of 2014. We also want to thank the Hutchcroft Fund of the Department of Mathematics and Statistics at Mount Holyoke for funding the summer research project in 2014.

1 Introduction

A discrete logarithm is an integer x solving the equation $g^x \equiv c \pmod{p}$ for some integers c, g, and for a prime p. Finding discrete logarithms for large primes and fixed values for c and g, referred to in this paper as the discrete logarithm problem (DLP), is thought to be difficult. The exponential function is used in different forms of public-key cryptography where the security depends on the difficulty of finding solutions to the DLP. One particular class of cryptosystems where the DLP is important are digital signature schemes, which enable a message's recipient to verify the identity of the sender.

A specific digital signature scheme important for our paper is the ElGamal digital signature scheme, which is a public key system. For this system the values made public are p, g, m, and $h = g^x \pmod{p}$, where m is the message, p is a large prime, g is a generator for p (that is, for each h from 1 to $p-1$, there exists some x where $g^x \equiv h \pmod{p}$), and $x \in \{1, \ldots, p-2\}$. The values known only to the sender are x and y, where $y \in \{1, \ldots, p-2\}$ such that $\gcd(y, p-1) = 1$. The signature (s_1, s_2) is computed as follows: $s_1 \equiv g^y \pmod{p}$ and $s_2 \equiv y^{-1}(m - xs_1) \pmod{p-1}$. The recipient of message m also receives the signature (s_1, s_2) and verifies the message by computing $v_1 \equiv h^{s_1} s_1^{s_2} \pmod{p}$ and $v_2 \equiv g^m \pmod{p}$. If $v_1 \equiv v_2 \pmod{p}$, then the signature is considered authentic.

In order to forge a signature, there are several methods with which to attack the system. One could solve the DLP by computing x from $h \equiv g^x \pmod{p}$ for a fixed g, h and prime p. Another method is to fix s_1 and solve for s_2, requiring finding solutions to the congruence $s_1^{s_2} \equiv g^m h^{-s_1} \pmod{p}$, which is equivalent to solving another DLP since the right hand side of this congruence is a constant. Both of these attacks are considered to be sufficiently hard and thus not feasible as a method of forgery. A third method is to fix s_2 and solve for s_1, requiring finding solutions to the congruence $h^{s_1} s_1^{s_2} \equiv g^m \pmod{p}$. Rewriting this congruence, we see that solving it for s_1 is equivalent to solving the congruence $s_1 (h^{{s_2}^{-1}})^{s_1} \equiv g^{m{s_2}^{-1}} \pmod{p}$ for s_1. Finally, setting $a = h^{{s_2}^{-1}}$ and $b = g^{m{s_2}^{-1}}$, we see that solving these congruences is equivalent to solving the congruence $s_1 a^{s_1} \equiv b \pmod{p}$ for s_1 with a fixed a and b. Due to its similarity to the Lambert W function [2], and to distinguish it from the DLP, we will refer to the map $s_1 \to s_1 a^{s_1} \pmod{p}$ as the discrete Lambert map. Thus we define the discrete Lambert problem (DWP) to be the problem of finding integers x such that $xg^x \equiv c \pmod{p}$ for fixed integers g and c.

While the DLP has been studied extensively, the DWP has received very little attention although some introductory work has been done by Chen and Lotts on the DWP modulo p [1]. The lack of attention received by the DWP is in part because it is considered to be more difficult to solve than the DLP, but due to the implications that it has on the security of the ElGamal scheme we believe that it is important to study.

Finding exact formulas for the solutions seems extremely difficult, but counting the number of solutions modulo p for a fixed g and c and in an extended range of values for x is much easier, and this is where we begin in Section 2. In Sections 3 and 4 we look at solutions modulo p^e in a similar fashion to what Holden and Robinson [5] do for the DLP to see whether the solution set follows the same behavior after we interpolate the equation within

a discrete set of known data points. In Section 5, we find patterns in the solutions that will give us additional insight into the DWP. We conclude in Section 6 with additional future work related to DWP for the completeness of this paper.

2 Counting Solutions

We begin by looking at the DWP modulo p, counting the solutions and finding patterns. The following theorems describe the number of solutions.

Theorem 1. *If p is an odd prime, g a generator modulo p, and $c \not\equiv 0 \pmod{p}$, then for fixed g and c, consider the function $f(x) = xg^x - c$, where $x \in \{1, \ldots, p(p-1)\}$ has $x \not\equiv 0 \pmod{p}$. Then the number of solutions to*

$$f(x) = xg^x - c \equiv 0 \pmod{p} \tag{1}$$

is $p-1$, and the solution set forms a complete residue system modulo $p-1$. In other words, the solutions are distinct modulo $p-1$.

Proof. Since g is a generator modulo p which means for each h from 1 to $p-1$, there exists some x where $g^x \equiv h \pmod{p}$. Therefore we can take the logarithm of (1) to get

$$\log_g x + x \equiv \log_g c \pmod{p-1}. \tag{2}$$

In order to show the solution set of (1) forms a complete residue system modulo $p-1$, we need to show there exist $p-1$ distinct solutions to (1), one for each x_0 such that

$$x \equiv x_0 \pmod{p-1}, \text{ for each } x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}. \tag{3}$$

If we subtract (3) from (2), we get

$$\log_g x \equiv \log_g c - x_0 \pmod{p-1}. \tag{4}$$

Then when we input both sides of (4) into the inverse of the log, we get

$$x \equiv \frac{c}{g^{x_0}} \pmod{p}. \tag{5}$$

Now, we recall the Chinese Remainder Theorem (see Ding et al.[3])

Theorem 2 (Chinese Remainder Theorem)**.** *Let a_1,a_2, …, a_t be any t integers and m_1,m_2, …, m_t be relatively prime in pairs. Then there is a number x with the property*

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, \ldots, t. \tag{6}$$

Moreover, x is unique in the following sense. Let M be the product $m_1 m_2 \ldots m_t$ and let y satisfy the system of congruences (6). Then $y \equiv x \pmod{M}$.

Finally we can apply the Chinese Remainder Theorem to (3) and (5) where p and $p-1$ are the relatively prime pair of moduli. For each x_0, we conclude that there exist $p-1$ distinct solutions and they form a complete residue system modulo $p-1$. □

We can also look at what happens when g is not a generator.

Theorem 3. *Let p be an odd prime and $m = \mathrm{ord}_p(g)$. For fixed g and c such that $p \nmid g$ and $p \nmid c$, if we consider the function*

$$f(x) = xg^x - c$$

where $x \in \{1, \ldots, pm\}$ has $x \not\equiv 0 \pmod{p}$, then the number of x such that $f(x) \equiv 0 \pmod{p}$ is equal to m, and they are all distinct modulo m.

Proof. Let

$$x \equiv x_0 \pmod{m}. \tag{7}$$

Then we have the following equivalent statements.

$$\begin{aligned} f(x) = xg^x - c &\equiv 0 \pmod{p} \\ xg^{x_0} - c &\equiv 0 \pmod{p} \\ xg^{x_0} &\equiv c \pmod{p} \\ x &\equiv cg^{-x_0} \pmod{p}. \end{aligned} \tag{8}$$

So for each $x_0 \in \{1, \ldots, m\}$, there is an $x \in \{1, \ldots, p\}$ that is a solution to $xg^{x_0} - c \equiv 0 \pmod{p}$, and so by the Chinese Remainder Theorem on equations (7) and (8) there is exactly one $x \in \{1, \ldots, pm\}$ such that x is a zero of $f(x)$ where $x \equiv x_0 \pmod{m}$. Hence, the number of zeros $f(x) \equiv 0 \pmod{p}$ is equal to m, and they are all distinct modulo m. □

3 Interpolation

Next we will count solutions of the DWP modulo p^e to see if the solution set here follows the same pattern as in DLP. We need to interpolate the function $f(x) = xg^x - c$, defined on $x \in \mathbb{Z}$ to a function on $x \in \mathbb{Z}_p$, for p an odd prime and fixed $g, c \in \mathbb{Z}_p$. However, interpolation is only possible when $g \in 1 + p\mathbb{Z}_p$ [5]. In order to apply the following theorem from Katok [6], we need to show $f(x) = xg^x - c$ is uniformly continuous if $g \in 1 + p\mathbb{Z}_p$. Then we can interpolate $f : \mathbb{Z} \to \mathbb{Z}_p$ to a new uniformly continuous function $f_{x_0} : \mathbb{Z}_p \to \mathbb{Z}_p$.

Theorem 4. *Katok [6, Theorem 4.15] Let E be a subset of $\mathbb{Z}_p$ and let $\bar{E}$ be its closure. Let $f : E \to \mathbb{Q}_p$ be a function uniformly continuous on E. Then there exists a unique function $F : \bar{E} \to \mathbb{Q}_p$ uniformly continuous and bounded on $\bar{E}$ such that*

$$F(x) = f(x) \text{ if } x \in E.$$

Proposition 5. *If p is an odd prime, $c \in \mathbb{Z}_p$ is fixed, and $g \in 1 + p\mathbb{Z}_p$, then $f(x) = xg^x - c$ is uniformly continuous for $x \in \mathbb{Z}$.*

Proof. Suppose $g = 1 + pA$ where $A \in \mathbb{Z}_p$. We know that given any $\epsilon > 0$, there exists an N such that $p^{-N} < \epsilon$. Let $x, y \in \mathbb{Z}$ such that

$$|x - y|_p \leq p^{-N} < p^{-(N-1)} = \delta,$$

or $(x - y) \in p^N\mathbb{Z}_p$, and $x = y + bp^N$ where $b \in \mathbb{Z}$, then we need to show that

$$|xg^x - c - (yg^y - c)|_p < \epsilon.$$

Note that

$$\begin{aligned} g^{bp^N} &= (1 + pA)^{bp^N} \\ &= 1 + bp^N pA + \cdots + (pA)^{bp^N} \\ &\in 1 + p^N\mathbb{Z}_p, \end{aligned}$$

so we know that $g^{bp^N} - 1 \in p^N\mathbb{Z}_p$, or $|g^{bp^N} - 1|_p \leq p^{-N}$. Further, since $y \in \mathbb{Z}$, $|y|_p \leq 1$. Also note that $|bp^N g^{bp^N}|_p \leq p^{-N}$. Now, consider

$$\begin{aligned} |xg^x - yg^y|_p &= |(y + bp^N)g^{y+bp^N} - yg^y|_p \\ &= |yg^{y+bp^N} + bp^N g^{y+bp^N} - yg^y|_p \\ &= |g^y|_p |yg^{bp^N} + bp^N g^{bp^N} - y|_p, \text{ and since } g \in 1 + p\mathbb{Z}_p,\ |g^y|_p = 1 \\ &= |yg^{bp^N} + bp^N g^{bp^N} - y|_p \\ &= |(g^{bp^N} - 1)y + bp^N g^{bp^N}|_p \\ &\leq \max\left(|g^{bp^N} - 1|_p |y|_p, |bp^N g^{bp^N}|_p\right) \\ &\leq p^{-N}. \end{aligned}$$

Hence, if p is an odd prime, $c \in \mathbb{Z}_p$ is fixed, and $g \in 1+p\mathbb{Z}_p$, we have shown that $f(x) = xg^x - c$ is uniformly continuous for $x \in \mathbb{Z}$. □

Now we can apply Theorem 4 of [citenumkatok] to interpolate $f : \mathbb{Z} \to \mathbb{Z}_p$ to a function $f_{x_0} : \mathbb{Z}_p \to \mathbb{Z}_p$. If we let $\omega(g)$ be the $(p-1)^{th}$ root of unity in $\mathbb{Z}_p$ which is also called the Teichmüller character of g, then we can rewrite $g = \omega(g)\langle g \rangle$ where $\langle g \rangle = \frac{g}{\omega(g)} \in 1 + p\mathbb{Z}_p$. So we can consider a new function $f_{x_0}(x) = \omega(g)^{x_0}\langle g \rangle^x - c$, and we have the following proposition.

Proposition 6. *For an odd prime p, let $g \in \mathbb{Z}_p$ such that $p \nmid g$ and $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$, and let*

$$I_{x_0} = \{x \in \mathbb{Z} \mid x \equiv x_0 \pmod{p-1}\} \subseteq \mathbb{Z}.$$

Then

$$f_{x_0}(x) = x\omega(g)^{x_0}\langle g \rangle^x - c$$

defines a uniformly continuous function on $\mathbb{Z}_p$ such that $f_{x_0}(x) = f(x)$ whenever $x \in I_{x_0}$.

4 Hensel's Lemma

We have shown that $f(x) = xg^x - c$ has a simple root modulo p and we are now ready to "lift" the solution to modulo higher powers of p using Hensels Lemma (see Holden and Robinson [5, Corollary 3.3]).

Lemma 7 (Hensel's Lemma)**.** *Let $f(x)$ be a convergent power series in $\mathbb{Z}_p[[x]]$, and let $a \in \mathbb{Z}_p$ such that $\frac{df}{dx}(a) \not\equiv 0 \pmod{p}$ and $f(a) \equiv 0 \pmod{p}$. Then there exists a unique $x \in \mathbb{Z}_p$ for which $x \equiv a \pmod{p}$ and $f(x) = 0$ in $\mathbb{Z}_p$.*

Lemma 8. *Let $f_{x_0}(x) = x\omega(g)^{x_0} \exp(x \log(\langle g \rangle)) - c$ for any $a \in \mathbb{Z}_p$ such that $f(a) \equiv 0 \pmod{p}$. Then $\frac{df}{dx}(a) \not\equiv 0 \pmod{p}$ for any $a \in \mathbb{Z}_p$ such that $f(a) \equiv 0 \pmod{p}$.*

Proof. Consider

$$f(x) = xg^x - c \pmod{p}.$$

If we take $x_0 \in \mathbb{Z}/m\mathbb{Z}$ where $m = \mathrm{ord}_p(g)$, we have

$$f_{x_0}(x) = x\omega(g)^{x_0} \exp(x \log(\langle g \rangle)) - c.$$

Note that $\langle g \rangle \in 1 + p\mathbb{Z}_p$. Furthermore, since $\log(\langle g \rangle) \in p\mathbb{Z}_p$, then by the definition of the p-adic exponential function we know that $\exp(x \log(\langle g \rangle)) \in 1 + p\mathbb{Z}_p$. Taking the derivative of $f_{x_0}(x)$ Gouvea [4, proposition 4.4.4]), we have

$$\begin{aligned}
\frac{df_{x_0}}{dx}(x) &= \omega(g)^{x_0} \exp(x \log(\langle g \rangle)) + x\omega(g)^{x_0} \exp(x \log(\langle g \rangle)) \log(\langle g \rangle) \\
&\equiv \omega(g)^{x_0} \exp(x \log(\langle g \rangle)) \pmod{p} \\
&\equiv \omega(g)^{x_0} \pmod{p} \\
&\not\equiv 0 \pmod{p}.
\end{aligned}$$

□

Proposition 9. *If p is an odd prime, for $g \in \mathbb{Z}_p^\times$ fixed and $m = \mathrm{ord}_p(g)$, consider the function $f_{x_0}(x) = x\omega(g)^{x_0} \langle g \rangle^x - c \pmod{p}$, where $x \in \mathbb{Z}_p$. Then the number of solutions to $f_{x_0}(x) = x\omega(g)^{x_0} \langle g \rangle^x - c \equiv 0 \pmod{p}$ is exactly one.*

Proof. We know that $\langle g \rangle \equiv 1 \pmod{p}$, so the equation simplifies to

$$x\omega(g)^{x_0} \equiv c \pmod{p}.$$

For fixed g and x_0, this has exactly one solution between 1 and p.

We know that $\langle g \rangle$ is in $1 + p\mathbb{Z}_p$, so we can say

$$\begin{aligned}
\langle g \rangle^x = \exp(x \log(\langle g \rangle)) = 1 \quad &+ \quad x \log(\langle g \rangle) + x^2 \log(\langle g \rangle)^2/2! \\
&+ \quad \text{higher order terms in powers of } \log(\langle g \rangle).
\end{aligned}$$

By the definition of the p-adic logarithm, we know $\log(\langle g\rangle) \in p\mathbb{Z}_p$. Since

$$\lim_{i\to\infty} |\log(\langle g\rangle)^i/i!|_p = 0,$$

we have a convergent power series. We showed in Lemma 8 that $f_{x_0}(x)$ satisfies the rest of the conditions of Hensel's Lemma, so we can apply the lemma to say there is a unique solution for $x \in \mathbb{Z}_p$ such that $f_{x_0}(x) \equiv 0 \pmod{p}$. □

Now we can take Theorems 1 and 3 and generalize them to consider solutions modulo p^e.

Theorem 10 (Generalization of Theorem 3)**.** *Let p be an odd prime and $m = \mathrm{ord}_p(g)$. For fixed g and c such that $p \nmid g$ and $p \nmid c$, if we consider the function*

$$f(x) = xg^x - c,$$

where $x \in \{1, \ldots, p^e m\}$ such that $x \not\equiv 0 \pmod{p}$, then the number of x such that $f(x) \equiv 0 \pmod{p^e}$ is equal to m, and they are all distinct modulo m.

Proof. We can use Hensel's Lemma to count the number of solutions modulo p^e given the number of solutions modulo p. In other words, the number of solutions to

$$f_{x_0}(x) = x\omega(g)^{x_0} \exp(x\log(\langle g\rangle)) - c \equiv 0 \pmod{p^e}$$

is the same as the number of solutions to

$$f_{x_0}(x) = x\omega(g)^{x_0} \exp(x\log(\langle g\rangle)) - c \equiv 0 \pmod{p}$$

because of the bijection from the solution set of $f_{x_0}(x) \equiv 0$ modulo p to the solution set modulo p^e. We showed in Proposition 9 that there is exactly one $x_1 \in \{1, \ldots, p\}$ such that

$$x_1\omega(g)^{x_0} \langle g\rangle^{x_1} \equiv c \pmod{p},$$

so using Hensel's Lemma there is exactly one $x_1 \in \{1, \ldots, p^e\}$ such that

$$x_1\omega(g)^{x_0} \langle g\rangle^{x_1} \equiv c \pmod{p^e}.$$

By the Chinese Remainder Theorem, there will be exactly one $x \in \{1, \ldots, p^e m\}$ such that

$$x \equiv x_0 \pmod{m}$$

and

$$x \equiv x_1 \pmod{p^e}.$$

From the interpolation above, we have $x \equiv x_0 \pmod{m}$, and we know that for this $x \in \{1, \ldots, p^e m\}$,

$$f_{x_0}(x) = x\omega(g)^{x_0} \langle g\rangle^{x} - c \equiv 0 \pmod{p^e}.$$

Since there is exactly one such x for each $x_0 \in \{1, \ldots, m\}$, there are m solutions to $f(x) \equiv 0 \pmod{p^e}$. □

Corollary 11 (Generalization of Theorem 1)**.** *If p is an odd prime, g a generator modulo p, and $c \not\equiv 0 \pmod{p}$, then for fixed g and c, if we consider the function*

$$f(x) = xg^x - c, \tag{9}$$

where $x \in \{1, \ldots, p^e(p-1)\}$ has $x \not\equiv 0 \pmod{p}$,then the number of x such that $f(x) \equiv 0 \pmod{p^e}$ is $p-1$, and the solution set forms a complete residue system modulo $p-1$.

Proof. Since g is a generator modulo p, $m = \mathrm{ord}_p(g) = p-1$. Applying Theorem 10, there are $p-1$ solutions to $xg^x \equiv c \pmod{p^e}$. These solutions form a complete residue system modulo $p-1$ because they are distinct modulo $p-1$. □

5 Patterns in the Solutions

After counting the number of solutions to the DWP, we looked at patterns relating to g and c in the solutions modulo p and modulo p^e. One such pattern relates the solutions to the c values associated with them, specifically that the set of solutions $x \in \{1, \ldots, p^e m\}$ is the same as the set of c values associated with those solutions.

Theorem 12. *Let p be an odd prime and $m = \mathrm{ord}_p(g)$. For fixed g and c such that $p \nmid g$ and $p \nmid c$, we will consider the function*

$$f(x) = xg^x - c,$$

where $x \in \{1, \ldots, p^e m\}$ such that $x \not\equiv 0 \pmod{p}$. For any other $c' \in \{1, \ldots, p^{e-1}(p-1)\}$, let $x_{i,c'}$ and $x_{j,c}$ for $1 \le i, j \le m$ index the m solutions to

$$x_{i,c'} g^{x_{i,c'}} \equiv c' \pmod{p^e}$$

and

$$x_{j,c} g^{x_{j,c}} \equiv c \pmod{p^e}, \text{ respectively.}$$

If $c' \equiv x_{j,c} \pmod{p}$, then for each $x_{i,c'}$, there exists a unique k, $1 \le k \le m$, and $x_{k,c}$ such that $x_{k,c} \equiv x_{i,c'} \pmod{p}$.

Proof. We know from Theorem 10 that there are m solutions to $f(x) \equiv 0 \pmod{p^e}$. We will show that for fixed i, j that if $c' \equiv x_{j,c} \pmod{p}$, then for all $x_{i,c'}$ there exists a unique $x_{k,c}$ such that $x_{i,c'} \equiv x_{k,c} \pmod{p}$. To begin, we have the equations

$$x_{i,c'} g^{x_{i,c'}} \equiv c' \pmod{p^e} \tag{10}$$

and

$$\begin{aligned} x_{j,c} g^{x_{j,c}} &\equiv c \pmod{p^e}, \text{ or equivalently} \\ x_{j,c} &\equiv c g^{-x_{j,c}} \pmod{p^e}. \end{aligned} \tag{11}$$

Since $x_{k,c}$ ranges through the solutions to

$$x_{k,c}g^{x_{k,c}} \equiv c \pmod{p^e} \tag{12}$$

where $k \in \{1, \ldots, m\}$ and by Theorem 10 the solutions $x_{k,c}$ are all distinct modulo m, we can choose a specific $x_{k,c}$ such that

$$x_{i,c'} \equiv x_{k,c} - x_{j,c} \pmod{m}. \tag{13}$$

This will give a unique $x_{k,c}$ for each $x_{i,c'}$ because $x_{i,c'}$ and $x_{j,c}$ are both fixed. Now, we originally said that $c' \equiv x_{j,c} \pmod{p}$, so we have the following equivalent statements from equations (10) and (11)

$$x_{i,c'}g^{x_{i,c'}} \equiv cg^{-x_{j,c}} \pmod{p}.$$

We can substitute c with equation (12)

$$\begin{aligned} x_{i,c'}g^{x_{i,c'}} &\equiv (x_{k,c}g^{x_{k,c}})g^{-x_{j,c}} \pmod{p} \\ x_{i,c'}g^{x_{i,c'}} &\equiv x_{k,c}g^{x_{k,c}-x_{j,c}} \pmod{p}. \end{aligned}$$

Finally, using equation (13) we simplify to

$$x_{i,c'} \equiv x_{k,c} \pmod{p}.$$

Thus, for all $i \in \{1, \ldots, m\}$, there is some unique k such that $x_{i,c'} \equiv x_{k,c} \pmod{p}$ when $c' \equiv x_{j,c} \pmod{p}$. □

Another pattern we found involves the sum of the solutions modulo p and modulo m.

Theorem 13. *Let p be an odd prime and $m = \mathrm{ord}_p(g)$. For fixed $g \not\equiv 1 \pmod{p}$ and c such that $p \nmid g$ and $p \nmid c$, if we consider the function*

$$f(x) = xg^x - c,$$

where $x \in \{1, \ldots, p^e m\}$ such that $x \not\equiv 0 \pmod{p}$, then for each c let $x_1, \ldots, x_m$ be the m solutions to $f(x) \equiv 0 \pmod{p^e}$. Then

$$\sum_{i=1}^{m} x_i \equiv 0 \pmod{p},$$

and for odd m

$$\sum_{i=1}^{m} x_i \equiv 0 \pmod{m}.$$

Proof. We know from Theorem 10 that there are m solutions to $f(x) \equiv 0 \pmod{p^e}$. First, we will show that for each c the solutions sum as follows.

$$\sum_{i=1}^{m} x_i \equiv 0 \pmod{p}.$$

Since we said in Theorem 10 that for each $i \in \{1, \ldots, m\}$, $x_i \equiv x_0 \pmod{m}$ where $x_0 \in \{1, \ldots, m\}$, we can let $x_i \equiv i \pmod{m}$. Then we know $x_i \equiv cg^{-i} \pmod{p}$. Taking the sum of these x_i gives us.

$$\begin{aligned}
\sum_{i=1}^{m} x_i &\equiv \sum_{i=1}^{m} cg^{-i} \pmod{p} \\
&\equiv \sum_{i=0}^{m-1} cg^{-i} \pmod{p} \\
&\equiv c\left(\frac{1-g^{-m}}{1-g}\right) \pmod{p} \\
&\equiv c\left(\frac{1-1}{1-g}\right) \pmod{p} \\
&\equiv 0 \pmod{p}.
\end{aligned}$$

Thus, $\sum_{i=1}^{m} x_i \equiv 0 \pmod{p}$ for each c.

Now, we will show that $\sum_{i=1}^{m} x_i \equiv 0 \pmod{m}$ when m is odd. Again, we have that $x_i \equiv i \pmod{m}$. For each $i \in \{1, \ldots, m\}$, we have

$$\begin{aligned}
\sum_{i=1}^{m} x_i &\equiv \sum_{i=1}^{m} i \pmod{m} \\
&\equiv \frac{m(m+1)}{2} \pmod{m} \\
&\equiv 0 \pmod{m}, \text{ for odd m.}
\end{aligned}$$

If m is even, then $\frac{m}{2} \not\equiv 0 \pmod{m}$. Thus, $\sum_{i=1}^{m} x_i \equiv 0 \pmod{m}$ for odd m. □

We conjecture that the same pattern of sums holds for solutions modulo p^e and modulo $\mathrm{ord}_{p^e}(g)$, based on the evidence for all odd primes $p \leq 17$ and $1 \leq e \leq 4$.

Conjecture 14. *Let p be an odd prime, $m_p = \mathrm{ord}_p(g)$ and $m_{p^e} = \mathrm{ord}_{p^e}(g)$. For fixed g and c such that $p \nmid g$ and $p \nmid c$, if we consider the function*

$$f(x) = xg^x - c,$$

where $x \in \{1, \ldots, p^e m_p\}$ such that $x \not\equiv 0 \pmod{p}$, then for each c, let $x_1, \ldots, x_{m_p}$ be the m_p solutions to $f(x) \equiv 0 \pmod{p^e}$. Then

$$\sum_{i=1}^{m_p} x_i \equiv 0 \pmod{p^e}$$

and for odd m

$$\sum_{i=1}^{m_p} x_i \equiv 0 \pmod{m_{p^e}}.$$

We also looked some patterns for fixed x and variable c.

Theorem 15. *Let p be an odd prime. For a fixed $x \in \{1, \ldots, p^e\}$ and for $p \nmid g$ and $c \in \{1, \ldots, p^{e-1}(p-1)\}$, if we consider $xg^x \equiv c \pmod{p^e}$ and let $x(g^{-1})^x \equiv c' \pmod{p^e}$, then $c \cdot c' \equiv x^2 \pmod{p^e}$. Furthermore, if we let $x(-g)^x \equiv c'' \pmod{p^e}$ then $c'' \equiv (-1)^x c \pmod{p^e}$.*

Proof. First, we will show that $c \cdot c' \equiv x^2 \pmod{p^e}$. Since $c \equiv xg^x \pmod{p^e}$ and $c' \equiv x(g^{-1})^x \pmod{p^e}$, we can say that

$$\begin{aligned} c \cdot c' &\equiv (xg^x)(x(g^{-1})^x) \pmod{p^e} \\ &\equiv x^2(g^x)(g^{-x}) \pmod{p^e} \\ &\equiv x^2 \pmod{p^e}. \end{aligned}$$

Hence, $c \cdot c' \equiv x^2 \pmod{p^e}$. Now, we need to show that $c'' \equiv (-1)^x c \pmod{p^e}$. We have

$$\begin{aligned} c'' &\equiv x(-g)^x \pmod{p^e} \\ &\equiv x(-1)^x g^x \pmod{p^e} \\ &\equiv (-1)^x x g^x \pmod{p^e} \\ &\equiv (-1)^x c \pmod{p^e}. \end{aligned}$$

Thus $c'' \equiv (-1)^x c \pmod{p^e}$. □

Proposition 16. *Let p be an odd prime and g be a generator modulo p^e. If $c = \frac{p^e + p^{e-1}}{2}$, and $p^e - 1$ is the only element of order 2 in the multiplicative group of $\mathbb{Z}/p^e\mathbb{Z}$, then $x = \frac{p^e - p^{e-1}}{2}$ is one of the solutions to*

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

Proof. By hypothesis, we see that

$$\begin{aligned} xg^x - c &= \frac{p^e - p^{e-1}}{2} g^{\frac{p^e - p^{e-1}}{2}} - \frac{p^e + p^{e-1}}{2} \\ &\equiv \frac{p^e - p^{e-1}}{2}(p^e - 1) - \frac{p^e + p^{e-1}}{2} \pmod{p^e} \\ &= \frac{p^{2e} - p^{2e-1} - p^e + p^{e-1} - p^e - p^{e-1}}{2} \pmod{p^e} \\ &= \frac{p^{2e} - p^{2e-1} - 2p^e}{2} \pmod{p^e} \\ &= \frac{p^e(p^e - p^{e-1} - 2)}{2} \pmod{p^e} \\ &= \frac{p^e(p^{e-1}(p-1) - 2))}{2} \pmod{p^e} \\ &\equiv 0 \pmod{p^e}. \end{aligned}$$

Note that if g is a generator modulo p^e, $\text{ord}_{p^e}(g) = p^e - p^{e-1}$, thus $g^{\frac{p^e-p^{e-1}}{2}} \equiv p^e - 1 \pmod{p^e}$ because $(p^e-1)^2 \equiv 1 \pmod{p^e}$. □

Proposition 17. *Let $n \geq 2$ and $n \in \mathbb{Z}^+$. If $\gcd(p,n) = 1$ and p is an odd prime, then*

$$\text{ord}_{p^e}(p-1)^n = \begin{cases} p^{e-1} & n \text{ is even} \\ 2p^{e-1} & n \text{ is odd.} \end{cases}$$

Proof. We will prove this by inducting on e.

For our base case, let $e = 1$

When n is even.

$$\begin{aligned}(p-1)^n &= 1 - np + \frac{n(n-1)}{2}p^2 + \cdots + p^n \\ &= 1 - mp \\ &\equiv 1 \pmod{p},\end{aligned}$$

where $m \in \mathbb{Z}$.

When n is odd.

$$\begin{aligned}(p-1)^{2n} &= 1 - 2np + \frac{2n(2n-1)}{2}p^2 + \cdots + p^{2n} \\ &= 1 + ap \\ &\equiv 1 \pmod{p}, \text{ and}\end{aligned}$$

$$\begin{aligned}(p-1)^n &= -1 + np - \frac{n(n-1)}{2}p^2 + \cdots + p^n \\ &= -1 + bp \\ &\equiv p - 1 \pmod{p} \\ &\not\equiv 1 \pmod{p},\end{aligned}$$

where $a, b \in \mathbb{Z}$.

So our base case holds.

$$\text{ord}_p(p-1)^n = \begin{cases} 1 & n \text{ is even} \\ 2 & n \text{ is odd.} \end{cases}$$

For our inductive hypothesis, we assume the following statement.

$$\text{ord}_{p^e}(p-1)^n = \begin{cases} p^{e-1} & n \text{ is even} \\ 2p^{e-1} & n \text{ is odd.} \end{cases}$$

Now, in our inductive step we need to show

$$\text{ord}_{p^{e+1}}(p-1)^n = \begin{cases} p^e & n \text{ is even} \\ 2p^e & n \text{ is odd.} \end{cases}$$

When n is even.

$$\begin{aligned}(p-1)^{np^e} &= 1 - np^e p + \frac{np^e(np^e-1)}{2}p^2 + \cdots + p^{np^e} \\ &= 1 - kp^{e+1} \\ &\equiv 1 \pmod{p^{e+1}},\end{aligned}$$

where $k \in \mathbb{Z}$.

When n is even, let x be the least integer such that the following equivalent equations hold.

$$\begin{aligned}(p-1)^{xn} &\equiv 1 \pmod{p^{e+1}}. \\ 1 - xnp + \frac{xn(xn-1)}{2}p^2 + \cdots + p^{xn} &\equiv 1 \pmod{p^{e+1}}. \\ -xnp + \frac{xn(xn-1)}{2}p^2 + \cdots + p^{xn} &\equiv 0 \pmod{p^{e+1}}. \\ px(-n+dp) &\equiv 0 \pmod{p^{e+1}}.\end{aligned}$$

where $d \in \mathbb{Z}$. Since $\gcd(p,n) = 1$, then $p \nmid -n + dp$. Therefore $p^e \mid x$, hence the least $x = p^e = \operatorname{ord}_{p^{e+1}}(p-1)^n$. The proof for showing $\operatorname{ord}_{p^e+1}(p-1)^n = 2p^e$ when n is odd is a parallel to the case when n is even.

Therefore p^e and $2p^e$ are the least integers such that

$$\begin{cases} (p-1)^{np^e} \equiv 1 \pmod{p^{e+1}} & n \text{ is even} \\ (p-1)^{2np^e} \equiv 1 \pmod{p^{e+1}} & n \text{ is odd.} \end{cases}$$

□

6 Conclusions and Future Work

Following Holden and Robinson [5], we counted solutions to the discrete Lambert problem modulo powers of a prime p and we found very similar results regarding the number of solutions for x in $\{1, \ldots, p^e(p-1)\}$ and $\{1, ..., p^e m\}$ where m is the multiplicative order of g modulo p. For a given g the value m is very important in understanding the number of solutions to the DWP. In addition, we found how solutions modulo p relate to c, as well as some special properties between the sum of the solutions and p^e. We also found that when g is a generator modulo p^e there is a special (x, c) that satisfies the DWP.

According to Chen and Lotts [1, Section 3.4], when $g = (p-1)$, the solutions to the DWP modulo p are very predictable. Therefore it is not an good choice to use in a cryptosystem. However, they did not consider the solutions to the DWP modulo p^e. Due to the change in the multiplicative order of $p-1$ modulo p^e, the patterns in the solutions to the DWP become erratic and cannot be foreseen as far as we can tell.

We should mention that since this work was completed Dara Zirlin [8] has extended our research to the case where $p = 2$ and has also counted the number of fixed points and

two-cycles of the discrete Lambert map for all primes p. In particular, she has counted the number of solutions x to $xg^x \equiv x \pmod{p^e}$ and the number of solutions (h, a) to the system of congruences:

$$hg^h \equiv a \pmod{p^e} \text{ and } ag^a \equiv h \pmod{p^e}$$

where x, a and h range through the appropriate sets of integers, g is fixed and p is any prime.

References

[1] 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.

[2] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth, *On the Lambert W function*, Advances in Computational Mathematics **5** (1996), 329-359.

[3] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*, 1st ed., World Scientific Publishing Co, 1996.

[4] F. Q. Gouvea, *p-adic Numbers: An Introduction*, 2nd ed., Springer, July 1997.

[5] J. Holden and M. Robinson, *Counting Fixed Points, Two-Cycles, And Collision of the Discrete Exponential Function Using p-adic Methods*, Journal of the Australian Mathematical Society (2010).

[6] S. Katok, *p-adic Analysis Compared with Real*, 1st ed., Student Mathematical Library, American Mathematical Society, 2007.

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

[8] D. Zirlin, *Problems motivated by Cryptology: Counting fixed points and two-cycles of the discrete Lambert Map*, Undergraduate thesis presented to the Mathematics and Statistics Department at Mount Holyoke College (2015).