5-20-2016

Counting Solutions to Discrete Non-Algebraic Equations Modulo Prime Powers

Abigail Mann
Rose-Hulman Institute of Technology, mannal@rose-hulman.edu

Advisors:
Joshua Holden

MSTR 16-02

Counting Solutions to Discrete Non-Algebraic Equations Modulo Prime Powers

Abigail Mann

May 20, 2016

Abstract

As society becomes more reliant on computers, cryptographic security becomes increasingly important. Current encryption schemes include the ElGamal signature scheme, which depends on the complexity of the discrete logarithm problem. It is thought that the functions that such schemes use have inverses that are computationally intractable. In relation to this, we are interested in counting the solutions to a generalization of the discrete logarithm problem modulo a prime power. This is achieved by interpolating to p-adic functions, and using Hensels lemma, or other methods in the case of singular lifting, and the Chinese Remainder Theorem.

1 Introduction

Society has become increasingly reliant on computers for storing information and communicating securely. People expect that the cryptographic schemes currently in use will keep their information confidential and will allow them to verify the authenticity of any piece of information that they see. Public key cryptography schemes involve functions that are easy to compute one way using a publicly available key (to encrypt or verify signatures), but have inverses that are difficult to compute without a private key, so that decryption or creating a signature is only feasible for one user. Cryptographic schemes such as Diffie-Hellman key exchange and ElGamal encryption and signature schemes often use exponential modular mappings like the discrete exponentiation map $f : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, where $x \mapsto g^x \pmod{p}$ and $g \in \mathbb{Z}$, p a prime. These are used since they are generally believed to be computationally infeasible to invert for large prime p [10, Chapter 7].

However, the security of these schemes is still being analyzed, since any insight into their structure may reveal a vulnerability. There has been previous analysis of the maps $x \mapsto g^x \pmod{p}$ and $x \mapsto g^{x^2} \pmod{p}$ using functional graphs in [8], [4], and [12]. Camenisch and Stadler look at the double discrete logarithm of y, $g^{a^x} \equiv y \pmod{c}$ as well as the nth root of the discrete logarithm of z, $g^{x^n} \equiv z \pmod{c}$, where $x, a, n, c \in \mathbb{Z}$, and g, y are in a cyclic group G, for use in cryptographic signature schemes where there are multiple keys that allow for the revelation of partial information [3].

We study the nth roots of discrete logarithms in this paper by counting integer solutions to $g^{x^n} \equiv x^k \pmod{p^e}$, where $g, n, k, e \in \mathbb{Z}$, p is a prime, and $p \nmid g$. This may give us some insight into the structure of nth roots of discrete logarithms. Although it is not directly used in any cryptographic schemes today, one may be built off of this equation if its structure acts sufficiently random. The idea for counting solutions to these types of congruences was inspired by [6], which uses p-adic interpolation, Hensel's lemma, and the Chinese remainder theorem. This type of analysis can also be found in [9] and [11], which applies these methods to the Welch Equation and the Discrete Lambert map.

In this paper we find that for x in a certain range, we can determine the exact number of solutions to $g^{x^n} \equiv x^k \pmod{p^e}$ when $p \nmid k$ and when $p = k$ and $n = 1$.

1.1 Terminology and Background

For this paper, we count solutions to $g^{x^n} \equiv x^k \pmod{p^e}$, where g, n, k, and e are fixed integers, p is a prime, and $p \nmid g$. In order to count solutions to our congruence modulo p^e for all positive integers e, we will find p-adic integers helpful, since each p-adic integer describes our solution modulo p^e for all e. Thus we will be using functions on the p-adics, or $\mathbb{Q}_p$, which are the completion of $\mathbb{Q}$ under the p-adic metric. First, we note the definition of the p-adic valuation of a rational number from [5, Section 2.1].

DEFINITION 1. Fix a prime number $p \in \mathbb{Z}$. The p-adic valuation on $\mathbb{Z}$ is the function

$$v_p : \mathbb{Z} - \{0\} \to \mathbb{R}$$

defined as follows: for each integer $n \in \mathbb{Z}$, $n \neq 0$, let $v_p(n)$ be the unique positive integer satisfying

$$n = p^{v_p(n)} n' \text{ with } p \nmid n'.$$

We extend v_p to the field of rational numbers as follows: if $x = a/b \in \mathbb{Q}^\times$, then

$$v_p(x) = v_p(a) - v_p(b),$$

which is well-defined.

We can now define the p-adic absolute value as follows:

DEFINITION 2. For any $x \in \mathbb{Q}$, we define the p-adic absolute value of x by

$$|x|_p = p^{-v_p(x)}$$

if $x \neq 0$, and we set $|0|_p = 0$.

The completion gives us all the rational p-adic numbers, while we need only to use a subset of $\mathbb{Q}_p$. From [5, Section 3.3], we find that the p-adic integers $\mathbb{Z}_p$ are defined as

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Now that we have defined $\mathbb{Z}_p$, we let μ_{p-1} be the set of all $(p-1)$-st roots of unity, where $\mu_{p-1} \subseteq \mathbb{Z}_p^\times$ by [5, Cor. 4.5.10]. As stated in [5, Cor. 4.5.10], we can write each element of $\mathbb{Z}_p^\times$ uniquely as an element of $\mu_{p-1} \times (1 + p\mathbb{Z}_p)$. So for each $x \in \mathbb{Z}_p^\times$ we write $x = \omega(x) \langle x \rangle$ for some $\omega(x) \in \mu_{p-1}$ and $\langle x \rangle \in 1 + p\mathbb{Z}_p$. For odd prime p, this decomposition defines a character of $\mathbb{Z}_p^\times$, which is the surjective homomorphism

$$\omega : \mathbb{Z}_p^\times \to \mu_{p-1}.$$

This character ω is called the Teichmüller character [5, Section 4.5]. We will use the factorization of x into $\omega(x) \langle x \rangle$ to aid in our analysis.

Additionally, we will need the p-adic exponential and logarithm functions. As in $\mathbb{R}$, we can define the p-adic exponential and logarithm functions on certain subsets of the p-adic numbers as formal power series:

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!},$$

$$\log_p(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1} x^n}{n}.$$

These functions have radii of convergence $|x|_p < p^{-1/(p-1)}$ and 1, respectively.

It is important to note that the identities $\exp_p(\log_p(1+x)) = 1 + x$ and $\log_p(\exp_p(x)) = x$ hold formally, and will also hold functionally when we have convergence. For more on these functions, see [5, Section 4.5].

Lastly, we will want to use a generalization of Hensel's lemma, which allows the lifting of solutions to congruences modulo p to solutions modulo p^e, that applies to the p-adics. First, we will need to define a restricted power series. A formal power series is an object of the form $\sum_{i=0}^{\infty} a_i x^i$, where the a_i are unrestricted coefficients, and addition and multiplication are performed similarly to polynomial operations. A restricted power series is a formal power series where $\lim_{i\to\infty} a_i = 0$. Now we can take this theorem from [6, Cor. 3.3].

Theorem 1. *Let $f(x)$ be a restricted power series in $\mathbb{Z}_p[[x]]$ and a be in $\mathbb{Z}_p$ such that $\frac{df}{dx}(a)$ is in $\mathbb{Z}_p^\times$ 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 $\mathbb{Z}_p$.*

With this knowledge in mind, we can now start our analysis. For this paper, we let n, k, and e be integers, p a prime, and g a unit modulo p (i.e. $p \nmid g$, so g has an inverse modulo p). We will be counting the integer solutions of the congruence $g^{x^n} \equiv x^k \pmod{p^e}$, or equivalently, the zeros of $f : \mathbb{Z} \to \mathbb{Z}/p^e\mathbb{Z}$, where $f(x) = g^{x^n} - x^k \pmod{p^e}$. We denote the multiplicative order of g modulo p as m.

2 Periodicity

The first thing to note about our function f is that it is periodic, since it will restrict the range of x to examine when counting solutions. The theorem in this section describes its periodicity.

Lemma 2. $g^{m\cdot p^{e-1}} \equiv 1 \pmod{p^e}$.

This lemma is obtained from the proof of [9, Theorem 1], and allows us to conclude with the following theorem.

Theorem 3. *Fixing all variables except x, we have that*

$$g^{(x+mp^e)^n} - (x+mp^e)^k \equiv g^{x^n} - x^k \pmod{p^e}.$$

In other words, $f(x) = f(x + mp^e)$.

Proof. First, consider $g^{(x+mp^e)^n} \pmod{p^e}$. We know

$$(x+mp^e)^n = \sum_{i=0}^{n} \binom{n}{i} x^i (mp^e)^{n-i}.$$

Since $mp^{e-1} | mp^e$ and mp^e divides all terms except x^n, by Lemma 2 we have

$$g^{(x+mp^e)^n} \equiv g^{x^n} \pmod{p^e}.$$

Now consider $(x+mp^e)^k$. We can also expand this to

$$(x+mp^e)^k = \sum_{i=0}^{k} \binom{k}{i} x^i (mp^e)^{k-i}.$$

Since $p^e | mp^e$ and mp^e divides all terms except x^k, we have

$$(x + mp^e)^k \equiv x^k \pmod{p^e}.$$

Thus $g^{(x+mp^e)^n} - (x + mp^e)^k \equiv g^{x^n} - x^k \pmod{p^e}$.

□

3 Interpolation

Since we would like to analyze our equation p-adically, our first goal is to interpolate our function $f : \mathbb{Z} \to \mathbb{Z}/p^e\mathbb{Z}$, $f(x) = g^{x^n} - x^k \pmod{p^e}$ to a function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$.

We find that although we cannot interpolate to a single continuous p-adic function, we can interpolate to a finite number of p-adic functions that agree with $f(x)$ on certain values of x.

Theorem 4. *For $p \neq 2$, let $g \in \mathbb{Z}_p^\times$ 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

$$F_{x_0}(x) = \omega(g)^{x_0^n} \langle g \rangle^{x^n}$$

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

Proof. By [5, Proposition 4.6.1], we need I_{x_0} to be dense in $\mathbb{Z}_p$ and for each $F_{x_0}(x)$ be uniformly continuous and bounded. We know that if a function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is continuous on $\mathbb{Z}_p$, then it is also uniformly continuous and bounded [7, Theorem 4.1.4]. Thus, it suffices to show density of I_{x_0}, continuity of each F_{x_0} as a function on I_{x_0}, and that $F_{x_0}(x) = g^{x^n}$ with the proper conditions on x.

We first need to prove density of I_{x_0} in $\mathbb{Z}_p$. This is shown in the proof of [9, Theorem 16] when we let $c = 1$.

Now we must show each $F_{x_0}(x) = \omega(g)^{x_0^n} \langle g \rangle^{x^n}$ is uniformly continuous on I_{x_0}. Given $\epsilon > 0$, find N such that $p^{-N} < \epsilon$. Now if $x, y \in I_{x_0}$ such that

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

then $x = y + p^N A$ for some $A \in \mathbb{Z}$. Consider

$$\begin{aligned} |\langle g \rangle^{x^n} - \langle g \rangle^{y^n}|_p = |\langle g \rangle^{(y+p^N A)^n} - \langle g \rangle^{y^n}|_p &= |\langle g \rangle^{y^n}|_p |\langle g \rangle^{(y+p^N A)^n - y^n} - 1|_p \\ &= |\langle g \rangle^{(y+p^N A)^n - y^n} - 1|_p, \end{aligned}$$

and using the binomial theorem, we get

$$\langle g \rangle^{(y+p^N A)^n - y^n} = \langle g \rangle^{\sum_{i=1}^n \binom{n}{i} y^{n-i} (p^N A)^i}.$$

If we factor out p^N from the exponent, we get

$$\langle g\rangle^{\sum_{i=1}^{n}\binom{n}{i}y^{n-i}(p^NA)^i} = \langle g\rangle^{p^Nb},$$

where $b = \sum_{i=1}^{n}\binom{n}{i}y^{n-i}(p^N)^{i-1}A^i$, which is an integer. So we have

$$|\langle g\rangle^{x^n} - \langle g\rangle^{y^n}|_p = |\langle g\rangle^{(y+p^NA)^n-y^n} - 1|_p = |\langle g\rangle^{p^Nb} - 1|_p$$

Using the binomial theorem again, and the fact that $\langle g\rangle = 1 + pM$, we get

$$(1+pM)^{p^Nb} = 1 + p^Nbp M + \frac{p^Nb(p^Nb-1)}{2}(pM)^2 + \ldots + (pM)^{p^Nb}.$$

Because all terms except for the first are in $p^{N+1}\mathbb{Z}_p$, we see that

$$|\langle g\rangle^{p^NA} - 1|_p \leq p^{-(N+1)} < p^{-N} < \epsilon.$$

So the function mapping $x \to \langle g\rangle^{x^n}$ is uniformly continuous on I_{x_0} and hence on $\mathbb{Z}_p$ by [7, Thm 4.15]. Since each $F_{x_0}(x) = \omega(g)^{x_0^n}\langle g\rangle^{x^n}$ for fixed x_0, and g, and $\omega(g)^{x_0^n}$ is a constant, we have that $F_{x_0}(x)$ is a constant times a uniformly continuous function. Hence, each $F_{x_0}(x)$ is uniformly continuous on $\mathbb{Z}_p$ [7, Exercise 89].

Lastly, we show that $F_{x_0}(x) = g^{x^n}$ when $x \in I_{x_0}$. Since $x \equiv x_0 \pmod{p-1}$, we have that

$$g^{x^n} = \omega(g)^{x^n}\langle g\rangle^{x^n} = \omega(g)^{x_0^n}\langle g\rangle^{x^n} = F_{x_0}(x).$$

□

We can extend this theorem to multiples of the order of g modulo p:

Theorem 5. *For this theorem only, we let m be any multiple of the multiplicative order of g modulo p, $p \neq 2$, so that $m \mid p-1$. Let $g \in \mathbb{Z}_p^\times$ and $x_0 \in \mathbb{Z}/m\mathbb{Z}$, and let*

$$J_{x_0} = \{x \in \mathbb{Z} \mid x \equiv x_0 \pmod{m}\} \subseteq \mathbb{Z}.$$

Then

$$F_{x_0}(x) = \omega(g)^{x_0^n}\langle g\rangle^{x^n}$$

defines a uniformly continuous function on $\mathbb{Z}_p$ such that $F_{x_0}(x) = g^{x^n}$ whenever $x \in J_{x_0}$.

Proof. Since $g^m \equiv 1 \pmod{p}$, $\omega(g)^{m^n} = \omega(g^{m^n}) = \omega(1) = 1$. If $x_0, x_0' \in \mathbb{Z}/(p-1)\mathbb{Z}$ and $x_0 \equiv x_0' \pmod{m}$, then the two functions F_{x_0} and $F_{x_0'}$ given by Theorem 4 are equal and are the same as g^{x^n} when $x \in I_{x_0} \cup I_{x_0'} \subseteq J_{x_0}$. □

4 Counting Solutions

Now that we have our p-adic functions, we can use those to begin counting solutions. We begin by counting solutions to our modified congruences modulo p, and then proceed by lifting these solutions to p-adic solutions modulo p^e. Lastly, we will refer back to our theorems on interpolation to find when the solutions to our modified congruences will give us solutions to our original congruence $g^{x^n} \equiv x^k \pmod{p^e}$.

The following lemma analyzes solutions modulo p.

Lemma 6. *Consider the equation*

$$g^{x_0^n} \equiv x^k \pmod{p}.$$

Define $d = \frac{\gcd(k,p-1)}{\gcd(k,\frac{p-1}{m})}$, *and let* $q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_i^{\alpha_i}$ *be the prime factorization of* d. *Then there are* $N = \frac{m \cdot \gcd(k,p-1)}{q_1^{\lceil \frac{\alpha_1}{n} \rceil} q_2^{\lceil \frac{\alpha_2}{n} \rceil} \cdots q_i^{\lceil \frac{\alpha_i}{n} \rceil}}$ *solution pairs* (x_0, x) *to the above equation, where* $x_0 \in \{0, 1, \ldots, m-1\}$ *and* $x \in \{0, 1, \ldots, p-1\}$.

Proof. Let h be a primitive root modulo p, so we can express $g \equiv h^a \pmod{p}$ and $x \equiv h^b \pmod{p}$. So $g^{x_0^n} \equiv x^k \pmod{p}$ becomes $(h^a)^{x_0^n} \equiv (h^b)^k \pmod{p}$. Since h is a primitive root, we have that $ax_0^n \equiv bk \pmod{p-1}$. From [1, Theorem 5.1], we have that there are $\gcd(k, p-1)$ mutually incongruent solutions for b (which correspond to a distinct values of x) if $\gcd(k, p-1) \mid ax_0^n$, and no solutions otherwise. So we must now count x_0 where $\gcd(k, p-1) \mid ax_0^n$.

We have that $\gcd(k, p-1) \mid ax_0^n$ if and only if $\frac{\gcd(k,p-1)}{\gcd(k,p-1,a)} \mid \frac{a}{\gcd(k,p-1,a)} x_0^n$. Note that $\gcd(k, p-1, a) = \gcd(\gcd(k, p-1), a)$ so $\frac{\gcd(k,p-1)}{\gcd(k,p-1,a)}$ is relatively prime to $\frac{a}{\gcd(k,p-1,a)}$. Now we only need to count x_0 that satisfy $\frac{\gcd(k,p-1)}{\gcd(k,p-1,a)} \mid x_0^n$.

Because we defined h and a so that $g \equiv h^a \pmod{p}$, and g has order m, we know that $\gcd(a, p-1) = \frac{p-1}{m}$. So $\gcd(k, p-1, a) = gcd(k, \gcd(a, p-1)) = \gcd(k, \frac{p-1}{m})$.

Now we are left with counting x_0 that satisfy $\frac{\gcd(k,p-1)}{\gcd(k,\frac{p-1}{m})} \mid x_0^n$, which is the same as $d \mid x_0^n$. In order to count the number of solutions, we look at the prime factorization of d. We have that

$$q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_i^{\alpha_i} \mid x_0^n \text{ if and only if } q_1^{\lceil \frac{\alpha_1}{n} \rceil} q_2^{\lceil \frac{\alpha_2}{n} \rceil} \cdots q_i^{\lceil \frac{\alpha_i}{n} \rceil} \mid x_0,$$

and thus we have $\frac{m}{q_1^{\lceil \frac{\alpha_1}{n} \rceil} q_2^{\lceil \frac{\alpha_2}{n} \rceil} \cdots q_i^{\lceil \frac{\alpha_i}{n} \rceil}}$ distinct $x_0 \in \{0, 1, \ldots, m\}$ that satisfy our conditions. Since there are $\gcd(k, p-1)$ solutions $x \in \{0, 1, \ldots, p-1\}$ for each x_0, we have a total of $\frac{m \cdot \gcd(k,p-1)}{q_1^{\lceil \frac{\alpha_1}{n} \rceil} q_2^{\lceil \frac{\alpha_2}{n} \rceil} \cdots q_i^{\lceil \frac{\alpha_i}{n} \rceil}}$ solution pairs (x_0, x) to $g^{x_0^n} \equiv x^k \pmod{p}$.

□

4.1 Counting solutions when $p \nmid k$

When we lift the solutions we found modulo p to solutions modulo p^e, we have to use different methods for when $p \nmid k$ than when $p \mid k$. We will be able to use

Hensel's lemma to lift to solutions modulo p^e when $p \nmid k$. The following lemma describes the result.

Lemma 7. *For $p \neq 2$, $p \nmid k$, let $g \in \mathbb{Z}_p^\times$ be fixed, and $x_0 \in \{0, 1, \cdots, m-1\}$. If a is a solution in $\{0, 1, \ldots, p-1\}$ to*

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

Then there is a unique solution in $\mathbb{Z}_p$ to the equation

$$\omega(g)^{x_0^n} \langle g \rangle^{x^n} = x^k$$

where $x \equiv a \pmod{p}$.

Proof. Since $\langle g \rangle$ is in $1 + p\mathbb{Z}_p$, we get

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

where from [5, Proposition 4.5.9], we know that $\log_p(\langle g \rangle) \in p\mathbb{Z}_p$. Now that we have a convergent power series since $|\log_p(\langle g \rangle)^i/i!|_p \to 0$ as $i \to \infty$ [2, Chapter 2, Theorem 3.1], we examine $f(x) = F_{x_0}(x) - x$ and its derivative to see if we can apply a generalization of Hensel's lemma.

Consider

$$\begin{aligned} f(x) = \omega(g)^{x_0^n}(1 &+ x^n \log_p(\langle g \rangle) + x^{2n} \log_p(\langle g \rangle)^2/2! \\ &+ \text{higher order terms in powers of } \log_p(\langle g \rangle)) - x^k. \end{aligned}$$

Since we know $\log_p(\langle g \rangle) \in p\mathbb{Z}_p$, so $\log_p(\langle g \rangle) \equiv 0 \pmod{p}$, we have that

$$\begin{aligned} f(a) \equiv \omega(g)^{x_0^n}(1 &+ a^n(0) + a^{2n}(0) \\ &+ \text{higher order terms congruent to 0 (mod p) }) - a^k \pmod{p} \\ &\equiv \omega(g)^{x_0^n} - a^k \equiv 0 \pmod{p}. \end{aligned}$$

Additionally, we have that

$$\begin{aligned} f'(x) = \omega(g)^{x_0^n}(nx^{n-1} \log_p(\langle g \rangle) + (2n)x^{2n-1} \log_p(\langle g \rangle)^2/2! \\ + 3nx^{3n-1} \log_p(\langle g \rangle)^3/3! + ...) - ka^{k-1} \end{aligned}$$

so that

$$\begin{aligned} f'(a) &\equiv \omega(g)^{x_0^n}(na^{n-1}(0) + (2n)a^{2n-1}(0)^2/2! + 3na^{3n-1}(0)^3/3! + ...) - ka^{k-1} \\ &\equiv 0 - ka^{k-1} \pmod{p}. \end{aligned}$$

We know $a^k \equiv \omega(g)^{x_0^n} \pmod{p}$ so then we know $a^k \not\equiv 0 \pmod{p}$ and thus $a^{k-1} \not\equiv 0 \pmod{p}$. Also, we have $p \nmid k$. So then $-ka^{k-1} \not\equiv 0 \pmod{p}$. Now we know we can apply Theorem 1, which states that there is a unique $x \in \mathbb{Z}_p$ for which $x \equiv a \pmod{p}$ and $f(x) = 0$ in $\mathbb{Z}_p$.

□

Now that we have found solutions to our modified equations, we need to be able to piece them together to give us solutions to our original equation. The following theorem uses the results from our lemmas to give us the number of solutions to $g^{x^n} \equiv x^k \pmod{p^e}$ when $p \nmid k$.

Theorem 8. *For $p \neq 2$, let $g \in \mathbb{Z}_p^\times$ and $n, k \in \mathbb{Z}$ be fixed and $p \nmid k$. Then there are $N = \frac{m \cdot \gcd(k, p-1)}{q_1^{\lceil \frac{\alpha_1}{n} \rceil} q_2^{\lceil \frac{\alpha_2}{n} \rceil} \cdots q_i^{\lceil \frac{\alpha_i}{n} \rceil}}$ solutions x to the equation*

$$g^{x^n} \equiv x^k \pmod{p^e}$$

for $x \in \{1, 2, \cdots, p^e m\}$.

Proof. We begin by considering the number of solutions modulo p to a slightly different equation. By Lemma 6, we have $\frac{m \cdot \gcd(k, p-1)}{q_1^{\lceil \frac{\alpha_1}{n} \rceil} q_2^{\lceil \frac{\alpha_2}{n} \rceil} \cdots q_i^{\lceil \frac{\alpha_i}{n} \rceil}}$ solution pairs (x_0, x_1) to $g^{x_0^n} \equiv x_1^k \pmod{p}$ where the x_0 are distinct $\pmod{m}$ and x_1 are distinct $\pmod{p}$. For each x_1 that appears in a solution pair to $g^{x_0^n} \equiv x_1^k \pmod{p}$, then by Lemma 7 we have a unique solution x' in $\mathbb{Z}_p$ to $\omega(g)^{x_0^n} \langle g \rangle^{(x')^n} = (x')^k$ where $x' \equiv x \pmod{p}$. By the Chinese Remainder Theorem, we have that there is exactly one $x \in \mathbb{Z}/mp^e\mathbb{Z}$ where $x \equiv x_0 \pmod{m}$ and $x \equiv x' \pmod{p^e}$. Thus by Theorem 5 we have exactly one solution to $g^{x^n} \equiv x^k \pmod{p^e}$ in $\mathbb{Z}/mp^e\mathbb{Z}$ for every solution pair to $g^{x_0^n} \equiv x^k \pmod{p}$, and therefore there are $\frac{m \cdot \gcd(k, p-1)}{q_1^{\lceil \frac{\alpha_1}{n} \rceil} q_2^{\lceil \frac{\alpha_2}{n} \rceil} \cdots q_i^{\lceil \frac{\alpha_i}{n} \rceil}}$ solutions in $\mathbb{Z}/mp^e\mathbb{Z}$ to the equation $g^{x^n} \equiv x^k \pmod{p^e}$.

□

We find that this theorem is consistent with our results. For example, looking at $g^{x^n} \equiv x^k \pmod{7^e}$ for $0 \leq x \leq m \cdot 7^e$, we get the following number of solutions for all n and e.

Table 1: $g^{x^n} \equiv x^k \pmod{7^e}$ for $0 \leq x < m \cdot 7^e$

g	**m**	**# solns: k=1**	**# solns: k=2**	**# solns: k=3**	**# solns: k=4**
1	**1**	1	2	3	2
2	**3**	3	6	3	6
3	**6**	6	6	6	6
4	**3**	3	6	3	6
5	**6**	6	6	6	6
6	**2**	2	2	6	2

So if we look at the case when $k = 4$, we find that

$$d = \frac{\gcd(k, p-1)}{\gcd(k, \frac{p-1}{m})} = \frac{\gcd(4, 7-1)}{\gcd(2, \frac{7-1}{m})} = \frac{2}{\gcd(4, \frac{6}{m})} = \begin{cases} 1 & \text{if } 2 \nmid m \\ 2 & \text{if } 2 \mid m \end{cases},$$

and

$$N = \begin{cases} \frac{m \gcd(4,7-1)}{1} = 2m & \text{if } 2 \nmid m \\ \frac{m \gcd(4,7-1)}{2} = m & \text{if } 2 \mid m \end{cases},$$

which matches the findings in Table 4.1.

4.2 Counting solutions when $p = k$ and $n = 1$

Our findings for when $p = k$ differs from our results when $p \nmid k$. For example, when $p = 11$, we find the number of solutions detailed in Table 4.2. We see that our N solutions modulo p lift to different numbers of solutions modulo p^e than in the $p \nmid k$ case. This suggests that we must lift solutions modulo p to solutions modulo p^e differently: we will end up using induction on e. So, we will count solutions modulo p^2 and use that as the base case in our induction.

g	**m**	**# solns: e=1**	**# solns: e=2**	**# solns: e=3**	**# solns: e=4**
1	**1**	1	11	11	11
2	**10**	10	0	0	0
3	**5**	5	55	55	55
4	**5**	5	0	0	0
5	**5**	5	0	0	0
6	**10**	10	0	0	0
7	**10**	10	0	0	0
8	**10**	10	0	0	0
9	**5**	5	55	55	55
10	**2**	2	0	0	0

Table 2: $g^x \equiv x^{11} \pmod{11^e}$ for $0 \leq x < m \cdot 11^e$

As we lift, we find that the value of g^{p-1} modulo p^2 is important. By Fermat's Little Theorem, we have for prime p and $p \nmid g$, that $g^{p-1} \equiv 1 \pmod{p}$. Looking at this equivalence modulo p^2 gives the following definition.

Definition 3. An integer g is called a Wieferich base modulo p if $g^{p-1} \equiv 1 \pmod{p^2}$.

Now we are able to count solutions to $g^x \equiv x^p \pmod{p^2}$, seeing that the result depends heavily on whether g is a Wieferich base modulo p.

Lemma 9. *Let $p \neq 2$, let a_0 be a solution to $g^x \equiv x^p \pmod{p}$, and let $x_0 \equiv a_0 \pmod{m}$. Then the following are equivalent:*

1. *$g = \omega(g)\,\langle g \rangle$, where $\langle g \rangle \equiv 1 \pmod{p^2}$.*
2. *g is a Wieferich base modulo p*
3. *a_0 lifts to at least one solution $a \in \mathbb{Z}/p^2\mathbb{Z}$ to $g^x \equiv x^p \pmod{p^2}$ where $a \equiv a_0 \pmod{p}$ and $a \equiv x_0 \pmod{m}$.*

Furthermore, in 3, we also have that if a_0 lifts to a solution in $\mathbb{Z}/p^2\mathbb{Z}$, it lifts to p distinct solutions in $\mathbb{Z}/p^2\mathbb{Z}$.

Proof. For this proof, we begin by finding a congruence that holds exactly when we have a solution a to $g^x \equiv x^p \pmod{p^2}$ that satisfies the conditions that $a \equiv x_0 \pmod{m}$ and $a \equiv a_0 \pmod{p}$. We will then use the equivalent statement to prove $3 \implies 2$ and $1 \implies 3$, and then finish by showing $2 \implies 1$.

Let $a \equiv x_0 \pmod{m}$ and $a \equiv a_0 \pmod{p}$, and consider when $0 \equiv g^a - a^p \pmod{p^2}$.

Recall from Theorem 5 that $g^a = \omega(g)^{x_0} \langle g \rangle^a$ when $a \equiv x_0 \pmod{m}$. So since $a \equiv x_0 \pmod{m}$, we have

$$\begin{aligned} 0 \equiv g^a - a^p &\equiv \omega(g)^{x_0} \langle g \rangle^a - a^p \\ &\equiv \omega(g)^{x_0} \sum_{i=0}^{\infty} \Big(\frac{a^i (\log_p \langle g \rangle)^i}{i!} \Big) - a^p \pmod{p^2}. \end{aligned} \tag{1}$$

We have $a \equiv a_0 \pmod{p}$, so we get $a \equiv a_0 + a_1 p \pmod{p^2}$, and thus equation (1) holds exactly when we get

$$\omega(g)^{x_0} \sum_{i=0}^{\infty} \Big(\frac{(a_0 + a_1 p)^i (\log_p \langle g \rangle)^i}{i!} \Big) - (a_0 + a_1 p)^p \equiv 0 \pmod{p^2}.$$

Since $\log_p \langle g \rangle \in p\mathbb{Z}_p$, this reduces to

$$\omega(g)^{x_0} (1 + a_0 \log_p \langle g \rangle) - (a_0 + a_1 p)^p \equiv 0 \pmod{p^2}. \tag{2}$$

When we expand the term $(a_0 + a_1 p)^p$ modulo p^2, we find that it is congruent to a_0^p, and we obtain

$$\omega(g)^{x_0} (1 + a_0 \log_p \langle g \rangle) - a_0^p \equiv 0 \pmod{p^2}. \tag{3}$$

Note that

$$\log_p \langle g \rangle = \sum_{i=0}^{\infty} \Big((-1)^{i+1} \frac{(\langle g \rangle - 1)^i}{i} \Big),$$

and since $\langle g \rangle - 1 \in p\mathbb{Z}_p$, we have

$$\log_p \langle g \rangle \equiv \langle g \rangle - 1 \pmod{p^2}.$$

So then we can replace $\log_p \langle g \rangle$ in equation (3) to obtain

$$\begin{aligned} \omega(g)^{x_0} (1 &+ a_0 (\langle g \rangle - 1)) - a_0^p \\ &\equiv \omega(g)^{x_0} a_0 (\langle g \rangle - 1) + \omega(g)^{x_0} - a_0^p \equiv 0 \pmod{p^2}. \end{aligned} \tag{4}$$

We have that $\langle g \rangle - 1 \equiv 0 \pmod{p}$. We also know

$$g^{a_0} - a_0^p \equiv \omega(g)^{a_0} \langle g \rangle^{a_0} - a_0^p \equiv \omega(g)^{x_0} - a_0^p \equiv 0 \pmod{p}, \tag{5}$$

so we can write equation (4) as

$$\frac{\omega(g)^{x_0} a_0 (\langle g \rangle - 1)}{p} + \frac{\omega(g)^{x_0} - a_0^p}{p} \equiv 0 \pmod{p}. \tag{6}$$

Now consider the following: by (4.2) and Fermat's Little Theorem we have

$$\omega(g)^{x_0} - a_0^p \equiv \omega(g)^{x_0} - a_0 \equiv 0 \pmod{p}.$$

By definition, this is true exactly when

$$\omega(g)^{x_0} - a_0^p = rp, \text{ for some } r \in \mathbb{Z}_p.$$

Now this is true if and only if

$$(\omega(g)^{x_0})^{p-1} = (a_0^p + rp)^{p-1}.$$

Since $\omega(g)$ is a $(p-1)$th root of unity, we find that $(\omega(g)^{x_0})^{p-1} = 1$. By using this fact and expanding $(a_0^p + rp)^{p-1}$, we find that the above is equivalent to

$$1 = \sum_{i=1}^{p-1} \left(\binom{p-1}{i} (rp)^i (a_0^p)^{p-1-i} \right).$$

Examining this equation modulo p^2, we find that

$$1 \equiv a_0^{p(p-1)} + p(p-1)ra_0^{p(p-2)} \pmod{p^2},$$

and since the order of the group $\mathbb{Z}/p^2\mathbb{Z}$ is $p(p-1)$, we get $a_0^{p(p-1)} \equiv 0 \pmod{p^2}$, so

$$1 \equiv a_0^{p(p-1)} + p(p-1)ra_0^{p(p-2)} \pmod{p^2},$$

and thus

$$0 \equiv (p-1)ra_0^{p(p-2)} \pmod{p}.$$

Since $p-1, a_0 \not\equiv 0 \pmod{p}$ (if $a_0 \equiv 0 \pmod{p}$, then $1 \equiv g^0 \equiv 0^p \equiv 0 \pmod{p}$), we must have $r \equiv 0 \pmod{p}$. So then $\omega(g)^{x_0} - a_0^p = (kp)p \equiv 0 \pmod{p^2}$ for some $k \in \mathbb{Z}$.

Thus we always have that $p \mid \frac{\omega(g)^{x_0} - a_0^p}{p}$, and we can reduce equation (6) further:

$$\frac{\omega(g)^{x_0} a_0(\langle g \rangle - 1)}{p} + \frac{\omega(g)^{x_0} - a_0^p}{p} \equiv \frac{\omega(g)^{x_0} a_0(\langle g \rangle - 1)}{p} \equiv 0 \pmod{p}. \tag{7}$$

Now we have that a solves $g^a \equiv a^p \pmod{p^2}$ if and only if the above equivalence holds, and we continue with our proof.

$1 \implies 3$:

Assuming 1, we have that $\langle g \rangle \equiv 1 \pmod{p^2}$. So then $p^2 \mid (\langle g \rangle - 1)$, and so we get

$$\frac{\omega(g)^{x_0} a_0(\langle g \rangle - 1)}{p} \equiv 0 \pmod{p}.$$

Thus all p choices for $a_1 \in \{0, 1, \ldots, p-1\}$ give a solution $a \equiv a_0 + a_1 p \pmod{p^2}$ to $g^x \equiv x^p \pmod{p^2}$ whenever $a \equiv a_0 \pmod{p}$ and $a \equiv x_0 \pmod{m}$.

By the Chinese Remainder Theorem, we have exactly one $a \in \{0, 1, \ldots, mp^2\}$ where both $a \equiv a_0 + a_1 p \pmod{p^2}$ and $a \equiv x_0 \pmod{m}$ are satisfied. Since there are p distinct choices for a_1, we have p solutions to $g^x \equiv x^p \pmod{p^2}$ in $\{0, 1, \ldots, mp^2\}$.

$3 \implies 2$:

Assuming 3, we know there is at least one a solving $\frac{\omega(g)^{x_0} a_0 (\langle g \rangle - 1)}{p} \equiv 0 \pmod{p}$. We know by equation (4.2) and Fermat's Little Theorem that $\omega(g)^{x_0} \equiv a_0^p \equiv a_0 \pmod{p}$, and since $\omega(g) \not\equiv 0 \pmod{p}$, then $p \nmid a_0$.

Thus we must have $p^2 \mid (\langle g \rangle - 1)$, so then

$$g^{p-1} \equiv \omega(g)^{p-1} \langle g \rangle^{p-1} \equiv \omega(g)^{p-1} 1^{p-1} \equiv 1 \pmod{p^2},$$

which means g is a Wieferich base modulo p.

$2 \implies 1$:

Assuming 2, we have that $g^{p-1} \equiv 1 \pmod{p^2}$. Write $\langle g \rangle = 1 + g_1 p$. Then we have

$$1 \equiv g^{p-1} \equiv \omega(g)^{p-1} \langle g \rangle^{p-1} \equiv \langle g \rangle^{p-1} \equiv (1 + g_1 p)^{p-1} \pmod{p^2}.$$

Expanding $(1 + g_1 p)^{p-1}$ we get

$$1 \equiv \sum_{i=0}^{i=p-1} \binom{p-1}{i} (g_1 p)^i \equiv 1 + (p-1) g_1 p \pmod{p^2}.$$

So then we have $0 \equiv (p-1) g_1 p \pmod{p^2}$, and dividing through by p, we obtain

$$(p-1) g_1 \equiv 0 \pmod{p}.$$

Since $p - 1 \not\equiv 0 \pmod{p}$, we must have $g_1 \equiv 0 \pmod{p}$. Thus

$$\langle g \rangle \equiv 1 + g_1 p \equiv 1 \pmod{p^2}.$$

□

The last theorem we give uses our previous lemma as a base case to count solutions to $g^x \equiv x^p \pmod{p^e}$ for $e > 1$.

Theorem 10. *For $p \neq 2$, let $g \in \mathbb{Z}_p^\times$ be fixed. Let N be the same as in Theorem 8. Then there are N solutions x to the equation $g^x \equiv x^p \pmod{p}$. Furthermore, for $e > 1$, the equation $g^x \equiv x^p \pmod{p^e}$ has Np solutions x if $g^{p-1} \equiv 1 \pmod{p^2}$ (i.e. g is a Wieferich base modulo p), and no solutions otherwise.*

Proof. First consider when $e = 1$. We have by Lemma 6 that there are N solution pairs $(x_0, x_1) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ to $g^{x_0} \equiv x_1^p \pmod{p}$. By the Chinese Remainder Theorem, there is exactly one $x \in \mathbb{Z}/mp\mathbb{Z}$ where $x \equiv x_0 \pmod{m}$ and $x \equiv x_1 \pmod{p}$, so there is exactly one solution $x \in \mathbb{Z}/mp\mathbb{Z}$ where $g^x \equiv g^{x_0} \equiv x_1^p \equiv x^p \pmod{p}$. Since there are N solution pairs, then there are N solutions to $g^x \equiv x^p \pmod{p}$.

Now consider when $e = 2$. If g is a Wieferich base modulo p, then for each of the N solutions above, we let a_0 be a solution and find that we have p solutions to $g^x \equiv x^p \pmod{p^2}$ by Lemma 9. Since this holds for all our N solutions modulo p, we have Np total solutions to $g^x \equiv x^p \pmod{p^2}$.

If g is not a Wieferich base modulo p, then by Lemma 9, none of the N solutions we found modulo p lift to a solution to $g^x \equiv x^p \pmod{p^2}$, so there cannot be any solutions modulo p^2. Furthermore, there cannot be any solutions to $g^x \equiv x^p \pmod{p^e}$ for $e \geq 3$.

When g is a Wieferich base modulo p and $e > 1$, we use induction. The base case ($e = 2$) is given above, and note that the solutions modulo p^2 take the form $a_0 + a_1 p \pmod{p^2}$, where a_1 takes any value in $\mathbb{Z}/p\mathbb{Z}$. Let

$$f_{x_0}(x) = F_{x_0}(x) - g^p = \omega(g)^{x_0} \langle g \rangle^x - x^p = \omega(g)^{x_0} \Big(\sum_{i=0}^{\infty} \frac{x^i (\log_p \langle g \rangle)^i}{i!} \Big) - x^p.$$

For the induction assumption, we assume that we have Np solutions $a \in \mathbb{Z}/mp^{e-1}\mathbb{Z}$ s.t. $g^x - x^k \equiv 0 \pmod{p^{e-1}}$, written $a \equiv a_0 + a_1 p + \cdots + a_{e-2} p^{e-2} \equiv a' + a_{e-2} p^{e-2} \pmod{p^{e-1}}$, where a_{e-2} can take any value modulo p.

Note that we have $\langle g \rangle \equiv 1 \pmod{p^2}$ by Lemma 9.

We want to find a solution x that solves $g^x \equiv x^p \pmod{p^e}$, so it must also solve $g^x \equiv x^p \pmod{p^{e-1}}$. So we must have $x \equiv a \pmod{p^{e-1}}$ for one of our solutions a. Thus we have that $x \equiv a + a_{e-1} p^{e-1} \pmod{p^e}$ for some a. Set $x_0 \equiv a \pmod{m}$. Note that $f_{x_0}(x) = g^x - x^p$ when $x \equiv x_0 \pmod{m}$ by Theorem 5, so $f_{x_0}(a) \equiv 0 \pmod{p^{e-1}}$.

So we have

$$\begin{aligned} f_{x_0}(x) &\equiv f_{x_0}(a + a_{e-1} p^{e-1}) \\ &\equiv \omega(g)^{x_0} \Big(\sum_{i=0}^{\infty} \frac{(a + a_{e-1} p^{e-1})^i (\log_p \langle g \rangle)^i}{i!} \Big) - (a + a_{e-1} p^{e-1})^p \pmod{p^e} \end{aligned}$$

Since for all $k \in \mathbb{Z}^+$, $p \mid \frac{(\log_p \langle g \rangle)^k}{k!}$ (by [5, Lemma 4.5.4]), and because $a \equiv a' + a_{e-2} p^{e-2} \pmod{p^{e-1}}$, we can simplify to get

$$\begin{aligned} f_{x_0}(x) &\equiv \omega(g)^{x_0} \Big(\sum_{i=0}^{\infty} \frac{(a' + a_{e-2} p^{e-2})^i (\log_p \langle g \rangle)^i}{i!} \Big) - (a' + a_{e-2} p^{e-2} + a_{e-1} p^{e-1})^p \\ &\equiv \omega(g)^{x_0} \Big(1 + (a' + a_{e-2} p^{e-2}) \log_p \langle g \rangle + \sum_{i=2}^{e-1} \frac{(a')^i (\log_p \langle g \rangle)^i}{i!} \Big) \\ &\qquad - (a' + a_{e-2} p^{e-2} + a_{e-1} p^{e-1})^p \pmod{p^e} \end{aligned}$$

Note that

$$\begin{aligned}(a' + a_{e-2}p^{e-2} &+ a_{e-1}p^{e-1})^p \\ &\equiv \sum_{i=0}^{p} \binom{p}{i} (a' + a_{e-2}p^{e-2})^{p-i} (a_{e-1}p^{e-1})^i \\ &\equiv (a' + a_{e-2}p^{e-2})^p \\ &\equiv \sum_{i=0}^{p} \binom{p}{i} (a')^{p-i} (a_{e-2}p^{e-2})^i \\ &\equiv (a')^p + (a')^{p-1} a_{e-2} p^{e-1} \pmod{p^e}.\end{aligned}$$

So now we have that, given a solution $x \equiv a \pmod{p^{e-1}}$, if it lifts to a solution modulo p^e, then it lifts to any $x \equiv a + a_{e-1}p^{e-1}$. When we set $f_{x_0}(x) \equiv 0 \pmod{p^e}$ to solve for x, we get

$$\begin{aligned}0 \equiv \omega(g)^{x_0} \Big(1 + (a' + a_{e-2}p^{e-2}) \log_p \langle g \rangle + \sum_{i=2}^{e-1} \frac{(a')^i (\log_p \langle g \rangle)^i}{i!}\Big) \\ -((a')^p + (a')^{p-1} a_{e-2} p^{e-1}) \pmod{p^e},\end{aligned}$$

so collecting all the a_{e-2} terms, we find that

$$\begin{aligned}-a_{e-2}(\omega(g)^{x_0} p^{e-2} \log_p \langle g \rangle &- (a')^{p-1} p^{e-1}) \\ &\equiv \omega(g)^{x_0} \Big(1 + a' \log_p \langle g \rangle + \sum_{i=2}^{e-2} \frac{(a')^i (\log_p \langle g \rangle)^i}{i!}\Big) - (a')^p \\ &\quad + \frac{\omega(g)^{x_0} (a')^{e-1} (\log_p \langle g \rangle)^{e-1}}{(e-1)!} \pmod{p^e}.\end{aligned}$$

Note that $f_{x_0}(x) \equiv f_{x_0}(a) \equiv 0 \pmod{p^{e-1}}$ and so since p^{e-1} divides the left hand side, p^{e-1} must also divide the right hand side, and we also know $p^{e-1} \mid (\log_p \langle g \rangle)^{e-1})$. So we can write

$$\begin{aligned}a_{e-2} &\frac{-(\omega(g)^{x_0} p^{e-2} \log_p \langle g \rangle - (a')^{p-1} p^{e-1})}{p^{e-1}} \\ &\equiv \frac{\omega(g)^{x_0} (1 + a' \log_p \langle g \rangle + \sum_{i=2}^{e-2} \frac{(a')^i (\log_p \langle g \rangle)^i}{i!}) - (a')^p}{p^{e-1}} \\ &\quad + \frac{\omega(g)^{x_0} (a')^{e-1} (\log_p \langle g \rangle)^{e-1}}{(e-1)! p^{e-1}} \pmod{p}\end{aligned}$$

It suffices to show that $\frac{-(\omega(g)^{x_0} p^{e-2} \log_p \langle g \rangle - (a')^{p-1} p^{e-1})}{p^{e-1}} \not\equiv 0 \pmod{p}$, since doing so would mean it has an inverse modulo p and we can solve uniquely for a_{e-2}. Then we would know that exactly one out of every p solutions $a \equiv a' + a_{e-2}p^{e-2} \pmod{p^{e-1}}$ lifts to a solution modulo p^e.

If we assume it is congruent to 0 modulo p, we have

$$\frac{-(\omega(g)^{x_0}p^{e-2}\log_p\langle g\rangle - (a')^{p-1}p^{e-1})}{p^{e-1}} \equiv 0 \pmod{p}$$

so

$$\frac{-(\omega(g)^{x_0}p^{e-2}\log_p\langle g\rangle)}{p^{e-1}} \equiv (a')^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Little Theorem. But

$$\frac{-(\omega(g)^{x_0}p^{e-2}\log_p\langle g\rangle)}{p^{e-1}} \equiv \frac{-\omega(g)^{x_0}\log_p\langle g\rangle}{p} \equiv \frac{\omega(g)^{x_0}(\sum_{i=1}^{\infty}\frac{(-1)^{i+1}(\langle g\rangle-1)^i}{i})}{p} \pmod{p}$$

and $\langle g\rangle \equiv 1 \pmod{p^2}$ so we get

$$\frac{\omega(g)^{x_0}(\sum_{i=1}^{\infty}\frac{(-1)^{i+1}(\langle g\rangle-1)^i}{i})}{p} \equiv 0 \pmod{p}.$$

This is a contradiction since $1 \not\equiv 0 \pmod{p}$. Thus we can solve uniquely for a_{e-2}, and for such an a_{e-2}, any $a_{e-1} \in \mathbb{Z}/p\mathbb{Z}$ solves $f_{x_0}(a + a_{e-1}p^{e-1}) \equiv 0 \pmod{p^e}$.

By our induction assumption, there are Np solutions to $f_{x_0}(a) \equiv 0 \pmod{p^{e-1}}$, $a \equiv a' + a_{e-2}p^{e-2} \pmod{p^{e-1}}$. Since for each solution a' to $f_{x_0}(a') \equiv 0 \pmod{p^{e-2}}$, $a' + a_{e-2}p^{e-2}$ is a solution modulo p^e for a unique $a_{e-2} \in \mathbb{Z}/p\mathbb{Z}$, we have exactly N distinct a that lift to p solutions to $f_{x_0}(x) \equiv f_{x_0}(a+a_{e-1}p^{e-1}) \equiv 0 \pmod{p^e}$. This gives a total of Np solutions modulo p^e.

□

Again, we see that this is consistent with our results. For an example, we return to our results when $p = 11$ detailed in Table 4.2. If we look at just $g = 3$ and $g = 4$, we have that $N = 5$ and so $Np = 55$. We find that $3^{10} \equiv 1 \pmod{11^2}$ and $4^{10} \not\equiv 1 \pmod{11^2}$, so $g = 3$ is a Wieferich base and has 55 solutions modulo 11^e for $e > 1$, which $g = 4$ is not a Wieferich base modulo 11 and thus has no solutions modulo p^e for $e > 1$. Both of these match our findings in Table 4.2.

5 Conclusions and Future Work

In this paper, we have applied the methods found in [6], [9], and [11] to count solutions to the equation $g^{x^n} \equiv x^k \pmod{p^e}$. When analyzing the equation for $x \in \{1, 2, \ldots, mp^e\}$, p an odd prime, we have found an exact number of solutions for the case when $p \not| k$, specifically $N = \frac{m\cdot\gcd(k,p-1)}{q_1^{\lceil\frac{\alpha_1}{n}\rceil}q_2^{\lceil\frac{\alpha_2}{n}\rceil}\cdots q_i^{\lceil\frac{\alpha_i}{n}\rceil}}$ solutions. In addition, we found that when p odd, $k = p$ and $n = 1$, that there are N solutions when $e = 1$, and either Np or 0 solutions when $e > 1$, depending on whether g is a Wieferich base modulo p.

It remains to be shown whether the same number of solutions is obtained for general n in the $k = p$ case. We suspect that similarly to the $p \nmid k$ case, n will only affect the value of N, and not the results of lifting solutions modulo p to solutions modulo p^e, but this has not been confirmed. Additionally, the case where $p \mid k$ but $k \neq p$ has not been analyzed yet. Based on a few test results, we suspect that k will affect the value of N, but that the number of solutions modulo p^e for $e > 1$ will be the same as in the $p = k$ case. Lastly, due to the fact that we need $x \in 1 + 4\mathbb{Z}_2$ rather than $x \in 1 + 2\mathbb{Z}_2$ for $\log_2(\exp_2(x))$ to converge, the case where $p = 2$ must be analyzed differently. We have done some testing that confirms that $p = 2$ yields different results than for odd prime p, leaving another avenue of analysis.

Besides counting solutions, further analysis can be done by exploring the distribution of solutions for x among intervals of length p^e rather than focusing on only the longer interval of length mp^e, since that range is generally more applicable to cryptographic schemes. There has been some analysis of the map $x \mapsto g^{x^n} \pmod{c}$ when $n = 2$ by Wood [12], and some statistical analysis of the map when $n = 1$ from [8] and [4], but more work remains to be done.

References

[1] George E. Andrews, *Number Theory*, Dover Publications, Inc., 1994.

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

[3] Jan Camenisch and Markus Stadler, *Efficient group signature schemes for large groups*, Lecture Notes in Computer Science **1294** (2006), 410–424.

[4] Daniel R. Cloutier, *Mapping the Discrete Logarithm*, Mathematical Sciences Technical Reports (MSTR) (2005).

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

[6] 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.

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

[8] Nathan Lindle, *A Statistical Look at Maps of the Discrete Logarithm*, Mathematical Sciences Technical Reports (MSTR) (2008).

[9] Abigail Mann and Adelyn Yeoh, *Deconstructing the Welch Equation Using p-adic Methods*, Rose-Hulman Undergraduate Mathematics Journal **16** (2015), no. 1, 1–23.

[10] Wade Trappe and Lawrence C. Washnigton, *Introduction to Cryptography with Coding Theory*, 2nd ed., Pearson, 2006.

[11] Anne Waldo and Caiyun Zhu, *The Discrete Lambert Map*, Rose-Hulman Undergraduate Mathematics Journal **16** (2015), no. 2, 182–194.

[12] A. Wood, *The Square Discrete Exponentiation Map*, Mathematical Sciences Technical Reports (MSTR) (2011).