Counting Solutions to Non-Algebraic Equations Modulo Prime Powers

Rae Tomarkin

Advisor:
Margaret Robinson

Thesis Committee:
Michael Davis,
Margaret Robinson, and
Jessica Sidman

A thesis submitted to the Department of Mathematics and Statistics in partial fulfillment of the requirements for the degree of Bachelor of Arts in mathematics.

Department of Mathematics and Statistics
Mount Holyoke College
South Hadley, MA 01075
May 2021

Abstract

In the digital age, cryptology, always important during conflicts, is becoming more and more significant as cybersecurity influences world affairs. We are interested in studying the mathematical properties of certain functions that are employed to create digital signatures, in particular via the ElGamal Digital Signature Scheme. Using techniques from Holden, Richardson and Robinson [3], we examine the properties of these non-algebraic functions and, more specifically, we count the number of fixed points of these functions modulo any positive power of a prime p. We show explicitly how the singular points of the function (i.e. the points where the derivative is zero modulo p) complicate the solution.

Acknowledgements

I am sincerely grateful for all that Professor Margaret Robinson has done to help me with this project, and I cannot be more thankful to have her as my advisor. I would also like to thank the Mount Holyoke Mathematics and Statistics Department, and Professor Jessica Sidman and Professor Michael Davis from my thesis committee.

Contents

Notations

Number symbols:

- $\mathbb{Z}$ The ring of integers in the rational numbers.
- $\mathbb{Z}^+$ The positive integers.
- $\mathbb{Z}_p$ The ring of p-adic integers for a prime p.
- $(\mathbb{Z}/p\mathbb{Z})^\times$ The multiplicative group of integers modulo p.
- $(\mathbb{Z}/p^e\mathbb{Z})^\times$ The multiplicative group of integers modulo p^e. (This group contains all elements x where $1 \leq x^e$ and $p \nmid x$
- $|S|$ The cardinality of the set S.
- $\lfloor x \rfloor$ The greatest integer $\leq x$

p-adic Notations:

- $\omega(x)$ The unique $(p-1)$st root of unity in $\mathbb{Z}_p$ such that $x \equiv \omega(x)$modulo p for $x \in \mathbb{Z}$.
- $< x >= \frac{x}{\omega(x)}$ A p-adic unit in $1 + p\mathbb{Z}_p$ constructed from x.
- $e_p(a)$ The smallest exponent $e \geq 1$ such that $a^e \equiv 1 \pmod{p}$, where p is a prime integer.
- $f_{x_0}(x) = \omega(x)^{g(x_0)} < x >^{g(x)} - x$ The auxiliary p-adic function whose Taylor series we are using to count solutions in the p-adic numbers. When $x \equiv x_0 \pmod{p-1}$ then $f_{x_0}(x) = x^{g(x)} - x$.
- $\psi(d)$ the number of elements $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ where $1 \leq a \leq p-1$ and $d = e_p(a)$ for $p \in \mathbb{P}$, the set of integer primes.
- $\phi(d)$ The number of integers k for $1 \leq k \leq d$ such that $\gcd(k, d) = 1$.
- where $N_{g-1}(d)$ is the number of solutions to $g(z)1 \equiv 0 modulo d$.

Chapter 1

Introduction

If Alice were to send Bob a digital letter, how can Bob be sure that the letter came from her? People are interested in digital signature schemes in order to sign digital documents in a way that is both secure and can verify an exact identity of the signer. The motivation for our work on this project is the "El-Gamal signature scheme." This scheme depends on the difficulty of the discrete logarithm problem for its security. The discrete logarithm problem is as follows: given a prime p and integers $g, a \in \mathbb{Z}$ solve for x such that $g^x \equiv a$ modulo p. Motivated by the need to understand the properties of the functions used in the El-Gamal Digital Signature Scheme, we will count the number of solutions to certain congruences modulo p^e. We will begin to document the growth patterns of these solutions, as well as examine the complications which occur at points where the derivative modulo p is zero. We examine the solutions in extended ranges for x, and then use Hensel's lemma and the Chinese Remainder Theorem, and some p-adic Analysis to solve the problem. We consider the congruence, $x^{g(x)} \equiv x$ modulo p^e, for $g(x) = x + 1$, $g(x) = x + 2$, and then give conjectures about what happens when $g(x) = x + c$ for other $c \in \mathbb{Z}$. More specifically, in chapter 2 we discuss the theorem that provide background for our theorems. In chapter 3 we discuss some known results from in order to understand the case

where $g(x) = x + 1$, which will help us with the case where $g(x) = x + 2$. In chapter 4 we go over some necessary definitions and a description of the problem explained through numerical examples. In chapter 5 we prove our main theorem, and then as our conclusion we discuss future work on a more general conjecture for the case where $g(x) = x + c$ and give final remarks in chapter 6.

Chapter 2

Background

The following theorems in this section will be used in order to defend the proofs in this paper.

Theorem 2.1 (Fermat's Little Theorem)**.** [11] Let p be a prime and a be an integer relatively prime to p. Then,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. Since a has no common factors with p we know that $ax \equiv ay \mod p$ if and only if $x \equiv y \pmod{p}$. This cancellation property allows us to see that the values $a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)$ are all distinct modulo p and thus that the set $\{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\} = \{1, 2, \ldots, p-1\}$ as sets modulo p. Hence,

$$a \cdot 1 \cdot a \cdot 2 \cdots a \cdot (p-1) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

From which we have that

$$a^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

Finally cancelling $1 \cdot 2 \cdots (p-1)$ from both sides we have our result that

$$a^{p-1} \equiv 1 \pmod{p}.$$

Q.E.D.

Theorem 2.2 (The Chinese Remainder Theorem)**.** [11] Suppose that d and e are coprime positive integers. There is a one-to-one correspondence between the set of pairs (a, b) with $0 \leq a \leq d$ and $0 \leq b \leq e$ and the set of numbers N with $0 \leq N \leq de$; such that each solution (a, b) to $x \equiv a \pmod{d}$ and $x \equiv b \pmod{e}$ corresponds to exactly one solution $x \equiv N \pmod{de}$.

Proof. We proceed by the pigeonhole principle. Gather de pigeons, and label them by numbers N between 0 and $de - 1$. Arrange the de pigeonholes, in d columns and e rows. and label them by brackets $[a, b]$ according to their column and row. Given a pigeon labeled N, there exist unique integers a, b such that $0 \leq a \leq d$ and $a \leq b < e$ and $N \equiv [a, b] \pmod{[d, e]}$. Send the pigeon N to the pigeonhole $[a, b]$ accordingly.

If two pigeons labeled M and N landed in the same pigeonhole $[a, b]$, then we would find

$$M \equiv [a, b] \pmod{[d, e]} \text{ and } N \equiv [a, b] \pmod{[d, e]}.$$

Then $M - N$ would be a multiple of d and a multiple of e. Since d and e are coprime, $M - N$ is a multiple of de. But since M and N are between 0 and $de - 1$, this implies $M = N$.

Hence no two pigeons land in the same pigeonhole, this gives a one-to-one correspondence and the result follows. Q.E.D.

Theorem 2.3. [10] For an arithmetic function F, if $\gcd(m, n) = 1$, then

$F(nm) = F(n)F(m)$.

Proof. Let

$$d_1, d_2, ..., d_r \text{be the divisors of } n$$

and

$$e_1, e_2, ..., e_r \text{be the divisors of } m.$$

The fact that m and n are relatively prime means that the divisors of mn are precisely the various products

$$d_1e_1, d_1e_2, ...d_1e_s, d_2e_1, d_2e_2..., .d_2e_2, ..., d_re_1, d_re_2, ..., d_re_s.$$

Furthermore, every d_i is relatively prime to every e_j so $\phi(d_ie_j) = \phi((d_i)\phi(e_j)$. Using this fact, we compute

$F(mn) = \phi(d_1e_1)+...+\phi(d_1e_s)+\phi(d_2e_1)+...+(d_2e_s)+...+\phi(d_re_1)+...\phi(d_re_s)$

$= \phi(d_1)\phi(e_1) + \phi(d_1)\phi(e_s) + \phi(d_2)\phi(e_1) + ... + \phi(d_2)\phi(e_2) + ... + \phi(d_r)\phi(e_1) +$

$... + \phi(d_r)\phi(e_s)$

$= (\phi(d_1) + \phi(d_2) + ... + \phi(d_r)) \cdot (\phi(e_1) + \phi(e_2) + ... + \phi(e_s))$

$= F(m)F(n).$ Q.E.D.

Theorem 2.4. [10] Let $d_1, d_2, ..., d_r$ be the divisors of a positive integer n. Then $\phi(d_1) + \phi(d_2) + ... + \phi(d_r) = n$

Proof. Let $d_1, d_2, ..., d_r$ be the positive integer divisors of n for a positive integer n. We will let $F(n) = \phi(d_1)+\phi(d_2)+...+\phi(d_r)$ and we need to verify that $F(n)$ always equals n. We will first show that $F(p^k) = p^k$. We have that $F(p^k) = \phi(1)+\phi(p)+\phi(p^2)+....+\phi(p^k)$. So this is equal to $1+(p-1)+p(p-1)+p^2(p-1)+....+p^{k-1}(p-1) = 1+(p-1)(1+p+p^2+...+p^{k-1})$ From here, by geometric sum, the right hand side is equal to $1+(p-1)(p^k-1)/(p-1) = 1+p^k-1 = p^k$.

We will now factor n into a product of prime powers, say $n = p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot$

$p_t^{k_t}$. The different prime powers are relatively prime to one another, so we can use the multiplicative property for F to compute $F(n) = F(p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_t^{k_t}) = F(p_1^{k_1}) \cdot F(p_2^{k_2}) \cdot ... \cdot F(p_t^{k_t})$. Since $F(p^k) = p^k$ for prime powers, the equation is equal to $p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_t^{k_t} = n$. Q.E.D.

Theorem 2.5. Let $G =< g >$ be the cyclic group generated by g in the integers where order of $g = n$. Then $G =< g^k >$ if and only if $gcd(k, n) = 1$.

Proof. We will first show that $g^k = 1$ if and only if $n|k$. If $n|k$ then $k = qn$ for some $q \in n$. Then $g^k = g^{qn} = (g^n)^q = 1^q = 1$. Conversely, if $g^k = 1$, we can use the division algorithm to see $k = nq + r$ with $0 \leq r < n$. Then $g^r = g^k g^{-nq} = 1^{-q} = 1$. Since $r < n$, this contradicts the minimality of the order n unless $r = 0$. Hence $r = 0$ and $k = qn$ so that $n|k$.

Next we show if $m = gcd(k, n)$ then $o(g^k) = n/m$. Let $k = ms$ and $n = mt$. Then $(g^k)^{n/m} = g^{kn/m} = g^{msn/m} = (g^n)^s = 1^s = 1$, since $g^k = 1$ if and only if $n|k$. Hence n/m divides $(k/m)r$ and since n/m and k/m are relatively prime, it follows that $n/m|r$. So n/m is the smallest power of g^k which equals 1. So $o(g^k) = n/m$. But $G =< g^k >$ if and only if $o(g^k) = |G| = n$. Hence $G =< g^k >$ if and only if $gcd(k, n) = 1$. Q.E.D.

Theorem 2.6 (Primitive Root Theorem)**.** [10] Every prime p has a primitive root. More precisely, there are exactly $\phi(p-1)$ primitive roots modulo p.

Proof. We will prove this theorem by counting. For each number between 1 and $p-1$, we know that the order $e_p(a)$ divides $p-1$. So for each number d dividing $p-1$, we might ask how many $a's$ have their order $e_p(a) = d$. We call this number $\psi(d)$. In other words, $\psi(a) =$ (the number of a's with $1 \leq a < p$ and $e_p(a) = d$.) In particular, $\psi(p-1)$ is the number of primitive roots modulo p. Let n be any number dividing say $p-1 = nk$. Then we can factor the polynomial $x^{p-1}-1$ as equal to $x^{nk}-1 = (x^n)^k-1 = (x^n-1)((x^n)^{k-1}+(x^n)^{k-2}+...+(x^n)^2+x^n+1)$.

We count how many roots these polynomials have $\pmod p$. First we observe that $x^{p-1} - 1 \equiv 0 \pmod p$ has exactly $p-1$ solutions. Since Fermat's Little Theorem tells us that $x = 1, 2, 3, ..., p-1$ are all solutions, the polynomial roots $\pmod p$ theorem says that a polynomial degree D with integer coefficients has at most D roots modulo p, so $(x^n)^{k-1} + (x^n)^{k-2} + ... + x^n + 1$ has at most $n(k-1)$ roots. The only way for this to be true is if $x^n - 1$ has exactly n roots $\pmod p$, since otherwise the right hand side won't have enough roots for the left hand side to have all $p - 1 = ak$ roots. Therefore if n divides $p-1$ then $x^n - 1 \equiv 0 \pmod p$ has exactly n solutions with $0 \leq x \leq p$.

Let's count the number of solutions a different way. If $x = a$ is a solution, the $a^n \equiv 1 \pmod p$, so by theorem 2.2, we know that $e_p(a)$ divides n. So if we look at the divisors of n and if for each divisor d of n we take those $a's$ with $e_p(a) = d$, then we end up with all the solutions of the congruence $x^n - 1 \equiv 0 \pmod p$. In other words, if $d_1, d_2, ..., d_r$ are the numbers of solutions to $x^n - 1 \equiv 0 \pmod p$ is equal to $\psi(d_1) + \psi(d_2) + ... + \psi(d_r)$ by the divisors of n (including both n and 1) then $\psi(d_1) + \psi(d_2) + ... + \psi(d_r) = n$. From above n is also equal to sum of the Euler-ψ function. We can use the fact that ψ and ϕ both satisfy this formula show that they are equal. We observe that $\phi(1) = 1$ and $\psi(1) = 1$, so we are ok if $n = 1$.Next we check that $\phi(q) = \psi(q)$ when $n = q$ is prime. The divisors of q are 1 and q, so $\phi(q) + \phi(1) = q = \psi(q) + \psi(1)$. But we know that $\phi(1) = \psi(1) = 1$, so subtracting 1 from both sides gives $\phi(q) = \psi(q)$. So, for each number n dividing $p-1$ there are exactly $\phi(n)$ numbers with $e_p(a) = p - 1$. But a's with $e_p(a) = p - 1$ are precisely the primitive roots modulo p, so we have proved that there are exactly $\phi(p-1)$ primitive roots modulo p. Q.E.D.

Theorem 2.7 (Lagrange's Remainder Theorem)**.** [1] Let f be differentiable

$N+1$ times on $(-R,R)$, define $a_n = f^{(n)}(0)/n!$ for $n = 0, 1, ...N$ and let

$$S_N(x) = a_0 + a_1 x + a_2 x^2 + ... + a_N x^N.$$

Given $x \neq 0$ in $(-R,R)$, there exists a point c satisfying $|c| < |x|$ where the error function $E_N(x) = f(x) - S_N(x)$ satisfies

$$E_N(x) = \frac{f^{(N+1)}(c)}{N+1!} x^{N+1}.$$

Proof. The Taylor coefficients are chosen so that the function f and the polynomial S_N have the same derivatives at zero, at least up through the Nth derivative, after which S_N becomes the zero function. In other words, $f^{(n)}(0) = S_N^{(n)}(0)$ for all $0 \leq n \leq N$, which implies the error function $E_N(x) = f(x) - S_N(x)$ satisfies

$$E_N^{(n)}(0) = 0 \text{ for all } n = 0, 1, 2, ..., N.$$

The key ingredient in this argument is the Generalized Mean Value Theorem, which states: if f and g are continuous on the closed interval $[a,b]$ and differentiable on the open interval (a,b),

then there exists a point $c \in (a,b)$ such where

$$[f(b) - f(a)]g(x) - [g(b) - g(a)]f'(c).$$

If g' is never zero on (a,b), then the conclusion can be stated as

$$\frac{f'(c)}{g'(c)} = \frac{f(b) - f(a)}{g(b) - g(a)}.$$

To simplify notation, let's assume $x > 0$ and apply the Generalized Mean Value Theorem to the functions $E_N(x)$ and x^{N+1} on the interval $[0,x]$. Thus,

there exists a point $x_1 \in (0,1)$ such that

$$\frac{E_N}{x^{N+1}} = \frac{E'_N(x_1)}{(N+1)x_1^x}.$$

Now apply the Generalized Mean Value Theorem to the function $E'_N(x)$ and $(N+1)x^N$ on the interval $[0,1]$ to get that there exists a point $x_2 \in (0, x_1)$ where

$$\frac{E_N}{x^{N+1}} = \frac{E'_N(x_1)}{(N+1)x_1^N} = \frac{E''_N(x_2)}{(N+1)x_2^N - 1}.$$

Continuing in this manner we find

$$\frac{E_N}{x^{N+1}} = \frac{E_N^{(N+1)}(x_{N+1})}{(N+1)!}$$

where $x_{N+1} \in (0, x_N) \subset ... \subset (0, x)$. Now set $c = x_{N+1}$. Because $s_N^{(N+1)}(x) = 0$, we have $E_N^{(X+1)} = f^{(N+1)}(x)$ and it follows that

$$E_N(x) = \frac{f^{N+1}(c)}{(N+1)!}x^{(N+1)}$$

as desired.

Lemma 2.1 (Hensel's Lemma)**.** [4] *Let $f(x)$ be a polynomial of the form $f(x) = a_0+a_1x+...+a_dx^d$, with $a_0, a_1, ..., a_d \in \mathbb{Z}$ and r such that $f(r) \equiv 0 \pmod{p}$,where $f'(r) \not\equiv 0 \pmod{p}$, then for all r there exists a unique $b = r_0+pr_1+...+p^{n-1}r_{n-1}$ where $0 \leq r_i \leq p1$ such that $f(b) \equiv 0 \pmod{p^n}$, where $n \in \mathbb{Z}^+$, and$r \equiv b \pmod{p}$.*

Proof. We will proceed by induction on n, where we are looking for solutions modulo p^n. We know from our assumption there exists an $r_0 \in \mathbb{Z}$ such that $r \equiv r_0 \pmod{p}$ and $f(r_0) \equiv 0 \pmod{p}$ where $f'(r_0) \not\equiv 0 \pmod{p}$. Thus, the base case $n = 1$ holds, for $b = r_0$. For our inductive hypothesis, we will assume

our theorem for $n = k-1$ and show there exists an r_k such that $f(r_0+pr_1+...+p^kr_k) \equiv 0 \pmod{p^{k+1}}$ and $b \equiv r_0 \pmod{p}$. Thus, our inductive assumption is that if there exists $a = r_0+pr_1+...+p^{k-1}r_{k-1}$ such that $f(a) \equiv 0 \pmod{p^k}, a \equiv r_0 \pmod{p}$, and $f'(a) \equiv f'(r_0) \not\equiv 0 \mod p$, then we can find b. To prove our inductive step, we will find r_k such that $b = a+r_kp^k$, and $f(b) \equiv 0 \pmod{p^{k+1}}$. Using the Taylor series for the polynomial $f(x)$ about $x = a$, we have $f(x) = f(a) + f'(a)(x-a) + ... + \frac{f^{(d)}(a)}{d!}(x-a)^d$. Letting $x = a + r_kp^k$, we have

$$f(a + r_kp^k) = f(a) + f'(a)(r_kp^k) + \frac{f''(a)}{2!}(r_kp^k)^2 + ... + \frac{f^d(a)}{d!}(r_kp^k)^d. \quad (2.1)$$

We set $f(a+r_kp^k) \equiv 0 \pmod{p^{k+1}}$ and solve for r_k so that the congruence holds. Considering equation (2.1) modulo p^{k+1} we get that equation (2.1) reduces modulo p^{k+1} to

$$f(a) + f'(a)(r_kp^k) \equiv 0 \pmod{p^{k+1}}.$$

So since $f(a) = p^kl$ and $f'(a) \not\equiv 0 \pmod{p}, r_k = -l(f'(a))^{-1} \pmod{p}$ and we have a unique solution for r_k. This proves our inductive step and shows $b = r_0 + ... + r_kp^k$ is the unique solution to f(b)$\equiv 0 \pmod{p^k}$ such that $b \equiv r_0 \pmod{p}$. Q.E.D.

Theorem 2.8. For $x \in \{1, 2, ..., p-1\}$, the number of solutions to $x^r \equiv 1 \pmod{p}$ is $\gcd(p-1, r)$.

Proof. We know from Fermat's Little Theorem that $x^{(p-1)} \equiv 1 \pmod{p}$ has all $x = 1, 2, ..., p-1$ values for x as solutions. So $\gcd(p-1, p-1) = p-1$ and $x^p - 1 \equiv 1 \pmod{p}$ has $p-1$ solutions. This argument shows that if $x^r \equiv 1 \pmod{p}$ then r must divide $p-1$. So if $\gcd(p-1, r) = 1$ then only $x = 1$ will be a solution to $x^r \equiv 1 \pmod{p}$. So $\gcd(p-1, r)$ will be the number of solutions in this case. Now suppose $\gcd(p-1, r) = d$ and $1 \leq d \leq p-1$. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group with multiplicative order modulo p, there is

an element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $(\mathbb{Z}/p\mathbb{Z})^\times = \{a, a^2, a^3, ..., a^{(p-1)} = 1\}$. Now since $r = dk$ and $p - 1 = d\ell$ for some $k, \ell \in \mathbb{Z}$, where $\gcd(k, \ell) = 1$. We see that $(a^\ell)^r = a^{\ell*(dk)} \equiv a^{(p-1)k} \equiv 1 \pmod{p}$. So a^l will be a solution to $x^r \equiv 1$ mod p. Now we also see that all the x values: $x = a^\ell, a^{2\ell}, a^{3\ell}, ..., a^{(d-1)\ell}, a^{de} \equiv 1 \pmod{p}$, and also $a^{d\ell} \equiv a^{(p-1)} = 1$ will solve $x^r \equiv 1 \pmod{p}$. So note there are exactly $d = \gcd(p - 1, r)$ solutions to $x^r \equiv 1 \pmod{p}$. These d solutions have to be all the solutions to $x^r \equiv 1 \pmod{p}$ because suppose $b \in (\mathbb{Z}/p\mathbb{Z})^\times$ was another solution then we would have that $b = a^e$ was a solution to $x^r \equiv 1$ mod p. This would imply that $a^{er} \equiv 1 \pmod{p}$. So dividing er by $p-1$, we have that $er = (p-1)q_1 + r_1$, where $0 \leq r_1 \leq p-1$. Now by Fermat's Little Theorem we know that $a^{p-1} \equiv 1 \pmod{p}$ and since a^e solves the congruence, we have that $1 \equiv a^{er} = a^{(p-1)q_1} \times a^{r_1} \equiv a^{r_1} \pmod{p}$ where $0 \leq r_1 \leq p - 1$. However, since a is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and so $\mathrm{ord}(a) = p - 1$ we cannot have $a^{r_1} \equiv 1 \pmod{p}$ for $0 \leq r_1 \leq p - 1$ unless $r_1 = 0$. So we have that $r_1 = 0$ and hence $a^{er} = a^{(p-1)q_1}$. Now $r = kd$ so $a^{er} = a^{edk} = a^{(p-1)q_1}$, $\ell \mid ek$ but $\gcd(k, \ell) = 1$. So $\ell \mid e$ implies $e = \ell m$ for $0 < m \leq d$. Thus $b = a^e = a^{\ell m}$ is one of the x values that we determined above $a^\ell, a^{2\ell}, ..., a^{d\ell} = 1$ that we found above. Thus we have shown that there are exactly $d = \gcd(p - 1, r)$ solutions. Q.E.D.

Chapter 3

Known Results

The theorems in this section are known results which come from Holden, Richardson, and Robinson [3] in order to give us a starting point for our research.

Theorem 3.1. [3] For each choice of x_0 in $(\mathbb{Z}/(p-1)\mathbb{Z})^\times$ and for $g(x) \in F[x]$, there are $\gcd(p-1, g(x_0)-1)$ elements $x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$ with the property that

$$\omega(x_1)^{g(x_0)} < x_1 >^{g(x_1)} \equiv x_1 \pmod{p}.$$

Theorem 3.2. [3] Let p be a prime, $p \neq 2$. Then there are

$$\left\{ \sum_{x_0=1}^{p-1} \gcd(p-1, g(x_0)-1) \right\} - \left\{ \sum_{g(x_1) \equiv 1 \pmod{p}} N_{g-1}(\mathrm{ord}_p(x_1)) \frac{p-1}{\mathrm{ord}_p(x_1)} \right\}$$

$$= \sum_{d|p-1} \left| \left\{ x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times \mid g(x_1) \not\equiv 1 \pmod{p},\ \mathrm{ord}_p(x_1) = d \right\} \right| \ \frac{p-1}{d} \ N_{g-1}(d)$$

solutions x to the congruence

$$x^{g(x)} \equiv x \pmod{p^e} \tag{3.1}$$

where $1 \leq x \leq p^e(p-1)$ such that $p \nmid x$ and $g(x) \not\equiv 1 \pmod{p}$.

These are in one-to-one correspondence with the solutions $(x, x_0) \in \mathbb{Z}_p \times \{1, \ldots, p-1\}$ to the equation

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

such that $p \nmid x$ and $g(x) \not\equiv 1 \pmod{p}$.

Proof. For the cases where $g(x_1) \equiv 1 \pmod{p}$, $x_1^{g(x_0)-1} \equiv 1 \pmod{p}$ for all $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$ such that $\operatorname{ord}_p(x_1) \mid (g(x_0)-1)$. There will be $N_{g-1}(\operatorname{ord}_p(x_1))(p-1)/\operatorname{ord}_p(x_1)$ such values of x_0. Now by the Chinese Remainder Theorem, there will be $N_{g-1}(\operatorname{ord}_p(x_1))(p-1)/\operatorname{ord}_p(x_1)$ values for x with $1 \leq x \leq p(p-1)$ where $p \nmid x$ and $g(x) \equiv 1 \pmod{p}$.

Now we have left to show that for a fixed $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$, any solution with $g(x_1) \not\equiv 1 \pmod{p}$ to the equation

$$\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} \equiv x \pmod{p}$$

will lift to a unique solution in $\mathbb{Z}_p$. This result will imply by the Chinese Remainder Theorem that the number of solutions to $x^{g(x)} \equiv x \pmod{p^e}$, where we allow $x \in \{1, 2, \ldots p^e(p-1)\}$ such that $p \nmid x$ and $g(x) \not\equiv 1 \pmod{p}$, will be exactly the number of solutions when $e = 1$.

Fix $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$, and consider the function $f_{x_0} : \mathbb{Z}_p \to \mathbb{Z}_p$ given by $f_{x_0}(x) = \omega(x)^{g(x_0)} \langle x \rangle^{g(x)} - x$. Note that

$$\begin{aligned} f_{x_0}(x) &= \omega(x)^{g(x_0)} \langle x \rangle^{g(x)} - x \\ &= \omega(x)^{g(x_0)} (\exp(g(x) \log \langle x \rangle)) - x \\ &= \omega(x)^{g(x_0)} \left(1 + g(x) \log \langle x \rangle + \frac{g(x)^2 (\log \langle x \rangle)^2}{2!} + \cdots \right) - x. \end{aligned}$$

Now $\log \langle x \rangle \in p\mathbb{Z}_p$, so

$$\begin{aligned} f'_{x_0}(x) &= \omega(x)^{g(x_0)} \left((g'(x_0) \log \langle x \rangle + g(x)/x) + (\text{terms containing } p) \right) - 1 \\ f'_{x_0}(x) &\equiv \omega(x)^{g(x_0)} g(x)/x - 1 \pmod{p} \\ &\equiv x^{g(x_0)-1} g(x) - 1 \text{ (since } \omega(x) \equiv x \pmod{p}). \end{aligned}$$

Suppose we have an $x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $g(x_1) \not\equiv 1 \pmod{p}$ and $\omega(x_1)^{g(x_0)} \langle x_1 \rangle^{g(x_1)} \equiv x_1 \pmod{p}$. Again, since $\omega(x_1) \equiv x_1 \pmod{p}$ and $\langle x_1 \rangle \equiv 1 \pmod{p}$, this gives us $x_1^{g(x_0)} \equiv x_1 \pmod{p}$. Hence,

$$\begin{aligned} f'_{x_0}(x_1) &\equiv x_1^{g(x_0)-1} g(x_1) - 1 \pmod{p} \\ &\equiv g(x_1) - 1 \pmod{p}. \end{aligned}$$

Since $g(x_1) \not\equiv 1 \pmod{p}$, we have that $f'_{x_0}(x_1) \not\equiv 0 \pmod{p}$.

By a previous proposition which states:

Let $f(x)$ be a restricted power series in $\mathbb{Z}p[[x]]$, and let a be in $\mathbb{Z}p$ such that $\frac{df}{dx}(a)$ is in $\mathbb{Z}_p^\times$ and $f(a) \equiv 0p$.

Then there exists a unique $x \in \mathbb{Z}p$ for which $x \equiv a \pmod{p}$ and $f(x) = 0$ in $\mathbb{Z}p$. Then for fixed $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$, each solution x_1 with $g(x_1) \not\equiv 1 \pmod{p}$ to the equation

$$\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} \equiv x \pmod{p}$$

will lift to a unique solution to $\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} - x$ in $\mathbb{Z}_p$. Thus this unique solution in $\mathbb{Z}_p$ will correspond to one solution to equation (3.1) for each e. Putting these results together with a previous corollary which states:

Let p be a prime. Then there are $\sum_{x_0-1}^{p-1} \gcd(p1, g(x0)1)$ solutions x to the congruence $x^{g(x)} \equiv x \pmod{p}$ where $1 \leq x \leq p(p1)$ and $p \nmid x$,

and taking out the solutions where $g(x) \equiv 1 \pmod{p}$, we have our theo-

rem.

The second summation follows by noting that for each choice of $x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$ of multiplicative order d modulo p such that $g(x_1) \not\equiv 1$ modulo p, there are $((p-1)/d)N_{g-1}(d)$ values of $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$ satisfying the congruence.

Q.E.D.

Chapter 4

Definitions and Numerical Examples

In order to better understand the main theorem we are trying to prove, we give two definitions, N_e and $\bar{N}_e$ which keep track of exactly what we are counting.

Definition 4.1. We will let N_e stand for the set of fixed points of the function $x^{g(x)}$ modulo powers of a prime p where $g(x)$ is any polynomial with integer coefficients. The set is defined as follows:

$$N_e = \{x \in \{1, 2, ..., p^e - 1\} |\ x^{g(x)} \equiv x \pmod{p^e} \text{ and } p \nmid x\}$$

where e is an integer greater than 0. We let $|N_e|$ be the cardinality of the set N_e.

Definition 4.2. We let $\bar{N}_e$ be the set of fixed points of the function $x^{g(x)}$ modulo powers of a prime where $g(x)$ is any polynomial with integer coefficients. The

set $\bar{N}_e$

$$\bar{N}_e = \{x \in \{1, 2, ..., p^e(p-1)| \ x^{g(x)} \equiv x \pmod{p^e} \text{ and } p \nmid x\}$$

.

We would like to compute $|N_e|$ but unfortunately this seems beyond our reach. We will see in the examples below that while we have a rough estimate for the value of $|N_e|$, we cannot come up with an exact formula for the size of this set. However, we find that when we extend the range for our solutions x in $\bar{N}_e$ for some $g(x)$ and for odd primes p, we can compute an exact value. We conjecture that $|N_e|(p-1) \approx \bar{N}_e$.

Using Magma, we can show that $|N_e|$ has the following values for several different $g(x)$ and values of p. These calculations show that a closed form expression for $|N_e|$ is difficult to compute.

In this paper, we have calculated the cardinalities of $|\bar{N}_e|$ for $g(x) = x+1$ and $g(x) = x+2$ and in general for $g(x) = x+c$ where $1 \leq c \leq p$ for many primes p and prime powers p^e.

The following Corollary 4.3 follows from Theorem 3.2[1].

Corollary 4.3. *For any prime p, a positive integer e, and $g(x) = x+1$,*

$$|\bar{N}_e| = \#\{x \in \{1, ..., p^e(p-1)\}, \ p \nmid x \mid x^{x+1} \equiv x \pmod{p^e}\}$$

$$= \sum_{x=1}^{p-1} \gcd(g(x) - 1, p-1)$$

One thing we would like to note from this theorem is that when $g(x) = x+1$,

the exponent e is independent of $|\bar{N}_e|$.

EXAMPLE 1. *Here are the values for* $|N_e|$ *when* $p = 5$ *and* $g(x) = x+1$ *over the smaller range where* $x \in (\mathbb{Z}/p^e\mathbb{Z})^\times$.

e	N_e	$\lvert N_e\rvert$
1	$\{1, 5^1 - 1\}$	*2*
2	$\{1, 5^2 - 1\}$	*2*
3	$\{1, 68, 5^3 - 1\}$	*3*
4	$\{1, 5^4 - 1\}$	*2*
5	$\{1, 1068, 5^5 - 1\}$	*3*
6	$\{1, 1068, 5^6 - 1\}$	*3*
7	$\{1, 5^7 - 1\}$	*2*

We can see that it is difficult to find a consistent pattern, so we enlarge the range of possible values for x so that $x \in 1, 2, ..., p^e(p-1)$.

EXAMPLE 2. *Here are the values for* $p = 5$, $g(x) = x + 1$ *over the larger range of values* $x \in \{1, 2, ..., (p-1)p^e\}$.

e	$\lvert N_e\rvert$	$\lvert \bar{N}_e\rvert$
1	*2*	*8*
2	*2*	*8*
3	*3*	*8*
4	*2*	*8*
5	*3*	*8*
6	*3*	*8*
7	*2*	*8*

We see in this example that the solutions modulo p^e each lift uniquely to solutions modulo p^{e+1}. Or in other words, the value for $|\bar{N}_e|$ is constant as e increases. In this case, 8 is the unique solution.

Definition 4.4. Multiplicative order of an integer modulo p: The multiplicative order of any x modulo any prime p is defined to be the smallest positive integer n such that $x^n = 1 \pmod{p}$. We denote this number $n = \mathrm{ord}_p(x)$, the order of x modulo p.

We start by examining $\bar{N}_e$ for the case where $g(x) = x + 1$ and $p = 3$.

Proposition 4.5. *For $p = 3$, $\bar{N}_e = \{1, p^e - 1, p^e + 1\}$ and hence $|\bar{N}_e| = 3$.*

Proof. Consider the congruence: $x^{x+1} \equiv x \pmod{p^e}$ where $1 \leq x \leq p^e(p-1)$ and $p \nmid x$. First we will show that each value in the set $\bar{N}_e$ solves our congruence. Let $x = 1$. In this case, it is clear that $x^{x+1} \equiv x \pmod{p^e}$.

Next consider $x = p^e - 1$. In this case we use the Binomial Theorem to expand x^{x+1} as follows:

$$(p^e - 1)^{p^e} = \sum_{k=0}^{p^e} \binom{p^e}{k} (-1)^{p^e - k} p^{ek}.$$

Because $e \geq 1$, each term of this expansion is divisible by p^e except the first term, $(-1)^{p^e}$ and we have that $(p^e + 1)^{p^e} \equiv -1 \pmod{p^e}$. As x itself is also congruent to $-1 \pmod{p^e}$, we see that this value of x solves our congruence.

Finally consider $x = p^e + 1$. In this case we again use the Binomial Theorem to expand x^{x+1} as follows:

$$(p^e + 1)^{p^e} = \sum_{k=0}^{p^e} \binom{p^e}{k} p^{ek}.$$

Because $e \geq 1$, each term of this expansion is divisible by p^e except the first term, 1 and we have that $(p^e - 1)^{p^e} \equiv 1 \pmod{p^e}$. As x itself is also congruent to $1 \pmod{p^e}$, we see that this value of x also solves our congruence.

Next we will show that no other value for x will solve this congruence. We are looking for solutions to $x^{x+1} \equiv x \pmod{p^e}$. Because we take x such that $p \nmid x$, the $\gcd(x, p^e) = 1$ and so we know we can cancel x from both

sides of this congruence to get that $x^x \equiv 1 \pmod{p^e}$. Thus we see that the multiplicative order of $x \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ must divide x. By Lagrange's theorem $\text{ord}_p(x)$ must divide order of the group, $(\mathbb{Z}/p^e\mathbb{Z})^\times$. The order of this cyclic group is $p^{e-1}(p-1)$. Thus the multiplicative order of x and by our argument x itself must be a power of p, a divisor of $(p-1)$, or a product of both. Since we have taken x such that $p \nmid x$, to solve our congruence x and its multiplicative order must divide $p-1=2$. Thus the only solutions to congruence must be values for x in the set $\{1, 2, ..., p^e(p-1)\}$ that are not divisible by p and have order 2 or 1 modulo p^e. Hence these values for x must be congruent to 1 or -1 modulo p^e. For x in the set $\{1, 2, ..., p^e(p-1)\}$ when $p = 3$ there are two elements congruent to 1 modulo p^e and they are 1 and $p^e + 1$ and one element congruent to -1 modulo p^e and that is $p^e - 1$. Hence we have shown that there are no other solutions to our congruence modulo p^e. Q.E.D.

We can show that for x in $\bar{N}_e$, for any odd p, $\text{ord}_p(x)$ must divide $p-1$ and $\text{ord}_p(x)$ must also divide x, itself, itself and the elements x such that $\text{ord}_p(x)|p-1$ and $ord_p(x)|x$ are all the elements in $\bar{N}_e$.

Proposition 4.6. *Given a prime p and a positive integer e for $g(x) = x + 1$, we have that $\bar{N}_e = \{x \in \{1, ..., p^e(p-1)\} \mid p \nmid x, \text{ord}(x)|(p-1)$ and $\text{ord}(x)|x\}$.*

Proof. By definition, $\bar{N}_e = \{$The set of solutions x to $x^{(x+1)} \equiv x \pmod{p^e}$ for $1 \leq x \leq p^e(p-1)$ where $p \nmid x\}$. To prove our proposition, we need to show that the set of solutions to $x^{(x+1)} \equiv x \pmod{p^e}$ are exactly the x values $1 \leq x \leq p^e(p-1)$ for which $p \nmid x$, $\text{ord}(x)|(p-1)$ and $\text{ord}(x)|x$. Thus, we must show that every solution to $x^{(x+1)} \equiv x \pmod{p^e}$ has the property that $\text{ord}(x)|(p-1)$ and $\text{ord}(x)|x$ and every such x is a solution to the congruence.

Suppose x is a solution to the congruence $x^{(x+1)} \equiv x \pmod{p^e}$. Since $p \nmid x$ we can cancel x from both sides of this congruence to see that any solution

to the original congruence must satisfy $x^{(x)} \equiv 1 \pmod{p^e}$, and, correspondingly, anything that satisfies $x^{(x)} \equiv 1 \pmod{p^e}$ must also satisfy the original congruence. Thus, any x that satisfies the original congruence must have $\text{ord}(x)|x$, and any x whose order divides it must be a solution to the congruence. Since x is restricted to lie $1 \leq x \leq p^e(p-1)$ and $p \nmid x$, we see that the values for x modulo p^e must sit inside the multiplicative group $(\mathbb{Z}/p^e\mathbb{Z})^\times$. This group has order $p^e - p^{e-1} = p^{e-1}(p-1)$ and this implies that the $\text{ord}(x)$ must divide $p^{e-1}(p-1)$. However, since $p \nmid x$ and $\text{ord}(x)|x$ the only possible values for $\text{ord}(x)$ are the divisors of $(p-1)$. Thus we have shown that every solution to the original congruence in the given interval must satisfy the three conditions: $p \nmid x$, $\text{ord}(x)|(p-1)$, and $\text{ord}(x)|x$. Any x that satisfies these three conditions must be a solution.

Q.E.D.

We can try an example of this to see how Proposition 4.6 works.

EXAMPLE 3. *Consider $p = 5$, $e = 1$. The values for x which satisfy $x \in \{1, ..., p^e(p-1)\}$, where $p \nmid x$ are $\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19\}$. We can calculate the order of each of these values for x.*

x	$\mathrm{ord}(x)$
1	*1*
2	*4*
3	*4*
4	*2*
6	*1*
7	*4*
8	*4*
9	*2*
11	*1*
12	*4*
13	*4*
14	*2*
16	*1*
17	*4*
18	*4*
19	*2*

Among these values for x, we can now eliminate the solutions where the $\mathrm{ord}_p(x)$ *does not divide x.*

x	ord(x)
1	*1*
4	*2*
6	*1*
8	*4*
11	*1*
12	*4*
14	*2*
16	*1*

We can now see these values of x are the set of solutions which solve $x^{x+1} \equiv x \pmod 5$.

At this point, we can observe our remark from Corollary 4.3, which states that when $g(x) = x + 1$, the exponent e is independent of $|\bar{N}_e|$. This implies that the number of solutions $|\bar{N}_e|$ for $g(x) = x + 1$ is constant as e increases. We can see this in Example 4.

We will also observe the following patters:

- Solutions of order 1 follow the format $p^e(a) + 1$.
- Solutions of order 2 follow the format $p^e(a) - 1$.

EXAMPLE 4. *Looking at the congruence $x^{g(x)} \equiv x \pmod{p^e}$ for $g(x) = x + 1$ when $p = 5$, we can evaluate the values of x which satisfy the congruence at different values for e and observe their pattern for the cases of order 1 and 2, as well as that the number of solutions x stays constant as e increases.*

order	*solutions* x *in* $\bar{N}_1$	*solutions* x *in* $\bar{N}_2$	*solutions* x *in* $\bar{N}_3$	*pattern*
1	*1*	*1*	*1*	*1*
2	*4*	*24*	*124*	$p^e - 1$
1	*6*	*26*	*126*	$p^e + 1$
4	*8*	*68*	*68*	
1	*11*	*51*	*251*	$2p^e + 1$
4	*12*	*32*	*432*	
2	*14*	*74*	*374*	$3p^e - 1$
1	*16*	*76*	*376*	$3p^e + 1$

EXAMPLE 5. *We can see that these same properties hold true for* $g(x) = x + 1$ *and* $p = 7$

order	*solutions* x *in* $\bar{N}_1$	*solutions* x *in* $\bar{N}_2$	*solutions* x *in* $\bar{N}_3$	*pattern*
1	*1*	*1*	*1*	*1*
2	*6*	*248*	*342*	$p^e - 1$
1	*8*	*50*	*344*	$p^e + 1$
3	*9*	*18*	*18*	
6	*12*	*30*	*324*	
1	*15*	*99*	*687*	$2p^e + 1$
3	*18*	*165*	*1047*	
2	*20*	*146*	*1028*	$3p^e - 1$
1	*22*	*148*	*1030*	$3p^e + 1$
6	*24*	*177*	*1353*	
1	*29*	*197*	*1373*	$4p^e + 1$
3	*30*	*264*	*1734*	
2	*34*	*244*	*1714*	$5p^e - 1$
1	*36*	*246*	*1716*	$5p^e + 1$
3	*39*	*264*	*2040*	

We can also observe the frequency of each order.

For $g(x) = x + 1$ The number of solutions order 2 are $1/2$ the number of solutions of order 1.

Note that we cannot make this statement for the ratio of solutions of order greater than 2 since the number of solutions x for any given p is not necessarily odd or even. However we can generalize that for any two orders a, b such that $b = 2a$, the cardinality of b is roughly $1/2$ the cardinality of a.

EXAMPLE 6. *We will examine the frequency of each order for* $p = 3, 5, 7, 11$ *where* $g(x) = x + 1$. *(Recall that* e *is independent of* $\bar{N}_e$ *for* $g(x) = x + 1$.*)*

p	*order*	*frequency*
3	*1*	*2*
	2	*1*
5	*1*	*4*
	2	*2*
	4	*2*
7	*1*	*6*
	2	*3*
	6	*2*
11	*1*	*10*
	2	*5*
	5	*8*
	10	*4*

We will now prove a few corollaries and propositions.

Corollary 4.7. *For p prime,* $p \neq 2 \sum_{d|(p-1)} \phi(d)(p-1)/d \cdot N_x(d)$ *solutions to the congruence* $x^{g(x)} \equiv x \pmod{p}$.

Proof. From 3.1, we have that $\omega(x_1)^g x_0 (x_1)^{g(x_1)} \equiv x_1 \pmod{p}$. By the Chinese Remainder Theorem, there will be exactly one x $\in (\mathbb{Z}/(p-1)\mathbb{Z})^\times$ such that $x \equiv x_0 \pmod{p-1}$ and $x \equiv x_0 \pmod{p}$. Since $x \equiv x_0 \pmod{p-1}$, we know that for each such x : $x^{g(x)} = \omega(x)^{g(x_0)}(x)^{g(x)} \equiv \omega(x_1)^{g(x_0)}(x_1)^{g(x_1)} \equiv x_1 \equiv x \pmod{p}$. Since exactly $\gcd(p-1, g(x_0)-1)$, such x exists for each x_0, we have $\sum_{x_0=1}^{p-1} \gcd(p-1, g(x_0)-1)$ solutions to the congruence. Alternatively, for each choice of $x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$ of multiplicative order of modulo p, there are $(p-1)/d$ values of $x_0 \in (\mathbb{Z}/p\mathbb{Z})^\times$ satisfying the congruence and $\phi(d)$ choices of x_1 with multiplicative order d for each $d|(p-1)$.

Q.E.D.

Proposition 4.8. *The congruence $x^{x+1} \equiv x \ mod\ 2^e$ always has only one solution for all $e \geq 1$ where x is any odd number between 1 and 2^e.*

Proof. Since we are counting solutions to $x^{x+1} \equiv x \pmod{2^e}$ where x is odd, we can cancel x from both sides of the congruence and count solutions to $x^x \equiv 1 \pmod{2^e}$ instead.

First, we will count solutions to $x^x \equiv 1 \pmod 2$ and we see that the only choice for x is $x = 1$ and that is clearly a solutions.

We can observe that for $e \geq 1$ the value $x = 1$ is certainly a solution to $x^x \equiv 1 \pmod{2^e}$. We now want to show that no other values for x work in the range $1 < x \leq 2^e$ and x odd. We see that since all values x must lie $1 < x < 2^e$ such that $2 \nmid x$ and we need $x^x \equiv 1 \pmod{2^e}$ to hold, it must be that the order of x must divide x which implies that order of x cannot be even. However x is an element in the cyclic group $(\mathbb{Z}/2^e\mathbb{Z})^\times$ of order 2^{e-1}, so by Lagrange's theorem $\text{ord}_{2^e}(x)$ must divide 2^{e-1} and so $\text{ord}_{2^e}(x) = 1$. This implies that $x = 1$. Q.E.D.

The remaining propositions will be discussed in detail and then proved more generally in the next section.

Proposition 4.9. *Given $p = 3$ and a particular positive integer e, $\bar{N}_e = \{x \in \{1, ..., p^e(p-1)\} \mid p \nmid x, x^{x+2} \equiv x \pmod{p^e}\} = 2 + 3^{\lfloor e/2 \rfloor}$.*

We will now plug in values to verify that the congruence holds when $1 \leq x \leq (p-1)$. For $g(x) = x + 2, p = 3$, since $p - 1 = 2$, our possible values for x_0 are $x_0 = 0, x_0 = 1$. When $x_0 = 0, |\bar{N}_e| = \gcd(2, 1) = 1$. So $\omega(x)^2 < x >^{x+2} \equiv x \pmod 3$ has exactly one solution. Since $\omega(x)^2 = 1$, this simplifies to $< x >^{x+2} \equiv x \pmod 3$. So $x = 1$ is a solution but $x = 2$ is not. For the case $x_0 = 0, x = 1$, we have that $\omega(1)^2 < 1 >^{x+2} \equiv 1 \pmod 3$ implies $\omega(1)^2(1 + p(a_1) + p^2(a_2) + ...)^{x+2} \equiv 1 \pmod 3$ implies $1 \equiv 1 \pmod p$, which

is true. So $x = 1$ is a solution. Now we will consider $x_0 = 0, x = 2$. So $x = \omega(2)^2 < 2 >^4 \equiv 2 \pmod 3$

implies $1\times < 2 >^4 \equiv 2 \pmod 3$. We have that $< 2 >= 2/\omega(2) = 1 + 3(a_1) + 3^2(a_2) + ...$, so $12 \pmod 3$. So $x = 2$ is not a solution. When $x_0 = 1, \gcd(2, 2) = 2$. So $\omega(x)^{g(x_0)} < x >^{g(x)} \equiv x \pmod 3$ becomes $\omega(x)^3 < x >^{x+2} \equiv x \pmod 3$, where our possibilities for x are $x = 1, 2$. Plugging in for $x = 1$, we have $\omega(1)^3 < 1 >^3 \equiv 1 \pmod 3$ which is true, so $x_0 = 1, x = 1$ is a solution. Plugging in for $x = 2$, we have $\omega(2)^3 < 2 >^4 \equiv 2 \pmod 3$. We know that $\omega(2) = \omega(2)^3 \equiv 2 \pmod 3$, so $2 \equiv 2 \pmod 3$ is a solution. This verifies that there are exactly 3 solutions to the congruence when $1 \leq x \leq (p-1)$. For the case where $x_0 \equiv 0 \pmod p - 1, x \equiv 1 \pmod p$ we know by the Chinese Remainder Theorem that $1 \leq x \leq p(p-1)$ has one solution $x = 4$. For the case where $x_0 \equiv 1 \pmod p - 1, x \equiv 1, 2 \pmod p$ there are 2 solutions $1 \leq x \leq p(p-1)$, which are $x = 1, x = 5$.

Propositions 10 through 12 can tested similarly, and then we will generalize for any odd p.

Proposition 4.10. *Given $p = 5$ and a particular positive integer e, $\bar{N}_e = \{x \in \{1, ..., p^e(p-1)\} \mid p \nmid x, x^{x+2} \equiv x \pmod{p^e}\} = 6 + 2 * 5^{\lfloor e/2 \rfloor}$.*

Proposition 4.11. *Given $p = 7$ and a particular positive integer e, $\bar{N}_e = \{x \in \{1, ..., p^e(p-1)\} \mid p \nmid x, x^{x+2} \equiv x \pmod{p^e}\} = 12 + 3 * 7^{\lfloor e/2 \rfloor}$.*

We can think of these equations more broadly by first defining values C and D as follows for ease in the statement of our theorems:

Definition 4.12. We can define C for $g(x) = x + c$ as:

$$C = \sum_{x_0=1}^{p-1} \gcd(g(x_0) - 1, p - 1) - \frac{(p-1)}{\mathrm{ord}_p(x_1)} \qquad where$$

$\mathrm{x}_1 \equiv 1 - c \pmod{p}$.

Definition 4.13 (The constant D)**.** We define D for $g(x) = x + c$ as:

$$D = \frac{(p-1)}{\mathrm{ord}_p(x_1)}$$

where $x_1 \equiv 1 - c \pmod{p}$.

or more simply, when $g(x) = x + 2$, we will show

$$D = (p-1)/2.$$

Definition 4.14. We define $C + D = \gcd(p - 1, g(x_0) - 1) =$ the number of solutions x to the congruence

$$\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} \equiv x \pmod{p}$$

where $x \in (\mathbb{Z}/p\mathbb{Z})^\times$.

We will examine the number of solutions to the congruence $\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} \equiv x \pmod{p}$ where $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ in order to verify that this value is the solution to $C + D$.

The main goal of our paper will be to prove the following conjecture for $c = 2$ as a formal theorem in the next section of this paper.

Conjecture 4.15. Given prime p and a particular positive integer e, $\bar{N}_e = \{x \in \{1, ..., p^e(p-1)\} \mid p \nmid x, x^{x+c} \equiv x \pmod{p^e}\}$ follows the trend $C + D \times p^{\lfloor e/2 \rfloor}$

for values where $c \leq p$.

Before proving this conjecture for $c = 2$, we will first consider the example where $p = 3$ in order to better understand what happens to $\bar{N}_e$ as e increases.

Looking at solutions to $x^{g(x)} \equiv x \pmod{p^e}$ for $g(x) = x + 2, p = 3$, we can identify the solutions x which will be in the set we have called D in the form $x = 2 + 3a + 3^2b + ...$ whose lifting to solutions modulo higher powers of p will be more complicated. In these examples, the form $x = 2 + 3a + 3^2b + ...$ is the value's 3-adic expansion, and lifting refers to the solution to $\bar{N}_e$ when moving from term e to $e + 1$.

In Examples 7-8, $g(x) = x + 2$ and $p = 3$.

EXAMPLE 7. *For $e = 2$, the solutions x are:*

1

$5 = 2 + 1 \cdot 3$

10

$11 = 2 + 0 \cdot 3 + 1 \cdot 3^2$

$17 = 2 + 2 \cdot 3 + 1 \cdot 3^2$

EXAMPLE 8. *For $e = 3$, the solutions x are:*

1

$17 = 2 + 2 \cdot 3 + 1 \cdot 3^2$

28

$35 = 2 + 2 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3$

$53 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + 1 \cdot 3^3$

EXAMPLE 9. *For $e = 4$, the solutions x are:*

1

$17 = 2 + 2 \cdot 3 + 1 \cdot 3^2$

$35 = 2 + 2 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3$

$53 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + 1 \cdot 3^3$

$71 = 2 + 2 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^3$

82

$89 = 2 + 2 \cdot 3 + 0 \cdot 3^2 + 0 \cdot 3^3 + 1 \cdot 3^4$

$107 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + 0 \cdot 3^3 + 1 \cdot 3^4$

$125 = 2 + 2 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4$

$143 = 2 + 2 \cdot 3 + 0 \cdot 3^2 + 2 \cdot 3^3 + 1 \cdot 3^4$

$161 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 1 \cdot 3^4$

Looking at the the 3-adic expansions of $5, 11$, and 17 in example 7, when $e = 2$, we see: $5 = 2 + 2 \times 3$, $11 = 2 + 1 \cdot 3 + 1 \cdot 3^2$, $17 = 2 + 2 \cdot 3 + 1 \cdot 3^2$. Moving to the case where $e = 3$, we see that only 17 lifts to a solution modulo p^3, and the other two solutions do not lift to solutions modulo p^3. When $e = 3$, the digit in the $3's$ place of all solutions is constant, (and in this case will always be equal to 2) and there are three new coefficients $0, 1, 2$ in the 3^2 place. The pattern when moving from $e = even$ to $e = odd$ is that $1/3$ of the values lift all three ways. To generalize, we will later see that $1/p$ of the values will lift in all p ways. Additionally, the coefficients which will lift will always be equal to $p - 1$.

Now looking at the jump from $e = 3$ to $e = 4$, where p is still equal to 3, we see that all three values from $e = 3$ each lift three times in $e = 4$. We can see that 17 lifts to

$17 = 2 + 2 \times 3 + 1 \times 3^2 + 0 \times 3^3$,

$125 = 2 + 2 \times 3 + 1 \times 3^2 + 2 \times 3^3$,

$125 = 2 + 2 \times 3 + 1 \times 3^2 + 1 \times 3^3 + 1 \times 3^4$.

We can see that while the 3^2 place is the same for these three values, there are now three different coefficients $0, 1, 2$ in the 3^3 place. The pattern is, when moving from $e = odd$ to $e = even$, everything lifts 3 times. Again, to generalize, we will later see that when moving from $e = odd$ to $e = even$ the number of solutions D in the form $x = 2 + 3a + 3^2b + ...$ will lift p times.

EXAMPLE 10. *To make counting easier, we will consider these values by their* $3-$*adic expansion. Where something of the form* $a_0+a_1p+a_2p^2+...a_np^n$ *would be abbreviated as* $a_0, a_1a_2...a_n(p)$ *Looking at the values D, for e=4, we have 17= 2,210(3)*

35= 2,201(3)

53= 2,221(3)

71= 2,212(3)

89= 2,2001(3)

107=2,2201(3)

125=2,2111(3)

143=2,2021(3)

161=2,2221(3)

We can examine these values organized in the following way

EXAMPLE 11. *For* $e = 4$*, the solutions x:*

17=2210	*35=2201*	*53=2221*
71=2212	*89=2200*	*107=2220*
125=2211	*143=2202*	*161=2222*

Here we can see the three values of the previous iteration along the first row, and each of their two other variations underneath. Notice that in each column, the 3rd digit of each of theses 3*-adic expansions has the same number. Each column*

has a value ending in $0, 1$, *and* 2. *In other words, all* 9 *of the solutions for* x *when* $e = 4$ *have* 2*'s in the first two digits of their* 3*-adic expansion. However in their third digit, there are three* 0*'s, three* 1*'s, and three* 2*'s.*

We can see that the third row in the previous Example will be what lifts when $e = 5$. So for every solutions x, each digit up through the 3^2's place will be the same value, 2, for $e \geq 5$.

EXAMPLE 12. *For* $e = 5$*, we see the* 9 *solutions* x *written in their* 3*-adic expansion. We observe that the three solutions from the third column in the previous example when* $e = 4$*, where the third digit of their* 3*-adic expansion was* 2*, are each lifting to different vales* $0, 1, 2$ *in their fourth digit.*

x *when* $e \geq 5$.

53=22210	*107=22200*	*161=22220*
22211	*22201*	*22221*
22212	*22202*	*22222*

Proposition 4.16. *The values of* x *that satisfy* $\{x \in \{1, ..., p^e(p-1)\} \mid p \nmid x, x^{x+2} \equiv x \pmod{p^e}\}$ *in their* 3*-adic expansion approach* -1 *more and more closely as* e *increases.*

Proof. We see in the previous examples that the coefficient that lifts on the odd iterations is the value $a = 2$. So a 3-adic expansion of the form $x = a_0 + a_1 \times 3 + a_2 \times 3^2 + ...$ becomes $x = 2 + 2 \times 3 + 2 \times 3^2 + ...$ We will show $x = 2+2\times3+2\times3^2+... = -1$. Consider $x = 2+2\times3+2\times3^2+...+2\times3^n$. Then let $x = \lim_{n\to\infty}(2+2\times3+2\times3^2+...+2\times3^n) = \lim_{n\to\infty} 2(1+3+3^3+...+3^n) = \lim_{n\to\infty} 2(3^{n+1} - 1/3 - 1) = \lim_{n\to\infty} 3^{n+1} - 1 = -1$. Q.E.D.

Chapter 5

Main Theorem

In this chapter we will go over Theorem 5.1 and prove it through a series of propositions.

Theorem 5.1. *Given p an odd prime and $g(x) = x + 2$ then*

$$|\bar{N}_e| = |C| + \left(\frac{p-1}{2}\right) p^{\lfloor e/2 \rfloor}$$

for e a positive integer, $\lfloor x \rfloor$ function of x, and where

$$|C| = \left(\sum_{x_0=1}^{p-1} \gcd(p-1, g(x_0)-1)\right) - (p-1)/2.$$

To prove this theorem we first prove several propositions, and then we will put the propositions together to prove Theorem 5.1.

Proposition 5.2. *Let p be an odd prime. For each $x_0 \in \{1, ..., p-1\}$ there are $\gcd(p-1, g(x)-1)$ solutions x to the congruence*

$$\omega(x)^{g(x_0)} < x >^{g(x)} \equiv x \pmod{p}$$

where $x \in \{1, 2, ..., p-1\}$.

Alternatively for $x \in \{1, 2, ..., p-1\}$ *there are* $N_{g-1}(ord_p(x)) \times \frac{(p-1)}{ord_p(x)}$ *values of* $x_0 \in \{1, 2, ..., p-1\}$ *such that*

$$\omega(x)^{g(x_0)} < x >^{g(x)} \equiv x \pmod{p}$$

where $N_{g-1}(d) = Card\{z \in \{1, 2, ..., d\} \mid g(z) - 1 \equiv 0 \pmod{d}\}$.

Proof. By definition $< x > \equiv 1 \pmod{p}$, so the congruence simplifies to

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

For fixed x_0, since by definition $\omega(x) \equiv x \pmod{p}$ and x^{-1} exists for all $x \not\equiv 0 \pmod{p}$, this equation has a solution if and only if

$$\omega(x)^{g(x_0)-1} \equiv 1 \pmod{p}$$

and this is equivalent to $x^{g(x_0)-1} \equiv 1 \pmod{p}$. These congruences are satisfied for $x \in \{1, 2, ..., p-1\}$ such that $\mathrm{ord}_p(x) | (g(x_0) - 1)$. Since for each divisor d of $\gcd(p-1, g(x_0)-1)$ there will be $\phi(d)$ elements $x \in \{1, 2, ..., p-1\}$ with order d, ? that there are exactly $\gcd(p-1, g(x_0)-1)$ values x with $\mathrm{ord}_p(x)$ dividing $p-1$ and $g(x_0)-1$. Thus we have proved the first part of our Proposition.

Alternatively, fixing x and counting all x_0 that satisfy the congruence above, the congruence is satisfied whenever $\mathrm{ord}_p(x) \mid (g(x_0) - 1)$ and this happens for some x_0 if and only if $g(x_0) - 1 \equiv 0 \pmod{\mathrm{ord}_p(x)}$. For each value of $\mathrm{ord}_p(x)$, there are exactly $N_{g-1}(\mathrm{ord}_p(x))$ values of x_0 where $1 \leq x_0 \leq \mathrm{ord}_p(x)$. Now since these values repeat in the set $\{1, 2, ..., p-1\}$ modulo $ord_p(x)$, there will be in total $N_{g-1}(\mathrm{ord}_p(x))(p-1)/\mathrm{ord}_p(x)$ such values of x_0 in the set $\{1, 2, ..., p-1\}$. Q.E.D.

Proposition 5.3. *Let p be an odd prime such that*

$$|\bar{N}_1| = \sum_{x_0}^{p-1} \gcd(p-1, g(x_0)-1) = \sum_{d|p-1} \phi(d) \left(\frac{p-1}{d}\right) N_{g-1}(d)$$

i.e. $|\bar{N}_1|$ *is the number of solutions to* $x^{g(x)} \equiv x \pmod{p}$ *where* $1 \leq x \leq p(p-1), p \nmid x$.

Proof. We know from the previous proposition that for each x_0 in the set $\{1, 2, ..., p-1\}$ there are $\gcd(p-1, g(x_0)-1)$ elements x_1 in the set $\{1, 2, ..., p\}$ such that $\omega(x_1)^{g(x_0)} < x_1 >^{g(x_1)} \equiv x_1 \pmod{p}$. So we know by the Chinese Remainder Theorem that there is exactly one solution x in the set $\{1, 2, ..., p(p-1)\}$ such that $x \equiv x_0 \pmod{p-1}$ and $x \equiv x_1 \pmod{p}$. Since $x \equiv x_1 \pmod{p}$ and $x \equiv x_0 \pmod{p-1}$ the first congruence reduces to the second.

$$\omega(x_1)^{g(x_0)} < x_1 >^{g(x_1)} \equiv x_1 \pmod{p}$$

$$\omega(x)^{g(x)} < x >^{g(x)} \equiv x^{g(x)} \equiv x \pmod{p}.$$

And since there exist $\gcd(p-1, g(x_0)-1)$ $x_1's$ for each x_0, by Proposition 5.2, there must be $\sum_{x_0=1}^{p-1} \gcd(p-1, g(x_0)-1)$ solutions to $|\bar{N}_1|$.

Alternatively, by Proposition 5.2, for each x_1 in $\{1, 2, ...p\}$ of order d modulo p, there are

$$\left(\frac{p-1}{d}\right) N_{g-1}(d)$$

values of $x_0 \in$ the set $\{1, 2, ..., p-1\}$ satisfying the congruence and since there are $\phi(d)$ such x_1 with order d we have our second formula for $|\bar{N}_1|$. Q.E.D.

Proposition 5.4. *For p an odd prime and $g(x) = x + 2$*

$$|C| = \left(\sum_{x_0=1}^{p-1} \gcd(p-1, g(x_0) - 1) \right) - \frac{p-1}{2}$$

is the number of solutions to the congruence $x^{g(x)} \equiv x \pmod{p^e}$ where $1 \leq x \leq p^e(p-1), p \nmid x$ and $g(x) \not\equiv 1 \pmod{p}$.

Proof. We first consider the case where $x_1 \in \{1, ..., p\}$ and $g(x_1) \equiv 1 \pmod{p}$. For $g(x) = x + 2$, this implies that $x_1 \equiv -1 \pmod{p}$. In Proposition 5.3 (with $x = x_1$), we showed that for a fixed $x_1 \equiv -1 \pmod{p}$ there were exactly $N_{g-1}(\mathrm{ord}_p(x_1))(p-1)/\mathrm{ord}_p(x_1)$ values of x_0 in the set $\{1, 2, ..., p-1\}$ such that $\omega(x_1)^{g(x_0)} < x_1 >^{g(x_1)} \equiv x_1 \pmod{p}$. Now since $x_1 \equiv -1 \pmod{p}$, $\mathrm{ord}_p(x_1) = 2$ and $N_{g-1}(\mathrm{ord}_p(x_1))(p-1)/\mathrm{ord}_p(x_1) = (p-1)/2$. Now we see that in fact these $(p-1)/2$ possible values for x_0, that are paired with $x_1 \equiv -1 \pmod{p}$, are exactly the odd values of x_0 that will allow $\omega(-1)^{g(x_0)} < -1 >^{g(-1)} \equiv -1 \pmod{p}$.

By the Chinese Remainder Theorem pairing $x_1 \equiv -1 \pmod{p}$ and each of the $(p-1)/2$ possible x_0, there will be $(p-1)/2$ values for x ($x \equiv x_1 \pmod{p}$ and $x \equiv x_0 \pmod{p-1}$) with $1 \leq x \leq p(p-1)$ such that $p \nmid x$ where $g(x) \equiv 1 \pmod{p}$.

Fix $x_0 \in$ the set $\{1, 2, ..., p-1\}$, and consider the function $f_{x_0} : \mathbb{Z}_p \to \mathbb{Z}_p$ given by $f_{x_0}(x) = \omega(x)^{g(x_0)} \langle x \rangle^{g(x)} - x$. Note that

$$\begin{aligned} f_{x_0}(x) &= \omega(x)^{g(x_0)} \langle x \rangle^{g(x)} - x \\ &= \omega(x)^{g(x_0)} (\exp(g(x) \log \langle x \rangle)) - x \\ &= \omega(x)^{g(x_0)} \left(1 + g(x) \log \langle x \rangle + \frac{g(x)^2 (\log \langle x \rangle)^2}{2!} + \cdots \right) - x. \end{aligned}$$

Now $\log \langle x \rangle \in p\mathbb{Z}_p$, so

$$\begin{aligned} f'_{x_0}(x) &= \omega(x)^{g(x_0)} \left((g'(x) \log \langle x \rangle + g(x)/x) + (\text{terms containing } p) \right) - 1 \\ f'_{x_0}(x) &\equiv \omega(x)^{g(x_0)} g(x)/x - 1 \pmod{p} \\ &\equiv x^{g(x_0)-1} g(x) - 1 \text{ (since } \omega(x) \equiv x \pmod{p}). \end{aligned}$$

Suppose we have an $x_1 \in$ the set $\{1, 2, ..., p\}$ such that $g(x_1) \not\equiv 1 \pmod{p}$ and $\omega(x_1)^{g(x_0)} \langle x_1 \rangle^{g(x_1)} \equiv x_1 \pmod{p}$. Again, since $\omega(x_1) \equiv x_1 \pmod{p}$ and $\langle x_1 \rangle \equiv 1 \pmod{p}$, this gives us $x_1^{g(x_0)} \equiv x_1 \pmod{p}$. Hence,

$$\begin{aligned} f'_{x_0}(x_1) &\equiv x_1^{g(x_0)-1} g(x_1) - 1 \pmod{p} \\ &\equiv g(x_1) - 1 \pmod{p}. \end{aligned}$$

Since $g(x_1) \not\equiv 1 \pmod{p}$, we have that $f'_{x_0}(x_1) \not\equiv 0 \pmod{p}$.

By Hensel's Lemma 2.1, for fixed x_0 in the set $\{1, 2, ..., p-1\}$, each solution x_1 with $g(x_1) \not\equiv 1 \pmod{p}$ to the equation

$$\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} \equiv x \pmod{p}$$

will lift to a unique solution to $\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} - x$ in $\mathbb{Z}p$, the p-adic integers. Thus this unique solution in $\mathbb{Z}_p$ will correspond to one solution to the congruence $f_{x_0} = \omega(x)^{g(x_0)} < x >^{g(x)} -1 \equiv 0 \pmod{p^e}$ for each e. Putting these results together with Proposition 5.3 and taking out the solutions where $g(x) \equiv 1$ modulo p, we have our theorem.

Q.E.D.

Proposition 5.5. *Let p be an odd prime. Suppose $g(x) = x + 2$ and $g(x) \equiv 1 \pmod{p}$. Then $x^{g(x)} \equiv x \pmod{p^e}$ has $\frac{p-1}{2} p^{\lfloor e/2 \rfloor}$ solutions for x such that $1 \leq x \leq p^e(p-1), p \nmid x$.*

Proof. We will prove our proposition by fixing $x_0 \in \{1, 2, ..., p-1\}$ where from Proposition 5.4 above we know that x_0 is odd. We use the Taylor series of the function $f_{x_0}(x)$ to count solutions $x_1 \in \{1, 2, ..., p^e\}$ where $p \nmid x_1$ modulo p^e by induction on e. That is, for $f_{x_0}(x) = \omega(x)^{g(x_0)} < x >^{g(x)} -x$ we will count the solutions x_1 to $f_{x_0}(x) \equiv 0 \pmod{p^e}$ by induction on e. Then we will use the Chinese Remainder Theorem to turn each solution pair $(x_0, x_1) \in \{1, 2, ..., p-1\} \times \{1, 2, ..., p^e\}$ where $p \nmid x$ into one$x$ for which $x \equiv x_0 \pmod{p-1}$ and $x \equiv x_1 \pmod{p^e}$ where $1 \leq x \leq p^e(p-1)$, and $p \nmid x$. These then are the values x that solve $x^{g(x)} \equiv x \pmod{p^e}$ where $1 \leq x \leq p^e(p-1)$, and $p \nmid x$.

First since we are considering only values for x where $g(x) \equiv 1 \pmod{p}$ and $g(x) = x + 2$, we have that $x \equiv -1 \pmod{p}$. Thus to examine values for x near -1 modulo p, we consider the Taylor series for $f_{x_0}(x)$ around $x = -1$. Now $f_{x_0}(x) = \omega(x)^{g(x_0)} < x >^{g(x)} -x$ and so its Taylor series has the form $f_{x_0}(x) = f_{x_0}(-1) + f'_{x_0}(-1)(x+1) + \frac{f''_{x_0}(-1)}{2!}(x+1)^2 + ...$higher degree terms.

Computing the coefficients of the Taylor series we first see that $f_{x_0}(-1) = 0$. This result follows because by definition $f_{x_0}(-1) = \omega(-1)^{g(x_0)} < -1 >^{g(-1)} -(-1)$. Since $p-1$ is even -1 itself is always a $(p-1)$-th root of 1 and so $\omega(-1) = -1$ and $< -1 >= 1$ since $\omega(-1) < -1 >= -1$ by definition. Thus, $f_{x_0}(-1) = (-1)^{g(x_0)} + 1 = 0$ since x_0 is an odd number. Similarly, we show that $f'_{x_0}(-1) = 0$. Here we have that $f_{x_0}(x) = \omega(x)^{g(x_0)} < x >^{g(x)} -x$. Using the relationship between the p-adic exponential function and the logarithm: $< x >^{g(x)} = e^{\ln(<x>^{g(x)})} = e^{g(x)\ln(<x>)} = \exp(g(x)\ln(x))$. Thus we have that $f_{x_0}(x) = \omega(x)^{g(x_0)} \exp(g(x)\ln(< x >)) - x$. Now, taking the derivative, we have $f'_{x_0}(x) = \omega(x)^{g(x_0)} \exp(g(x)\ln < x >) \times (g'(x)\ln < x > +g(x)/x) - 1$. We will also use that $g(x) = x + 2$ implies $g'(x) = 1$. And again, $\omega(-1) = -1$ and x_0 is

odd. Thus we have the following:

$$\begin{aligned} f'_{x_0}(-1) &= \omega(-1)^{g(x_0)} \exp(g(-1)\ln < -1 >)[\ln < -1 > -g(-1)] - 1 \\ &= -(0-1) - 1 = 1 - 1 = 0. \end{aligned}$$

We will next show that $v_p(f_{x_0}(x)) = 2v_p(x+1)$. Calculating the second derivative, we have that

$$\begin{aligned} f''_{x_0}(x) &= \omega(x)^{g(x_0)}[\exp(g(x)\ln < x >]\times \\ &\quad \left\{[g'(x)\ln < x > +g(x)/x]^2 + g''(x)\ln < x > +2g'(x)/x - g(x)/x^2\right\}. \end{aligned}$$

Thus $f''_{x_0}(-1) = -\{(0-1)^2 - 2 - 1\} = 2$.
Evaluating the first three terms of the Taylor series for $f_{x_0}(x)$, we have

$$f_{x_0}(x) = 0 + 0 + 2/2!(x+1)^2 + f'''(-1)(x+1)^3/6 + ... + \text{higher degree terms}.$$

Assuming, for now without proof, that $v_p(f^{(n)}(-1)/n!)) \geq 0$ for $n \geq 3$, we complete the argument. Considering this series modulo p, we see that $v_p(f_{x_0}(x)) = 2v_p(x+1)$ as long as $x \neq -1$. To elaborate, if x is not -1, then the first nonzero term in the Taylor series is $(x+1)^2$ and so $f_{x_0}(x) \equiv 0 \pmod{p^e}$ if and only if $v_p(f_{x_0}(x)) \geq e$, and this happens if and only if $2v_p(x+1) \geq e$.

We can see now from the Taylor series that if $f_{x_0}(x) = 0 \pmod{p}$ then $f_{x_0}(x+ap) = 0 \pmod{p^2}$ has p solutions of the form $x+ap$ such that $x \equiv p-1 \pmod{p}$. This is the base case for our induction.

Our inductive hypothesis if e is odd is as follows. We assume $f_{x_0}(x) = 0 \pmod{p^e}$ and $e = 2k-1$ (odd), $k \geq 1$. Thus x is of the form $x = x_0 + x_1 p + ... + x_{e-1}p^{e-1} \pmod{p^e}$ where $0 \leq x_i \leq p-1$. Then we want to show there are p solutions $x + ap^e$ to $f_{x_0}(x + ap^e) = 0 \pmod{p^{e+1}}$ for each x solving

$f_{x_0}(x) \equiv 0 \pmod{p^e}, e = 2k-1$ and $k \geq 1$. Since, $v_p(f_{x_0}(x)) = 2v_p(x+1)$ we have, $e \leq v_p(f_{x_0}(x)) = 2v_p(x+1)$ So we can substitute in $2k-1 \leq 2v_p(x+1)$. So it must also be that $2k \leq 2v_p(x+1) = v_p(f_{x_0}(x))$. So $p^{2k} | f_{x_0}(x)$ and $2k = e+1$. So we have that no matter what a is where $0 \leq a \leq p-1$ $f_{x_0}(x + ap^e) \equiv 0 \pmod{p^{e+1}}$ where $x = x_0 + x_1 p + ... + x_{e-1}p^{e-1}$. So we can say $f_{x_0}(x+ap^e) \equiv 0 \pmod{p^{e+1}}$ for all $0 \leq a \leq p-1$. These are our p solutions so that $|\bar{N}_{e+1}| = p|\bar{N}_e|$ when e is odd.

Suppose $e = 2k$ (even). Then $v_p(f_{x_0}(x)) = 2v_p(x+1)$. So $f_{x_0}(x) \equiv 0 \pmod{p^e}$ where $x = x_0 + x_1 p + ... + x_{e-1}p^{e-1} \pmod{p^e}$. It must be that $v_p(f_{x0}(x)) \geq e = 2k$ if and only if $2v_p(x+1) \geq e = 2k$. And we have that $v_p(x+1) \geq k$. If the $v_p(f_{x_0}(x + ap^e)) \geq e+1 = 2k+1$ then only the $x's$ where $x_i = p-1$ for $0 \leq i \leq k$ will lift, and each of them will lift in p different ways. This means that only $1/p$ of the solutions modulo p^e will lift to solutions modulo p^{e+1}. And since each of those that lift in p ways in the case where $e = 2k$ the number of solutions modulo p^{e+1} will equal the number of solutions modulo p^e, so that $|\bar{N}_{e+1}| = |\bar{N}_e|$ when e is even.

We can see $v_p(f_{x_0}(x)) \geq 2k+1$ if and only if $2v_p(x+1) \geq 2k+1$ if and only if $2v_p(x+1) \geq 2k+2$ if and only if $v_p(x+1) \geq k+1$. So $x+1 \equiv 0 \pmod{p^{k+1}}$ and $x \equiv -1 \pmod{p^{k+1}}$.

In other words only x of form $x = (p-1) + (p-1) \cdot p + (p-1) \cdot p^2 + ...(p-1) \cdot p^{k-1} + ...$ lift to solutions modulo p^{e+1} and the ones of the form $x = (p-1)+(p-1)\cdot p+...+(p-1)p^{k-1}+ap^k+\cdots$ where $a \neq (p-1)$ will not. So the lifted values for x will equal $(p-1)+(p-1)\cdot p+...+(p-1)\cdot p^{k-1}+(p-1)\cdot p^k+a\cdot p^k$.

Since there are $(p-1)/2$ possible choices for x_0 and for each of these x_0 there are $p^{\lfloor e/2 \rfloor}$ solutions x modulo p^e to $f_{x_0}(x) \pmod{p^e}$.

Now letting the solutions x of $f_{x_0}(x) \equiv 0 \pmod{p^e}$ that we found above modulo p^e be denoted by x_1. By the Chinese Remainder theorem, each solution

pair $(x_0, x_1) \in \{1, 2, ..., p-1\} \times \{1, 2, ..., p^e\}$ where $p \nmid x$, becomes one solution $x \in \{1, 2, 3, ..., (p-1)p^e\}$ which are the values which solve $x^{g(x)} \equiv x \pmod{p^e}$ where $1 \leq x \leq p^e(p-1)$, and $p \nmid x$. Q.E.D.

Finally we are ready to prove our Theorem 5.1 from above.

Theorem 5.1. *Given p an odd prime and $g(x) = x + 2$ then*

$$|\bar{N}_e| = |C| + \left(\frac{p-1}{2}\right) p^{\lfloor e/2 \rfloor}$$

for e a positive integer, $\lfloor x \rfloor$ function of x, and where

$$|C| = \left(\sum_{x_0=1}^{p-1} \gcd(p-1, g(x_0) - 1)\right) - (p-1)/2.$$

Proof. We see from Proposition 5.5 that when $g(x) \equiv 1 \pmod{p}$, then the congruence $x^{g(x)} \equiv x \pmod{p^e}$ has $\left(\frac{(p-1)}{2}\right) p^{\lfloor e/2 \rfloor}$ solutions for $1 \leq x \leq p^e(p-1)$ where $p \nmid x$. We also see from Proposition 5.4 that, since the cases where $g(x) \not\equiv 1 \pmod{p}$ lift uniquely, $|C|$ is equal to the total number of solutions in $|\bar{N}_1| = \sum_{x_0}^{p-1} \gcd(p-1, g(x_0) - 1)$ minus the $(p-1)/2$ solutions modulo p that lift in a more complicated way because $g(x) \equiv 1 \pmod{p}$ causes the derivative modulo p to be 0. Putting these two results together, we have that

$$|\bar{N}_e| = |C| + \left(\frac{p-1}{2}\right) p^{\lfloor e/2 \rfloor}$$

for any positive integer e. Q.E.D.

Chapter 6

Conclusion and Future Work

In this paper, we reviewed the known theorems from Holden, Richardson, and Robinson [3] that count solutions $|\bar{N}_e|$ to the congruence $x^{g(x)} \equiv x \pmod{p^e}$ in the range where p is prime, $x \in 1, 2, ..., p^e(p-1)$ and $p \nmid x$. We examined the patterns of the solutions x when $g(x) = x + 1$ and we proved that for an odd prime p and $g(x) = x + 2$ then $|\bar{N}_e| = |C| + \left(\frac{p-1}{2}\right) p^{\lfloor e/2 \rfloor}$.

We have yet to prove the formula for $|\bar{N}_e|$ when $g(x) = x + 2$ and $p = 2$, since our main theorem only covers when p is an odd prime. However, we state the following conjecture:

Conjecture 6.1. For $p = 2$ and $g(x) = x + 2$, $|\bar{N}_e| = 2^{e-1}$ when $e = 1, 2, 3$ and $|\bar{N}_e| = 2^{\lfloor e/2 \rfloor} + 2$ for $e \geq 4$.

This conjecture implies that $|\bar{N}_e| = 1, 2, 4, 6, 6, 10, 10, 18, 18,$ etc. when $p = 2$.

Notice that for $p = 2$ the pattern $|\bar{N}_e| = |C| + \left(\frac{p-1}{2}\right) p^{\lfloor e/2 \rfloor}$ only holds for

$e \geq 4$. We see a similar phenomenon when considering $|\bar{N}_e|$ for $g(x) = x + c$ for a positive integer c. We state the following conjecture:

Conjecture 6.2. For $g(x) = x + c$, $|\bar{N}_e| = |C| + |D|p^{\lfloor e/2 \rfloor}$ only holds for all $e \geq 1$ when $p \geq c + 1$.

Below we include data to back up this claim. Further steps after this point would be to prove these two conjectures, as well as to come up with a new formula for the p's where our formula does not hold.

To get a sense of this trend, we observe the values for C and D in the next few examples when they satisfy the equation of the form $|\bar{N}_e| = |C| + |D|p^{\lfloor e/2 \rfloor}$ for all e and $g(x) = x + c$, at a few different values for c. When there was no value that satisfied C or D in the equation for $|\bar{N}_e|$ and all e, the space was left blank.

EXAMPLE 13. *The following is the pattern for* $g(x) = x + 3$

p	C	D	C+D
2			
3	2	1	3
5	6	2	8
7	12	3	15
11	22	5	27

EXAMPLE 14. *We see that when* $g(x) = x + 4$ *the pattern only works for* $p \geq 3$

p	C	D	C+D
2			
3	*3*	*0*	*3*
5	*6*	*2*	*8*
7	*12*	*3*	*15*
11	*22*	*5*	*27*

EXAMPLE 15. *Similarly, we see that when g(x)=x+5 the pattern only works for* $p \geq 3$

p	C	D	C+D
2			
3			
5	*4*	*4*	*8*
7	*14*	*1*	*15*
11	*26*	*1*	*27*

Note that $p \geq c + 1$ is satisfied by Examples 13-15.

Bibliography

[1] Stephen Abbott, *Understanding analysis*, Springer Science & Business Media, 2012.

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

[3] Joshua and Richardson Holden Pamela A and Robinson, *Counting Fixed Points and Rooted Closed Walks of the Singular Map*, p-Adic Numbers, Ultrametric Analysis and Applications **12** (2020), no. 1, 12–28.

[4] Joshua Holden, *Fixed Points and Two-Cycles of the Discrete Logarithm*, Algorithmic number theory (ANTS 2002), 2002, pp. 405–415.

[5] ———, *Addenda/corrigenda: Fixed Points and Two-Cycles of the Discrete Logarithm*, 2002. Unpublished, available at `http://xxx.lanl.gov/abs/math.NT/0208028`.

[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), 163–178.

[7] Nanoko Honda, *Counting Three-Cycles of the Discrete Exponential Function and Other Porblems Using p-adic Analysis*, 2019.

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

[9] Abigail Mann, *Counting Solutions to Discrete Non-Algebraic Equations Modulo Prime Powers*, Senior Thesis, Rose-Hulman Institute of Technology, 2016, `http://scholar.rose-hulman.edu/math_mstr/153`.

[10] Joseph H Silverman, *A friendly introduction to number theory*, Vol. 10, 2006.

[11] Martin H Weissman, *An illustrated theory of numbers*, Vol. 105, American Mathematical Soc., 2020.

[12] A. Wood, *The Square Discrete Exponentiation Map*, Technical Report MSTR 11-05, Mathematical Sciences Technical Reports, Rose-Hulman Institute of Technology, 2011, `http://scholar.rose-hulman.edu/math_mstr/9/`.

[13] Dara Zirlin, *Problems Motivated by Cryptology: Counting Fixed Points and Two-Cycles of the Discrete Lambert Map*, 2015.

Appendix A

Appendices

The following Magma code was used in order to prove to examine solutions to the congruence $x^{x+1} \equiv x$ modulo p^e for every x in the range $1 \leq x \leq p^e(p-1)$. This code can be edited to examine solutions for values $x^{x+c} \equiv x$ modulo p^e for an integer c.

```
rae:= function(p,e)
local x, h, b, count;
count:=0;
for x in [1..p^e*(p-1)] do h:=(x mod p);
            if (h ne 0) then
b:= (x^(x+1)-x) mod p^e;
print x, b;
if (b eq 0) then count := count +1;
end if;
end if;
end for;
return p, e, count;
```

```
end function;
```