Rose-Hulman Undergraduate Mathematics Journal

Volume 16
Issue 1

Article 1

Deconstructing the Welch Equation Using p-adic Methods

Abigail Mann
Rose-Hulman Institute of Technology

Adelyn Yeoh
Mount Holyoke College

Rose-Hulman Undergraduate Mathematics Journal

Deconstructing the Welch Equation Using p-adic Methods

Abigail Mann[a] Adelyn Yeoh[b]

Volume 16, No. 1, Spring 2015

Sponsored by

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

[a]Rose-Hulman Institute of Technology
[b]Mount Holyoke College

Rose-Hulman Undergraduate Mathematics Journal
Volume 16, No. 1, Spring 2015

Deconstructing the Welch Equation Using p-adic Methods

Abigail Mann Adelyn Yeoh

Abstract. The Welch map $x \to g^{x-1+c}$ is similar to the discrete exponential map $x \to g^x$, which is used in many cryptographic applications including the ElGamal signature scheme. This paper analyzes the number of solutions to the Welch equation, $g^{x-1+c} \equiv x \pmod{p^e}$, where p is a prime and g is a unit modulo p, and looks at other patterns of the equation that could possibly be exploited in a similar cryptographic system. Since the equation is modulo p^e, where p is a prime number, p-adic methods of analysis are used in counting the number of solutions modulo p^e. These methods include p-adic interpolation, Hensel's Lemma and the Chinese Remainder Theorem.

Acknowledgements: Both authors would like to thank Joshua Holden and Margaret M. Robinson for their endless support and guidance during their summer REU. The first author would like to thank the Rose-Hulman Weaver and Rose Summer Undergraduate Research Programs, the Rose-Hulman Mathematics Department, and Dr. William Heller for their financial support, and Mount Holyoke College for their hospitality during her REU. The second author would like to thank the Mount Holyoke College Hutchcroft Fund for funding her summer REU.

1 Introduction

The Welch equation, $g^{x-1+c} \equiv x \pmod{p^e}$, is typically used as an algorithm to produce Costas arrays, which are permutation matrices with certain desirable properties [6]. These arrays have applications in SONAR detection [1]. The Welch equation is typically not associated with cryptography. However, the complexity associated with this equation may allow application in cryptography as well. In particular, we note that if viewed as a map, $x \to g^{x-1+c}$, the equation looks very similar to the discrete exponential map, $x \to g^x$.

Most of the analysis previously done on the Welch equation modulo p is statistical and looks only at $x \in \{1, 2, \cdots, p\}$. However, we follow a suggestion from Holden and Robinson [5, Section 8] to count the number of solutions to the Welch equation modulo p^e on a larger range, and we discover clear formulas (in terms of p and multiplicity of g) for this number of solutions.

In dissecting this problem, we first turn the equation into a function, $f_g(x, c) : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/p^e\mathbb{Z}$, where $f_g(x, c) = g^{x-1+c} - x \pmod{p^e}$. When g is fixed throughout a theorem we will suppress it and write $f(x, c)$. When c is fixed, we write $f(\cdot, c)$, and when x is fixed, we write $f(x, \cdot)$. We then observe the output when p is an odd prime. We also consider the special case when p is equal to 2. In the process leading up to counting the number of solutions, we observe that the output of $f(x, c)$ is periodic in c and in x, allowing us to restrict the domain for these variables. The periodic nature of the Welch equation is detailed in Section 2.

There are other characteristics of the Welch equation on the smaller range, $x \in \{1, 2, \cdots, p\}$, shown in Section 3, which may help in understanding the distribution of solutions. Most notably, when g is a primitive root modulo p^e, we find it easy to count the pairs of solutions (x, c). The difficulty in this equation is how to count in the cases when g is not a primitive root. Section 3.3 describes a method to overcome this obstacle.

Our approach to counting solutions is to first begin with the function modulo p. In order to successfully count solutions modulo p^e, we will need to interpolate the equation. Section 4 goes over the process of p-adic interpolation for our function. Finally in Section 5, we count the solutions using different approaches to the equation by fixing c and treating x as a variable, by treating both x and c as variables, and by looking at p equal to 2.

For this paper, we assume that g is a unit modulo p. Further, note that when g is a unit, x must also be a unit modulo p in order to be a solution. Note that, unless otherwise stated, we take m to be the multiplicative order of g modulo p.

2 Periodicity

One property of the Welch equation is that it is periodic modulo p^e. The following two theorems describe how the Welch equation is periodic modulo p^e.

Theorem 1. *Let f be the function $f(x, \cdot) = g^{x-1+c} - x \pmod{p^e}$, where $c \in \mathbb{Z}$, and p is a prime. Then $f(x, c) = f(x, c + m \cdot p^{e-1})$.*

Proof. We will prove the equivalent statement that $g^{m\cdot p^{e-1}} \equiv 1 \pmod{p^e}$. This equivalence follows since

$$\begin{aligned} f(x,c) &= f(x, c + m\cdot p^{e-1}) \\ g^{x-1+c} - x &\equiv g^{x-1+c+m\cdot p^{e-1}} - x \pmod{p^e} \\ g^{x-1+c} &\equiv g^{x-1+c}\cdot g^{m\cdot p^{e-1}} \pmod{p^e} \\ g^{m\cdot p^{e-1}} &\equiv 1 \pmod{p^e}. \end{aligned}$$

Thus, it is sufficient to show that $g^{m\cdot p^{e-1}} \equiv 1 \pmod{p^e}$. By definition, $g^m \equiv 1 \pmod{p}$ so $g^m = 1 + p\cdot A$, where $A \in \mathbb{Z}$. Now observe that by the binomial theorem we obtain

$$\begin{aligned} g^{m\cdot p^{e-1}} &\equiv (g^m)^{p^{e-1}} \pmod{p^e} \\ &\equiv (1+p\cdot A)^{p^{e-1}} \pmod{p^e} \\ &\equiv 1 + p^{e-1}(p\cdot A) + \frac{p^{e-1}(p^{e-1}-1)}{2!}(p\cdot A)^2 + \\ &\quad \frac{p^{e-1}(p^{e-1}-1)(p^{e-1}-2)}{3!}(p\cdot A)^3 + \ldots + \\ &\quad \frac{p^{e-1}(p^{e-1}-1)\ldots(p^{e-1}-n+1)}{n!}(p\cdot A)^n + \ldots + \\ &\quad (pA)^{p^{e-1}} \pmod{p^e}. \end{aligned}$$

Consider the nth term of this expression

$$\begin{aligned} &\frac{p^{e-1}(p^{e-1}-1)\ldots(p^{e-1}-n+1)}{n!}(p\cdot A)^n \\ &= p^e\left(\frac{p^{n-1}(p^{e-1}-1)\ldots(p^{e-1}-n+1)}{n!}(A)^n\right). \end{aligned}$$

In this nth term, for all $1 \le n \le p^{e-1}$, we have $p^e > n$. Thus, there are no multiples of p^e in the denominator. Hence, the nth term is clearly divisible by p^e.

Now observe the last term, $(pA)^{p^{e-1}}$. By induction, we can easily show that $p^{e-1} \ge e$ for all $p \ge 2$, and for all $e \ge 1$. Thus with that result, $(pA)^{p^{e-1}}$ is a multiple of p^e, thus $(pA)^{p^{e-1}} \equiv 0 \pmod{p^e}$.

Since the nth term and the last term are all divisible by p^e, it is then clear that $g^{m\cdot p^{e-1}} \equiv 1 \pmod{p^e}$. □

Theorem 2. *Given a fixed g and c, we have that*

$$g^{x-1+c+mp^e} - (x + mp^e) \equiv g^{x-1+c} - x \pmod{p^e}.$$

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

Proof. From Theorem 1 we now know that $g^{mp^{e-1}} \equiv 1 \pmod{p^e}$, so we have

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

□

3 Characteristics of the Welch Equation

We are able to make several observations on the Welch equation. When g is a primitive root, we can find certain symmetries to the values of c. For more general cases of g, we are able to find a specific solution c for some given values of x.

3.1 When g is a primitive root

For the case where g is a primitive root, we can find patterns in which values of c will provide a solution to $f_g(x, c)$ for a given x, and find some periodicity in the solutions.

Proposition 3. *Consider $f_g(x, c) = g^{x-1+c} - x \pmod{p^e}$ for odd prime p. If g is a primitive root mod p^e (i.e. the order of g is $p^{e-1}(p-1)$), there is a c' for each c where*

$$f_g(x, c) = -f_{g^{-1}}(p^{e+1} - x, c')$$

for all $x \in \mathbb{Z}$. This corresponding c' is given by $c' \equiv \frac{p^{e-1}(p-3)+4}{2} - c \pmod{p^{e-1}(p-1)}$ and is unique modulo $p^{e-1}(p-1)$.

Proof. To prove this c' satisfies the requirements, it suffices to show

$$f_g(x, c) + f_{g^{-1}}(p^{e+1} - x, c') \equiv 0 \pmod{p^e}.$$

So we have

$$\begin{aligned} g^{x-1+c} - x + (g^{-1})^{(p^{e+1}-x)-1+\frac{p^{e-1}(p-3)+4}{2}-c} - (p^{e+1} - x) &\pmod{p^e} \\ \equiv g^{x-1+c} - x + g^{x-p^{e+1}+1+\frac{3p^{e-1}-p^e-4}{2}+c} + x &\pmod{p^e} \\ \equiv g^{x-1+c}(1 + g^{-p^{e+1}+\frac{3p^{e-1}-p^e}{2}}) &\pmod{p^e} \\ \equiv g^{x-1+c}(1 + g^{\frac{p^{e-1}(-2p^2-p+3)}{2}}) &\pmod{p^e} \\ \equiv g^{x-1+c}(1 + g^{\frac{p^{e-1}(p-1)(-2p-3)}{2}}) &\pmod{p^e}. \end{aligned}$$

Since g is a primitive root modulo p^e, $g^{\frac{p^{e-1}(p-1)}{2}} \equiv -1 \pmod{p^e}$. So the expression we have reduces to

$$\equiv g^{x-1+c}(1 + (-1)^{-2p-3}) \pmod{p^e}.$$

Since $-2p-3$ will always be odd, we have that

$$\equiv g^{x-1+c}(1-1) \equiv 0 \pmod{p^e}.$$

Now suppose there is a $c'' \neq c'$ such that

$$f_g(x,c) = -f_{g^{-1}}(p^{e+1}-x,c') = -f_{g^{-1}}(p^{e+1}-x,c'').$$

Then

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

Since g and hence g^{-1} are both primitive roots,

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

Therefore, $f_g(x,c) = -f_{g^{-1}}(p^{e+1}-x,c')$ for a unique c' modulo $p^{e-1}(p-1)$, where $c' \equiv \frac{p^{e-1}(p-3)+4}{2} - c \pmod{p^{e-1}(p-1)}$.

□

Lemma 4. *Let p be an odd prime, and g is a primitive root of p^e. Then for each unit x from 1 to p^e, there exists a unique value of $c \in \{1,2,\ldots,(p-1)\cdot p^{e-1}\}$ that is a solution to $g^{x-1+c} \equiv x \pmod{p^e}$.*

Proof. Let $x \equiv g^k \pmod{p^e}$, so we obtain $g^{x-1+c} \equiv g^k \pmod{p^e}$. Now solve for c, and we obtain $c \equiv (k+1)-x \pmod{(p-1)\cdot p^{e-1}}$. Hence, we have shown that some unique c exists, since it has to be in the range $1 \leq c \leq m \cdot p^{e-1}$. □

Lemma 5. *Let p be an odd prime. Let g be a primitive root of both p and p^e. Then, when $x = p^e - 1$, we observe that*

$$c \equiv \tfrac{p^{e-1}(p-3)+4}{2} \pmod{p^{e-1}(p-1)}$$

is the solution to $g^{x-1+c} \equiv x \pmod{p^e}$.

Proof. We will show that $g^{(p^e-1)-1+\frac{p^{e-1}(p-3)+4}{2}} \equiv p^e - 1 \pmod{p^e}$.

$$\begin{aligned} g^{(p^e-1)-1+\frac{p^{e-1}(p-3)+4}{2}} &\equiv g^{p^e-2+\frac{1}{2}p^{e-1}(p-3)+2} \pmod{p^e}\\ &\equiv g^{\frac{2p^e+p^{e-1}(p-3)}{2}} \pmod{p^e}\\ &\equiv g^{p^{e-1}(p-1)} \cdot g^{\frac{p^{e-1}(p-1)}{2}} \pmod{p^e}\\ &\equiv (1)\cdot(-1) \pmod{p^e}\\ &\equiv p^e - 1 \pmod{p^e}\ . \end{aligned}$$

□

Theorem 6. *Let g be a primitive root modulo p^e, and let g^{-1} be its multiplicative inverse. By Lemma 4, there exists a pair (x, c) that solves $g^{x-1+c} \equiv x \pmod{p^e}$.*

Then the pair $(p^e - x, c')$ solves $(g^{-1})^{p^e-x-1+c'} \equiv p^e - x \pmod{p^e}$, where $c' \equiv c_{p^e-1} - c \pmod{p^{e-1}(p-1)}$, and $c_{p^e-1} = \frac{p^{e-1}(p-3)+4}{2}$.

Proof. By Lemma 4 there exists some c' where $(p^e - x, c')$ is a solution to $(g^{-1})^{p^e-x-1+c'} \equiv p^e - x \pmod{p^e}$. Then we will show that $c' \equiv c_{p^e-1} - c$. We know that $g^{x-1+c} \equiv x \pmod{p^e}$ and $g \cdot g^{-1} \equiv 1 \pmod{p^e}$. So we observe $(g^{-1})^{p^e-x-1+c'} \equiv p^e - x \pmod{p^e}$ and obtain the following equivalences

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

Lemma 5 implies that $p^e - 1 \equiv g^{\frac{3p^{e-1}(p-1)}{2}} \pmod{p^e}$ by expanding the lemma as follows

$$\begin{aligned}
p^e - 1 &\equiv g^{(p^e-1)-1+\frac{p^{e-1}(p-3)+4}{2}} \pmod{p^e} \\
&\equiv g^{\frac{2p^e+p^{e-1}(p-3)}{2}} \pmod{p^e} \\
&\equiv g^{\frac{3p^{e-1}(p-1)}{2}} \pmod{p^e}\ . \qquad (2)
\end{aligned}$$

Thus, we can equate (1) and (2) to obtain

$$\begin{aligned}
g^{\frac{3p^{e-1}(p-1)}{2}} &\equiv g^{-2+c+p^e+c'} \pmod{p^e} \\
\frac{3p^{e-1}(p-1)}{2} &\equiv -2 + c + p^e + c' \pmod{(p-1)\cdot p^{e-1}} \\
c' &\equiv \frac{p^{e-1}(p-3)+4}{2} - c \pmod{(p-1)\cdot p^{e-1}}\ .
\end{aligned}$$

□

3.2 For more general values of g

Even when g is not a primitive root, we find patterns in the solution pairs to our equation.

Theorem 7. *Let p be an odd prime. Consider x_0 a unit modulo p. Let (x_0, c_0) be a solution to $g^{x-1+c} \equiv x \pmod{p^e}$. Let $x_0 \equiv x_1 \equiv x_2 \equiv \ldots \equiv x_n \pmod{p^e}$ where*

$$\begin{aligned} x_1 &= x_0 + 1 \cdot p^e \\ x_2 &= x_0 + 2 \cdot p^e \\ &\vdots \\ x_n &= x_0 + n \cdot p^e \ . \end{aligned}$$

Then,

$$c_n \equiv c_0 - n \cdot p^{e-1} \pmod{m \cdot p^{e-1}}$$

is the solution to the equation $g^{x_n-1+c_n} \equiv x_0 \pmod{p^e}$.

Proof.

$$\begin{aligned} g^{x_n-1+c_n} &\equiv g^{(x_0+n\cdot p^e)-1+(c_0-n\cdot p^{e-1})} \pmod{p^e} \\ &\equiv g^{x_0-1+c_0} \cdot g^{n\cdot p^{e-1}(p-1)} \pmod{p^e} \\ &\equiv x_0 \pmod{p^e}. \end{aligned}$$

□

From Theorem 7 we explicitly highlight the case when we take $n = m$, and obtain the following corollary. We note that the statement is similar to Theorem 1 except that this corollary highlights the particular (x_0, c_0) pair that produces a repeated solution.

Corollary 8. *Let p be an odd prime. Let (x_0, c_0) be a solution pair to $g^{x-1+c} \equiv x \pmod{p^e}$. Let $x_m = x_0 + m \cdot p^e$. Then*

$$c_m \equiv c_0 - m \cdot p^e \equiv c_0 \pmod{m \cdot p^{e-1}}$$

is the solution to the equation $g^{x_m-1+c_m} \equiv x_0 \pmod{p^e}$.

3.3 Observing $x \equiv p \pmod{p}$

When we set $x = p$, we obtain some interesting results, especially regarding the determination of which values of x will be a part of a solution pair (x, c).

Proposition 9. *For all c and $g \in \mathbb{Z}$, when $x \equiv p \pmod{p}$, $g^{x-1+c} \not\equiv x \pmod{p}$.*

Proof. It is easy to show why Proposition 9 holds. If $x = p$, then $x \equiv 0 \pmod{p}$. However, g^k can never be equal or congruent to 0. □

When $x \equiv p \pmod{p}$ we get an interesting result. When we create the function $f(x,c) = g^{x-1+c} - x \pmod{p}$, and let c range from 1 to m, we obtain a value set, $V = \{f(x,c) \mid 1 \leq c \leq m\}$. Note that we use this range because for a fixed x, the value of $f(x,c)$ starts to repeat when $c > m$. See Theorem 1. When $x \equiv p \pmod{p}$, the value set clues us in to the exact values of x which have solutions to the Welch equation. This result is particularly useful to look in the case where g is not a primitive root as not all values of x will be a solution. Additionally, the size of the value set gives us insight into the number of solutions to modulo p for the range of $x \in \{1, 2, \ldots, p\}$. Hence, we have the following theorems.

Lemma 10. *Let p be an odd prime. Let f be a function defined by $f(x,c) = g^{x-1+c} - x \pmod{p}$. When $x = p$, then $f(p,c) \equiv g^c \pmod{p}$ for all $1 \leq c \leq m$.*

Proof. All we need to show is that $g^c \equiv g^{p-1+c} - p \pmod{p}$. This is fairly simple. Start with left hand side $g^{p-1+c} - p \equiv g^{p-1} \cdot g^c \equiv (1) \cdot g^c \equiv g^c \pmod{p}$. □

Theorem 11. *Let p be an odd prime, and fix g a unit modulo p. Consider any $x \in \{g^{p-1+c} - p \mid 1 \leq c \leq m\}$. Then a solution c' exists, which solves $g^{x-1+c'} \equiv x \pmod{p}$. Furthermore, this solution is unique modulo m.*

The statement of this theorem may be a little confusing so we give an example before providing the proof. It is best to consider a g that is not a primitive root, as this case best highlights the point of the theorem.

EXAMPLE 1. Consider $p = 7$, and $g = 2$. The multiplicative order of 2 modulo 7 is 3. When $x = 7$ we obtain

$$\begin{aligned} c = 1 : 2^{7-1+1} - 7 \equiv 2^7 - 7 \equiv 128 - 7 \equiv 2 \pmod{7} \\ c = 2 : 2^{7-1+2} - 7 \equiv 2^8 - 7 \equiv 256 - 7 \equiv 4 \pmod{7} \\ c = 3 : 2^{7-1+3} - 7 \equiv 2^9 - 7 \equiv 512 - 7 \equiv 1 \pmod{7} \end{aligned}$$

So the value set, $V = \{1, 2, 4\}$. Check $f(x,c) = g^{x-1+c} - x \pmod{p}$ for $x \in \{1, 2, 3, 4, 5, 6, 7\}$, and for $c \in \{1, 2, 3\}$. When $f(x,c) \equiv 0 \pmod{p}$, we know that this pair (x,c) is a solution to the equation $g^{x-1+c} \equiv x \pmod{p}$.

As we can see in Table 1, the values of x which have solutions are the same as those in the value set.

Proof. By Lemma 4 if x is a solution, there will exist a corresponding c. Let c' be the solution to $g^{x-1+c} \equiv x \pmod{p}$ for $x \equiv g^{p-1+c} - p \pmod{p}$. So we have the following equivalences

$$\begin{aligned} g^{x-1+c'} &\equiv x \pmod{p} \\ g^{x-1+c'} &\equiv g^{p-1+c} - p \pmod{p} \\ x - 1 + c' &\equiv c \pmod{m} \\ c' &\equiv -x + 1 - c \pmod{m}. \end{aligned}$$

Now we show that c' solves $g^{p-1+c} \equiv x \pmod{p}$.

x	c = 1	c = 2	c = 3
1	1	3	0
2	2	6	0
3	5	6	1
4	5	0	4
5	6	3	4
6	2	3	5
7	1	2	4

Table 1: Values of $f(x, c)$

$$g^{x-1+c'} = g^{x-1+(-x+1-c)} \equiv g^c \equiv g^c \cdot g^{p-1} - p \equiv g^{p-1+c} - p \equiv x \pmod{p}.$$

□

3.4 Symmetry in multiplicative inverses

Another pattern we discover is that for g and its multiplicative inverse, the value sets described in the previous subsection are the same.

Proposition 12. *Let p be an odd prime. If g^{-1} is the multiplicative inverse of g modulo p, then when $x = p$, we have $g^{p-1+c} \equiv (g^{-1})^{p-1+(m-c)} \pmod{p}$.*

Proof.

$$\begin{aligned}(g^{-1})^{p-1+(m-c)} &\equiv g^{-(p-1+(m-c))} \pmod{p} \\ &\equiv g^{-(p-1)} \cdot g^{-m} \cdot g^c \pmod{p} \\ &\equiv (1) \cdot (1) \cdot g^c \pmod{p} \\ &\equiv g^{p-1+c} \pmod{p},\end{aligned}$$

where the last equivalence follows from Lemma 10. □

Theorem 13. *Let p be an odd prime. Let f be the function $f_g(p, c) = g^{p-1+c} - p \pmod{p}$. When g and g^{-1} are multiplicative inverses we observe that the value sets produced are equal, such that $\{f_g(p, c) \mid 1 \leq c \leq m\} = \{f_{g^{-1}}(p, c) \mid 1 \leq c \leq m\}$.*

Proof. By Proposition 12, $g^{p-1+c} \equiv (g^{-1})^{p-1+(m-c)} \pmod{p}$. Hence, if we consider $f_g(p, c)$ and take it over $1 \leq c \leq m$, the value set will be equal to the value set of $f_{g^{-1}}(p, c)$. □

3.5 Other patterns

The following two propositions discuss patterns in the solutions that resemble a type of periodicity.

Proposition 14. *Consider* $f(x,c) \equiv g^{x-1+c} - x \pmod{p^e}$. *Then*

$$f(x+y,c) \equiv f(x,c+y) - y \pmod{p^e}.$$

Proof. It suffices to show $f(x+y,c) - (f(x,c+y)-y) \equiv 0 \pmod{p^e}$. We have

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

□

Proposition 15. *Consider* $f(\cdot,c) \equiv g^{x-1+c} - x \pmod{p^e}$. *Then*

$$f(x,c) \equiv f(x+p^{e-1}(p-1),c) - p^{e-1} \pmod{p^e}.$$

Proof. It suffices to show $f(x,c) - f(x+p^{e-1}(p-1),c) + p^{e-1} \equiv 0 \pmod{p^e}$. The left hand side becomes

$$g^{x-1+c} - x - (g^{x+p^{e-1}(p-1)-1+c} - x - p^{e-1}(p-1) - p^{e-1}).$$

Since the order of g divides $p^{e-1}(p-1)$, this is congruent modulo p^e to

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

□

4 Interpolation and Hensel's Lemma

To reach our goal of counting solutions to the Welch equation, we first interpolate our discrete functions into the p-adics. The following theorems provide a way to more easily analyze the number of solutions in a later section. Hensel's Lemma is also briefly introduced at the end of the section as a tool for counting solutions.

4.1 When p is an odd prime

We first apply interpolation to the Welch equation in our function form when p is an odd prime, and address $p = 2$ later.

Let $g \in \mathbb{Z}$ be fixed and let p be an odd prime. We will need to interpolate the function $f(\cdot, c) = g^{x-1+c}$, which is defined on $x \in \mathbb{Z}$, to a function on $x \in \mathbb{Z}_p$ so that we can count solutions to $g^{x-1+c} \equiv x \pmod{p^e}$. However, this is not possible for $g \notin 1 + p\mathbb{Z}_p$ [2, Section 4.6], [4, Section II.2]. So we will have to change the function slightly in order to interpolate.

To do this, we use methods similar to that of [5, Section 2]. Let $\mu_{p-1} \subseteq \mathbb{Z}_p^\times$ be the set of all $(p-1)$-st roots of unity. Then for odd prime p, we have the Teichmüller character

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

which is a surjective homomorphism. As stated in [2, Corollary 4.5.10], we can write each element of $\mathbb{Z}_p^\times$ as an element of $\mu_{p-1} \times (1+p\mathbb{Z}_p)$. So for each $x \in \mathbb{Z}_p^\times$ as $\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1+p\mathbb{Z}_p)$ we have $x = \omega(x)\,\langle x \rangle$ for some $\langle x \rangle \in 1 + p\mathbb{Z}_p$.

Theorem 16. *For $p \neq 2$, let $g \in \mathbb{Z}_p^\times$ and $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$, and let*

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

Then

$$F_{x_0}(x) = \omega(g)^{x_0}\,\langle g \rangle^{x-1+c}$$

defines a uniformly continuous function on $\mathbb{Z}_p$ such that $F_{x_0}(x) = g^{x-1+c}$ whenever $x \in I_{x_0}$.

Proof. By [2, 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. By [3, Theorem 4.1.4], if a function is continuous in $\mathbb{Z}_p$, it is also uniformly continuous and bounded. 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 $F_{x_0}(x) = g^{x-1+c}$ with the proper conditions on x.

We first prove density of I_{x_0} in $\mathbb{Z}_p$: for the sake of clarity, we rename I_{x_0} as $I_{s_0} = \{s \in \mathbb{Z} \mid s - 1 + c \equiv s_0 \pmod{p-1}\}$ in this proof. Let $x \in \mathbb{Z}_p$, so it can be written as $x = x_0 + x_1 p + x_2 p^2 + \ldots$. Now let $s_1 \in \{0, 1, \ldots, p-2\}$ such that $s_1 \equiv s_0 + 1 - c - x_0 - x_1 - \ldots - x_{i-1} \pmod{p-1}$ and $y_i = x_0 + x_1 p + \ldots + x_{i-1}p^{i-1} + s_1 p^i$ for any given $i \in \mathbb{Z}$. Then we know

$$y_i \equiv x_0 + x_1 + x_2 + \cdots + x_{i-1} + s_1 \equiv s_0 + 1 - c \pmod{p-1},$$

so $y_i \in I_{s_0}$ for all y_i. Now let $\epsilon > 0$, and we can find N such that $p^{-N} < \epsilon$. For any $n > N$, we have

$$\begin{aligned} |y_n - x|_p &= |x_0 + x_1 p + \ldots + x_{n-1}p^{n-1} + s_1 p^n - (x_0 + x_1 p + x_2 p^2 + \ldots)|_p \\ &= |s_1 p^n - (x_n p^n + x_{n+1} p^{n+1} + \ldots)|_p \\ &= |p^n|_p |s_1 - (x_n + n_{n+1} p + \ldots)|_p \\ &\leq p^{-n} < p^{-N} < \epsilon. \end{aligned}$$

So for every $x \in \mathbb{Z}_p$ we have a sequence $\{y_i\}$ in I_{s_0} that converges to x, so then I_{s_0} (which was the new notation for our original set I_{x_0}) is dense in $\mathbb{Z}_p$.

Now we must show each $F_{x_0}(x) = \omega(g)^{x_0} \langle g \rangle^{x-1+c}$ 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

$$|\langle g \rangle^x - \langle g \rangle^y|_p = |\langle g \rangle^{y+p^N A} - \langle g \rangle^y|_p = |\langle g \rangle^y|_p |\langle g \rangle^{p^N A} - 1|_p = |\langle g \rangle^{p^N A} - 1|_p$$

and using the binomial theorem for some $M \in \mathbb{Z}$, we get

$$\langle g \rangle^{p^N A} = (1 + pM)^{p^N A} = 1 + p^N ApM + \frac{p^N A(p^N A - 1)}{2}(pM)^2 + \ldots + (pM)^{p^N A}.$$

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

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

So the function mapping $x \to \langle g \rangle^x$ is uniformly continuous on I_{x_0} and hence on $\mathbb{Z}_p$ by [3, Theorem 4.15]. Since each $F_{x_0}(x) = \omega(g)^{x_0} \langle g \rangle^{x-1+c} = \omega(g)^{x_0} \langle g \rangle^{c-1} \langle g \rangle^x$ for fixed x_0, c, and g, and $\omega(g)^{x_0} \langle g \rangle^{c-1}$ 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 $\mathbb{Z}_p$ [3, Exercise 89].

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

$$g^{x-1+c} = \omega(g)^{x-1+c} \langle g \rangle^{x-1+c} = \omega(g)^{x_0} \langle g \rangle^{x-1+c} = F_{x_0}(x).$$

□

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

Theorem 17. *For this theorem, 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*

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

Then

$$F_{x_0}(x) = \omega(g)^{x_0} \langle g \rangle^{x-1+c}$$

defines a uniformly continuous function on $\mathbb{Z}_p$ such that $F_{x_0}(x) = g^{x-1+c}$ whenever $x \in I_{x_0}$.

Proof. Since $g^m \equiv 1 \pmod{p}$, $\omega(g)^m = \omega(g^m) = \omega(1) = 1$. 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 16 are equal and are the same as g^{x-1+c} when $x \in I_{x_0} \cup I_{x_0'}$. □

4.2 When p is equal to 2

In the case that $p = 2$, we use the same ideas to interpolate the function $f(\cdot, c) = g^{x-1+c} - x \pmod{p^e}$ a little differently. We will still decompose $g \in \mathbb{Z}_2^\times$ as $\omega(g)\langle g\rangle$, but now we take $\omega(g) \in \{-1, 1\}$ and $\langle g\rangle \in 1 + 4\mathbb{Z}_2$. It is known that this factorization exists and is unique [2, Corollary 4.5.10].

Now we will show how we can form two new functions by interpolation when $p = 2$.

Theorem 18. *For $p = 2$, let $g \in \mathbb{Z}_2^\times$ and $c \in \mathbb{Z}$. Then $F_0(x) = \langle g\rangle^{x-1+c}$ and $F_1(x) = -\langle g\rangle^{x-1+c}$ define functions on $1 + 2\mathbb{Z}_2$ such that $F_0(x) = g^{x-1+c}$ either when $g \in 1 + 4\mathbb{Z}_2$ or when $g \in 3 + 4\mathbb{Z}_2$ and $x - 1 + c \equiv 0 \pmod 2$ and $F_1(x) = g^{x-1+c}$ when $g \in 3 + 4\mathbb{Z}_2$ and $x - 1 + c \equiv 1 \pmod 2$.*

Proof. As with the proof for odd primes [Theorem 16], it suffices to show that $1 + 2\mathbb{Z}$ is dense in $1 + 2\mathbb{Z}_2$, each function is uniformly continuous on $1 + 2\mathbb{Z}$, and the functions agree with g^{x-1+c} for the proper conditions on x.

The density of $1 + 2\mathbb{Z}$ in $1 + 2\mathbb{Z}_2$ is simple to show. For any $x \in 1 + 2\mathbb{Z}_2$,

$$x = 1 + a_1(2) + a_2(2^2) + a_3(2^3) + \ldots \quad \text{where } a_i \in \{0, 1\}.$$

We let $\{y_n\}$ be the sequence defined by $y_n = x \pmod{2^n}$. Since each $y_n \in 1 + 2\mathbb{Z}$ and $\{y_n\}$ converges to x, we know that $1 + 2\mathbb{Z}$ is dense in the set $1 + 2\mathbb{Z}_2$.

Next, we show that each function is uniformly continuous on $1 + 2\mathbb{Z}$. Let $\epsilon > 0$. We take N such that $\frac{1}{2^N} < \epsilon$. Now let $x, y \in 2\mathbb{Z} + 1$, and take $\delta > 0$ such that

$$|x - y|_2 \leq \frac{1}{2^N} < 2^{-(N-1)} = \delta.$$

Then $x - y \in 2^N\mathbb{Z}$, so $x = y + 2^N A$ for some $A \in \mathbb{Z}$. So

$$|\langle g\rangle^y - \langle g\rangle^x|_2 = |\langle g\rangle^y - \langle g\rangle^{y+2^N A}|_2 = |\langle g\rangle^y|_2 |1 - \langle g\rangle^{2^N A}|_2 = |\langle g\rangle^{2^N A} - 1|_2.$$

Notice that for $g = 1 + 4M$ with $M \in Z_2$ we have

$$\langle g\rangle^{2^N A} = (1 + 4M)^{2^N A} = 1 + 2^N A(4M) + \frac{2^N A(2^N A - 1)}{2}(4M)^2 + \ldots + (4M)^{2^N A},$$

and all terms except the first are in $2^{N+1}\mathbb{Z}_2$. So $|\langle g\rangle^{2^N A} - 1|_2 \leq 2^{-(N+1)} < 2^{-N} < \epsilon$.
So $\langle g\rangle^x$ is uniformly continuous on $1 + 2\mathbb{Z}$. Since $\langle g\rangle^{-1+c}$ and $-\langle g\rangle^{-1+c}$ are constants, both $F_0(x)$ and $F_1(x)$ are uniformly continuous on $1 + 2\mathbb{Z}_2$ as well by interpolation.

Now we have that for fixed $c \in \mathbb{Z}$ and $g \in \mathbb{Z}_2^\times$, $g^{x-1+c} = \omega(g)^{x-1+c}\langle g\rangle^{x-1+c}$. If $g \in 1+4\mathbb{Z}_2$ then $g^{x-1+c} = 1^{x-1+c}\langle g\rangle^{x-1+c} = \langle g\rangle^{x-1+c}$. If $g \in 3 + 4\mathbb{Z}_2$, then $g^{x-1+c} = (-1)^{x-1+c}\langle g\rangle^{x-1+c}$. Since $(-1)^2 = 1$, we have two cases. Suppose $x-1+c \equiv 0 \pmod 2$. Then $(-1)^{x-1+c} = 1$ and $g^{x-1+c} = \langle g\rangle^{x-1+c}$. If $x - 1 + c \equiv 1 \pmod 2$, then $(-1)^{x-1+c} = -1$ and $g^{x-1+c} = -\langle g\rangle^{x-1+c}$. So we have two equations for $f(\cdot, c) = g^{x-1+c}$. For $g \in 1+4\mathbb{Z}_2$ or $g \in 3+4\mathbb{Z}_2$ and $x-1+c \equiv 0 \pmod 2$

$$F_0(x) = \langle g\rangle^{x-1+c}.$$

Otherwise (when $g \in 3 + 4\mathbb{Z}_2$ and $x - 1 + c \equiv 1 \pmod 2$),

$$F_1(x) = -\langle g \rangle^{x-1+c}.$$

□

We have thus shown that we can interpolate our function $f(\cdot, c) \equiv g^{x-1+c} - x \pmod{p^e}$. Since our goal is to count solutions, we find that we can form a power series to conduct further analysis of the function, where we use Hensel's lemma to discuss how our function is able to "lift" from solutions modulo p to solutions modulo p^e. We use the generalizations of Hensel's lemma from [5, Section 3] in our analysis. The reader will see use of Hensel's lemma throughout Section 5 in finding the number of solutions modulo p^e from those modulo p.

5 Counting solutions

Now that we have interpolated our functions, we can count solutions and use this knowledge to tell us about the number of solutions in the original Welch Equation. We first do this when c is constant, then look at (x, c) pair solutions, and finally discuss the case when c is constant and $p = 2$.

5.1 Treating c as a fixed constant

When we fix c and look only at counting solutions to $f(\cdot, c)$, we find that there are a clear number of solutions in a given range of x. The following theorems work toward this result.

In the proof of the following theorem, we use the p-adic log and exp functions. They are defined as

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \quad |x|_p < p^{-1/(p-1)},$$

$$\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1} x^n}{n}, \quad |x|_p < 1.$$

It is important to note that for x where everything is defined, $\exp(\log(1 + x)) = 1 + x$ and $\log(\exp(x)) = x$. For more on these functions, see [2, Section 4.5].

Theorem 19. *For $p \neq 2$, let $g \in \mathbb{Z}_p^\times$ be fixed (and again let m be the multiplicative order of g modulo p). Then for each $x_0 \in \mathbb{Z}/m\mathbb{Z}$, there is exactly one solution to the equation*

$$\omega(g)^{x_0} \langle g \rangle^{x-1+c} = x$$

for $x \in \mathbb{Z}_p$.

Proof. Similarly to the proof found in [5, Section 4], we start by finding solutions modulo p. Since $\langle g\rangle \equiv 1 \pmod{p}$, we now have

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

We fixed g and x_0, so this clearly has exactly one solution.

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

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

where from [2, Proposition 4.5.9], we know that $\log(\langle g\rangle) \in p\mathbb{Z}_p$. Now that we have a convergent power series since $|\log(\langle g\rangle)^i/i!|_p \to 0$ as $i \to \infty$ [7, Chapter 2, Theorem 3.1], we examine $f(\cdot, c) = F_{x_0}(x) - x$ and its derivative to see if we can apply a generalization of Hensel's lemma.

We let $a \in \{0, 1, \ldots, p-1\}$ such that $a \equiv \omega(g)^{x_0} \pmod{p}$ and let

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

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

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

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

Additionally, we have that

$$f'(\cdot, c) = (\omega(g)^{x_0}\langle g\rangle^{c-1})(\log(\langle g\rangle) + x\log(\langle g\rangle)^2 + x^2\log(\langle g\rangle)^3/2! + ...) - 1$$

so that

$$f'(a, c) = (\omega(g)^{x_0}\langle g\rangle^{c-1})(\log(\langle g\rangle) + a\log(\langle g\rangle)^2 + ...) - 1 \equiv -1 \not\equiv 0 \pmod{p},$$

which is also convergent [2, Proposition 4.4.4]. Now we know we can apply a generalization of Hensel's lemma [5, Corollary 3.3], which states that there is a unique $x \in \mathbb{Z}_p$ for which $x \equiv a \pmod{p}$ and $f(x, c) = 0$ in $\mathbb{Z}_p$.

□

Corollary 20. *For odd prime p, let $g \in \mathbb{Z}$ be fixed where $p \nmid g$. Then there are exactly m solutions to the congruence*

$$g^{x-1+c} \equiv x \pmod{p^e}$$

for $x \in \{1, 2, \ldots, p^e m\}$. These solutions are also all distinct modulo m and relatively prime to p.

Proof. Theorem 19 implies that for each $x_0 \in \mathbb{Z}/m\mathbb{Z}$ there is exactly one $x_1 \in \mathbb{Z}/p^e\mathbb{Z}$ where

$$\omega(g)^{x_0} \langle g \rangle^{x_1 - 1 + c} \equiv x_1 \pmod{p^e}.$$

The Chinese Remainder Theorem states that there will be exactly one $x \in \mathbb{Z}/p^e m\mathbb{Z}$ where $x - 1 + c \equiv x_0 \pmod{m}$ and $x \equiv x_1 \pmod{p^e}$. Since $x - 1 + c \equiv x_0 \pmod{m}$, we know that for this x,

$$g^{x-1+c} = \omega(g)^{x_0} \langle g \rangle^{x-1+c} \equiv x \pmod{p^e}.$$

Since for each x_0 there is exactly one such x, we have exactly m solutions to the congruence. Note that, as stated in the introduction, x must be a unit modulo p since g is a unit, and thus all solutions x are relatively prime to p.

□

Furthermore, we can extend our knowledge of the number of solutions to a larger range of x.

Proposition 21. *For an odd prime p, let $g \in \mathbb{Z}$ be fixed such that $p \nmid g$, and let $k \in \mathbb{Z}$. Then there are exactly km solutions to the congruence*

$$g^{x-1+c} \equiv x \pmod{p^e} \tag{3}$$

for $x \in \{1, 2, \ldots, p^e km\}$, each x relatively prime to p. Note that the order of g modulo p must always divide $p - 1$, so when $k = \frac{p-1}{m}$ there are $p - 1$ solutions for $x \in \{1, 2, \ldots, (p-1)p^e\}$.

Proof. From Theorem 2, we notice that

$$g^{x-1+c+mp^e} - (x + mp^e) \equiv g^{x-1+c} - x \pmod{p^e}.$$

So we know that $g^{x-1+c} \equiv x \pmod{p^e}$ has the same number of solutions for $x \in \{1, 2, \ldots, p^e m\}$ as it does for $x \in \{k_1 m+1, k_1 m+2, \ldots, k_1 m+p^e m\}$ for any $k_1 \in \mathbb{Z}$. Since $\{1, 2, \ldots, kp^e m\} = \{1, 2, \ldots, p^e m\} \cup \{p^e m+1, p^e m+2, \ldots, 2p^e m\} \cup \ldots \cup \{(k-1)p^e m+1, (k-1)p^e m+2, \ldots, kp^e m\}$, and we know that there are m solutions for $x \in \{1, 2, \ldots, p^e m\}$ from Corollary 20, then the number of solutions for $x \in \{1, 2, \ldots, p^e km\}$ is equal to km, and each solution x is relatively prime to p since g is a unit.

□

5.2 Treating both x and c as variables

As we begin to look at both variables in our equation, there is an added complexity. However, our results in the following theorems are just as nice as those for fixed c.

In this case, it is important to note that one difficulty with the Welch equation is to ensure that the domains of x and c modulo p will scale nicely modulo p^e. A key problem is that we cannot predict how the multiplicative order of g modulo p changes when g is considered modulo p^e. Generally, the multiplicative order of g modulo p^e is simply $p^{e-1} \cdot \mathrm{ord}_p(g)$. When this happens, we can predict the exact period [Theorem 1].

However, it is not always the case that the multiplicative order of g modulo p^e is $p^{e-1}\operatorname{ord}_p(g)$. Sometimes, the multiplicative order of g modulo p^e is equal to the multiplicative order of g modulo p^{e-1}.

Example 2. Let $p = 11$ and $g = 3$. Let $e = 1$, and take powers of g as follows: $3^1 \equiv 3 \pmod{11}$, $3^2 \equiv 9 \pmod{11}$, $3^3 \equiv 5 \pmod{11}$, $3^4 \equiv 4 \pmod{11}$, $3^5 \equiv 1 \pmod{11}$. Thus, the multiplicative order of 3 modulo 11 is 5.

Now take $e = 2$, and take powers of g as before. Observe that $3^5 \equiv 1 \pmod{11^2}$. Thus, the multiplicative order of 3 modulo 11^2 is 5.

When the multiplicative orders are equal, the exact period of c modulo p^e is shorter than we expect. To account for such a problem we have the following remark followed by a theorem.

Remark 1. Let p be an odd prime, and fix g. Consider $a \in \mathbb{Z}$. Then $\log_g(a)$ may or may not exist.

Theorem 22. *Let p be an odd prime. Given a fixed x, the number of solutions, c, to $g^{x-1+c} \equiv x \pmod{p^e}$ for $c \in \{1, 2, \ldots, m \cdot p^{e-1}\}$ is either $\frac{mp^{e-1}}{\operatorname{ord}_{p^e}(g)}$ when $\log_g(a)$ exists or 0 when $\log_g(a)$ does not exist.*

Proof. Let $x \equiv a \pmod{p^e}$, and by Remark 1 we note that there are two cases: when $\log_g(a)$ exists, and when $\log_g(a)$ does not exist. Now if $\log_g(a)$ exists then we obtain

$$\begin{aligned} g^{a-1+c} &\equiv a \pmod{p^e} \\ a - 1 + c &\equiv \log_g(a) \pmod{\operatorname{ord}_{p^e}(g)} \\ c &\equiv (\log_g(a)) - a + 1 \pmod{\operatorname{ord}_{p^e}(g)}. \end{aligned} \tag{4}$$

Thus, when $\log_g(a)$ exists, we can solve equation 4 modulo $\operatorname{ord}_{p^e}(g)$, since we are looking at values for $c \in \{1, 2, \ldots, mp^{e-1}\}$. There will be a solution for c every multiple of $\operatorname{ord}_{p^e}(g)$. Hence, the number of possible values for c is $\frac{mp^{e-1}}{\operatorname{ord}_{p^e}(g)}$.

When $\log_g(a)$ does not exist, we are not able to solve for c in equation 4. For this case, we are not able to find c. Thus, the number of possible values for c is 0. □

Now we try to count the number of (x, c) pairs of solutions modulo p^e. Proposition 23 gives the number of pairs of solutions modulo p. Theorem 26 gives the number of pairs of solutions modulo p^e by using a multivariable Hensel's lemma from [5, Proposition 3.4] together with the Chinese Remainder Theorem.

Definition 1. We let T_e denote the set of solution pairs (x, c), where $x \in \{1, 2, \ldots, mp^e\}$ and $c \in \{1, 2, \ldots, mp^{e-1}\}$, $p \nmid x$ to the equivalence

$$g^{x-1+c} \equiv x \pmod{p^e}.$$

Also, let $|T_e|$ denote the number of solution pairs (x, c) modulo p^e in the set T_e.

Proposition 23. *Let p be an odd prime. Then $|T_1| = m^2$ for $x \in \{1, 2, \ldots, mp\}$, and for $c \in \{1, 2, \ldots, m\}$.*

Proof. Consider $f(x, c) = g^{x-1+c} - x$. We first want to find the number of solutions modulo p, where $f(x, c) \equiv 0 \pmod{p}$. From Theorem 11 we know that the size of the value set, $V = \{f(p, c) \pmod{p} \mid 1 \leq c \leq m\}$ gives us the number of (x, c) solutions for $x \in \{1, 2, \ldots, p\}$. We know that the elements in V are unique because they are simply powers of g, as shown in Lemma 10. So, there will be m unique values of $x \in V$.

Expand the range to $x \in \{1, 2, \ldots, p, p+1, \ldots, m \cdot p - 1, m \cdot p\}$. Since we are concerned with solutions pairs of x and c, we need to ensure that the solution pairs do not repeat after expanding our range of x.

Consider values of x such that $x_0 \equiv x_1 \ldots \equiv x_n$, and that are defined such as in Theorem 7. Further, Theorem 7 implies that each x_i will get a unique value of c_i, so that for all (x_i, c_i) solution pairs, $c_i \neq c_j$. We know this because of periodicity of c. In particular, there will be m different values of c that correspond to m different multiples of x. So when we expand the range of x to $\{1, 2, \ldots, p, p+1, \ldots, m \cdot p - 1, m \cdot p\}$, number of unique solutions will increase by a multiple of m. Thus $|T_1| = m^2$.

□

Lemma 24. *Let p be an odd prime, and consider a fixed $x_0 \in \mathbb{Z}/m\mathbb{Z}$, and $g \in \mathbb{Z}_p$, $p \nmid g$. Consider the function $f(x, c) = \omega(g)^{x_0} \langle g \rangle^{x-1+c} - x$, and let*

$$|N_1| = |\{(\bar{x}, \bar{c}) \in (\mathbb{Z}_p/p\mathbb{Z}_p)^\times \times (\mathbb{Z}_p/p\mathbb{Z}_p)) \mid f(x, c) \equiv 0 \pmod{p}\}|.$$

Then $|N_1| = p$.

Proof. Consider the power series representation of the function, $f(x, c)$

$$\begin{aligned} f(x, c) &= \omega(g)^{x_0} \langle g \rangle^{x-1+c} - x \\ &= \omega(g)^{x_0} \exp((x - 1 + c) \log \langle g \rangle) - x \\ &= \omega(g)^{x_0} (1 + (x - 1 + c) \log(\langle g \rangle) + (x - 1 + c)^2 \log(\langle g \rangle)/2! \\ &\quad + \text{ higher-order terms in powers of} \log(\langle g \rangle)) - x \\ &\equiv \omega(g)^{x_0} - x \pmod{p}. \end{aligned}$$

Similarly to Theorem 19, we observe that if $f(x, c) \equiv 0 \pmod{p}$, then $\omega(g)^{x_0} \equiv x \pmod{p}$. Since x_0 and g are fixed, and c is free to be anything, there will be p solutions to this equation. Thus, $|N_1| = p$.

□

Proposition 25. *Let p be an odd prime, $g \in \mathbb{Z}_p$, $p \nmid g$, and consider a fixed $x_0 \in \mathbb{Z}/m\mathbb{Z}$. Consider the function $f(x, c) = \omega(g)^{x_0} \langle g \rangle^{x-1+c} - x$, and let*

$$|N_e| = |\{(\bar{x}, \bar{c}) \in (\mathbb{Z}_p/p^e\mathbb{Z}_p)^\times \times (\mathbb{Z}_p/p^e\mathbb{Z}_p)) \mid f(x, c) \equiv 0 \pmod{p^e}\}|.$$

Then

$$|N_e| = p^{e-1}|N_1|.$$

Proof. First recall that we can expand the function, $f(x,c)$ as

$$\begin{aligned} f(x,c) &= \omega(g)^{x_0} \langle g \rangle^{x-1+c} - x \\ &= \omega(g)^{x_0}(1 + (x-1+c)\log(\langle g \rangle) + (x-1+c)^2 \log(\langle g \rangle)/2! \\ &\quad + \text{ higher-order terms in powers of} \log(\langle g \rangle)) - x \\ &\equiv \omega(g)^{x_0} - x \pmod{p}. \end{aligned}$$

Now, we consider the partial derivatives of $f(x,c)$ where we note that $\log \langle g \rangle \equiv 0 \pmod{p}$, since $\langle g \rangle \equiv 1 \pmod{p}$, thus obtaining

$$\begin{aligned} \frac{\partial f}{\partial x}(x,c) &= \omega(g)^{x_0}(\exp((x-1+c)\log \langle g \rangle) \cdot \log \langle g \rangle) - 1 \\ &\equiv -1 \pmod{p}, \text{ and} \\ \frac{\partial f}{\partial c}(x,c) &= \omega(g)^{x_0}(\exp((x-1+c)\log \langle g \rangle) \cdot \log \langle g \rangle) \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Observe that $\frac{\partial f}{\partial x}(x,c) \not\equiv 0 \pmod{p}$. Thus, we can apply a multivariable version of Hensel's lemma [5, Proposition 3.4] to observe that there are p^{e-1} possible ways to lift each solution modulo p to a solution modulo p^e.

Thus, $|N_e| = p^{e-1}|N_1|$. □

Theorem 26. *Let p be an odd prime, and fix g where $p \nmid g$. Then $|T_e| = p^{e-1}|T_1| = m^2 p^{e-1}$ is the number of solutions to the congruence*

$$g^{x-1+c} \equiv x \pmod{p^e}$$

for (x,c) such that $x \in \{1, 2, \ldots, mp^e\}$, and $c \in \{1, 2, \ldots, mp^{e-1}\}$. Further the set of x that solve this equation are all distinct modulo p^e.

Proof. We are going to count the solution pairs (x,c) modulo mp^e by counting pairs of (x_0, c_0) modulo m and (x_1, c_1) modulo p^e. Then we will combine them into (x,c) using the Chinese Remainder Theorem.

Here x_0 is defined by interpolation in Section 4. So we have the solution pair (x_0, c_0) modulo m which solves $g^{x-1+c_0} = \omega(g)^{x_0} \langle g \rangle^x \equiv x \pmod{p^e}$. From this, we can obtain the following equivalences

$$\begin{aligned} x - 1 + c_0 &\equiv x_0 \pmod{m} \\ x &\equiv x_0 + 1 - c_0 \pmod{m}. \end{aligned} \tag{5}$$

Now let (x_1, c_1) modulo p^e be the solution pair to $g^{x_1+1-c_1} \equiv x_1 \pmod{p^e}$. Putting (x_0, c_0) and (x_1, c_1) together, both pairs should be a solution to

$$g^{x_0+1-c_0} \equiv x_1 \pmod{p^e}. \tag{6}$$

So we will find the number of x and c that are solutions to equation 6. First consider x. We have equation 5 and $x \equiv x_1 \pmod{p^e}$. By the Chinese Remainder Theorem, there will be exactly one $x \in \mathbb{Z}/p^e m\mathbb{Z}$ for each combination of x_0 and x_1.

Next we consider c. We will obtain values of c that satisfy the following two equations: $c \equiv c_0 \pmod{m}$ and $c \equiv c_1 \pmod{p^e}$. Again by the Chinese Remainder Theorem, there will be exactly one $c \in \mathbb{Z}/p^e m\mathbb{Z}$ for each combination of c_0 and c_1.

Here we note that there are m possible choices of x_0 and m possible choices of c_0. Proposition 25 and Lemma 24 show that there are $p \cdot p^{e-1}$ choices for (x_1, c_1) modulo p^e. So the combinations of x_0, c_0 modulo m and (x_1, c_1) pairs modulo p^e will yield $m^2 p^e$ solutions for $x \in \{1, 2, \ldots, mp^e\}$, and $c \in \{1, 2, \ldots, mp^e\}$.

Notice that the domain of c is not the size that we want. We produced values of $c \in \{1, \ldots, mp^{e-1}, \ldots, mp^e\}$ but we want $c \in \{1, \ldots, mp^{e-1}\}$. However by Theorem 1 we know that the period of c is length mp^{e-1}. Thus, we can divide mp^e by p. Hence, we obtain $|T_e| = m^2 p^{e-1}$.

□

5.3 Considering $p = 2$

Now that we have seen what the results of counting solutions to the Welch equation are for odd p, we will explore the number of solutions when $p = 2$. Recall that we use a different interpolation for $p = 2$. Before we move ahead, we will look at solutions modulo 2.

Lemma 27. *For fixed $c \in \mathbb{Z}$ and $g \in 2\mathbb{Z} + 1$, all solutions $x \in \mathbb{Z}$ to the equation $f(\cdot, c) = g^{x-1+c} \equiv x \pmod{2^e}$ are odd.*

Proof. Let $g \in 2\mathbb{Z} + 1$ and $c \in \mathbb{Z}$ be fixed.

$$\begin{aligned} g^{x-1+c} - x &\equiv 0 \pmod{2^e} \\ g^{x-1+c} - x &\equiv 0 \pmod{2}. \end{aligned}$$

Since g is odd, g^{x-1+c} is also odd for $x - 1 + c \in \mathbb{Z}$. Then $g^{x-1+c} \equiv 1 \pmod{2}$ and we get

$$\begin{aligned} 1 - x &\equiv 0 \pmod{2} \\ x &\equiv 1 \pmod{2}. \end{aligned}$$

So all integer solutions x are odd. □

Theorem 28. *For $p = 2$, let $c \in \mathbb{Z}$ and $g \in \mathbb{Z}_2^\times$ be fixed. Then there is exactly one solution to each of the equations*

$$\langle g \rangle^{x-1+c} = x$$

and

$$-\langle g \rangle^{x-1+c} = x$$

for $x \in 1 + 2\mathbb{Z}_2$.

Proof. As with the analogous proof for odd primes, we start by finding solutions modulo $p = 2$. Since $\langle g\rangle \equiv 1 \pmod 2$, both equations reduce to

$$1 \equiv x \pmod 2.$$

This expression clearly has exactly one solution, and note that this expression agrees with Lemma 27.

Since we know that $\langle g\rangle$ is in $1 + 4\mathbb{Z}_2$, we have that

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

where we know that $\log(\langle g\rangle) \in 4\mathbb{Z}_2$ [2, Proposition 4.5.9]. Now we have a convergent power series since $|\log(\langle g\rangle)^i/i!|_2 \to 0$ as $i \to \infty$ [7, Chapter 2, Theorem 3.1], and we will look at $f(\cdot, c)$ and its derivative to see if we can apply Hensel's lemma.

To count solutions to $F_0(x) \equiv \langle g\rangle^{x-1+c} \equiv x$, we let $a = 1$, and let

$$\begin{aligned}f(\cdot, c) = F_0(x) - x = \langle g\rangle^{c-1}(1 &+ x\log(\langle g\rangle) + x^2\log(\langle g\rangle)^2/2!\\ &+ \text{higher order terms in powers of } \log(\langle g\rangle)) - x.\end{aligned}$$

Then we have

$$\begin{aligned}f(a, c) &\equiv (1)(1 + 1(0) + 1^2(0)\\ &\quad + \text{higher order terms equivalent to } 0 \pmod 2\ ) - 1 \pmod 2\\ &\equiv 1 - 1 \equiv 0 \pmod 2.\end{aligned}$$

Also, since we know $\log(\langle g\rangle) \in 4\mathbb{Z}_2$, $\log(\langle g\rangle) \equiv 0 \pmod 2$, and we have

$$f'(\cdot, c) = \langle g\rangle^{c-1}(\log(\langle g\rangle) + x\log(\langle g\rangle)^2 + x^2\log(\langle g\rangle)^3/2! + ...) - 1, \text{ and}$$

$$f'(a, c) = \langle g\rangle^{c-1}(\log(\langle g\rangle) + \log(\langle g\rangle)^2 + ...) - 1 \equiv -1 \not\equiv 0 \pmod 2,$$

which is also convergent [2, Proposition 4.4.4]. Now we know we can apply a generalization of Hensel's lemma [5, Corollary 3.3], which states that there is a unique $x \in \mathbb{Z}_2$ for which $x \equiv 1 \pmod p$ and $f(x) = 0$ in $\mathbb{Z}_2$.

Note that similar steps can be used to show there is one solution in $\mathbb{Z}_2$ to $F_1(x) \equiv -\langle g\rangle^{x-c+1} \equiv x$ as well.

□

Corollary 29. *For $p = 2$, let $g, c \in \mathbb{Z}$ be fixed. Then there is exactly 1 solution to the congruence*

$$g^{x-1+c} \equiv x \pmod{2^e}$$

for $x \in \{1, 2, \ldots, 2^e\}$.

Proof. Having determined that x is odd by Lemma 27, we know that $x-1+c \equiv 1-1+c \equiv c \pmod 2$. Because c is fixed and our functions $F_0(x)$ and $F_1(x)$ are defined on $x \in 1+2\mathbb{Z}_2$, we only need to count solutions to $F_1(x)$ if $\langle g \rangle \in 3+4\mathbb{Z}_2$ and c is odd and $F_0(x)$ otherwise. The number of solutions where x is odd in the correct equation will be the same as the number of solutions to $f(\cdot, c)$.

Theorem 28 implies that there is exactly one $x \in 1+2\mathbb{Z}_2$ in the appropriate function $F_0(x)$ or $F_1(x)$ that we have chosen based on c. Note that since each lifting in the proof is equivalent to 1 modulo 2, we know $f(\cdot, c)$ and $f'(\cdot, c)$ are still defined, and $x-1+c$ is still equivalent to c, we can use the same function after each lift. So we get the unique solution to our congruence, $g^{x-1+c} \equiv x \pmod{2^e}$.

□

6 Conclusion

Most of the previous analysis on the Welch equation, $g^{x-1+c} \equiv x \pmod{p^e}$, has looked at solutions only modulo p and for $x \in \{1, 2, \ldots, p\}$, and the conclusions about the number of solutions on this range are mainly statistical [1]. We have found here that there are clear patterns for this equation modulo p^e when we extend the range of x to $x \in \{1, 2, \ldots, p^e m\}$, where m is the order of g modulo p. Specifically, there are always m solutions (for all primes) on this range when we fix c, and $m^2 p^{e-1}$ solutions (for odd primes) when we consider $c \in \{0, 1, \ldots, p^{e-1}m\}$ as an additional variable. If we can find how these solutions are distributed on subintervals of length p^e, we may have a better understanding of what happens on the original range of x from 1 to p^e.

The value set described in Theorem 11 (i.e. $f(p, c) \equiv g^{p-1+c} - p \pmod p$) also helps us find which values of x in the range from 1 to p are solutions modulo p. This is especially helpful in the cases where g is not a primitive root, since there is a smaller value set that restricts the values of x that may be a solution.

Finally, there are several other patterns found in analyzing the function $f(\cdot, c) \equiv g^{x-1+c} - x \pmod{p^e}$ that are left unexplored in this paper, such as the appearance of p pairs of "doubles," where $f(x, c) \equiv f(x+1, c) \pmod{p^e}$ when g is a primitive root, whose investigation may help with understanding the distribution of solutions.

References

[1] Konstantinos Drakakis, *Three Challenges in Costas Arrays*, Ars Combinatoria **89** (2008), 167–182.

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

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

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

[5] 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.

[6] Scott Rickard, *Open Problems in Costas Arrays*, Proceedings of the 7th IMA International Conference on Mathematics of Signal Processing, 2006. `http://ima.org.uk/_db/_documents/Rickard_2.pdf`.

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