Counting Solutions to the Welch Equation: $g^{x-1+c} \equiv x \pmod{p^e}$

Adelyn Yeoh

Department of Mathematics and Statistics, Mount Holyoke College

Introduction

The Welch function $x \to g^{x-1+c}$ is similar to the discrete exponential function $x \to g^x$, which is used in the ElGamal signature scheme. Counting fixed points of the Welch function could give a benchmark of the difficulty in finding the inverse, which is thought to be computationally intractable in cryptography.

Dissecting the problem

- Study the fixed points of $g^{x-1+c} \equiv x \pmod{p^e}$ (call it the Welch equation)
- Change the equation into this function: $f(x,c) \equiv g^{x-1+c} - x$
- Identify (x,c) pairs in modulo p where $f(x,c) \equiv 0 \pmod{p}$
- Use Hensel's lemma to count solution pairs in modulo p^e

Repetition of function $f(x,c)$

Theorem 1. *Consider $f(x,c) = g^{x-1+c} - x$, where $c \in \mathbb{Z}$, and p is an odd prime. Take $m = \mathrm{ord}_p(g)$. Fix x, then $f(x,c) \equiv f(x, c+mp^{e-1}) \pmod{p^e}$.*

Theorem 2. *Consider $f(x,c) = g^{x-1+c} - x$, where $x \in \mathbb{Z}$, and p is an odd prime. Take $m = \mathrm{ord}_p(g)$. Fix c, then $f(x,c) \equiv f(x+mp^e, c) \pmod{p^e}$.*

Unique c

Lemma 3. *Let p be an odd prime, and g be a primitive root of p^e. Then for each $x \in \{1,2,\dots,p^e\} \backslash \{p, 2p, \dots, p^e\}$ there exists a unique value of $c \in \{1,2,\dots,p^{e-1}(p-1)\}$ that is a solution to $g^{x-1+c} \equiv x \pmod{p^e}$.*

Primitive roots vs. Non-primitive roots

Primitive Roots

Let $p=7, g=5$, and so $m = \mathrm{ord}_7(5) = 6$

$1 \le x \le p$	**Solutions**	$[f(x,c) : 1 \le c \le m]$
1	1	[4, 3, 5, 1, 2, 0]
2	1	[2, 4, 0, 1, 6, 3]
3	1	[3, 6, 0, 5, 2, 1]
4	1	[5, 6, 4, 1, 0, 2]
5	1	[5, 3, 0, 6, 1, 4]
6	1	[2, 6, 5, 0, 3, 4]
7	0	[5, 4, 6, 2, 3, 1]

Non-Primitive Roots

Let $p=7, g=2$, and so $m = \mathrm{ord}_7(2) = 3$

$1 \le x \le p$	**Solutions**	$[f(x,c) : 1 \le c \le m]$
1	1	[1, 3, 0]
2	1	[2, 6, 0]
3	0	[5, 6, 1]
4	1	[5, 0, 4]
5	0	[6, 3, 4]
6	0	[2, 3, 5]
7	0	[2, 4, 1]

Pathway to the main result

- Theorems 1 and 2 tell us that we can restrict the domain of c when we fix x, and vice versa.
- Theorem 3 tells us that we need to find the values of x that have solutions, so we can find an associated c.
- When g is not a primitive root modulo p, it is difficult to predict values of x which have solutions modulo p (see example above). The trick is to construct this set: $\{f(p,c) \pmod{p} : 1 \le c \le m\}$. From this we have the Value Set Theorem.

Main Result: m^2p^{e-1} pairs of solutions

Theorem 4. *Let p be an odd prime, and let $g \in \{1,2,\dots,p-1\}$. Take $m = \mathrm{ord}_p(g)$. Then for $x \in \{1,2,\dots,mp^e\}$, and for $c \in \{1,2,\dots,mp^{e-1}\}$, the number of (x,c) pairs of solutions to $g^{x-1+c} \equiv x \pmod{p^e}$ is m^2p^{e-1}.*

Proof of main result.

First we find the number of solutions modulo p. From the Value Set Theorem we see that the number of solutions modulo p will be m, if $x \in \{1,2,\dots,p\}$. Extend the domain of x to $\{1,2,\dots,p,p+1,\dots,mp\}$, then the number of solutions will increase by a multiple of m. So the number of solutions modulo p is m^2.

We expand the expression for $f(x,c)$ using a power series and check its partial derivatives. It turns out that at least one of the partial derivaties is non-zero modulo p. Now we use a multivariable Hensel's Lemma and observe that there are p^{e-1} possible ways to lift each solution modulo p to a solution modulo p^e. Thus, there will be m^2p^{e-1} pairs of of solutions. □

Value set

Theorem 5. (Value Set Theorem) *Let p be an odd prime, fix g and let $m = \mathrm{ord}_p(g)$. Consider all $x \in \{f(p,c) \pmod{p} : 1 \le c \le m\}$. Then a solution c' exists, which solves $g^{x-1+c'} \equiv x \pmod{p}$.*

Other patterns

In the process of counting solutions, we were able to predict other results such as:

- If g is a primitive root, one solution pair is: $(x,c) = \left(p^e - 1, \frac{p^{e-1}(p-3)+4}{2}\right)$
- If (x,c) solves $g^{x-1+c} \equiv x \pmod{p^e}$ where g is a primitive root, then we can predict the solution to $(g^{-1})^{x-1+c} \equiv x \pmod{p^e}$

Conclusion

Theorems 1 and 2 helps us understand how to construct the domains of x and c. The Value Set Theorem helps us identify the solutions modulo p for the stated domains. However, it is not easy to determine the solution pairs in an arbitrary domain of x or c. By using these fixed domains, the number of solutions modulo p^e will always be m^2p^{e-1}.

Acknowledgements

The author would like to thank Mount Holyoke College for funding her summer REU project, and Professor Joshua Holden and Professor Margaret Robinson for their guidance and patience throughout this research.