Discrete Lambert Map $xg^x \equiv c \pmod{p^e}$

Anne Waldo '15 and Caiyun Zhu '15

Mathematics and Statistics Department of Mount Holyoke College

Introduction

- A **discrete logarithm** is an integer x solving the equation $g^x \equiv c \pmod{p}$
- Finding discrete logarithms for large primes is called the **Discrete Logarithm Problem (DLP)**
- Solving the DLP is thought to be difficult and is used as the basis for some forms of public-key cryptography
- The ElGamal Digital Signature Scheme is one such scheme
- One way to forge a signature is to manipulate the ElGamal algorithm and solve for x in $xg^x \equiv c \pmod{p}$ - referred to as the **Discrete Lambert Problem (DWP)**
- The DWP is thought to be more difficult than the DLP
- Due to its implications on the security of the ElGamal scheme we believe that it is important to study the DWP

Approach

- Counting solutions to $xg^x \equiv c \pmod{p^e}$ for fixed c and g and $x \in \{1, \ldots, p^e\}$ seems extremely difficult
- It is much easier to count the number of solutions for a wider range of x
- We also looked at patterns in the solutions that can give us insight into the DWP

Counting Solutions

Theorem 1. *If p is an odd prime, g is an generator modulo p, and $c \not\equiv 0 \pmod{p}$, then for fixed g and c, the solution set for the equation*

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

forms a Complete Residue System modulo $p-1$, for $x \in \{1, \ldots, p^e(p-1)\}$ and $p \nmid x$.

Proposition 2. *Let p be an odd prime and $m = \mathrm{ord}_p(g)$. For fixed g and c such that $p \nmid g$ and $p \nmid c$, if we consider the function*

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

where $x \in \{1, \ldots, p^e m \mid x \not\equiv 0 \mod p\}$, then the number of x such that $f(x) \equiv 0 \pmod{p^e}$ is equal to m.

Example. ($p = 7$, $e = 1$)

$g = 3$, $m = 6$

c	x	# solutions
1	$\{16, 17, 19, 27, 32, 36\}$	6
2	$\{4, 8, 30, 31, 33, 41\}$	6
3	$\{1, 23, 24, 26, 34, 39\}$	6
4	$\{2, 3, 5, 13, 18, 22\}$	6
5	$\{9, 10, 12, 20, 25, 29\}$	6
6	$\{6, 11, 15, 37, 38, 40\}$	6

$g = 2$, $m = 3$

c	x	# solutions
1	$\{2, 4, 15\}$	3
2	$\{1, 9, 11\}$	3
3	$\{3, 19, 20\}$	3
4	$\{8, 16, 18\}$	3
5	$\{12, 13, 17\}$	3
6	$\{5, 6, 10\}$	3

Some Patterns in the Solutions

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

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

where $x \in \{1, \ldots, p^e m_p \mid x \not\equiv 0 \mod p\}$, then for each c there are m_p solutions, $x_1, \ldots, x_{m_p}$, such that

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

and

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

Example. ($p = 7$, $e = 2$)

$g = 2$, $m_7 = 3$, and $m_{7^2} = 21$

c	x	Sum of x_i	Sum of $x_i \pmod{7^2}$	Sum of $x_i \pmod{21}$
1	$\{15, 46, 86\}$	147	0	0
2	$\{1, 9, 137\}$	147	0	0
3	$\{61, 104, 129\}$	294	0	0
4	$\{79, 81, 134\}$	294	0	0
5	$\{12, 55, 80\}$	147	0	0
6	$\{69, 89, 136\}$	294	0	0

Theorem 4. *Let p be an odd prime and $m = \mathrm{ord}_p(g)$. For fixed g and c such that $p \nmid g$ and $p \nmid c$, if we consider the function*

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

where $x \in \{1, \ldots, p^e m \mid x \not\equiv 0 \mod p\}$, then for any other $c' \in \{1, \ldots, p^{e-1}(p-1)\}$, let $x_{i,c'}$ and $x_{j,c}$ range through the solutions to

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

and

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

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

Example. ($p = 7$, $e = 2$)

$g = 2$, and $m = 3$

c	x	$x \pmod 7$
1	$\{15, 46, 86\}$	$\{1, 2, 4\}$
2	$\{1, 9, 137\}$	$\{1, 2, 4\}$
3	$\{61, 104, 129\}$	$\{3, 5, 6\}$
4	$\{79, 81, 134\}$	$\{1, 2, 4\}$
5	$\{12, 55, 80\}$	$\{3, 5, 6\}$
6	$\{69, 89, 136\}$	$\{3, 5, 6\}$

Existence of a Solution

Proposition 5. *Let p be an odd prime and g be a generator modulo p^e. If $c = \frac{p^e + p^{e-1}}{2}$, then $x = \frac{p^e - p^{e-1}}{2}$ is one of the solutions to the equation*

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

Proof. By hypothesis, we see that

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

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

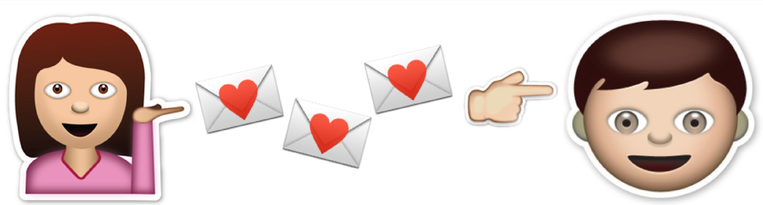
Mutiplicative Order of $p-1$ modulo p^e

Proposition 6. *Let $n \geq 2$ and $n \in \mathbb{Z}^+$. If $\gcd(p, n) = 1$ and p is an odd prime, then*

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

Conclusion

In Theorem 1 and Proposition 2, the multiplicative order of g modulo p is very important in counting the number of solutions to the DWP. In addition, we found a special property of $\sum_{i=0}^{m_p} x_i$ modulo p^e and m_{p^e} in Theorem 3, as well as how the solutions modulo p relate to c in Theorem 4. In Proposition 5, we found that when g is a generator modulo p^e there is a special (x, c) that satisfies the discrete Lambert equation. Finally, we found a formula for the multiplicative order of $p-1$ modulo p^e, seen in Proposition 6.



<waldo22a@mtholyoke.edu, zhu22c@mtholyoke.edu>