Collisions of the Discrete Lambert Map

Yu Liu

MOUNT HOLYOKE

The Discrete Lambert Map

We refer to the map

$$x \mapsto xg^x \pmod p$$

for fixed g as the *Discrete Lambert Map (DLM)*.

- This map is of practical importance because the difficulty of inverting this map plays a significant role in the level of security of the ElGamal Digital Signature Scheme.

Collisions

We call the set of solutions (x, y) that satisfy the equivalence

$$xg^x \equiv yg^y \pmod p$$

collisions of the Discrete Lambert Map. And we give the following definition:

DEFINITION 1. The *multiplicative order* of a modulo p, denoted by $ord_p(a)$, is the smallest positive integer m such that $a^m \equiv 1 \pmod p$, if it exists.

Consider a positive integer g where $p \nmid g$ and let $m = ord_p(g)$. Our goal is to investigate:

- The number of collisions $|C_{L_1}|$ that are solutions to the equivalence
$$xg^x \equiv yg^y \pmod p$$
where x and $y \in \{1, 2, 3, ..., pm\}$, $p \nmid x$ and $p \nmid y$.
- The number of collisions $|C_{L_e}|$ that are solutions to the equivalence
$$xg^x \equiv yg^y \pmod{p^e}$$
where x and $y \in \{1, 2, 3, ..., p^e m\}$, $p \nmid x$ and $p \nmid y$.

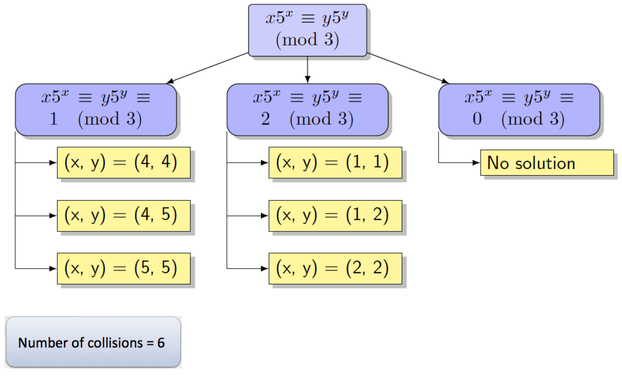
In both cases p is an odd prime, and we do not distinguish between the collision (x, y) and the collision (y, x).

(I). The Number of Collisions Modulo p

Theorem 1. *For an odd prime p and a positive integer g ($p \nmid g$), let $m = ord_p(g)$. Then the number of collisions that are solutions to $xg^x \equiv yg^y \pmod p$ is equal to $|C_{L_1}| = \frac{m(m+1)(p-1)}{2}$ for x and $y \in \{1, 2, 3, ..., pm\}$, $p \nmid x$ and $p \nmid y$.*

Example

The diagram illustrates an example where $p = 3$, $g = 5$ and $m = ord_3(5) = 2$. $x, y \in \{1, 2, 4, 5\}$. The method we use to count the collisions is as follows: if (x, y) is a collision, then $xg^x \equiv yg^y \equiv c \pmod p$ where $c \in \{1, 2, ..., p-1\}$ ($c \neq 0$ since $p \nmid x, p \nmid y$ and $p \nmid g$). For a fixed value of c, there exist m solutions for x and m solutions for y respectively, resulting in $\frac{m(m+1)}{2}$ pairs of (x, y) [1]. For the $(p-1)$ different values of c, we have a total of $\frac{m(m+1)(p-1)}{2}$ collisions.



(II). The Number of Collisions Modulo p^e

We wish to find an approach that will allow us to deduce the number of collisions modulo p^e from the number of collisions modulo p. In order to do this for a fixed $g \in \mathbb{Z}_p$ ($p \nmid g$) and $x_0, y_0 \in \mathbb{Z}/m\mathbb{Z}$, we define by interpolation a function for $x, y \in \mathbb{Z}_p$:

$$f(x, y) = x\omega(g)^{x_0} \langle g \rangle^x - y\omega(g)^{y_0} \langle g \rangle^y.$$

In the function above we write $g = \omega(g) \langle g \rangle$ where $\omega(g)$ is a $(p-1)$st root of unity and $\langle g \rangle = \frac{g}{\omega(g)} \in 1 + p\mathbb{Z}_p$. Note for $x \equiv x_0 \pmod m$ and $y \equiv y_0 \pmod m$ where $m = ord_p(g)$, $f(x, y) = xg^x - yg^y$. This function is uniformly continuous on $\mathbb{Z}_p \times \mathbb{Z}_p$ and always non-singular modulo p, i.e. $\frac{\partial f}{\partial x}(x, y) \not\equiv 0 \pmod p$. Thus using a multivariable Hensel's Lemma, we can lift each solution modulo p to p^{e-1} solutions modulo p^e. Finally, we use the Chinese Remainder Theorem to prove the theorem below:

Theorem 2. *For an odd prime p, there are exactly $|C_{L_e}| = p^{e-1}|C_{L_1}|$ collisions that are solutions to the congruence*

$$xg^x \equiv yg^y \pmod{p^e}$$

for (x, y) such that x and $y \in \{1, 2, \ldots p^e m\}$, $p \nmid x$, $p \nmid y$.

Future Work

In the theorems above we consider p as an odd prime. Further work can be done to study the case where $p = 2$. One could also investigate other properties of the Discrete Lambert Map, one of which is the number of *two-cycles*, which are solution pairs (x, y) that satisfy the equations $xg^x \equiv y \pmod{p^e}$ and $yg^y \equiv x \pmod{p^e}$.

References

[1] Anne Waldo and Caiyun Zhu, *The Discrete Lambert Map*. preprint.

[2] 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.