CS409 Chalk and Talk
Pohlig-Hellman Algorithm

Arnav Bhate (23B3947)   Aviral Vishesh Goel (22B2156)

1 Introduction

Given cyclic group $(\mathbb{G}, q, g)$, the discrete logarithm is defined as

$$\mathrm{Dlog}_g(h) := \text{unique } x \in \mathbb{Z}_q \text{ such that } h = g^x \text{ for each } h \in \mathbb{G}$$

Finding the discrete logarithm is a hard problem in some groups. Many algorithms have been found to find the discrete logarithm of a number in a general group, one of which is the Pohlig-Hellman algorithm.

The algorithm assumes the existence of an algorithm for groups of prime order, with runtime $\mathcal{O}(S_q)$, and then uses it for groups with prime power orders. This algorithm is then used for groups whose order is not a prime power.

2 The Main Algorithm

Let $\mathbb{G}$ be a group, and suppose that we have an algorithm to solve the discrete logarithm problem in $\mathbb{G}$ for any element whose order is a power of a prime. To be concrete, if $g \in \mathbb{G}$ has order q^e, suppose that we can solve $g^x = h$ in $O(S_{q^e})$ steps.
Now let $g \in \mathbb{G}$ be an element of order N, and suppose that N factors into a product of prime powers as

$$N = {q_1}^{e_1} \cdot {q_2}^{e_2} \dots {q_t}^{e_t}$$

Then the discrete logarithm problem $g^x = h$ can be solved in

$$\mathcal{O}\left(\sum_{i=1}^{t} S_{{q_i}^{e_i}} + \log N\right) \text{steps}$$

using the following procedure:

Step 1 - for each $1 \leq i \leq t$, let

$$g_i = g^{N/{q_i}^{e_i}}, h = h^{N/{q_i}^{e_i}}$$

Notice that g_i has prime power order ${q_i}^{e_i}$, so use the given algorithm to solve the discrete logarithm problem

$${g_i}^y = h_i$$

Let $y = y_i$ be a solution to the above equation

Step 2 - Use the Chinese remainder theorem to solve

$$x \equiv y_1 \pmod{{q_1}^{e_1}}, x \equiv y_2 \pmod{{q_2}^{e_2}}, \dots, x \equiv y_t \pmod{{q_t}^{e_t}}$$

3 Proof of the Algorithm

3.1 Time Complexity Analysis

Step 1 - Each discrete logarithm problem takes $\mathcal{O}\left(S_{{q_i}^{e_i}}\right)$ steps to solve, and hence the total time for this step is

$$\mathcal{O}\left(\sum_{i=1}^{t} S_{{q_i}^{e_i}}\right)$$

Step 2 - The runtime of the CRT algorithm with k congruences and moduli up to $\mathcal{O}(N)$ is $\mathcal{O}(k \log N)$

3.2 Proof of convergence

$$x = y_i + {q_i}^{e_i} \cdot z_i \text{ for some } z_i$$

$$\begin{aligned}
(g^x)^{N/{q_i}^{e_i}} &= \left(g^{y_i + {q_i}^{e_i} . z_i}\right)^{N/{q_i}^{e_i}} \\
&= \left(g^{N/{q_i}^{e_i}}\right)^{y_i} \cdot g^{N \cdot z_i} \\
&= {g_i}^{y_i} \\
&= h_i \\
&= h^{N/{q_i}^{e_i}}
\end{aligned}$$

What we have now,

$$\frac{N}{{q_i}^{e_i}} \cdot x \equiv \frac{N}{{q_i}^{e_i}} \cdot \mathrm{Dlog}_g(h) \pmod{N}$$

We can find c_i's such that (Using repeated extended Euclidean Algorithm)

$$\sum_{i=1}^{t} \frac{N}{{q_i}^{e_i}} \cdot c_i = 1$$

$$\sum_{i=1}^{t} \frac{N}{{q_i}^{e_i}} \cdot c_i \cdot x \equiv \sum_{i=1}^{t} \frac{N}{{q_i}^{e_i}} \cdot c_i \cdot \mathrm{Dlog}_g(h) \pmod{N}$$

Input: Two integers a and b
Output: GCD of a and b, and coefficients x and y such that $ax + by = \mathrm{GCD}(a, b)$
Initialize $x_0 \leftarrow 1$, $x_1 \leftarrow 0$, $y_0 \leftarrow 0$, $y_1 \leftarrow 1$;
while $b \neq 0$ **do**
  $q \leftarrow \lfloor a/b \rfloor$ `// Integer division`
  $r \leftarrow a \mod b$;
  $a, b \leftarrow b, r$;
  $(x_0, x_1) \leftarrow (x_1, x_0 - q \cdot x_1)$;
  $(y_0, y_1) \leftarrow (y_1, y_0 - q \cdot y_1)$;
end
return (a, x_0, y_0)

Algorithm 1: Extended Euclidean Algorithm

4 Regarding Groups of Prime Power Order

Theorem 1. *Let $\mathbb{G}$ be a group. Suppose that q is a prime, and suppose that we know an algorithm that takes S_q steps to solve the discrete logarithm problem $g^x = h$ in $\mathbb{G}$ whenever g has order q. Now, let $g \in \mathbb{G}$ be an element of order q^e with $e \geq 1$. Then we can solve the discrete logarithm problem*

$$g^x = h \text{ in } \mathcal{O}\left(eS_q\right) \text{ steps.}$$

Proof. The key idea is to write the exponent in the form

$$x = x_0 + x_1 q + x_2 q^2 + \cdots + x_{e-1} q^{e-1}$$

and then successively determine $x_0, x_1, x_2, \ldots$

Consider the element $g^{q^{e-1}}$. This element is of order q, as

$$\left(g^{q^{e-1}}\right)^q = g^{q^e} = 1$$

Now

$$\begin{aligned} h^{q^{e-1}} &= \left(g^x\right)^{q^{e-1}} \\ &= \left(g^{x_0 + x_1 q + x_2 q^2 + \cdots + x_{e-1} q^{e-1}}\right)^{q^{e-1}} \\ &= \left(g^{q^{e-1}}\right)^{x_0} \cdot \left(g^{q^e}\right)^{x_1 + x_2 q + x_3 q^2 + \cdots + x_{e-1} q^{e-2}} \\ &= \left(g^{q^{e-1}}\right)^{x_0} \end{aligned}$$

Thus,

$$\left(g^{q^{e-1}}\right)^{x_0} = h^{q^{e-1}}$$

This is a discrete logarithm problem and can be solved in $\mathcal{O}\left(S_q\right)$ steps.

Similarly,

$$\begin{aligned} h^{q^{e-2}} &= \left(g^x\right)^{q^{e-2}} \\ &= \left(g^{x_0 + x_1 q + x_2 q^2 + \cdots + x_{e-1} q^{e-1}}\right)^{q^{e-2}} \\ &= \left(g^{x_0}\right)^{q^{e-2}} \cdot \left(g^{q^{e-1}}\right)^{x_1} \cdot \left(g^{q^e}\right)^{x_2 + x_3 q + x_4 q^2 + \cdots + x_{e-1} q^{e-2}} \\ &= \left(g^{x_0}\right)^{q^{e-2}} \cdot \left(g^{q^{e-1}}\right)^{x_0} \end{aligned}$$

Thus,

$$\left(g^{q^{e-1}}\right)^{x_1} = \left(h \cdot g^{-x_0}\right)^{q^{e-2}}$$

Since we already know x_0, this can also be solved in $\mathcal{O}\left(S_q\right)$ steps.

In general, after determining $x_0, \ldots, x_{i-1}$, we can write

$$\begin{aligned} h^{q^{e-i-1}} &= \left(g^x\right)^{q^{e-i-1}} \\ &= \left(g^{x_0 + x_1 q + x_2 q^2 + \cdots + x_{e-1} q^{e-1}}\right)^{q^{e-i-1}} \\ &= \left(g^{x_0 + x_1 q + x_2 q^2 + \cdots + x_{i-1} q^{i-1}}\right)^{q^{e-i-1}} \cdot \left(g^{q^{e-1}}\right)^{x_i} \cdot \left(g^{q^e}\right)^{x_{i+1} + x_{i+2} q + x_{i+3} q^2 + \cdots + x_{e-1} q^{e-i-1}} \\ &= \left(g^{x_0 + x_1 q + x_2 q^2 + \cdots + x_{i-1} q^{i-1}}\right)^{q^{e-i-1}} \cdot \left(g^{q^{e-1}}\right)^{x_0} \end{aligned}$$

Thus,

$$\left(g^{q^{e-1}}\right)^{x_i} = \left(h \cdot g^{-x_0-x_1q-x_2q^2-\cdots-x_{i-1}q^{i-1}}\right)^{q^{e-i-1}}$$

which is a discrete logarithm problem and can be solved in $\mathcal{O}\left(S_q\right)$ steps.

Finding all x_i's requires solving e discrete logarithm problems, and therefore x can be found in $\mathcal{O}\left(eS_q\right)$ steps. $\square$

5 A Solved Example

Example 1. *Find x such that*

$$23^x \equiv 9689 \pmod{11251}$$

Solution 11251 is a prime. The base 23 has order 11251-1=11250 in this group. Thus,

$$g = 23, h = 9689, N = 11250 = 2 \cdot 3^2 \cdot 5^4$$

We have to first solve three subsidiary discrete logarithm problems:

1. $q = 5, e = 4, g^{N/q^e} = 5448, h^{N/q^e} = 6909$
   The first step is to solve
   $$\left(5448^{5^3}\right)^{x_0} = 6909^{5^3}$$
   which reduces to $11089^{x_0} = 11089$. Thus, $x_0 = 1$. Next
   $$\left(5448^{5^3}\right)^{x_1} = \left(6909 \cdot 5448^{-x_0}\right)^{5^3} = \left(6909 \cdot 5448^{-1}\right)^{5^3}$$
   which reduces to $11089^{x_1} = 3742$. Thus, $x_1 = 2$. Similarly, we can find that $x_2 = 0$ and $x_3 = 4$. Therefore $x = 1 + 2 \cdot 5 + 4 \cdot 5^3 = 511$

2. $q = 3, e = 2, g^{N/q^e} = 5029, h^{N/q^e} = 10724$
   Using a similar procedure, we can find that $x = 4$

3. $q = 2, e = 1, g^{N/q^e} = 11250, h^{N/q^e} = 11250$
   Here, $x = 1$

The next step is to use the Chinese Remainder Theorem to solve the simultaneous congruences

$$x \equiv 1 \pmod 2, x \equiv 4 \pmod{3^2}, x \equiv 511 \pmod{5^4}$$

which gives $x = 4261$. We can check this by computing that 23^{4261} is indeed $9689 \pmod{11251}$

6 Conclusion

The Pohlig–Hellman algorithm thus tells us that the discrete logarithm problem in a group $\mathbb{G}$ is not secure if the order of the group is a product of powers of small primes. More generally, $g^x = h$ is easy to solve if the order of the element g is a product of powers of small primes. This applies, in particular, to the discrete logarithm problem in $\mathbb{F}_p$ if $p - 1$ factors into powers of small primes.