Discrete Logarithm

Lucas

Shanghai Jiao Tong University

December 26, 2016

Problem

Find a smallest non-negative number x satisfying

$$A^x = B \ (mod \ P)$$

which P is a prime, $A, B \in [0, P)$.

Naive Approach

According to Fermat Theorem, when A, P is coprime, we have:

$$A^P = A \ (mod \ P)$$

the only special case is $A = 0$, and in this case, B must be zero.

For $A \neq 0$, we can just iterate x from 0 to $P - 1$ to check if $A^x = B \ (mod \ P)$. The complexity is $O(P)$.

Yet Another Naive Algorithm

We mapped $A^x \to x, x \in [0, P)$ by using a Hash-Table.

In order to B, we just need to query B in this Hash-Table, which only takes $O(1)$ time.

Precalculating this Hash-Table costs $O(P)$ time, and the total complexity of which is $O(P + 1) = O(P)$.

Balanced Programming

- First we choose a number $S \in [1, P-1]$.
- We mapped $A^x \to x, x \in [0, S)$ by using a Hash-Table.
- Calculate A^{-S} by using Fast Exponentiation.

In this step, we needs $S + \log P$ operations.

$$A^x = B \ (mod \ P)$$

x can be represented as $i \times S + j$, we can do such transforming:

$$A^{i \times S + j} = B \Leftrightarrow A^j = B \times (A^{-S})^i \ (mod \ P)$$

which $j \in [0, S)$, and $i < \frac{P}{S}$.

We can just iterate i from 0 to $\frac{P}{S}$ to check if $B \times (A^{-S})^i$ is in Hash-Table. In the worst occasion, we need to iterate $\frac{P}{S}$ times.

Total complexity evaluation

As you can see, the total operations we need to do are

$$S + \log P + \frac{P}{S}$$

we want to choose S optimally to get the best total complexity.

when $S = \sqrt{P}$, the total operations are:

$$S + \log P + \frac{P}{S} = 2\sqrt{P} + \log P = O(\sqrt{P})$$

thus we get an $O(\sqrt{P})$ algorithm by choosing S optimally.