Discrete Logarithm Algorithms in Practice

1. $G = (\mathbb{Z}_p{}^*, \cdot)$, p prime, α a primitive element modulo p
2. $G = (\mathbb{Z}_p{}^*, \cdot)$, p, q prime, $p \equiv 1 \bmod q$, α an element in $\mathbb{Z}_p$ having order q
3. $G = (\mathbb{F}_{2^n}{}^*, \cdot)$, α a primitive element in $\mathbb{F}_{2^n}{}^*$
4. $G = (E, +)$, where E is an elliptic curve modulo a prime p, $\alpha \in E$ is a point having prime order $q = \#E/h$, where (typically) $h = 1, 2$ or 4
5. $G = (F, +)$, where E is an elliptic curve over a finite field $\mathbb{F}_{2^n}$, $\alpha \in E$ is a point having prime order $q = \#E/h$, where (typically) $h = 2$ or 4

Stinson, p. 267

The Pohlig-Hellman Algorithm

$\alpha^a = \beta$ $$n = \prod_{i=1}^{k} p_i^{c_i},$$ $(= p-1)$

Use Chinese Rem. for moduli $p_i^{c_i}$

let's suppose that q is prime,

$$n \equiv 0 \pmod{q^c}$$

and

$$n \not\equiv 0 \pmod{q^{c+1}}.$$

We will show how to compute the value

$$x = a \bmod q^c,$$

where $0 \leq x \leq q^c - 1$. We can express x in radix q representation as

$$x = \sum_{i=0}^{c-1} a_i q^i,$$

where $0 \leq a_i \leq q - 1$ for $0 \leq i \leq c - 1$. Also, observe that we can express a as

$$a = x + sq^c$$

$$a = \sum_{i=0}^{c-1} a_i q^i + s q^c.$$

The first step of the algorithm is to compute a_0.

$$\beta^{n/q} = \alpha^{a_0 n/q}. \qquad (6.1)$$

We prove that equation (6.1) holds as follows:

$$\begin{aligned}
\beta^{n/q} &= (\alpha^a)^{n/q} \\
&= (\alpha^{a_0 + a_1 q + \cdots + a_{c-1} q^{c-1} + s q^c})^{n/q} \\
&= (\alpha^{a_0 + Kq})^{n/q} \qquad \text{where } K \text{ is an integer} \\
&= \alpha^{a_0 n/q} \alpha^{Kn} \\
&= \alpha^{a_0 n/q}.
\end{aligned}$$

$$\gamma = \alpha^{n/q}, \gamma^2, \ldots,$$

until

$$\gamma^i = \beta^{n/q}$$

for some $i \leq q - 1$. When this happens, we know that $a_0 = i$.

great example: mod 2251

Now, if $c = 1$, we're done. Otherwise $c > 1$, and we proceed to determine $a_1, \ldots, a_{c-1}$. This is done in a similar fashion as the computation of a_0. Denote $\beta_0 = \beta$, and define

$$\beta_j = \beta\alpha^{-(a_0+a_1q+\cdots+a_{j-1}q^{j-1})}$$

for $1 \leq j \leq c-1$. We make use of the following generalization of equation (6.1):

$$\beta_j{}^{n/q^{j+1}} = \alpha^{a_jn/q}. \tag{6.2}$$

Observe that equation (6.2) reduces to equation (6.1) when $j = 0$.

$$\begin{aligned}
\beta_j{}^{n/q^{j+1}} &= (\alpha^{a-(a_0+a_1q+\cdots+a_{j-1}q^{j-1})})^{n/q^{j+1}} \\
&= (\alpha^{a_jq^j+\cdots+a_{c-1}q^{c-1}+sq^c})^{n/q^{j+1}} \\
&= (\alpha^{a_jq^j+K_jq^{j+1}})^{n/q^{j+1}} \qquad \text{where } K_j \text{ is an integer} \\
&= \alpha^{a_jn/q}\alpha^{K_jn} \\
&= \alpha^{a_jn/q}.
\end{aligned}$$

Hence, given β_j, it is straightforward to compute a_j from equation (6.2).

$$\beta_{j+1} = \beta_j\alpha^{-a_jq^j}.$$

Therefore, we can compute $a_0, \beta_1, a_1, \beta_2, \ldots, \beta_{c-1}, a_{c-1}$

The algorithm calculates $a_0, \ldots, a_{c-1}$, where

$$\log_\alpha \beta \bmod q^c = \sum_{i=0}^{c-1} a_i q^i.$$

Algorithm 6.3: POHLIG-HELLMAN$(G, n, \alpha, \beta, q, c)$

$j \leftarrow 0$
$\beta_j \leftarrow \beta$
while $j \leq c - 1$
do $\begin{cases} \delta \leftarrow \beta_j^{\,n/q^{j+1}} \\ \text{find } i \text{ such that } \delta = \alpha^{in/q} \\ a_j \leftarrow i \\ \beta_{j+1} \leftarrow \beta_j \alpha^{-a_j q^j} \\ j \leftarrow j + 1 \end{cases}$
return $(a_0, \ldots, a_{c-1})$

$O(c\sqrt{q})$

Example 6.4 Suppose $p = 29$ and $\alpha = 2$. p is prime and α is a primitive element modulo p, and we have that

$$n = p - 1 = 28 = 2^2 7^1.$$

Suppose $\beta = 18$, so we want to determine $a = \log_2 18$. We proceed by first computing $a \bmod 4$ and then computing $a \bmod 7$.

We start by setting $q = 2$ and $c = 2$ and applying Algorithm 6.3. We find that $a_0 = 1$ and $a_1 = 1$. Hence, $a \equiv 3 \pmod{4}$.

Next, we apply Algorithm 6.3 with $q = 7$ and $c = 1$. We find that $a_0 = 4$, so $a \equiv 4 \pmod{7}$.

$$a \equiv 3 \pmod{4}$$
$$a \equiv 4 \pmod{7}$$

using the Chinese remainder theorem, we get $a \equiv 11 \pmod{28}$.

$$\log_2 18 = 11 \text{ in } \mathbb{Z}_{29}.$$

$\log_3 11 \bmod 17$ by Pohlig – Hellman

$p-1 = 2^4, \quad c=4, \quad q=2$

1. $\gamma_i = \alpha^{i(p-1)/q}, \quad 0 \le i \le q-1$

$\gamma_0 = 3^0 = 1, \quad \gamma_1 = 3^{16\cdot 1/2} = 3^8 = 16$

2. $j=0, \quad \beta_0 = 11$

3. while $j \le 3$

$j=0$ 4. $\delta = 11^{16/q} = 11^8 = 16$

5. $i=1$

6. $a_0 = 1$

7. $\beta_1 = \beta_0 \alpha^{-1\cdot 2^0} = 11\cdot 6 = 15$

$j=$[redacted] 4. $\delta = 15^{16/4} = 15^4 = 16$

5. $i=1, \quad a_1 = 1$

7. $\beta_2 = 15\cdot\alpha^{-1\cdot 2} = 15\cdot 6^2 = 13$

$j=2$ 4. $\delta = 13^{16/8} = 13^2 = 16$

5. $i=1, \quad a_2 = 1$

7. $\beta_3 = 13\cdot 3^{-1\cdot 4} = 13\cdot 6^4 = 1$

$j=3$ 4. $\delta = 1$

5. $i=0, \quad a_3 = 0$

+1

$x = \log_\alpha \beta \bmod 16 = \sum_{i=0}^{c-1} a_i q^i = 0\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 +$

$= \underline{\underline{7}}$

The Index Calculus Method

$$\mathcal{B} = \{p_1, p_2, \ldots, p_B\}$$

$$\alpha^{x_j} \equiv {p_1}^{a_{1j}} {p_2}^{a_{2j}} \ldots {p_B}^{a_{Bj}} \pmod{p},$$

$$x_j \equiv a_{1j} \log_\alpha p_1 + \ldots + a_{Bj} \log_\alpha p_B \pmod{p-1},$$

Choose a random integer s ($1 \leq s \leq p-2$) and compute

$$\gamma = \beta\alpha^s \bmod p.$$

$$\beta\alpha^s \equiv {p_1}^{c_1} {p_2}^{c_2} \ldots {p_B}^{c_B} \pmod{p}.$$

$$\log_\alpha \beta + s \equiv c_1 \log_\alpha p_1 + \ldots + c_B \log_\alpha p_B \pmod{p-1}.$$

is $O\left(e^{(1/2+o(1))\sqrt{\ln p \ln \ln p}}\right)$.

Example [redacted] 6.5

Suppose $p = 10007$ and $\alpha = 5$ is the primitive element used as the base of logarithms modulo p. Suppose we take $\mathcal{B} = \{2, 3, 5, 7\}$ as the factor base. Of course $\log_5 5 = 1$, so there are three logs of factor base elements to be determined.

Some examples of "lucky" exponents that might be chosen are 4063, 5136 and 9865.

With $x = 4063$, we compute

$$5^{4063} \bmod 10007 = 42 = 2 \times 3 \times 7.$$

This yields the congruence

$$\log_5 2 + \log_5 3 + \log_5 7 \equiv 4063 \pmod{10006}.$$

Similarly, since

$$5^{5136} \bmod 10007 = 54 = 2 \times 3^3$$

and

$$5^{9865} \bmod 10007 = 189 = 3^3 \times 7,$$

we obtain two more congruences:

$$\log_5 2 + 3\log_5 3 \equiv 5136 \pmod{10006}$$

and

$$3\log_5 3 + \log_5 7 \equiv 9865 \pmod{10006}.$$

We now have three congruences in three unknowns, and there happens to be a unique solution modulo 10006, namely $\log_5 2 = 6578$, $\log_5 3 = 6190$ and $\log_5 7 = 1301$.

Now, let's suppose that we wish to find $\log_5 9451$. Suppose we choose the "random" exponent $s = 7736$, and compute

$$9451 \times 5^{7736} \bmod 10007 = 8400.$$

Since $8400 = 2^4 3^1 5^2 7^1$ factors over $\mathcal{B}$, we obtain

$$\begin{aligned}\log_5 9451 &= 4\log_5 2 + \log_5 3 + 2\log_5 5 + \log_5 7 - s \bmod 10006\\ &= 4 \times 6578 + 6190 + 2 \times 1 + 1301 - 7736 \bmod 10006\\ &= 6057.\end{aligned}$$

To verify, we can check that $5^{6057} \equiv 9451 \pmod{10007}$. $\square$