1. \( G = (\mathbb{Z}_p^*, \cdot) \), \( p \) prime, \( \alpha \) a primitive element modulo \( p \)

2. \( G = (\mathbb{Z}_p^*, \cdot), p, q \) prime, \( p \equiv 1 \mod q \), \( \alpha \) an element in \( \mathbb{Z}_p \) having order \( q \)

3. \( G = (\mathbb{F}_{2^*}, \cdot) \), \( \alpha \) a primitive element in \( \mathbb{F}_{2^*} \)

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

\[ a^k \equiv b \pmod{p-1} \]

\[ n = \prod_{i=1}^{k} p_i^{c_i} \]

Use Chinese Remainder 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

\[ x = a \mod q^c, \]

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

\[ a = x + sq^c \]
\[ a = \sum_{i=0}^{c-1} a_i q^i + sq^c. \]

The first step of the algorithm is to compute \( a_0 \).

\[ \beta^n/q = \alpha^{a_0 n}/q. \] (6.1)

We prove that equation (6.1) holds as follows:

\[
\begin{align*}
\beta^n/q &= (a^a)^n/q \\
&= (a^{a_0+aq}\cdots+a_{-1}q^{e-1}+sq^e)^n/q \\
&= (a^{a_0+Kq})^n/q \quad \text{where } K \text{ is an integer} \\
&= a^{a_0n}/q \alpha^{Kn} \\
&= a^{a_0n}/q.
\end{align*}
\]

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

until

\[ \gamma^i = \beta^n/q \]

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

great example: mod 2257
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

$$\beta_j = \beta \alpha^{-(a_0 + a_1 q + \cdots + a_{j-1} q^{j-1})}$$

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

$$\beta_j^{n/q^{j+1}} = \alpha^{a_j n/q}.$$  \hfill (6.2)

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

$$\beta_j^{n/q^{j+1}} = (\alpha^{a_0 + a_1 q + \cdots + a_{j-1} q^{j-1}})^{n/q^{j+1}}$$

$$= (\alpha^{a_j q^j + \cdots + a_{c-1} q^{c-1} + q^c})^{n/q^{j+1}}$$

$$= (\alpha^{a_j q^j - K_j q^{j+1}})^{n/q^{j+1}}$$

where $K_j$ is an integer

$$= \alpha^{a_j n/q} \alpha^{K_j n}$$

$$= \alpha^{a_j n/q}.$$

Hence, given $\beta_j$, it is straightforward to compute $a_j$ from equation (6.2).

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

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

$$\log_\alpha \beta \mod q^c = \sum_{i=0}^{c-1} a_i q^i.$$
Example 6.4 Suppose $p = 29$ and $\alpha = 2$. $p$ is prime and $\alpha$ 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 $\alpha = \log_2 18$. We proceed by first computing $\alpha \mod 4$ and then computing $\alpha \mod 7$.

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, $\alpha \equiv 3 \pmod{4}$.

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

\[
\begin{align*}
\alpha & \equiv 3 \pmod{4} \\
\alpha & \equiv 4 \pmod{7}
\end{align*}
\]

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

$$\log_2 18 = 11 \text{ in } \mathbb{Z}_{29}.$$
\[ p-1 = 2^9, \quad c = 4, \quad q = 2 \]

1. \[ \alpha_i = \alpha^{i \cdot (p-1)/q}, \quad 0 \leq i \leq q-1 \]
   \[ \beta_0 = 3^0 = 1, \quad \beta_1 = 3^{16 \cdot 1/2} = 3^8 = 16 \]

2. \[ \hat{j} = 0, \quad \beta_0 = 11 \]

3. while \[ \hat{j} \leq 3 \]
   \[ \hat{j} = 0 \]

4. \[ \hat{\sigma} = 11^{16/2} = 11^8 = 16 \]

5. \[ i = 1 \]

6. \[ a_0 = 1 \]

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

\[ \hat{j} = 0 \]

4. \[ \hat{\sigma} = 15^{16/4} = 15^4 = 16 \]

5. \[ i = 1, \quad a_1 = 1 \]

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

\[ \hat{j} = 2 \]

4. \[ \hat{\sigma} = 13^{16/8} = 13^2 = 16 \]

5. \[ i = 1, \quad a_2 = 1 \]

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

\[ \hat{j} = 3 \]

4. \[ \hat{\sigma} = 1 \]

5. \[ i = 0, \quad a_3 = 0 \]

\[ x = \log_\alpha \beta \mod 16 = \sum_{i=0}^{c-1} a_i q^i = 0 \cdot 2^3 + 1 \cdot 2 + 12 + \]

\[ \equiv 7 \]

**4 L**
The Index Calculus Method

\[ B = \{p_1, p_2, \ldots, p_B\} \]

\[ \alpha^{x_j} \equiv p_1^{a_1j} p_2^{a_2j} \ldots p_B^{a_Bj} \pmod{p}, \]

\[ x_j \equiv a_1 j \log_\alpha p_1 + \ldots + a_B j \log_\alpha p_B \pmod{p - 1}, \]

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

\[ \gamma = \beta \alpha^s \pmod{p}. \]

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

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

is \( O \left(e^{(1/2+\mathcal{O}(1))\sqrt{\ln p \ln \ln p}}\right). \)
Example 6.5
Suppose \( p = 10007 \) and \( \alpha = 5 \) is the primitive element used as the base of logarithms modulo \( p \). Suppose we take \( B = \{2, 3, 5, 7\} \) 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

\[
5^{4063} \mod 10007 = 42 = 2 \times 3 \times 7.
\]
This yields the congruence

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

Similarly, since

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

and

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

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

\[
9451 \times 5^{7736} \mod 10007 = 8400.
\]

Since \( 8400 = 2^4 3^1 5^2 7^1 \) factors over \( B \), we obtain

\[
\log_5 9451 = 4 \log_5 2 + \log_5 3 + 2 \log_5 5 + \log_5 7 - s \mod 10006
= 4 \times 6578 + 6190 + 2 \times 1 + 1301 - 7736 \mod 10006
= 6057.
\]

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