We first note that $b' = b^{(q-1)/(p-1)}$ is a generator of $\mathbf{F}_p^*$ (see Exercise 17 of §II.1). Thus, we immediately know the discrete logs to the base b of these constants once we solve the discrete log problem in $\mathbf{F}_p^*$ (to the base b'). But we have assumed that p is small, and so a table of such discrete logs can easily be constructed. In the important special case $p = 2$, in fact, the only nonzero constant is 1, whose discrete log to any base is 0. In what follows we shall suppose that we can easily find the discrete log of a constant.

For the rest of this section we shall let $ind(a(X))$ (from the word "index") denote the discrete log of $a(X) \in \mathbf{F}_q^*$ to the base $b(X)$. The base $b(X)$ is fixed throughout the discussion, and so will not be indicated in the notation.

There are two basic stages of the index–calculus algorithm. The first stage is called a "precomputation," because it does not depend on the element $y(X) \in \mathbf{F}_q^*$ whose discrete log we ultimately want to determine. It has only to be carried out once, and can then be used for many computations of various discrete logs to the fixed base $b(X)$. (Recall that there was also an analogous precomputation stage in the Silver–Pohlig–Hellman algorithm, namely, the compilation of the table of $\{r_{p,j}\}$.)

We first choose a subset $B \subset \mathbf{F}_q$ which will serve as our "basis." Usually B consists of all monic irreducible polynomials over $\mathbf{F}_p$ of degree $\leq m$, where $m < n$ is determined in some optimal way so that the set B has a suitable size $h = \#(B)$ of intermediate magnitude between $p = \#(\mathbf{F}_p)$ and $q = p^n = \#(\mathbf{F}_q)$. The precomputation stage consists in determining the discrete logs of all $a(X) \in B$, as follows.

Choose a random integer t between 1 and $q-2$, and compute $b^t \in \mathbf{F}_q$, i.e., compute the polynomial $c(X) \in \mathbf{F}_p[X]$ of degree $< n$ such that

$$c(X) \equiv b(X)^t \ \ mod\ f(X).$$

(Here one uses the repeated squaring method, at each step reducing modulo $f(X)$.) Factor out the leading coefficient c_0 from $c(x)$, and determine whether or not the resulting monic polynomial can be written as a product of the $a(X) \in B$, i.e., whether or not $c(X)$ can be written in the form

$$c(X) = c_0 \prod_{a \in B} a(X)^{\alpha_{c,a}}.$$

One way to determine this is to run through all $a(X) \in B$ and divide $c(X)$ successively by $a(X)^{\alpha_{c,a}}$ (where $\alpha_{c,a}$ is the highest power of $a(X)$ which divides $c(X)$ in $\mathbf{F}_p[X]$). If the constant c_0 is all that remains after dividing by powers of all of the $a(X) \in B$, then $c(X)$ has the above form; otherwise, start over again at the beginning of this paragraph with a different random integer t. (A second way — in some cases quicker — to determine whether $c(X)$ factors into a product of $a(X) \in B$ is simply to factor $c(X)$ using an algorithm for factoring elements of $\mathbf{F}_p[X]$. For a description of a good algorithm for this purpose (due to Berlekamp), see Volume II of Knuth, §4.6.2.)