

Now suppose that we have found a  $c(X) \equiv b(X)^t \pmod{f(X)}$  which has the desired type of factorization. Taking the discrete log of both sides of the above equality, we obtain

$$\text{ind}(c(X)) - \text{ind}(c_0) = \sum_{a \in B} \alpha_{c,a} \text{ind}(a(X)),$$

where equality here should be interpreted as congruence modulo  $q - 1$  (since the discrete log is defined only modulo  $q - 1$ ). The left side of this equality is known, since  $\text{ind}(c(X)) = t$  and the discrete logs of constants are assumed to be known. The coefficients  $\alpha_{c,a}$  on the right are also known. The unknowns are the  $h$  values  $\text{ind}(a(X))$ ,  $a(X) \in B$ , on the right.

Thus, we have obtained a linear equation in  $\mathbf{Z}/(q - 1)\mathbf{Z}$  with  $h$  unknowns. Now suppose we continue to choose random integers  $t$  until we obtain a large number of different  $c(X)$ 's which factor into a product of  $a(X)$ 's. As soon as we obtain  $h$  independent congruences of the type

$$t - \text{ind}(c_0) \equiv \sum_{a \in B} \alpha_{c,a} \text{ind}(a(X)) \pmod{q - 1}$$

(here “independent” means that the determinant of the coefficient matrix  $\{\alpha_{c,a}\}$  is prime to  $q - 1$ ), then we can solve the system for the unknowns modulo  $q - 1$ . (See §III.2 for a discussion of linear algebra modulo  $N = q - 1$ .) This completes the first stage of the index-calculus algorithm. The precomputation has given us a large “data-base,” namely the discrete logs of all  $a(X) \in B$ , from which to compute any discrete log we are interested in.

Before proceeding to a description of the second stage of the index-calculus algorithm, we should comment on the choice of  $m$ , which was not specified when we described  $B \subset \mathbf{F}_p[X]$  as the set of all monic irreducible polynomials of degree  $\leq m$ . The size  $h$  of the set  $B$  grows rapidly as  $m$  increases. For example, if  $m$  is prime, then we saw (Corollary to Proposition II.1.8) that in degree  $m$  alone there are  $(p^m - p)/m$  monic irreducible polynomials. Since we are required to find at least  $h$  different  $c(X)$ 's which give us the  $h \times h$  system of independent linear congruences in the  $h$  unknowns  $\text{ind}(a(X))$ , and then we have to solve the system, it would be helpful if  $h$  were not too large, i.e., if  $m$  were not too large. On the other hand, if  $m$  is small, then a “typical” monic polynomial  $c_0^{-1}c(X)$  of degree  $\leq n - 1$  is not likely to factor into a product of  $a(X)$  of degree  $\leq m$ ; it is more likely to have at least one irreducible factor of degree  $> m$ . That is, if  $m$  is small, it will take us an inordinate amount of time to make even a single lucky random choice of  $t$  for which  $c(X) \equiv b(X)^t \pmod{f(X)}$  has the desired type of factorization. Thus,  $m$  must be not too small, though quite a bit smaller than  $n$ . The optimal choice of  $m$  — depending, of course, on  $p$  and  $n$  — requires a lengthy analysis of probabilities and time estimates, which go beyond the scope of this book. For example, when  $p = 2$  and  $n = 127$ , the