## 6.4 Application to discrete logarithms in generic groups

Collisions can be used to computed discrete logarithms in arbitrary groups, using the baby-step, giant-step method. Before presenting this method, it is useful to first show that computing discrete logarithms in a group whose cardinality is known is, assuming that the factorization of the cardinality is given, no harder than computing discrete logarithms in all subgroups of prime order. The Pohlig-Hellman algorithm is a constructive method to compute discrete logarithm in the whole group from a small number of calls to discrete logarithms computations in the subgroups of prime order.

### 6.4.1 Pohlig-Hellman algorithm

First, let us recall the definition of discrete logarithm. Given a group $\mathbb{G}$, denoted multiplicatively and two elements of $\mathbb{G}$, say $g$ and $h$, computing the discrete logarithm of $h$ in basis $g$ amounts to finding, if it exists, an integer $a$, such that $h = g^a$ in $\mathbb{G}$. For discrete logarithms computations are not necessarily possible for all elements $h$ of $\mathbb{G}$. However, if $\mathbb{G}$ is a cyclic group generated by $g$, then the discrete logarithm is defined for all elements of $\mathbb{G}$. In the sequel, we make this assumption.

Note that, if $N$ denotes the cardinality of $\mathbb{G}$, the discrete logarithm of $h$ in basis $g$ is only determined modulo $N$, since $g^N = 1$ the identity element in $\mathbb{G}$. An interesting consequence is that any algorithm able to compute discrete logarithm can be used to obtain $N$. For simplicity, assume that we know the order of magnitude of $N$ and, more precisely, assume that $N$ lies in the range $[N_0 + 1, 2N_0]$. If the discrete logarithm algorithm outputs a normalized value between 0 and $N - 1$, it suffices to ask for the discrete logarithm of $g^{2N_0}$, say $a$. Then we know that $N$ divides $2N_0 - a$ and even that $N = 2N_0 - a$. If the discrete logarithm is allowed to output any of the multiple possible values for the discrete logarithm, choose a random integer $b$ between 0 and some multiple of $N_0$, say $10N_0$. Then ask for a discrete logarithm of $g^b$ and let $a$ denote the resulting value. Since $g^a = g^b$, $|b - a|$ is a small multiple of $N$, possibly 0. If $a \neq b$, it is a non-zero multiple. Since there are not many divisors of this multiple in the range $[N_0 + 1, 2N_0]$, we can easily recover $N$. However, we need to make sure that the discrete logarithm algorithm does not systematically output $a = b$. This comes from the fact that we are choosing $b$ at random in a large range. With this strategy, even an adversarial discrete logarithm algorithm cannot systematically determine $b$ and, at some point, it outputs some other value for the discrete logarithm. Finally, even if we do not know a precise range, it is usually possible to find $N$ by computing the GCD of a few multiples obtained as above.

As a consequence, in the context of discrete logarithm computations, it is reasonable to ask for the group cardinality $N$ in advance. We also assume that