Calculating the Order of a Group Element

**Question:** If \( g \in G \) is an element of a finite group, how fast can we calculate its order \( \text{ord}(g) \)?

**Answer:** 1) In general, we only have the naive algorithm, i.e. calculate successively \( g, g^2, \ldots g^k, \ldots \) and find the first \( k \) such that \( g^k = 1 \). (Exponential!)

2) However, if we know the prime decomposition of \( n = |G| \), then there is a fast algorithm.

**Theorem:** Assume that \( n = |G| \) and its set \( S(n) = \{p : p|n, p \text{ prime}\} \) of prime divisors are known. Then \( \text{ord}(g) \) can be computed quickly by using the formula

\[
\text{ord}(g) = \prod_{p \in S(n)} p^{e(p) - f(p)},
\]

where \( e(p) = \max\{k : p^k | n\} \),

\[ f(p) = \max\{k \leq e(p) : g^{n/p^k} = 1\} \]

**Note:** By using the binary power method, \( f(p) \) can be computed in polynomial time, provided that multiplication in \( G \) takes polynomial time. Thus, if \( n \) and \( S(n) \) are known, then \( \text{ord}(g) \) can be calculated in polynomial time.