

A. In the generalization of Grover's problem, where  $\sum_{\alpha} f(\alpha) = m$ , why is it important that  $m$  be small compared to  $2^n$ ?

B. Describe an integer factoring algorithm, that uses Grover's algorithm, that factors  $n$ -bit unsigned integers in time  $\mathcal{O}(2^{n/4})$ .