In class, we haven't yet seen why this first problem is important, but we will soon.

A. Let m be a large positive integer. Let n be an integer large enough that $2^n \geq m^2$. Let c/d and c'/d' be distinct positive rational numbers, in lowest terms, such that $d, d' < m$ and $2^n \geq m^2$. (Lowest terms means $\gcd(c, d) = 1 = \gcd(c', d')$.) Prove that the distance between c/d and c'/d' (on the real number line) is greater than 2^{-n}. [This is a short, algebra-heavy problem.]

B. Why does Shor's algorithm insist on using an n large enough that $2^n \geq m^2$? So far, we have seen three places where that assumption is important. Jog my memory by briefly describing them. (If you believe me that problem A is important, then that problem gives a fourth reason.) [This problem is medium-length. It encourages you to understand the analysis of Shor's algorithm.]

If you were able to factor large integers m quickly, then you could quickly compute the Euler phi function $\phi(m)$. The following exercise partially establishes the converse. So it demonstrates the general idea that several number theory problems, which underlie most of contemporary cryptography, are roughly equivalent to each other. This idea is important in our upcoming number theory discussion.

C. Suppose that m is a large positive integer. You know m and $\phi(m)$. You also know that $m = ab$, where a and b are distinct primes. Explain how to compute a and b quickly. [This is a medium-short, algebra-heavy problem.]

The following problem is optional. Do not hand it in. In fact, you already did it around Day 02 or Day 03. I repeat it here, just because we have finally used it.

D. Prove, for any real number t, that $\left|e^{i2t} - 1\right|^2 = 4 \sin^2 t$.