Homework 35, due December 6

(1) (Page 466, problem 3)
   (a) Suppose j/r and j_1/r_1 are two distinct rational numbers, with $0 < r < n$ and $0 < r_1 < n$ (j, j_1, r, r_1 are integers). Show that
   $$\left|\frac{j_1}{r_1} - \frac{j}{r}\right| > \frac{1}{n^2}.$$
   (b) Suppose, as in Shor's algorithm, that we have
   $$\left|\frac{c}{2^m} - \frac{j}{r}\right| < \frac{1}{2n^2} \quad \text{and} \quad \left|\frac{c}{2^m} - \frac{j_1}{r_1}\right| < \frac{1}{2n^2}.$$
   Show that $j/r = j_1/r_1$.

(2) Let $f(x) = x^4 - x - 1$. Use the extended Euclidean algorithm for polynomials to find $g(x), h(x)$ such that
$$1 = f(x)g(x) + (x^7 - 1)h(x).$$

(3) Read the Wikipedia page for post-quantum cryptography. Click at least two links on the page that interest you, and read those articles as well. Write five things you learned or found interesting.