Homework 22, due November 20

(1) (Page 466, problem 1) Consider the sequence $2^0, 2^1, 2^2, \dots \pmod{15}$.

 $c\equiv$

- (a) What is the period of this sequence?
- (b) Suppose you want to use Shor's algorithm to factor n = 15. What value of m would you take?
- (c) Suppose the measurement in Shor's algorithm yields c = 192. What value do you obtain for r? Does this agree with your earlier answer?
- (d) Use the value of r from part c to factor 15.
- (2) (Page 466, problem 2a) Let $0 < s \le m$. Fix an integer c_0 with $0 \le c_0 < 2^s$. Show that

$$\sum_{\substack{0 \le c < 2^m \\ \text{ico} \pmod{2^s}}} e^{\frac{2\pi i cx}{2^m}} = 0$$

if $x \not\equiv 0 \pmod{2^{m-s}}$ and that this sum equals

$$2^{m-s}e^{2\pi i x c_0/2^m}$$

if $x \equiv 0 \pmod{2^{m-s}}$. (Hint: Write $c = c_0 + j2^s$.)

(3) (Page 466, problem 3a) Suppose j/r and j_1/r_1 are two distinct rational numbers with $0 < r, r_1 < n$. Show that

$$\left|\frac{j_1}{r_1} - \frac{j}{r}\right| > \frac{1}{n^2}.$$

(4) (Page 466, problem 3b) Now suppose, as in Shor's algorithm, that we have

$$\left|\frac{c}{2^m} - \frac{j}{r}\right| < \frac{1}{2n^2}, \left|\frac{c}{2^m} - \frac{j_1}{r_1}\right| < \frac{1}{2n^2}.$$

Show that $j/r = j_1/r_1$.