Math 259: Spring 2019
Quiz 2

NAME:

Are you taking this class for graduate credit?

Time: **30 minutes**

Problem	Value	Score
1	5	
2	4	
3	7	
4	4	
Grad	4	
TOTAL	20	
Grad TOTAL	24	
Score		

Problem 1 : (5 points) A helpful friend notices that

$$34^2 \equiv 1 \pmod{55}.$$

Explain how to use this information to factor 55. This means that you should use *some* words, and there should be at least *some* equations supporting/justifying your work.

Problem 2 : (4 points) You are given a sequence of length 30, and for fun you compute the first few terms of its Discrete Fourier Transform. You record the following data:

j	0	1	2	3	4	5	6
$\lvert b_j \rvert$	0	0	0	0	0	0	5.7

What is a good guess for the frequency of your sequence? Its period? There is no need to justify here but you can justify for partial credit if you are not sure.

Problem 3 : (7 points) Suppose that you want to factor $N = 21$ using Shor's algorithm. In the set up to the quantum steps, since $N^2 = 441$ and $2^9 = 512$ is such that

$$441 \leq 512 < 2 \cdot 441 = 882,$$

you pick $q = 9$.
Furthermore, you randomly pick the value $a = 10$ to begin the quantum steps.

a) (3 points) At the outcome of the quantum steps, you observe the value $j = 85$. A helpful friend computes the continued fraction expansion of $\frac{85}{512}$ to be

$$\cfrac{1}{6 + \cfrac{1}{42 + \cfrac{1}{2}}} = [\,0; 6, 42, 2\,].$$

Using this information, what should you conclude is likely to be the multiplicative order of 10 modulo 21?

b) (1 point) Check that your answer from part a) is correct.

c) (3 points) Using the information you gathered from this problem, how can you factor 21? Note that you must use the ideas developed in class and relating to Shor's algorithm to factor 21 to receive credit.

Problem 4 : (4 points) You are given a sequence of length 30, and again for fun you compute the first few terms of its Discrete Fourier Transform. You record the following data:

j	0	1	2	3	4	5	6	7	8	9
$\lvert b_j \rvert$	1.095	0.286	0.327	0.404	0.539	0.795	1.411	4.530	4.869	1.752

If you know that the period of the sequence is no longer than 10, what is a good guess for the period of this sequence?

Problem 5 : (4 points) This is an extra problem for graduate credit
Let N be the product of two distinct odd primes. Prove that there exists x such that $x \not\equiv \pm 1 \pmod{N}$, but $x^2 \equiv 1 \pmod{N}$.
Hint: You can assume the Chinese Remainder Theorem without proof. You may also ask for one (1) extra hint for free during the quiz if you need it.