Math 259 - Spring 2019
Practice Problems for Quiz 2

1. You are given a sequence of length 106. For fun you compute the terms of its Discrete Fourier Transform, but because there are so many, you only record the first few whose absolute value is greater than 1. You record:

j	0	23	24	25	26	27	28	29	30	31	53
$\lvert b_j \rvert$	2.428	1.176	1.678	2.853	8.734	8.915	3.034	1.859	1.356	1.078	2.233

   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?

2. For this question, consider the Pauli Z-gate, which acts on 1-qbit superpositions by sending

$$|0\rangle \mapsto |0\rangle \quad \text{and} \quad |1\rangle \mapsto -|1\rangle,$$

   and extending linearly.

   (a) Give the matrix representation of this gate.

   (b) If you input the superposition

$$\frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$$

   into the Pauli Z-gate, what is the **probability** that you will observe $|0\rangle$ as the output?

3. Suppose that you want to factor $N = 33$ using Shor's algorithm.

   In the set up to the quantum steps, since $N^2 = 1089$ and $2^{10} = 1024$ is such that

$$1089 \leq 1024 < 2 \cdot 1089 = 2178,$$

   you pick $q = 10$.

   Furthermore, you randomly pick the value $a = 7$ to begin the quantum steps.

   (a) At the outcome of the quantum steps, you observe the value $j = 101$. A helpful friend computes the continued fraction expansion of $\frac{101}{1024}$ to be

$$\cfrac{1}{10 + \cfrac{1}{7 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{2}}}}} = [\,0; 10, 7, 4, 1, 2\,].$$

Using this information, what should you conclude is likely to be the multiplicative order of 7 modulo 33?

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

(c) Using the information you gathered from this problem, how can you factor 33?