1. GHZ paradox. (50)
Consider the following game: Alice, Bob, and Charlie are given input bits a, b, and c respectively. They are promised that $a \oplus b \oplus c = 0$. Their goal is to output bits x, y, and z respectively such that $x \oplus y \oplus z = a \lor b \lor c$. They can agree on a strategy in advance but cannot communicate after receiving their inputs.

1. Show that in a classical universe, there is no strategy that enables them to win this game with certainty.

2. Suppose Alice, Bob, and Charlie share the entangled state
$$\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$$
Show that now there exists a strategy by which they can win the game with certainty. [Hint: Have each player measure its qubit in one basis if its input bit is 0, or in a different basis if its input bit is 1.]

2. Discrete Fourier Transform. (25)

1. N-th roots of unity are defined as solutions to the equation: $\omega^N = 1$. There are exactly N distinct N-th roots of unity.
Let $\omega$ be a primitive root of unity, for example $\omega = exp(2\pi i/N)$. Show the following:
$$\sum_{k=0}^{N-1} \omega^{mk} = \begin{cases} N, & \text{if } N \text{ divides } m \\ 0, & \text{otherwise} \end{cases}$$
2. Fix an integer \( N \geq 2 \). Let \( f = (f(0), \ldots, f(N - 1)) \) a vector (function) \( f : [N] \to \mathbb{C} \). The Discrete Fourier Transform of \( f \) is another complex vector (function) \( F : [N] \to \mathbb{C}, F = (F(0), \ldots, F(N - 1)) \) of the same dimension \( N \),
\[
F(k) = \sum_n \omega^{kn} f(n)
\]
Thus Fourier transform is a linear operator represented by the \( N \times N \) matrix \( A = (a_{kn}), a_{kn} = \omega^{kn} \).

- Write explicitly the Fourier matrix of order 4 using \( \omega = \exp(2\pi i/4) = i \).
- Find the Fourier Transform of the vector \((2, 1, -2, 1)\) using the matrix above.
- Using item (1) from this problem, verify that the inverse matrix is \( A^{-1} = \frac{1}{N}(\omega^{-kn}) \). In other words, a vector \( f \) can be recovered from its Fourier Transform \( F \) by the Fourier Inversion Formula:
\[
f(n) = \frac{1}{N} \sum_k \omega^{-nk} F(k)
\]

3 Number Theory Basics. (25)

1. Suppose \( a \) and \( t \) are integers, \( s \) and \( m \) are positive integers, and that \( as + mt \equiv 2 \pmod{m} \). Which of the following necessarily must be true?
   - \( as \equiv 1 \pmod{m} \)
   - \( as \equiv 2 \pmod{m} \)
   - \( as = 1 \)
   - \( as + mt = 0 \)

2. Fermat’s little theorem states that if \( p \) is a prime number, then for any integer \( a, a^p \equiv a \pmod{p} \).
   - Show that if \( p \) does not divide \( a \), then \( a^{p-1} \equiv 1 \pmod{p} \).
   - What is \( 5^{2600000000000002} \pmod{7} \)?