Read carefully and follow the rules below.

1. This exam consists of 10 pages and 4 problems. The space provided should be enough for the answers. Do not add additional pages to the exam.

2. Justify your answers. Make sure that you explain clearly each step in your reasoning.

3. The exam is closed book.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td>25</td>
</tr>
<tr>
<td>3</td>
<td>25</td>
</tr>
<tr>
<td>4</td>
<td>25</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
</tr>
</tbody>
</table>
Problem 1 (25 points)

1. Show that the two-qubit state

$$|\psi\rangle := \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$$

cannot be expressed as a tensor product of two one-qubit states.

2. Construct a quantum circuit that transforms the initial state $|00\rangle$ to the state $|\psi\rangle$ in 1.
3. Show that the $4 \times 4$-matrix

$$A := |0\rangle\langle 0| \otimes \left(|+\rangle\langle +| + |\rangle\langle -|\right) + |1\rangle\langle 1| \otimes \left(|0\rangle\langle 0| - |1\rangle\langle 1|\right)$$

cannot be expressed as a tensor product of two $2 \times 2$-matrices. Hint: Determine first the matrix representation of $A$ in the standard basis.
Problem 2 (25 points)

1. Show that the quantum circuits

\[
\begin{pmatrix}
e^{i\alpha} & 0 \\
0 & e^{i\alpha}
\end{pmatrix}
\]

are equivalent.
2. Prove that the quantum circuit

\[ \begin{array}{c}
\text{H} & \text{X} & \text{H} \\
\text{Z} & & \\
\end{array} \]

implements the identity.
3. Let $V$ be a unitary operator such that $V^2 = U$. Show that the quantum circuit

![Quantum Circuit Diagram]

implements the controlled-controlled-$U$ gate

![Controlled-Controlled-U Gate Diagram]
4. Construct a quantum circuit $U_f$ that (reversibly) implements the 3-bit Boolean function

$$f(x_1, x_2, x_3) = x_1 \cdot x_2 \oplus x_3,$$

i.e., $U_f$ should act as follows

$$U_f(|x_1, x_2, x_3\rangle \otimes |y\rangle) = |x_1, x_2, x_3\rangle \otimes |y \oplus f(x_1, x_2, x_3)\rangle$$

for all $x_1, x_2, x_3, y \in \{0, 1\}$. Hint: You can use controlled-controlled-$U$ gates for arbitrary $U$. 

Problem 3 (25 points)
Many quantum algorithms produce states of the form $\sum_x |x\rangle |f(x)\rangle$, including Shor’s factoring algorithm. Let $a = 2$, $N = 21$ and $q = 128$. In this case, the first step in Shor’s algorithm creates the state

$$|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle |a^x \text{ mod } N\rangle$$

1. What is the post measurement state $|\psi'\rangle$ if the second register was measured and the outcome was 16.

2. Once we have determined the order of $a$, explain how we can use this information to extract a prime factor of $N$. Discuss the general method and apply it to the above example.
Problem 4 (25 points)
Consider the quantum circuit

\[ U = (|+\rangle\langle+| \otimes |+\rangle\langle+|) + (|+\rangle\langle-| \otimes |-\rangle\langle+|) + (-|\rangle\langle+| \otimes |+\rangle\langle-|) + (-|\rangle\langle-| \otimes |-\rangle\langle-|) \]

and \( |\psi_1\rangle \) and \( |\psi_2\rangle \) are arbitrary quantum states.

1. Derive a formula for the probability of obtaining 0 and 1 when the first qubit is measured.
2. What happens in the following cases

(a) $|\psi_1\rangle = |\psi_2\rangle$

(b) $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal?