Name: _____

Entry number: _____

There are 1 questions for a total of 10 points.

---

1. (10 points) Let $N \geq 2$ be an arbitrary positive integer and let $a \in \mathbb{Z}_N^*$ such that order of a modulo N divides N. Suppose you are given the following n-qubit quantum gates, where $2 \leq N \leq 2^n - 1$.

   1. U_N: This gate returns a uniform superposition of states $|0\rangle, |1\rangle, ..., |N-1\rangle$ when given input $|0\rangle$.
   2. QFT_N: This performs the Quantum Fourier transform on orthonormal basis $|0\rangle, ..., |N-1\rangle$.
   3. $\mathsf{ME}_{a,N}$: This performs the operation $|z\rangle |y\rangle \rightarrow |z\rangle |a^z y \ (mod \ N)\rangle$.

   Construct a quantum circuit that finds the order of a modulo N using just the above gates. You may also use controlled operations. Discuss correctness and running time of your algorithm.

.