QUANTUM ALGORITHMS
HOMEWORK 3 ADDITIONAL PROBLEMS

PROF. MATTHEW MOORE

DUE: 2021-02-23

1. Compute $2^{3^{4^5}} \bmod 79$. I suggest that you do this without using a computer.
[*Hint:* $78 = 2 \cdot 3 \cdot 13$.]

2. **(i)** Compute $14^{15} \bmod 10$. [*Hint: look for a pattern or use* $10 = 2 \cdot 5$.]

(ii) Compute $13^{14^{15}} \bmod 11$.

3. Implement the Miller-Rabin probabilistic primality testing algorithm as presented in class (or in the textbook). Fill in the function `is_prime_MR(q)` in the python source file. You need only submit your function with the homework, not the entire source file.

4. Find five pairs of numbers $q \in \mathbb{Z}$ and $a \in \{1, \ldots, q-1\}$ such that q is composite but passes the Miller-Rabin test with the given choice of a.