QUANTUM ALGORITHMS
HOMEWORK 4 ADDITIONAL PROBLEMS

PROF. MATTHEW MOORE

DUE: 2021-03-02

1. For each of the following values of q, generate 5 random members of $\{1, \ldots, q-1\}$ and run the Miller-Rabin test using them. What is the probability that q is prime?

You should run the algorithm by hand, but I suggest using a computer to do the calculations themselves.

(i) $q = 10601$

(ii) $q = 101101$

(iii) $q = 15841$

2. **(i)** Compute 7^7 in $\mathbb{Z}_4$.

(ii) Compute 7^{7^7} in $\mathbb{Z}_4$.

(iii) Compute $7^{7^{7^7}}$ in $\mathbb{Z}_5$ [*Hint 1: use the previous part and Fermat's little theorem.*] [*Hint 2:* 7^3.]

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

4. Let $n \in \mathbb{N}$ and define $\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$ (i.e. the number of numbers coprime to n between 1 and n).

(i) Prove that if $\gcd(m, n) = 1$ then $\varphi(m \cdot n) = \varphi(m)\varphi(n)$.

(ii) Prove that if p is a prime then

$$\varphi(p^k) = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right).$$

(iii) Use the previous parts to prove that

$$\varphi(n) = n \prod_{\substack{p \text{ prime}, \\ p \mid n}} \left(1 - \frac{1}{p}\right)$$

(the product is over all prime divisors of n).