Exercise 1
Due: 12/11/2020

1. (a) Prove $2^{340} = 1 \pmod{341}$.
   (b) Compute $4^{66} - 8^{1132} \pmod{21}$.
   (c) Prove or disprove: $5^{3001} = 12^{301} \pmod{31}$.

2. Given an n-bit integer N, find a polynomial (in n) time algorithm that decides whether N is a power (that is, there are integers a and $k > 1$ so that $a^k = N$).

3. Show an efficient randomized algorithm to factor Carmichael numbers (that is, we want a polynomial time algorithm, that given any Carmichael number C, with probability at least 3/4 finds a nontrivial factor of C). *Hint: use the Rabin-Miller test.*

4. Assume we try to implement the RSA algorithm with public key (p, e) for a prime p (and e such that $gcd(e, p-1) = 1$). Show that this scheme is insecure. That is, show an efficient algorithm that given p, e and $m^e \pmod{p}$, computes $m \pmod{p}$.