M 343 L Midterm

name:

1. Verify that 341 passes the Fermat primality test with base 2 but fails the Miller-Rabin primality test with base 2. Use your computation to produce an integer x with $x^2 \equiv 1 (\mathrm{mod}\, 341)$ but $x \not\equiv \pm 1 (\mathrm{mod}\, 341)$ and then use this information to factor 341.

2. Bob is using RSA with modulus $n = 341$ and encryption exponent $e = 7$. He receives a cyphertext $c = 16$. What is the plaintext message?

3. Let a, b be relatively prime integers and u, v be integers with $au + bv = 1$. Let $x = au - bv$. Show that $x \equiv 1 (\mathrm{mod}\, b)$ and $x \equiv -1 (\mathrm{mod}\, a)$. Find u, v, x when $a = 23, b = 31$.