

## Extra Credit 4

**Due:** November 22, 2023

**Points:** 20

Euler's generalization of Fermat's Little Theorem says that, for integers  $a$  and  $n$  such that  $a$  and  $n$  are relatively prime,  $a^{\phi(n)} \bmod n = 1$ . Use this to show that deciphering of an enciphered message produces the original message with the RSA cryptosystem. Does enciphering of a deciphered message produce the original message also?