Extra Credit 3

Due: November 6, 2024 **Points:** 30

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 mathematically 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?
Hint: You need to prove the case where m and n are relatively prime, and the case when they are not.