CPSC 418/MATH 318 Practice Problems

RSA

1. Consider the RSA public key $(n, e) = (65, 19)$.
   (a) Compute $\phi(n)$.
   (b) Use the extended Euclidean algorithm to compute the corresponding private key d.
   (c) Use the binary exponentiation algorithm to encrypt $M = 3$.
   (d) Use the binary exponentiation algorithm to decrypt $C = 4$.

2. Consider the (rather unluckily chosen) RSA public key $(n, e) = (65, 37)$. A handful of test encryptions seem to suggest that every ciphertext is identical to its corresponding original plaintext (try a few for practice to see this). This suggests that $M^{37} \equiv M \pmod{65}$ for all $M \in \mathbb{Z}_{65}^*$. Prove this as follows:
   (a) Use Fermat's Little Theorem to prove that $M^{37} \equiv M \pmod{5}$ for all $M \in \mathbb{Z}_{65}^*$.
   (b) Similarly prove that $M^{37} \equiv M \pmod{13}$ for all $M \in \mathbb{Z}_{65}^*$.
   (c) Formally conclude that $M^{37} \equiv M \pmod{65}$ for all $M \in \mathbb{Z}_{65}^*$.