Math 370 Number Theory
Assignment # 8

1. Consider the RSA setup: $m = pq$ where p, q are distinct primes, $d, e \in \mathbb{N}$ where $d = e^{-1} \pmod{\phi(m)}$. Then if M is a message we let $C \equiv M^e \pmod{m}$. We then showed that as long as $\gcd(C, m) = 1$ then $C^d \equiv M \pmod{m}$. We've previously showed that $\gcd(C, m) = 1$ exactly when $\gcd(M, m) = 1$. So the question is what if you are unlucky and the message you want to send is not relatively prime to m. In practice this never happens since p and q or so big that the chances your M is divisible by either p or q is basically 0. However with the small numbers that we use in class and the homework this could happen. Let's show that RSA still works. We will show in this problem that even if $\gcd(M, m) > 1$ (so either p, q or m), then $C^d \equiv M \pmod{m}$. With no assumption on $\gcd(C, m)$ show:
   (a) $C^d \equiv M \pmod{p}$
   (b) $C^d \equiv M \pmod{q}$
   (c) $C^d \equiv M \pmod{m}$.