Homework 4
(Units, Euler's function, RSA, primitive roots.)
Due Wednesday, October 23 at 11:30am in class.

Note: Be sure to justify your answers. No credit will be given for answers without work/justification. In addition, all written homework assignments should be neat and well-organized; **this assignment has only one part and can be submitted as a single packet**.

(1) Calculate $\phi(72)$ and confirm it by finding a reduced set of residues modulo 72.
(2) Show that if $\gcd(m, n) \neq 1$, then $\phi(mn) > \phi(m)\phi(n)$.
(3) Show that if m and n are positive integers such that $m \mid n$, then $\phi(m) \mid \phi(n)$.
Hint: Use the prime factorizations of m and n.
(4) Find all n such that $\phi(n) = 12$.
(5) Consider the groups of units U_{15} and U_7. For each group, complete the following.
   (a) List the elements of the group.
   (b) Match each element with its multiplicative inverse.
   (c) Find the order of each element.
   (d) Is the group cyclic? If it is cyclic, find all primitive roots.
(6) Consider the RSA algorithm with $p = 5$ and $q = 11$
   (a) Find both the public and private keys.
   (b) Encrypt the value $n = 8$. (Use successive squaring and a calculator, if needed.)
   (c) Decrypt the value $c = 3$. (Use successive squaring and a calculator, if needed.)

Fun problem (will not be graded): For each of the following statements, produce examples (values of integers x, y, and z) where the statement holds.

(1) $\phi(x) + \phi(y) = \phi(x + y)$.
(2) $\phi(x) + \phi(y) \neq \phi(x + y)$.
(3) $\phi(x^2) + \phi(y^2) = \phi(z^2)$ and $x^2 + y^2 = z^2$.
(4) $\phi(x^2) + \phi(y^2) \neq \phi(z^2)$ and $x^2 + y^2 = z^2$.

Do you think there are infinitely many examples in (1) and (3)?