Midterm 3 Study Guide

1. Be able to do general versions of the following:
   a. Determine the last digit in the decimal expansion of 23^{123}.
   b. Show that $17^{24} - 36^{12}$ is divisible by 11.
   c. Find all solutions to the equation $5x = 10 \mod 35$ and the equation $5x = 6 \mod 21$.
   d. Find the order of various elements modulo a prime.
   e. Determine if a number a is a quadratic residue modulo a prime p.
   f. Compute g and $T(a, p)$.
2. State in mathematical terms and either prove or provide a counterexample:
   a. Every natural number is congruent, modulo n, to exactly one number from $\{0, 1, 2, \ldots, n-1\}$
   b. Any set of n integers, any two of which are incogruent modulo n, forms a *complete residue system* modulo n.
   c. If modulo n a number a has order 3 and a number b has order 5, then their product ab must have order dividing 15.
   d. If modulo n a number a has order 3 and a number b has order 5, then their product ab must have order 15.
   e. For every natural numbers a and n there is a positive integer k such that $a^k = 1 \mod n$.
   f. For every natural numbers a and n there are distinct positive integers k, j such that $a^k = a^j \mod n$.
   g. If two numbers are inverses modulo n, then they must have the same order.
3. State and prove:
   a. The various parts of theorem 3.24 about the solution to the equation $ax = b \mod n$.
   b. Theorems 3.27 and 3.28 about simultaneous solution to two congruence equations (chinese remainder theorem).
   c. Fermat's little theorem (4.14)
4. State/Define:
   a. The $\phi(n)$ function.
   b. Euler's theorem (4.32).
   c. What it means for a number to be a quadratic residue modulo another number
   d. The Legendre symbol.
   e. Euler's criterion (7.9).
   f. Gauss' lemma (7.14), and the definition of g.
   g. The three laws for computing quadratic residues