Homework 5

(Cyclic U_n, powers modulo n, and quadratic residues.)

Due Monday, November 4 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) Recall that an element $[a] \in U_n$ is a primitive root if and only if $a^{\phi(n)/q} \not\equiv 1 \pmod{n}$ for each prime q dividing $\phi(n)$.
 (a) If $[g]$ is a primitive root modulo 37, which of the classes $[g^2], [g^3], [g^4], \ldots, [g^8]$ are primitive roots modulo 37?
 (b) Find all values n, where $6 \leq n \leq 16$, for which $[3]$ is a primitive root modulo n.

(2) Read the proof of Theorem 6.10 on p.107 of the text. Then prove the following statement: If $e \geq 3$, then $U_{2^e} = \{[\pm 3^i] \mid 0 \leq i < 2^{e-2}\}$.

(3) For each of the following, find all of the solutions x satisfying the congruence.
 (a) $x^5 \equiv 2 \pmod{37}$ (Hint: 2 is a primitive root modulo 37.)
 (b) $x^2 \equiv 5 \pmod{88}$

(4) Consider the set of quadratic residues mod 30, Q_{30}.
 (a) For each $[a] \in Q_{30}$, how many elements $[t] \in U_{30}$ are such that $t^2 \equiv a \pmod{30}$?
 (b) Use your result from part (a) to find all elements in Q_{30} without squaring every element in U_{30}.

(5) (a) Show that $(p - b)^2 \equiv b^2 \pmod{p}$.
 (b) Let p be an odd prime. Show that there are exactly $(p - 1)/2$ quadratic residues modulo p and exactly $(p - 1)/2$ nonresidues modulo p.

Fun problem (will not be graded): A number a is called a cubic residue modulo p if it is congruent to a cube modulo p.

(1) Make a list of the cubic residues modulo 5, 7, and 11.

(2) If p is prime and $p \equiv 2 \pmod{3}$, make a conjecture about which classes are cubic residues modulo p. Prove your conjecture.