Dartmouth College
Mathematics 25

Assignment 4
due Friday, October 23

1. Let p be an odd prime, and a an integer not divisible by p. Show that $x^2 \equiv a \pmod{p}$ is solvable if and only if $x^2 \equiv a \pmod{p^2}$ is solvable.

2. Determine how many solutions there are to $x^2 \equiv 124 \pmod{225}$ and find one of them using methods from the course.

3. Let p be a prime and $u, v \in \mathbb{Z}$ with $u \equiv v \pmod{(p-1)}$. Show that for any integer a, $a^u \equiv a^v \pmod{p}$.

4. Let p be an odd prime and a an integer not divisible by p. By Fermat's little theorem, we know that the set of positive integers h so that $a^h \equiv 1 \pmod{p}$ is nonempty. Denote the smallest such h by $e_p(a)$. Show that $e_p(a)$ divides $p-1$. Hint: Whenever you want to show one integer divides another, you use the division algorithm and try to show the remainder is zero.

5. Solve $3^{999} \equiv b \pmod{7}$ for $0 \leq b < 7$.

6. Find the least nonnegative residue of $7^{127} \pmod{12}$.

7. Show that for all integers a with $\gcd(a, 10) = 1$, that $a^{20} \equiv 1 \pmod{100}$.