Math 25, Homework 4, October 20, 2008

1. If p is a prime and u, v are integers with $u \equiv v \pmod{p-1}$, show that $a^u \equiv a^v \pmod{p}$ for every integer a.

2. Now generalize problem 1 and suppose n is a squarefree integer (that is, it is not divisible by any square larger than 1) and positive, and u, v are integers with $u \equiv v \pmod{\varphi(n)}$. Show that $a^u \equiv a^v \pmod{n}$ for every integer a.

3. If n is a positive integer and the integer a is coprime to n, let $\mathrm{ord}(a, n)$ be the least positive integer h with $a^h \equiv 1 \pmod{n}$. Prove that $\mathrm{ord}(a, n)$ exists and that it is a divisor of $\varphi(n)$.

4. Show that if $(a, 10) = 1$, then $a^{20} \equiv 1 \pmod{100}$.

5. Show that if $(a, 1001) = 1$, then $a^{60} \equiv 1 \pmod{1001}$.

6. Prove that if a is an integer, then $2730 \mid a^{13} - a$.

7. Prove that if a is an odd integer and j is an integer at least 3, then $a^{2^{j-2}} \equiv 1 \pmod{2^j}$.

8. Prove that 2047 is a base-2 strong pseudoprime. (Hint: isn't there a power of 2 nearby?)

9. Find a solution to $x^3 \equiv 2 \pmod{343}$.