Your Name Goes Here

Math 25

Homework 4

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. Let $n \geq 2$ and a be integers, with $\gcd(a, n) = 1$. Let

$$S = \{h \in \mathbb{Z}_+ \mid a^h \equiv 1 \pmod{n}\}.$$

   By Euler's theorem, we know that $S \neq \emptyset$. Denote by $e_n(a)$ the smallest element of S, that is the smallest positive integer h so that $a^h \equiv 1 \pmod{n}$. Show that $e_n(a) \mid \phi(n)$, where ϕ is Euler's function.

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

4. Show that 25 is a strong pseudoprime to the base 7.

5. Show that 1387 is a pseudoprime to the base 2, but not a strong pseudoprime to the base 2.