Math 105, Fall 2010, HW3

1. Show that if $p > 3$ is prime, then $n = (4^p - 1)/3$ is a pseudoprime (base 2). (That is, n is composite and $2^{n-1} \equiv 1 \pmod{n}$.)

2. More generally show that if $a > 1$, then $(a^{2p} - 1)/(a^2 - 1)$ is a base a pseudoprime for every odd prime p not dividing $a^2 - 1$.

3. Show that $n = (4^p + 1)/5$ is a base 2 strong pseudoprime for every prime $p > 5$. (That is, n is composite and if $n - 1 = 2^j k$, with k odd, then either $2^k \equiv 1 \pmod{n}$ or $2^{2^i k} \equiv -1 \pmod{n}$ for some $i < j$.) (Hint: The polynomial $4z^4 + 1$ is reducible in $\mathbb{Z}[x]$.)

4. We saw that if n is squarefree and $p - 1 \mid n - 1$ for each prime $p \mid n$, then $a^{n-1} \equiv 1 \pmod{n}$ for every integer a coprime to n. Prove the converse.

5. Show that if $a^{n-1} \equiv 1 \pmod{n}$ for every a coprime to n, then $a^n \equiv a \pmod{n}$ for every integer a.

6. Show that if $a^{n-1} \equiv 1 \pmod{n}$ for every a coprime to n, and n is composite, then n has at least 3 prime factors.