Number Theory Homework #9

Prof. Zeev Rudnick

To be handed in by Monday, January 9, 2012.

---

1. Decide which of the following congruences are solvable, and if so, find all solutions:

a) $x^2=c \bmod 363$, $c=1,5,31$. b) $x^2 = 54 \bmod 125$.

2. A composite integer $n>1$ is a **pseudo-prime to base 2** (PP_2) if $2^n = 2 \bmod n$. Show that there are infinitely many PP_2's.

Hint: Show that 341 is a PP_2, and that if $n=ab$ is a PP_2 then so is 2^n-1.

3. A *Carmichael number* is a composite integer $N>1$ which satisfies $a^{N-1} = 1 \bmod N$ for all a coprime to N. Show that if $p=6k+1$, $q=12k+1$, $r=18k+1$ are all prime then their product $N=pqr$ is a Carmichael number. Find two values of k which satisfy this assumption.

4. Korselt's criterion states that a composite integer N is a Carmichael number if and only if N is odd, square-free and all prime divisors p of N satisfy p-1 divides N-1.
Check which of the following integers are Carmichael numbers: 1105, 1235, 2821, 6601, 8910.
