Math 445 Homework 2

Due Wednesday, September 15

6. [The "only if" part of the characterization of Charmichael numbers.]

   Show that if $N = p_1 \cdots p_k$ is a product of distinct primes and $(p_i - 1)|(N - 1)$, for every i, then N is a pseudoprime to every base a satisfying $(a, N) = 1$.

   (Hint: Show that a number $\equiv 1 \pmod{p_i}$ for every i is $\equiv 1 \pmod{N}$.)

7. Show that if $n = pq$ with $p < q$ and p, q both prime, then it is not possible for $q - 1$ to divide $n - 1$. (Consequently, Carmichael numbers must have at least three prime factors...)

   (Hint: If it did, then show that the other factor would have to be too big....)

8. Show that 2465, 2821, and 6601 are Carmichael numbers.

9. (NZM, Problem 2.4.9) [For a pseudoprime, failing the Miller-Rabin test <u>finds</u> factors.]

   Show that if $x^2 \equiv 1 \pmod{n}$ and $x \not\equiv \pm 1 \pmod{n}$, then $1 < (x - 1, n) < n$ and $1 < (x + 1, n) < n$.

10. Show that $n = 3277 = 29 \times 113$ is a strong pseudoprime to the base 2.
    [Do the calculations by hand....]