Math 445 Homework 2

Due Friday, September 13

5. 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: the other factor would have to be too big....

6. Locate (by whatever means you choose) a Carmichael number n other than 561, and show that it is a pseudoprime to every base relatively prime to n.

7. (NZM, Problem 2.1.41) Find all triples of integers $a, b, c > 0$ for which

   $$a \equiv b \pmod{c}\ ,\ b \equiv c \pmod{a}, \text{ and } c \equiv a \pmod{b}$$

   simultaneously.

   Hint: Up to changing names, you can assume that either $a = b$ or $0 < a < b < c$. Each says something important about c.

8. (NZM, Problem 2.4.9) [for a pseudoprime, failing the Miller-Rabin test finds 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 $1 < (x + 1, n) < n$.

9. Show that $n = 3277 = 29 \times 113$ is a strong pseudoprime to the base 2.