Math 445 Homework 2

Due Wednesday, Sept. 17

5. Show, by induction, that for every $n \in \mathbb{N}$, $f(n) = \dfrac{1}{2}n^4 + \dfrac{1}{3}n^3 + \dfrac{1}{6}n$ is an integer.

   (Note, however, that it is *not* a multiple of n !)

6. Show that 8321=53×157 is a strong pseudoprime to the base 2.
   [Do the calculations by hand....]

7. Show that $\gcd(ab, n)$ divides $[\gcd(a, n)][\gcd(b, n)]$.

   (There are at least 3 distinct proofs, depending on how you characterize gcd's?)

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