Math 445 Homework 2

Due Wednesday, Sept. 17

5. Show, by induction, that for every $n \in \mathbb{N}$, $f(n) = \frac{1}{2}n^4 + \frac{1}{3}n^3 + \frac{1}{6}n$ is an integer. (Note, however, that it is *not* a multiple of n !)

We proceed by induction. For $n = 1$, $f(1) = \frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$, which is an integer. This gives us our base case. We now assume that $f(n)$ is an integer and compute

$f(n+1) = \frac{1}{2}(n+1)^4 + \frac{1}{3}(n+1)^3 + \frac{1}{6}(n+1) =$

$\frac{1}{2}(n^4 + 4n^3 + 6n^2 + 4n + 1) + \frac{1}{3}(n^3 + 3n^2 + 3n + 1) + \frac{1}{6}(n+1) =$

$(\frac{1}{2}n^4 + \frac{1}{3}n^3 + \frac{1}{6}n) + \frac{1}{2}(4n^3 + 6n^2 + 4n + 1) + \frac{1}{3}(3n^2 + 3n + 1) + \frac{1}{6}(1) =$

$f(n) + \frac{1}{2}(4n^3) + (\frac{1}{2} \cdot 6 + \frac{1}{3} \cdot 3)n^2 + (\frac{1}{2} \cdot 4 + \frac{1}{3} \cdot 3)n + (\frac{1}{2} + \frac{1}{3} + \frac{1}{6}) =$

$f(n) + 2n^3 + 4n^2 + 3n + 1$,

which is the sum of $f(n)$, an integer, and $2n^3 + 4n^2 + 3n + 1$, an integer. So $f(n+1)$ is an integer, and so by induction, $f(n)$ is an integer for every $n \in \mathbb{N}$. Note, however, that $f(2) = f(1) + 2 + 4 + 3 + 1 = 11$, which is not a multiple of 2....

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

To show that 8321 is a strong pseudoprime to the base 2, we compute:
$8321 - 1 = 8320 = 2 \cdot 4160 = 2 \cdot 4 \cdot 1040 = 2^3 \cdot 4 \cdot 260 = 2^5 \cdot 4 \cdot 65 = 2^7 \cdot 65$.
So we first compute 2^{65} mod 8321, noting that $65 = 64 + 1 = 2^6 + 1$, so we start squaring:
$2^2 = 4$, $2^4 = 4^2 = 16$, $2^8 = 16^2 = 256$, and $2^{16} = 256^2 = 65536 = 8321 \cdot 7 + 7289 \equiv 7289$ mod 8321. Then $2^{32} \equiv 7289^2 = 53129521 = 8321 \cdot 6384 + 8257 \equiv 8257 \equiv -64$ mod 8321, and then $2^{64} \equiv (-64)^2 = 4096$ mod 8321, so $2^{65} = 2^{64} \cdot 2^1 \equiv 4096 \cdot 2 = 8192 \equiv -129$ mod 8321.

This is neither 1 nor -1, so we start squaring:

$2^{130} \equiv (-129)^2 = 16641 = 8321 \cdot 1 + 8320 \equiv 8320 \equiv -1$ mod 8321. So that didn't take long; $2^{260} \equiv (-1)^2 = 1$ so the sequence of repeated squares reaches -1 just before it reaches 1, <u>and</u> it reaches 1 (by the time the squarings reach raising 2 to the 8320, so 8321 passes the Miller-Rabin test for the base 2. But since $8321 = 53 \cdot 157$ is not prime, it is a strong pseudoprime to the base 2.

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?)

Proof #1, using $(a, n) =$ product of prime powers, where we always choose the smaller exponent found in a and n; or, symbolically, if $a = \prod p_i^{\epsilon_i}$ and $b = \prod p_i^{\delta_i}$, then $(a, b) = \prod p_i^{\gamma_i}$, where $\gamma_i = \min\{\epsilon_i, \delta_i\}$. Then:

If we write $a = \prod p_i^{\epsilon_i}$ and $b = \prod p_i^{\delta_i}$, $n = \prod p_i^{\eta_i}$, then $(a,n) = \prod p_i^{\gamma_i}$, with $\gamma_i = \min\{\epsilon_i, \eta_i\}$, $(b,n) = \prod p_i^{\theta_i}$, with $\theta_i = \min\{\delta_i, \eta_i\}$, and, since $ab = \prod p_i^{\epsilon_i+\delta_i}$, $(ab,n) = \prod p_i^{\phi_i}$, with $\phi_i = \min\{\epsilon_i + \delta_i, \eta_i\}$.

But then to show that $\prod p_i^{\phi_i} = (ab,n)|(a,n)(b,n) = \prod p_i^{\gamma_i+\theta_i}$, it is enough to show that $\phi_i \leq \gamma_i + \theta_i$ for every i, that is, $\min\{\epsilon_i + \delta_i, \eta_i\} \leq \min\{\epsilon_i, \eta_i\} + \min\{\delta_i, \eta_i\}$, i.e., $\min(x+y,z) \leq \min(x,z) + \min(y,z)$ for any $x,y,z \geq 0$. But if either of the terms on the rightside <u>is</u> z, then $\min(x+y,z) \leq z \leq \min(x,z)+\min(y,z)$ (the first by definition of min, the second since one of the numbers <u>is</u> z and the other is ≥ 0). But if the terms on the right side are x and y, then $\min(x+y,z) \leq x+y \leq \min(x,z)+\min(y,z)$, as desired. This establishes our argument, so $(ab,n)|(a,n)(b,n)$, as desired.

Proof #2: (a,n) is the largest integer that can be expressed as $(a,n) = ax + ny$ for $x, y \in \mathbb{Z}$. similarly, we may write $(b,n) = bu + nv$. So $(a,n)(b,n) = (ax+ny)(bu+nv) = (ab)(xu) + n(ybu + axv + yv)$ and so can be expressed as an integer-linear combination of ab and n. But (ab,n) divides any number that can be so expressed, so $(ab,n)|(a,n)(b,n)$, as desired.

Proof #3: $(a,n)|a$, so $(a,n)|ab$, and $(a,n)|n$, so together these give $(a,n)|(ab,n)$ (by the definition of (ab,n)). So we can write $(ab,n) = x(a,n)$. To show that $(ab,n)|(a,n)(b,n)$ then, it is enough to show that $x|(b,n)$ (since then $(ab,n) = (a,n)x|(a,n)(b,n)$). But to show this, it is enough to show that $x|b$ and $x|n$. But: $(ab,n)|n$, so $x(a,n)|n$, so $x|n$. Further, $k(m,n) = (km,kn)$, since $(m,n)|m,n$, so $k(m,n)|km,kn$, so $k(m,n)|(km,kn)$, while $k(m,n)$ can be expressed as a $\mathbb{Z}$-linear combination of km and kn, so $(km,kn)|k(m,n)$. So:

$x(a,n) = (ab,n) = ((a,n)\frac{a}{(a,n)}b, (a,n)\frac{n}{(a,n)}) = (a,n)(\frac{a}{(a,n)}b, \frac{n}{(a,n)})$, we have $x = (b\frac{a}{(a,n)}, \frac{n}{(a,n)})$. So $x|b\frac{a}{(a,n)}$ and $x|\frac{n}{(a,n)}$. But since $(\frac{a}{(a,n)}, \frac{n}{(a,n)}) = 1$, we can express $1 = \frac{a}{(a,n)}u + \frac{n}{(a,n)}v$, so $b = \frac{a}{(a,n)}bu + \frac{n}{(a,n)}bv$, and then $x|b$ since it divides factors of both terms in the sum.

So $x|b$ and $x|n$, so $x|(b,n)$, so $(ab,n) = (a,n)x|(a,n)(b,n)$, as desired.

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 $1 < (x+1,n) < n$.

   If $x^2 \equiv 1 \pmod{n}$ and $x \not\equiv \pm 1 \pmod{n}$, then we have $n|x^2 - 1 = (x-1)(x+1)$, but $n \not| x-1$ (since $x \not\equiv 1 \pmod{n}$) and $n \not| x+1$ (since $x \not\equiv -1 \pmod{n}$). But if $(n, x-1) = 1$, then since $n|(x-1)(x+1)$ we have $n|x+1$, a contradiction. [E.g., problem #7 says $n = (x^2-1,n)|(x-1,n)(x+1,n) = (x+1,n)$, so $n|(x+1)$.] So $(n,x-1) > 1$. Similarly, if $(n,x+1) = 1$, then since $n|(x-1)(x+1)$ we have $n|x-1$, a contradiction. So $(n,x+1) > 1$. $(n,x-1) \geq n$ implies $(n,x-1) = n$ (the gcd of two numbers cannot exceed the numbers), which in turn implies $n|x-1$ (since $(a,b)|b$), a contradiction. So $(n,x-1) < n$. Similarly, $(n,x+1) < n$. So we have $1 < (n,x-1) < n$ and $1 < (n,x+1) < n$, as desired.