CS 202, PSET 7

7.1
Show for $n \in N : 12|(n(n+1)(n+2)(n+3))$
In other words, $(n(n+1)(n+2)(n+3)) \equiv 0(\text{mod}12)$
Chinese remainder theorem:
For $m1$ and $m2$ as relatively prime, if
n mod $m1 = n1$
n mod $m2 = n2$
Then, there exists a unique solution $n : 0 \leq n < m1 * m2$
Let $prod = n(n+1)(n+2)(n+3)$
Propose that $prod \equiv 0(\text{mod}3)$ and prod $\equiv 0(\text{mod}4)$
If this is true, then $prod \equiv 0(\text{mod}12)$
Proof that $prod \equiv 0(\text{mod}3)$:
if $n = 0$, $prod = 0(0+1)(0+2)(0+3) = 0 \equiv 0(\text{mod}3)$
if $n = 1$, $prod = 1(1+1)(1+2)(1+3) = 24 \equiv 0(\text{mod}3)$
if $n = 2$, $prod = 2(2+1)(2+2)(2+3) = 120 \equiv 0(\text{mod}3)$
if $n = 3$, $prod = 3(3+1)(3+2)(3+3) = 360 \equiv 0(\text{mod}3)$
Proof that $prod \equiv 0$ mod 4:
if $n = 0$, $prod = 0(0+1)(0+2)(0+3) = 0 \equiv 0(\text{mod}4)$
if $n = 1$, $prod = 1(1+1)(1+2)(1+3) = 24 \equiv 0(\text{mod}4)$
if $n = 2$, $prod = 2(3)(4)(5) = 120 \equiv 0(\text{mod}4)$
if $n = 3$, $prod = 3(4)(5)(6) = 360 \equiv 0(\text{mod}4)$
if $n = 4$, $prod = 4(5)(6)(7) = 840 \equiv 0(\text{mod}4)$
So $(n(n+1)(n+2)(n+3)) \equiv 0(\text{mod}12)$
$12|(n(n+1)(n+2)(n+3))$

7.2
1) $x^2 \equiv y^2(\text{mod}p)$ premise
2) $p|x^2 - y^2$ definition of congruence
3) $p|(x-y)(x+y)$ algebraic equality
4) $p|(x-y) \vee p|(x+y)$ from Euclid's Lemma that $p|ab \leftrightarrow p|a \vee p|b$
5) $p|(x-y) \vee p|(x-(-y))$ rewrite the right part of the or
6) $x \equiv y(\text{mod}p) \vee x \equiv -y(\text{mod}p)$ definition of congruence in reverse

7.3
$x_{i+1} = x_i^k$ in N
$x_{i+1} = x_i^k$ in mod2^b
Show that if x_0 is odd, and k is odd then $x_{2^{b-2}} = x_0$
In other words, show $x_{2^{b-2}} \equiv x_0(\text{mod}2^b)$
Come up with a non-recursive expression:
$x_0 = x_0$
$x_1 = (x_0)^k$
$x_2 = (x_1)^k = ((x_0)^k)^k = (x_0)^{k^2}$
$x_3 = (x_2)^k = ((x_0)^{k^2})^k = (x_0)^{k^3}$

So we get $x_i = (x_0)^{k^i}$
Proof by induction:
Base case, $i = 0:\ x_0 = (x_0)^{k^0} = x_0$ so it works
Inductive step: hypothesis: $x_i = (x_0)^{k^i}$
Prove for $x_{i+1} = (x_0)^{k^{i+1}}$
We know from the question that $x_{i+1} = x_i^k = (x_i)^k$
And by ind. hypothesis, we can sub in to get: $(x_0^{k^i})^k = x_0^{k^{i+1}} = (x_0)^{k^{i+1}}$ and we're done.
Using $x_i = (x_0)^{k^i}$, we can say $x_{2^{b-2}} = (x_0)^{k^{2^{b-2}}}$
Euler's Thm:
if $gcd(a, p) = 1$, then $a^{\phi(p)} \equiv 1(\text{mod} p)$
if $gcd(x_0, 2^b)$ is true, because x_0 is odd and, 2^b is a power of 2
then $x_0^{\phi(2^b)} \equiv 1(\text{mod} 2^b)$
Simplifying the totient: $\phi(2^b) = (2^{b-1})(2-1) = (2^{b-1})$
So $x_0^{2^{b-1}} \equiv 1(\text{mod} 2^b)$
Euler's again to bring in k:
if $gcd(k, 2^{b-1}) = 1$ is true because k is odd, and 2^{b-1} is a power of 2
then $k^{\phi(2^{b-1})} \equiv 1(\text{mod} 2^{b-1})$
Simplifying the totient: $\phi(2^{b-1}) = 2^{b-2}$
So $k^{2^{b-2}} \equiv 1(\text{mod} 2^{b-1})$
Lastly:
$k^{2^{b-2}} = 1 + m * 2^{b-1}$, for some $m \in N$ by definition
$x_2^{b-2} = x_0^{k^{2^{b-2}}}$ (from the top of this page)
$x_2^{b-2} = x_0^{1+m*2^{b-1}}$
$x_2^{b-2} = x_0 * (x_0^{2^{b-1}})^m$
But from the second Euler's we know:
$\equiv x_0 * 1^m(\text{mod} 2^b)$
$\equiv x_0(\text{mod} 2^b)$