Math 522 Exam 7 Solutions

1. Use the Chinese Remainder theorem to find three consecutive integers, each divisible by the square of a prime.

   There are many ways to set up this problem. We seek x such that $4|x-2, 9|x-1, 25|x$. This corresponds to the system of modular equations $\{x \equiv 2(\text{mod } 4), x \equiv 1(\text{mod } 9), x \equiv 0(\text{mod } 25)\}$. In the notation of Thm. 5.4, we have $c_1 = 2, c_2 = 1, c_3 = 0, m_1 = 4, m_2 = 9, m_3 = 25$. Hence $n_1 = 225, n_2 = 100, n_3 = 36$. We now find the inverse of $n_1 = 225 \equiv 1(\text{mod } 4)$, which is 1. We find the inverse of $n_2 = 100 \equiv 1(\text{mod } 9)$, which is also 1. We don't need to find the inverse of $n_3 = 36 \equiv 11(\text{mod } 25)$, but it happens to be -9 (or 16). Hence our solution is $x = 2(225)(1) + 1(100)(1) + 0(36)(-9) = 550$, giving the desired three consecutive integers $\{548, 549, 550\}$.

2. Prove that if p denotes an odd prime, then $2^{\frac{p-1}{2}} \equiv \pm 1(\text{mod } p)$.
   BONUS: Characterize all $n \in \mathbb{Z}$ such that $n^{\frac{p-1}{2}} \equiv \pm 1(\text{mod } p)$.

   Set $x = 2^{\frac{p-1}{2}}$. Note that $\gcd(2, p) = 1$, so by Euler's Theorem, $x^2 = 2^{p-1} \equiv 1(\text{mod } p)$. Hence $x^2 - 1 = (x-1)(x+1) \equiv 0(\text{mod } p)$. Now, by problem 2 from exam 5, either $x - 1 \equiv 0(\text{mod } p)$ or $x + 1 \equiv 0(\text{mod } p)$. [More detailed proof: if $p|(x-1)(x+1)$ then either $p|x-1$ or $p|x+1$]. Hence $x \equiv \pm 1(\text{mod } p)$.

   BONUS: The identical argument works if we replace 2 by any n with $\gcd(n, p) = 1$. On the other hand, if $\gcd(n, p) \neq 1$, then $\gcd(n, p) = p$, so $p|n$. Now we have $n^{\frac{p-1}{2}} \equiv 0^{\frac{p-1}{2}} \equiv 0 \not\equiv \pm 1(\text{mod } p)$. Hence the modular equation holds if and only if $p \nmid n$.

3. High score=102, Median score=77, Low score=53