Math 522 Exam 8 Solutions

1. Find *all* solutions to the following system of congruences:

$$\begin{aligned} x &\equiv 3 \pmod{6} \\ x &\equiv 7 \pmod{10} \\ x &\equiv 12 \pmod{15} \end{aligned}$$

   We first reduce the congruences as: $x \equiv 3 \pmod 2, x \equiv 3 \pmod 3, x \equiv 7 \pmod 2, x \equiv 7 \pmod 5, x \equiv 12 \pmod 3, x \equiv 12 \pmod 5$. Simplifying and eliminating redundancies, these become $x \equiv 1 \pmod 2, x \equiv 0 \pmod 3, x \equiv 2 \pmod 5$.

   Now, $M = 30, n_1 = 15, n_2 = 10, n_3 = 6$. We calculate $n_1^{-1} = 1 \pmod 2$, $n_2^{-1} = 1 \pmod 3$, $n_3^{-1} = 1 \pmod 5$. Hence we may take $x = 1n_1n_1^{-1} + 0n_2n_2^{-1} + 2n_3n_3^{-1} = 15 + 12 = 27$. This solution is unique modulo 30, hence the set of all solutions is $\{27 + 30n : n \in \mathbb{Z}\}$.

2. Let p be an odd prime, and suppose that $x^2+1 \equiv 0 \pmod p$ has exactly two solutions (that are distinct modulo p). Prove that $x^2 + 1 \equiv 0 \pmod{p^3}$ has exactly two solutions (that are distinct modulo p^3).

   Let a, b be the two solutions mod p; that is, $a^2 + 1 \equiv b^2 + 1 \equiv 0 \pmod p$.[1] Note that $p \nmid a$ since otherwise $1 \equiv 0 \pmod p$. Similarly, $p \nmid b$.

   Consider $f(x) = x^2 + 1$; note that $f'(x) = 2x$. If $p|f'(a) = 2a$, since p is odd we have $p|a$; but we have shown that is impossible. Similarly, $p \nmid f'(b)$. Hence we may apply Hensel's lifting lemma to find just two solutions a' and b' to $f(x) \equiv 0 \pmod{p^2}$. Further, $a' = a + pt$ for some integer t, so $p \nmid a'$ since $p \nmid a$. Similarly, $p \nmid b'$.

   Now, if $p|f'(a') = 2a'$, since p is odd we have $p|a'$; but we have shown that is impossible. Similarly, $p \nmid f'(b')$. Hence we may apply Hensel's lifting lemma again to find just two solutions a'', b'' to $f(x) = x^2+1 \equiv 0 \pmod{p^3}$.

   NOTE: In fact, we could continue this inductively to prove that $x^2+1 \equiv 0$ has exactly two solutions modulo p^k, for any $k \in \mathbb{N}$. Typically, the solutions will vary as k varies, but there will always be two of them!

[1] In fact $a \equiv -b \pmod p$ but that's not important here.