MA2316: solutions to the quiz

1. Note that $84 = 3 \cdot 4 \cdot 7$, and $36 = 4 \cdot 9$. Therefore the systems of congruences in question can be replaced by equivalent systems

$$(\mathbf{a}) \begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 4, \\ x \equiv 4 \pmod 7, \\ x \equiv 0 \pmod 4, \\ x \equiv 8 \pmod 9. \end{cases} (\mathbf{b}) \begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 4, \\ x \equiv 4 \pmod 7, \\ x \equiv 3 \pmod 4, \\ x \equiv 7 \pmod 9. \end{cases} (\mathbf{c}) \begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 4, \\ x \equiv 4 \pmod 7, \\ x \equiv 3 \pmod 4, \\ x \equiv 5 \pmod 9. \end{cases}$$

From this we instantly see that the first system does not have solutions since it has contradicting congruences $x \equiv 3 \pmod 4$ and $x \equiv 0 \pmod 4$, the second system does not have solutions because it has contradicting congruences $x \equiv 2 \pmod 3$ and $x \equiv 7 \pmod 9$ (since $x \equiv 7 \pmod 9$ implies $x \equiv 1 \pmod 3$), and the third system is equivalent to the system

$$\begin{cases} x \equiv 3 \pmod 4, \\ x \equiv 4 \pmod 7, \\ x \equiv 5 \pmod 9. \end{cases}$$

(since $x \equiv 5 \pmod 9$ implies $x \equiv 2 \pmod 3$, the latter congruence can be thrown away without changing the solution set). It remains to describe solutions to this, where we are in the usual setup of the Chinese Remainder Theorem. First of all, since we have $4 \cdot 2 + 7 \cdot (-1) = 1$, the first two congruences can be assembled into $x \equiv 3 \cdot 7 \cdot (-1) + 4 \cdot 4 \cdot 2 = 32 - 21 = 11 \pmod{28}$. Second, since $28 \cdot 1 + 9 \cdot (-3) = 1$, the remaining congruence can be merged in, obtaining

$$x \equiv 11 \cdot 9 \cdot (-3) + 5 \cdot 28 \cdot 1 = 140 - 297 = -157 \equiv 95 \pmod{252}.$$

2. A general remark: solving polynomial congruences modulo prime numbers is hard, unless we deal with quadratic equations, in which case we can use Legendre symbols, as we shall see below. Once that is done, solving them modulo prime powers, if needed, is done using Hensel's lemma, and solving them modulo products of prime powers is done using the Chinese Remainder Theorem.

(**a**) $x^2 - 10x + 11 \equiv 0 \pmod{61}$: completing the square, we get $(x-5)^2 - 14 \equiv 0 \pmod{61}$, so we just need to know if 14 is a square modulo 61. Since 61 is a prime, we need to compute $\left(\frac{14}{61}\right)$.

$$\left(\frac{14}{61}\right) = \left(\frac{2}{61}\right)\left(\frac{7}{61}\right) = (-1)^{\frac{61^2-1}{8}}(-1)^{\frac{(61-1)(7-1)}{4}}\left(\frac{61}{7}\right) =$$
$$= -\left(\frac{5}{7}\right) = -(-1)^{\frac{(7-1)(5-1)}{4}}\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) = -(-1)^{\frac{5^2-1}{8}} = 1,$$

therefore the congruence has solutions.

(**b**) $x^2 - 10x + 11 \equiv 0 \pmod{183}$: since $183 = 61 \cdot 3$, this congruence has solutions if the two congruences modulo 61 and modulo 3 do. We already looked at 61 above, so we just need to know if 14 is a square modulo 3. Since $14 \equiv 2 \pmod 3$, there are no solutions.

(**c**) $x^2 + 2x - 9 \equiv 0 \pmod{97}$: completing the square, we get $(x+1)^2 - 10 \equiv 0 \pmod{97}$, so we need to know if 10 is a square modulo 97. Since 97 is a prime, we need to compute $\left(\frac{10}{97}\right)$.

$$\left(\frac{10}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{5}{97}\right) = (-1)^{\frac{97^2-1}{8}}(-1)^{\frac{(97-1)(5-1)}{4}}\left(\frac{97}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

therefore the congruence has no solutions.

3. Note that $f'(x) = 3x^2 + 3$, so in $\mathbb{Z}/5\mathbb{Z}$ we have $f'(3) = 0$ and $f'(4) \neq 0$. Therefore, the root $x = 4$ admits the unique lift to $\mathbb{Z}/25\mathbb{Z}$ by Hensel's lemma. To investigate the root $x = 3$, let us try to lift it in some way, letting $x = 3 + 5k$. We have

$$(3+5k)^3+3(3+5k)+9 \equiv 3^3+3\cdot 3^2\cdot 5k+9+15k+9 \equiv 2+10k+18+15k \equiv 20 \pmod{25},$$

so there is no way to choose k to yield a root. We conclude that this equation has just one root modulo 25.