MATH 115A Number Theory, Quiz 4

1. Solve the system of congruences

\[
\begin{align*}
    x &\equiv 1 \pmod{5} \\
    x &\equiv 2 \pmod{6} \\
    x &\equiv 3 \pmod{7}.
\end{align*}
\]

By the proof of the Chinese remainder theorem, if we let

\[
\begin{align*}
    M &= 210, \\
    M_1 &= 42, \\
    M_2 &= 35, \\
    M_3 &= 30,
\end{align*}
\]

\[
y_1 = 3 \text{ be an inverse of } M_1 \text{ modulo 5, } y_2 = 5 \text{ be an inverse of } M_2 \text{ modulo 6, and } y_3 = 4 \text{ be an inverse of } M_3 \text{ modulo 7, then}
\]

\[
x = 1 \cdot M_1 \cdot y_1 + 2 \cdot M_2 \cdot y_2 + 3 \cdot M_3 \cdot y_3 = 126 + 350 + 360 = 836
\]

is one solution to the system of congruences given in the problem statement. Moreover, by the statement of the Chinese remainder theorem there is a unique solution to this system modulo \(5 \cdot 6 \cdot 7 = 210\). Thus, every solution to this system is given by

\[
x \equiv 836 \equiv 206 \pmod{210}.
\]
2. Let \( f(x) = x^4 - 3x^3 + x^2 + 4 \). Solve the polynomial congruence
\[
f(x) \equiv 0 \mod 9.
\]

Be sure to explicitly describe all of the congruence classes of solutions modulo 9, and to justify why you have found all the solutions.

Any solution to the above congruence must satisfy
\[
f(x) \equiv 0 \mod 3.
\]

By inspection, the \( x \) satisfying this congruence are \( x \equiv 1 \mod 3 \) and \( x \equiv 2 \mod 3 \).

Note that \( f'(x) = 4x^3 - 9x^2 + 2x \).

We compute that \( f'(1) = -3 \equiv 0 \mod 3 \). Also, \( f(1) = 3 \not\equiv 0 \mod 9 \). Thus by Hensel’s lemma (case (iii)), there are no solutions to \( f(x) \equiv 0 \mod 9 \) such that \( x \equiv 1 \mod 3 \).

Now we compute that \( f'(2) = 0 \equiv 0 \mod 3 \). Also, \( f(2) = 0 \equiv 0 \mod 9 \). Thus by Hensel’s lemma (case (ii)), there are 3 solutions to \( f(x) \equiv 0 \mod 9 \) such that \( x \equiv 2 \mod 3 \). These are \( x \equiv 2 \mod 9 \), \( x \equiv 5 \mod 9 \), and \( x \equiv 8 \mod 9 \).

Because every solution to \( f(x) \equiv 0 \mod 9 \) must come from a solution to \( f(x) \equiv 0 \mod 3 \) in the manner of Hensel’s lemma, we conclude that all of the solutions to \( f(x) \equiv 0 \mod 9 \) are the integers \( x \) such that
\[
x \equiv 2 \mod 9, \quad x \equiv 5 \mod 9, \quad \text{or} \quad x \equiv 8 \mod 9.
\]