Quiz # 3

(10 points for each question).

Problems:

1. Determine if the congruence \( x^2 \equiv 3 (\text{mod} 53) \) has a solution.
   
   Solution:
   The question is whether the Legendre symbol \( \left( \frac{3}{53} \right) \) is 1 or \(-1\). Since 53 \( \equiv 1 \) (mod 4) and since 53 \( \equiv 2 \) (mod 3), we have by Quadratic Reciprocity
   \[
   \left( \frac{3}{53} \right) = \left( \frac{53}{3} \right) = \left( \frac{2}{3} \right)
   \]
   Again by Quadratic Reciprocity, the last Legendre symbol is \(-1\) since 3 \( \equiv -1 \) (mod 3) and use Quadratic reciprocity. This the original quadratic congruence has no solutions.

2. Compute \( \left( \frac{21}{53} \right) \);
   
   Solution:
   \[
   \left( \frac{21}{53} \right) = \left( \frac{3}{53} \right) \left( \frac{7}{53} \right) = \left( \frac{53}{3} \right) \left( \frac{53}{7} \right) \left( -1 \right)^{1-26} \left( \frac{53}{7} \right) \left( -1 \right)^{3-26} = \left( \frac{2}{3} \right) \left( \frac{4}{7} \right)
   \]
   \[
   = (-1) \left( \frac{2}{7} \right)^2 = (-1)(-1)^{(7^2-1)/4} = (-1)(-1)^{12} = -1.
   \]

3. Give the number of element in \( U_9 \). Give a primitive root mod 9. Describe explicitly all the element of \( U_9 \) in term of this primitive root mod 9.
   
   Solution:
   Number of elements: \( \phi(9) = 6 \).
   \( 2^i \equiv 1 \) mod 9, for \( i \in \{1, 2, \ldots, 6\} \) and \( 2^6 \equiv 1 \) mod 9.
   \( U_9 = \{2, 2^2, 2^3, 2^4, 2^5, 2^6\} \).

4. Give explicitly all the elements of \( U_{2^n} \) where \( n \in \mathbb{N} \).
   
   Solution:
   \( (-1)^s 5^t \) where \( s \in \{0, 1\} \) and \( 0 \leq t \leq 2^{n-2} \).

5. List all \( a \in (\mathbb{Z}/35\mathbb{Z})^* \) such that \( a \) is not a quadratic residue (mod 35).
   
   Solution:
   \( 1^2 \equiv 1 \) mod 35, \( 2^2 \equiv 4 \) mod 35, \( 3^2 \equiv 9 \) mod 35, \( 4^2 \equiv 16 \) mod 35, \( 5^2 \equiv 25 \equiv -10 \) mod 35
\[6^2 \equiv 1 \mod 35, 7^2 \equiv 49 \equiv 4 \mod 35, 8^2 \equiv 64 \equiv -6 \mod 35, 9^2 \equiv 81 \equiv 11 \mod 35\]
\[10^2 \equiv 100 \equiv -5 \mod 35, 11^2 \equiv 121 \equiv 16 \mod 35, 12^2 \equiv 2^2 6^2 \equiv 4 \mod 35\]
\[13^2 \equiv 169 \equiv -6 \mod 35, 14^2 \equiv 2^2 7^2 \equiv 4 \times 4 \equiv 16 \mod 35\]
\[15^2 \equiv 3^2 5^2 \equiv 9 \times (-10) \equiv 15 \mod 35, 16^2 \equiv 2^2 8^2 \equiv (-6) \times 4 \equiv 11 \mod 35, 17^2 \equiv 289 \equiv 9 \mod 35\]

\[-10, -6, -5, 1, 4, 9, 11, 15, 16 \text{ are quadratic residue}\]

\[\text{and then } -17, -16, -15, -14, -13, -12, -11, -9, -8, -7, -4, -3, -2, -1\]

\[2, 3, 5, 6, 7, 8, 10, 12, 13, 14, 17 \text{ are the non residue.}\]