Handout for sections 9.1, 9.2, & 9.3

1. Remember the relation between the solutions of 
\[ ax^2 + bx + c \equiv 0 \pmod{p} \land y^2 \equiv d \pmod{p}, \]
where \( y = 2ax + b \land d = b^2 - 4ac \)

2. Does \( x^2 \equiv 7 \pmod{31} \) have a solution?
   i.e., is 7 a quadratic residue \( \pmod{31} \)?
   \( 7^2 \equiv 49 \equiv 18 \pmod{31}, \quad 7^4 \equiv 18^2 \equiv 324 \equiv 14 \pmod{31}, \)
   \( 7^8 \equiv 14^2 \equiv 196 \equiv 10 \pmod{31}, \quad 7^{16} \equiv 10^2 \equiv 100 \equiv 7 \pmod{31} \)
   Since, 7 and 31 are coprime, we get \( 7^{15} \equiv 1 \pmod{31} \).
   So, a solution exists. Since \( (7^8)^2 \equiv 7 \pmod{31} \), \( x \equiv 7^8 \) is a solution.
   \( 7^8 \equiv 10 \pmod{31} \), \( 6 \cdot 10 \equiv 10 \pmod{31} \) is a solution.
   The second solution is \( x \equiv 21 \pmod{31} \) (\( 21 = 31 - 10 \)).

3. Does \( x^2 \equiv 85 \pmod{97} \) have a solution? i.e., find \( (85/97) \).
   \( (85/97) = (-12/97) = (-1/97) \cdot (4/97) \cdot (3/97) \)
   Since \( 85 \equiv -12 \pmod{97} \) by multiplicativity \( = (-1/97) \cdot (3/97) = 1 \)
   \( -1/97 \equiv (-1)^{48} = 1 \)
   \( 3/97 \equiv (97/3) = (1/3) = 1 \)
   By QL, \( \frac{97}{3} \equiv 1 \pmod{3} \)
   So, a solution exists.

4. Solve \( 3x^2 + 9x + 7 \equiv 0 \pmod{13} \)
   This is the same as \( y^2 \equiv 10 \pmod{13} \) where \( y \equiv 6x + 9 \pmod{13} \)
   Clearly, \( y \equiv \pm 6 \pmod{13} \) is one of the solutions.
   So, \( 6x + 9 \equiv 6 \pmod{13} \) & \( 6x + 9 \equiv -6 \pmod{13} \) give the solutions for \( x \).
   \( 6x \equiv -3 \pmod{13} \) gives \( x \equiv 6 \pmod{13} \), by EA or Bland.
   \( 6x \equiv -15 \pmod{13} \) gives \( x \equiv 4 \pmod{13} \), by __________

5. \( (19/23) = (-4/23) = (4/23)(-1/23) = 1 \cdot (-1) = -1 \)
   \( (-23/59) = (36/59) = (6^2/59) = 1 \)
4. Find \((7/13)\) using Gauss Lemma.

\[13^{-1} = 6 \text{ so, } S = \{7, 14, 21, 28, 35, 42\}\]

Modulo 13, \(7 \equiv 7, 14 \equiv 1, 21 \equiv 8, 28 \equiv 2, 35 \equiv 9, 42 \equiv 3\).

Out of which \(7, 8, \text{ and } 9\) are larger than 6.5

\[\therefore (7/13) = (-1)^3 = -1\]


\[= (-1)(1)(382/73)\]

You should be able to justify all the steps.

\[=-(18/73) = -(9/73)(2/73) = -(1)(+1)\]

\[= -1\]