Problem 6 (Solutions)

1. \( f(x) = x^3 + x + 57 \)

   \( \text{Solutions of } f(x) \equiv 0 \mod 5: x_0 = 4 \) \( (5) \)

   Now \( f'(x) = 3x^2 + 1 \Rightarrow f'(x_0) = 4 \neq 0, \) so by Hensel's Lemma we may lift \( x_0 \) uniquely to a \( x_1 \) mod \( 5^2 \) and hence to a \( x_2 \) mod \( 5^3 \). With \( x_1 = x_0 + 5t = 4 + 5t, \) then

   \( 0 \equiv (4 + 5t)^3 + (4 + 5t) + 7 \equiv 20t + 7 \equiv 0 \mod (5^2) \) \( (\mod 5^2) \)

   \( \therefore x_2 \equiv 4 \) \( (\mod 5^3) \) as well.

2. More precisely, checking that \( 2x^2 + 5x^2 + 6x + 1 \bigg| x^7 - x \) \( \mod 5^2 \) \( (\mathbb{F}_7[x]) \)

   shows that there are 3 distinct solutions. One can finds these "by hand": \( x = 1, 2, 5. \)

3. \( (\mathbb{Z}/7\mathbb{Z})^* \) has order 16 (it is a cyclic group).

   \( -1 \) is the unique element of order 2; if \( x \equiv -1 \) \( (17) \)

   then \( x \) has order 16 (= \( x \) is generator) since the order must divide 16 (and clearly isn't 2, 4, or 8).

4. \( x^{20} \equiv 13 \mod 17 \) has solutions \( \iff 13^{16} \equiv 1 \mod 17 \) \( \iff 13^4 \equiv 1 \mod 17 \)

   Moreover \( \# \text{ of sol ns is } \varphi(17) = 16 \).
5. \( S^5 \equiv 15 \Rightarrow 8^{15} = 2^{3 \cdot 15} = (2^{22})^2 \cdot 2 \equiv 1^2 \cdot 2 = 2 \).  

6. (a) in \( \mathbb{Z}/13\mathbb{Z} \), \( \log_{13} 3 = 7 \)
(b) in \( \mathbb{Z}/27\mathbb{Z} \), \( \log_{27} 2 \approx 11 \).

7. \( p = 101, \ g = 15, \ g^2 = 42, \ g^8 = 24 \)

\[
\begin{array}{c}
g^2 \equiv 23 \\
g^3 \equiv 23 \cdot \text{con} \\
g^6 \equiv 23 \cdot 23 \equiv 100 \pmod{101}
\end{array}
\]

\[\Rightarrow \text{ord}(g) = 3\Rightarrow \text{order} \ k_7 = (g^8)^4 = (24)^3 \equiv 88 \pmod{101} \]

8. \( 8,734 = 2^{13} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 = 0100100001110 \pmod{2} \)

\[\Rightarrow \text{ord} \ (\text{Ker}) \begin{array}{c}
0101000011100 \pmod{2}
\end{array}
\]

\[\begin{array}{c}
\overline{11011000100111} \\
\overline{110011000100111} \Rightarrow \\
2^0 + 2^1 + 2^2 + 2^5 + 2^9 + 2^{10} + 2^12 + 2^{13} = 13563
\end{array}
\]

9. left to you.