Problem 1: Find the smallest primitive root of 109 that is greater then 2. Let \( \alpha \) be this primitive root in problem 2. **Work saving hint:** If \( \alpha^t \equiv 1 \pmod{p} \), then \( \text{ord}_n(\alpha) \mid t \).

Problem 2: Compute \( L_\alpha(10) \) using the Pohlig-Hellman algorithm.

Problem 3: Find \( \text{ord}_{31}(4) \).

Problem 4: Use the Chinese Remainder Theorem to solve the following system of simultaneous congruences.
\[
\begin{align*}
x & \equiv 5 \pmod{22} \\
x & \equiv 6 \pmod{39} \\
x & \equiv 4 \pmod{35}
\end{align*}
\]

Problem 5: Carefully present a proof of the following: Let \( u \) be an integer, and let \( v \) and \( w \) be positive integers such that \( w \mid v \). Then \( (u \% v) \% w = u \% w \). (Note that the expression \( a \% b \) has the same meaning as the expression \( a \mod b \).)

For the next two problems, see section 9.1 of Trappe and Washington for the RSA approach to digital signatures. First, the RSA digital signature protocol:

Suppose Alice chooses two large primes, \( p \) and \( q \) and calculates \( n = pq \). Alice then chooses a positive integer \( e_A \) such that \( 1 < e_A < \phi(n) \), where \( \phi \) is Euler’s \( \phi \), and \( e_A \)
is relatively prime to $\phi(n)$. Alice then calculates $d_A \equiv e_A^{-1} \pmod{\phi(n)}$. Alice makes public $e_A$ and $n$, but keeps $d_A$, $p$ and $q$ private.

Suppose $m$ is a positive integer that encodes a document, i.e. a plaintext. Alice wants to sign the document with her digital signature so that receivers of the signed document can verify that it is really Alice who signed it. Alice generates her digital signature $y$ for the message $m$ where

$$y \equiv m^{d_A} \pmod{n}$$

Suppose Bob receives the message $m$ and signature $y$. Bob authenticates the pair as follows:

Bob looks up Alice’s publicly available authenticator $(e_A, n)$ and calculates

$$z \equiv y^{e_A} \pmod{n}$$

Bob accepts $(m, y)$ as authentic iff $z = m$.

**Problem 6:** Explain why $m$ is the only value that can be paired with $y$ that will pass the authentication test.

**Problem 7:** Given a positive integer $m$ that encodes a document, explain $y$ not just anyone can find $y$ such that $(m, y)$ passes the authentication test.

**Problem 8:** Consider any encryption system for which the security of the system is dependent on the infeasibility of computing discrete logs mod $p$, where $p$ is prime. What important property or properties of $p$ should be considered to avoid obvious feasible ways to compute discrete logs mod $p$?

**Problem 9:** Find either the square roots of 10 mod 19 or the square roots of 9 mod 19.
Problem 10: Find the last two digits of $63^{511}$. 