Answer the following questions. The answers must be clear, intelligible, and you must show your work. Provide explanation for all your steps. Your grade will be determined by adherence to these criteria. Each problem is worth 12 points.
1. Given that $x = 3$ is a solution of the congruence $x^3 - x + 1 \equiv 0 \pmod{25}$, lift this value to a solution of the congruence $x^3 - x + 1 \equiv 0 \pmod{125}$. You don’t need to find other solutions.

Let $x = 3 + 25y$.

$F(x) = x^3 - x + 1$ and $F'(x) = 3x^2 - 1$.

$F(3) = 27 - 3 + 1 = 25$ and $F'(3) = 27 - 1 = 26 \equiv 1 \pmod{5}$.

Solve for $y$ in

$$\frac{F(3)}{25} + F'(3)y \equiv 0 \pmod{5}$$

thus

$$1 + y \equiv 0 \pmod{5}$$

and $y \equiv 4 \pmod{5}$.

The corresponding solution for the given congruence is

$$x \equiv 3 + 25 \cdot 4 \equiv 103 \pmod{125}$$
2. Answers the following questions.

a). How many quadratic nonresidues are there (mod 47)?

Answer: \((47 - 1)/2 = 23\).

b). Use quadratic reciprocity and other properties of the Legendre symbol to evaluate \(\left(\frac{35}{43}\right)\).

\[
\left(\frac{35}{43}\right) = \left(\frac{5}{43}\right) \left(\frac{7}{43}\right) = \left(\frac{43}{5}\right) \left(\frac{43}{7}\right) = \left(-\right) \left(\frac{43}{5}\right) \left(\frac{43}{7}\right) = \\
\left(-\right) \left(\frac{3}{5}\right) \left(\frac{1}{7}\right) = \left(-\right) \left(\frac{5}{3}\right) \cdot 1 = \left(-\right) \left(\frac{2}{3}\right) = \left(-\right) \cdot (-1) = 1
\]

By inspection we find that \(\left(\frac{2}{3}\right) = -1\).

c). If \(m\) is an odd number such that \(2^{\frac{m-1}{2}} \equiv 2 \pmod{m}\) can we make any conclusions as to whether \(m\) is prime or not? Explain.

If \(m\) is prime then \(2^2 \equiv 2^{m-1} \equiv 1 \pmod{m}\) and therefore \(m|3\), which implies \(m = 3\). Thus either \(m = 3\) or \(m\) is composite.
3. a). If \( f(x) \) is a polynomial of degree 5, what is the greatest number of solutions the congruence \( f(x) \equiv 0 \pmod{7} \) can have? Assume \( f(x) \) is not identically zero.

5 by Lagrange Theorem.

b). What is the greatest number of solutions \( f(x) \equiv 0 \pmod{35} \) can have? Assume that \( f(x) \) is not identically zero \( \pmod{5} \) or \( \pmod{7} \).

25 since \( f(x) \equiv 0 \pmod{5} \) can have at most 5 solutions and \( f(x) \equiv 0 \pmod{7} \) can have at most 5 solutions.

c). Find a complete set of solutions (if any) of the congruence:

\[
5x^3 + 7x^2 + 15x + 14 \equiv 0 \pmod{35}
\]

The given congruence is equivalent with the following system:

\[
\begin{align*}
5x^3 + 7x^2 + 15x + 14 &\equiv 0 \pmod{5} \\
5x^3 + 7x^2 + 15x + 14 &\equiv 0 \pmod{7}
\end{align*}
\]

Consider the first congruence, which can be rewritten as:

\[
2x^2 + 4 \equiv 0 \pmod{5}
\]

or equivalently

\[
x^2 \equiv 3 \pmod{5}
\]

which has no solution.

The original congruence has no solution.
4. Let $p$ be an odd prime. Prove that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{4}$.

By Euler’s criterion

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

If $p \equiv 1 \pmod{4}$, $p = 1 + 4k$, $\frac{p-1}{2} = 2k$, $(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$.

If $p \equiv 3 \pmod{4}$, $p = 3 + 4k$, $\frac{p-1}{2} = 2k + 1$, $(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$.

Thus $\left(\frac{-1}{p}\right) = 1$ iff $p \equiv 1 \pmod{4}$.

Note: $1 \not\equiv -1 \pmod{p}$ for any odd prime $p$. 
5. Circle True (T) or False (F).

T  F  (1) The largest power of 3 that divides 200! is 51.
T  F  (2) The congruence \( x^2 + 8x - 2 \equiv 0 \text{mod 73} \) has no solution.
T  F  (3) The integer 252179 cannot be written as a sum of four squares.
T  F  (4) 37 is a quadratic residue (mod 67).
T  F  (5) If \( x \equiv 2 \text{mod 4} \) then there is no primitive Pythagorean triple \((x, y, z)\).
T  F  (6) The integer 697 can be written as the sum of two squares.

(1). F. 200 = 66 \cdot 3 + 2 = 22 \cdot 3^2 + 2 = 7 \cdot 3^3 + 11 = 2 \cdot 3^4 + 38. The largest power of 3 that divides 200 is 66 + 22 + 7 + 2 = 97.

(2). F. \( b^2 - 4ac = 64 + 8 = 72 \equiv -1 \text{mod 73} \). Since -1 is a quadratic residue mod 73 it follows that the equation has two solutions.

(3). F. Every positive integer can be written as a sum of four squares.

(4). T.

(5). T.

(6). T. 697 = 17 \cdot 41 \text{ and } 17 \equiv 41 \equiv 1 \text{ (mod 4) }