PLEASE, READ THE FOLLOWING INSTRUCTIONS:

- This is a closed-book, closed-device exam: You may not make use of any lecture notes, books or electronic devices (e.g., calculators).
- You have 80 minutes to answer all of the questions. The entire exam is worth 100 points. The point value of each question is given.
- Partial credit will be given. **Full credit** will be given only in the case where the correct answer has been properly justified with complete explanations. Do not spend *disproportionate time* on any one question.
- Write your answers in the spaces provided: You must turn in this printed form. The back side of each page may be used as scratch pad.
- All writings must be neat, well-organized, and include sufficient explanations in the delineation of the solutions. Messy, poorly organized, or illegible material will be returned ungraded.
- Questions during the exam should be about the wording of the exam only. If you have a question, raise your hand and we will come to you.
- Please turn your exam in at the end of the class.
- Good luck!

<table>
<thead>
<tr>
<th>Question</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>40</td>
</tr>
<tr>
<td>Score</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TOTAL: ___________________________________________________________
Problem 1 [15 points]

Consider the linear congruence $6x \equiv 9 \pmod{15}$, and answer the following three questions:

(a) The above linear congruence admits a solution $x$. Why?
(b) Compute an integer $x$ that satisfies the above congruence.
(c) How many *incongruent* solutions are there for the above linear congruence? Justify your answer.
Problem 2 [15 points]
Consider the linear congruence

\[ 14x \equiv b \pmod{p} \]

where \( b \) is any integer, \( p \) is a prime number, and \( x \) is an unknown. So, answer the following three questions:

(a) What can you say about \( \text{GCD}(14, p) \)? Justify your answer.

(b) Suppose that \( p \) does NOT divide 14. Then, for which values of \( b \) does the above linear congruence admit a solution \( x \)? Justify your answer.

(c) Suppose that \( p \) does NOT divide 14. Then, for which values of \( b \) does the above linear congruence admit a solution \( x \) that is unique modulo \( p \)? Justify your answer.
Problem 3 [30 points]

You are now asked to prove or disprove three given statements. If you think a statement is false, you must provide a counterexample. Otherwise, you must provide a (short) proof for the statement.

(a) If \( a, b, \) and \( c \) are any three integers such that \( c \neq 0 \) and \( a = b \mod c \), then we can conclude that \( a < c \).

(b) If \( a, b, \) and \( c \) are any three integers such that \( c \neq 0 \) and \( (a \mod c) = (b \mod c) \), then \( a \equiv b \pmod{c} \) and \( b \equiv a \pmod{c} \).

(c) If \( a, b, \) and \( c \) are any three integers such that \( c \neq 0 \) and \( a \equiv b \pmod{c} \), then, for any integer \( k \), we have that \( ak \equiv bk \pmod{c} \).
Problem 4 [40 points]

Let $n$, $p$ and $q$ be any three integers such that $p$ and $q$ are distinct prime numbers and $n = p \cdot q$, and let $a$ be any integer such that $a$ and $n$ are not relatively prime and $a < n$. Then, consider the following items:

(a) Prove that either $p$ divides $a$ or $q$ divides $a$ but not both.

(b) If $q$ does not divide $a$, then use Euler’s theorem and some basic property of linear congruences (e.g., multiplication) to show that $a^{(q-1)k} \equiv 1 \pmod{q}$, for any positive integer $k$.

(c) If $q$ does not divide $a$, then use the result in item (b) and some basic property of linear congruence (e.g., multiplication) to show that $a^{(q-1)(p-1)+1} \equiv a \pmod{q}$.

(d) If $q$ does not divide $a$, then use the results in items (a), (b), and (c) to show that $a^{(q-1)(p-1)+1} \equiv a \pmod{n}$.

Recall that the Euler’s theorem says that, for any two integers $x$ and $y$ such that $\text{GCD}(x, y) = 1$ and $y > 0$, we have that $x^{\phi(y)} \equiv 1 \pmod{y}$, where $\phi(y)$ is the value of the Euler $\phi$-function at $y$. 
