Name:

- This is a closed-book, closed-notes exam. No electronic aids are allowed.

- Read each question carefully. Proof questions should be written out with all the details. You may use results proven in class, but you should explicitly cite the results being used.

- Answer the questions in the spaces provided on the question sheets. If you need extra paper, make sure to write your name on it and attach it to this exam. Do not unstaple or detach pages from this exam.

<table>
<thead>
<tr>
<th>Section</th>
<th>Points</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>5 (bonus)</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Grand Total</td>
<td>50</td>
<td></td>
</tr>
</tbody>
</table>
1. SECTION 1

Exercise 1.1. (5 points) Find all the least nonnegative incongruent solutions of
\[ 12x \equiv 16 \pmod{32}. \]
Following the techniques of Chapter no. 2, the solutions can be found to be
4, 12, 20 and 28.
Use the three theorems that characterize solutions of congruences in one variable.

Exercise 1.2. (5 points) Find the inverse modulo \( m = 81 \) of the integer \( n = 40 \) below
Similarly, by using the early tools of chapter 2 and the theorems to characterization
solutions of congruences in one variable
one finds that the inverse does not exist.
2. Section 2

Exercise 2.1. (10 points) State and prove Euler’s theorem. Make sure you quote any previous results clearly. If you use reduced residue systems, then make sure you state and prove any results you need.
This is all bookwork. See Theorem 2.17 of the textbook.

Exercise 2.2. (5 points - bonus) How can one recover Fermat’s little theorem from Euler’s theorem?
This is all bookwork. See Theorem 2.16 of the textbook.
Exercise 3.1. (10 points) Solve the following.

(a) What is the Euler totient function $\phi(n)$? Write $\phi(n)$ as a divisor sum.

(b) It is known that $\phi(n)$ is multiplicative. Disprove (via a counterexample) that $\phi(n)$ is completely multiplicative.

(c) How would you write $\phi(n)$ as a finite product over primes $p$ such that $p|n$? (You may state the formula from the course).

(d) Let $n \in \mathbb{N}$. If $p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ is the prime factorization of $n$, use part (c) above to prove that

$$\phi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_m^{a_m-1} \prod_{i=1}^{m} (p_i - 1).$$

This is now all bookwork.
4. Section 4

**Exercise 4.1.** (5 points) Use Fermat’s little theorem to find all incongruent solutions of

\[ 11x \equiv 15 \mod 29. \]

The answer is 4 mod 29. To see this, use \((11, 29) = 1\). Then \(11a \equiv 1 \mod 29\). Note that \(20|(11 \times 8 - 1) = 87\). Then deduce that \(a = 8\), thus \(x \equiv 15 \times 8 \mod 29\), which can be reduced to \(x \equiv 4 \mod 29\).

---

**Exercise 4.2.** (5 points) Use Euler’s theorem to find all incongruent solutions of

\[ 5x \equiv 21 \mod 36. \]

Note that \((5, 36) = 1\) and \(\phi(36) = 12\). Then \(5^{12} \equiv 1 \mod 36\). Use \(5^{12} = 5^{11} \times 5 \equiv 1\) and write \(11 = 8 + 2 + 1\). Then \(5^{2} \equiv 25 \equiv -11 \mod 36\).

\[ 5^{4} \equiv 13 \equiv -11 \mod 36. \]
\[ 5^{8} \equiv 25 \equiv -11 \mod 36. \]
\[ 5^{11} \equiv 29 \equiv -11 \mod 36. \]

Finally \(29 \times 5 \equiv 1 \mod 36\) and \(5 \times 29 \times 21 \equiv 21 \mod 36\). So \(x \equiv 29 \times 31 \mod 36\) which means that \(x \equiv 33 \mod 36\).
Exercise 4.3. (5 points) Use Wilson’s theorem to find the least nonnegative residue modulo $m = 67$ of $n = 64!$.
Application of Wilson’s theorem yields the answer 33.

Exercise 4.4. (5 points) Find the least nonnegative solution of each system of congruences below.

\[
\begin{align*}
    x &\equiv 2 \mod 3 \\
    x &\equiv 1 \mod 5 \\
    x &\equiv 4 \mod 7 
\end{align*}
\]

Application of Chinese Remainder Theorem (and its proof) yields the answer $x \equiv 11 \mod 105$. 