Mathematics 3320: Exam Replacement IIa

Your Name:

For credit you must show ALL work.

Academic Integrity is expected of all students of Cornell University at all times, whether in presence or absence of members of the faculty.

Understanding this, I declare I shall not give, use, or receive unauthorized aid in this examination.

Signature of the Student: ________________________________

<table>
<thead>
<tr>
<th>Problem</th>
<th>Pts</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15</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>15</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Extra</td>
<td>10</td>
<td></td>
</tr>
</tbody>
</table>
Problem 1 (15 pts): Show that $x^k \equiv a \pmod{m}$ has a unique solution if $(k, \phi(m)) = 1$. 
Problem 2 (10 pts): Find the remainder of $16!$ when divided by $323 = 17 \cdot 19$. 
Problem 3 (10 pts): Prove that $\phi(n)$ is even for $n \geq 3$. 
Problem 4 (15 pts): Find all the solutions $x \in \mathbb{Z}_7[i]$ to the equation $x^2 = 3 + 4i$. 
Problem 5 (10 pts):
Only attempt this after you have finished with problems 1-4.

1. Let $G$ be a finite cyclic group. Show that any subgroup must be cyclic.

2. Let $p$ be an odd prime such that 3 is not a square. Show that

\[ T_p = \{ a + b\sqrt{3} : a^2 - 3b^2 = 1 \} \]

is a subgroup of $\mathbb{Z}_p[\sqrt{3}]$, and compute its order. You may use the fact that $\mathbb{Z}_p[\sqrt{3}]^\times$ is cyclic of order $p^2 - 1$. 


FORMULAS

\[ a^{p-1} \equiv 1 \pmod{p}, \quad a^{\phi(n)} = 1 \pmod{n}. \]

\[ \left( \frac{2}{p} \right) = (-1)^{\frac{p-1}{2}}, \quad \left( \frac{m}{p} \right) = m^{\frac{p-1}{2}}, \quad \left( \frac{p}{q} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left( \frac{q}{p} \right). \]

\[ (p-1)! \equiv -1 \pmod{p}. \]

\[ n = p_1^{a_1} \cdots p_n^{a_n}, \]
\[ \phi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdots (p_n^{a_n} - p_n^{a_n-1}), \]
\[ \tau(n) = (a_1 + 1) \cdots (a_n + 1), \]
\[ \sigma(n) = \frac{(p_1^{a_1+1} - 1)}{p_1 - 1} \cdots \frac{(p_n^{a_n+1} - 1)}{p_n - 1}. \]

\[ x^2 \equiv a \pmod{p} \text{ has a solution } \iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}, \]

(Gauss Lemma) \( S = \{1, 2, \ldots, \frac{p-1}{2}\}, \) \( ax \equiv \epsilon_x s_x, s_x \in S, \) \( \text{then } \left( \frac{a}{p} \right) = \prod_{x \in S} \epsilon_x. \)

\[ f(x + p^k t) = f(x) + f'(x) p^k (p^{k+1}) \]

\[ n = 2^a \prod p_i^{a_i} \prod q_j^{b_j}, \quad N(n) = 4 \prod (a_i + 1). \]