Midterm 1

Name: ____________________________

SID: ______________________________

Section time: __F 10-11 __F 11-12 __F 2-3

You may open the exam and start working at 3:40pm. The exam ends at 4:55pm. You may not use lecture notes or books. You may use one single-sided 8.5” x 11” sheet of notes. You may not use a calculator.

Show all work. Write out proofs in enough detail to convince us that you know exactly how the reasoning for each step works.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Total:</td>
<td></td>
</tr>
</tbody>
</table>
1. Quick Questions

(a) (3 pts) You want to prove by contradiction the statement “If \( n \) is even then \( n^3 \) is even.”
The first sentence in your proof should be the following (circle one option in each pair):

Let \( \{n, n^3\} \) be \{even, odd\}. Suppose \( \{n, n^3\} \) is \{even, odd\}.

(b) (4 pts) Compute \( 5^{17} \mod 7 \).

(c) (6 pts) Let \( P(x,y) \) be the proposition, for integers \( x \) and \( y \), that “\( x + y = x - y \)”.
Which of the following statement are true? Explain each answer in 1 sentence.

i. \( \forall x. \exists y. P(x,y) \)

ii. \( \exists y. \forall x. P(x,y) \)

iii. \( \forall y. \exists x. P(x,y) \)

(d) (3 pts) Write the negation of 1(c)iii above (that is, \( \neg \forall y. \exists x. P(x,y) \)) in terms of the proposition \( Q(x,y) \), which states that \( x + y \neq x - y \) (that is, \( Q(x,y) \equiv \neg P(x,y) \)). Use De Morgan’s law to simplify.

(e) (6 pts) For each of the following pairs, is there a graph with \( n \) vertices and \( m \) edges that has an Eulerian Tour? Give an example or briefly explain why not. For the purposes of this problem, graphs \textit{may not} have “self-loops” (edges from that start and end at the same vertex), but \textit{may} have parallel edges (several edges connecting the same two endpoints).

(a) \( (n = 6, m = 6) \)        (a) \( (n = 6, m = 7) \)        (a) \( (n = 6, m = 3) \)
2. **Variants of Induction** (12 pts)
   Consider the following two variants of induction.

   (a) Let $P$ be a property of positive integers, and suppose you have proved that
   
   i. $P(1)$ is true;
   
   ii. For every $n \geq 1$, $P(n) \iff P(n + 3)$
   
   iii. For every $n \geq 1$, $P(n) \iff P(n + 5)$
   
   Does it follow that $P(n)$ is true for every $n \geq 1$? Either prove that, for every $P$ that satisfies properties (i), (ii), (iii), $P(n)$ must be true for every $n \geq 1$, or provide a counterexample.
   
   (A counterexample is a property $P$ that is false for some $n \geq 1$, even though is satisfies properties (i), (ii), (iii).)

   (b) Let $P$ be a property of positive integers, and suppose you have proved that
   
   i. $P(1)$ is true;
   
   ii. For every $n \geq 1$, $P(n) \iff P(n + 4)$
   
   iii. For every $n \geq 1$, $P(n) \iff P(n + 6)$
   
   Does it follow that $P(n)$ is true for every $n \geq 1$? Either prove that, for every $P$ that satisfies properties (i), (ii), (iii), $P(n)$ must be true for every $n \geq 1$, or provide a counterexample (in the same sense of “counterexample” as above).
3. Solving Systems of Equations (10 pts)

Solve for $x$ and $y$ (show all steps):

\[
\begin{align*}
2x + 3y &\equiv 2 \pmod{13} \\
x + 5y &\equiv 3 \pmod{13}
\end{align*}
\]
4. Secret Sharing (10 pts)

In a 3-out-of-5 secret sharing system, a secret $s \in \{0, 1, 2, 3, 4, 5, 6\}$ is shared among 5 people.

Two random numbers $a, b$ are chosen to define the polynomial $p(x) = ax^2 + bx + s$, and then shares $p(1), \ldots, p(5)$ are given to the five people. (All operations are done mod 7)

Three of them get together, and share that $p(1) \equiv 3 \pmod{7}$, $p(3) \equiv 0 \pmod{7}$ and $p(4) \equiv 0 \pmod{7}$.

What is the secret?