CS 2800 - Homework 5 - Due Wednesday March 3
at the beginning of lecture

INCLUDE THIS COVER PAGE WITH YOUR HOMEWORK

NETID:

NAME:

<table>
<thead>
<tr>
<th>problem</th>
<th>grade</th>
<th>memo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>total</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
You should justify/prove all your answers.

Problem 1
Find a multiplicative inverse of 2 modulo 17.

Problem 2
Prove that the product of 4 consecutive integers is divisible by 12.

Problem 3
Last year, the course staff for cs2800 devised a private-key cryptosystem for exchanging secret notes about students. Let \( p \) be a publicly known prime number and \( k \), the private key, be an integer between 1 and \( p - 1 \) inclusive. A message \( m \) is encrypted into \( m^* \) where

\[ m^* \equiv mk \pmod{p} \]

(a) If you receive \( m^* \) and know \( k \), how can you recover \( m \)?
(b) This system is not secure in the following sense: Suppose you happen to know the message \( m \) corresponding to some encrypted message \( m^* \). This provides enough information to recover \( k \). Give a method for recovering \( k \) from \( m \) and \( m^* \), and prove that it works correctly in all cases.

Problem 4
Let \( p \) be a prime number. Show that if \( p | ab \) than \( p | a \) or \( p | b \).

Problem 5
Let \( p \) be a prime number. An integer \( k \) is self-inverse modulo \( p \) if \( k^2 \equiv 1 \pmod{p} \). Find all integers that are self-inverse modulo \( p \)

Hint: note that \((k - 1)(k + 1) = k^2 - 1\).

Problem 6
Determine if the following are tautologies
(a) \((P \land (P \Rightarrow Q)) \Rightarrow Q\)
(b) \((P \Rightarrow Q) \lor (Q \Rightarrow \neg P)\)