Homework 5
Due: Wednesday, March 13th

All homeworks are due at 12:55 PM on Gradescope.

Please do not include any identifying information about yourself in the handin, including your Banner ID.

Be sure to fully explain your reasoning and show all work for full credit.

Problem 1

Let $p, q$ be consecutive odd primes, with $p < q$. Prove that $p + q$ can be written as a product of 3 integers, each greater than 1.

Problem 2

Let $a \mod b$ return the remainder of $a$ when divided by $b$. That is, $a \mod b$ returns $r$, where $a = qb + r$, and $q \in \mathbb{Z}, 0 \leq r < b$.

Bea and Elle want to establish a shared secret, while in the presence of an adversary, Tee.

To do this, Bea and Elle agree on some large number $A$, and some prime number $p$. They then each independently generate a number: Bea generates $x$ and Elle generates $y$.

After doing this, Bea transmits $A^x \mod p$ to Elle over a public channel, and Elle transmits $A^y \mod p$ to Bea.

Elle generates the shared secret by computing $(A^x \mod p)^y \mod p$, and Bea generates the shared secret by computing $(A^y \mod p)^x \mod p$. Doing this gives both of them the shared secret, $A^{xy} \mod p$.

Tee, who has been listening to their communications over the public channel, knows $A, p, (A^x \mod p)$ and $(A^y \mod p)$. However, without knowing $x$ or $y$, it is very hard for Tee to calculate the shared secret.

Show that $(A^x \mod p)^y \mod p = (A^y \mod p)^x \mod p$, thereby allowing Bea and Elle to calculate the shared secret without Tee’s knowing.

Note: it may be helpful when starting this problem to try this out with actual numbers, in order to better understand what you need to show.
Problem 3

Which of the following is correct? There is exactly one answer.

a) none of the below
b) none of the below
c) one of the below
d) all of the below
e) none of the above
f) all of the above

Problem 4

Let $B$ be the set of all possible propositions. Define the relation $R$ over $B$ such that, for $a, b \in B$, $aRb$ if and only if $a$ and $b$ return the same output given the same input.

a. Prove that $R$ is an equivalence relation.

b. Let $x$ be a proposition with the following input/output table:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$r$</th>
<th>$x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Write a proposition corresponding to the input/output table given above.

c. The equivalence class of a proposition $x$ is $[x]_R = \{ a \in B \mid aRx \}$. That is, an equivalence class of proposition is the set of propositions that for every possible input, give the same output.

Prove that $|[x]_R|$ is infinite for any $x \in B$.

d. How many equivalence classes of three-input, one-output propositions are there? Explain your answer.
Problem 5

a. Smore has developed insomnia wondering about the following: Can we express the OR (\(\lor\)) operation using only IMPLIES (\(\Rightarrow\)) operations? Justify your answer and help Smore sleep again.

b. Suppose we define a new operation \(\ast\) on logical propositions such that

\[ x \ast y \equiv \neg (x \land y) \]

Create a truth table for each of the following expressions, and state which logical operator the expression is equivalent to.

i \( x \ast x \)

ii \( (x \ast y) \ast (x \ast y) \)

iii \( (x \ast x) \ast (y \ast y) \)

iv \( (x \ast (x \ast y)) \ast (y \ast (y \ast x)) \)