Quiz 1

- The quiz is **closed book**, but you may have one 8.5” × 11” sheet with notes in your own handwriting on both sides.
- Calculators and electronic devices are not allowed.
- You may assume all of the results presented in class.
- Please show your work. Partial credit cannot be given for a wrong answer if your work isn’t shown.
- Write your solutions in the space provided. If you need more space, write on the back of the sheet containing the problem. Please keep your entire answer to a problem on that problem’s page.
- Be neat and write legibly. You will be graded not only on the correctness of your answers, but also on the clarity with which you express them.
- If you get stuck on a problem, move on to others. The problems are not arranged in order of difficulty.

NAME: __________________________________________

TA: __________________________________________

<table>
<thead>
<tr>
<th>Problem</th>
<th>Value</th>
<th>Score</th>
<th>Grader</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Problem 1. [10 points]

Show whether or not the following two expressions are logically equivalent using either truth tables or rules of inference:

\[ \neg x \to (y \to z) \]

and

\[ y \to (x \lor z) \]

**Solution.** Truth table for \( \neg x \to (y \to z) \):

<table>
<thead>
<tr>
<th>( x )</th>
<th>( y )</th>
<th>( z )</th>
<th>( \neg x )</th>
<th>( y \to z )</th>
<th>( \neg x \to (y \to z) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

Truth table for \( y \to (x \lor z) \):

<table>
<thead>
<tr>
<th>( x )</th>
<th>( y )</th>
<th>( z )</th>
<th>( x \lor z )</th>
<th>( y \to (x \lor z) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

The two expressions yield the same truth table, so they are logically equivalent.
Problem 2. [10 points]

Find integers $a$ and $b$ such that $11a + 57b = 1$.

Solution. Since $\gcd(11, 57) = 1$, we can use the Pulverizer to find a linear combination of 11 and 57 that equals 1.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
<th>$\text{rem}(x, y) = x - q \cdot y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>57</td>
<td>11</td>
<td>2 = 57 - 5 \cdot 11</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>1 = 11 - 5 \cdot 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>= 11 - 5 \cdot (57 - 5 \cdot 11)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>= 26 \cdot 11 - 5 \cdot 57</td>
</tr>
</tbody>
</table>

Then $a = 26$ and $b = -5$. 
Problem 3. [10 points]

Alice chooses primes $p = 5$ and $q = 11$. The public key she generates is the pair $(7, 55)$ and the private key is $(23, 55)$. Bob wants to encrypt the message $m = 53$ using the RSA algorithm and send it to Alice. What is the encrypted message? Express your answer as an integer in $\{0, 1, \ldots, 54\}$.

Solution. The encrypted message $m^*$ is congruent to $m^e \mod n$, or, specifically, $53^7 \mod 55$. Using modular exponentiation, and noting that $53 \equiv -2 \mod 55$ we obtain the following:

\[
\begin{align*}
53^1 & \equiv (-2)^1 \equiv -2 \mod 55 \\
53^2 & \equiv (-2)^2 \equiv 4 \mod 55 \\
53^4 & \equiv (-2)^4 \equiv 16 \mod 55 \\
53^7 &= 53^{4+2+1} \\
&= 53^4 \cdot 53^2 \cdot 53^1 \\
&\equiv -2 \cdot 4 \cdot 16 \\
&\equiv -128 \\
&\equiv 37 \mod 55
\end{align*}
\]

(In case you didn’t note the congruency and went ahead and attempted to brute-force-exponentiate $53^7$, the following should be indicative of your work)

\[
\begin{align*}
53^1 & \equiv 53 \mod 55 \\
53^2 & \equiv 53^2 \\
&\equiv 2089 \\
&\equiv 4 \mod 55 \\
53^4 & \equiv 4^2 \\
&\equiv 16 \mod 55 \\
53^7 &= 53^{4+2+1} \\
&= 53^4 \cdot 53^2 \cdot 53^1 \\
&\equiv 16 \cdot 4 \cdot 53 \\
&\equiv 64 \cdot 53 \\
&\equiv 9 \cdot 53 \\
&\equiv 477 \\
&\equiv 37 \mod 55
\end{align*}
\]
Problem 4. [13 points]
Prove that $\forall n \in \mathbb{N}^+$:

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$$

Solution.

Proof: (by induction)

$P(n)$: $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$

Base Case: $P(1)$.

$$1^3 = (1)^2$$
$$1 = 1$$

so our base case holds.

Inductive Step: Show that $P(n) \rightarrow P(n+1)$.

Assume $P(n)$. Then

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$$

Note that $(1 + 2 + \cdots + n)^2$ can be expanded as the sum of a total of $n^2$ pairs of terms (n of which are the terms paired with themselves, or the square of the terms). Let us try to simplify the expression $(1 + 2 + \cdots + n + (n + 1))^2$

$$= (1 + 2 + \cdots + n)^2 + (n + 1)(n + 1) + \sum_{i=1}^{n}(n + 1)i + \sum_{i=1}^{n} i(n + 1)$$
$$= (1 + 2 + \cdots + n)^2 + (n + 1)^2 + 2(n + 1)\sum_{i=1}^{n} i \text{ (apply } P(n))$$
$$= \sum_{i=1}^{n} i^3 + (n + 1)^2 + 2(n + 1) \cdot \frac{n(n+1)}{2} \text{ (apply formula for triangular numbers)}$$
$$= \sum_{i=1}^{n} i^3 + (n + 1)^2 + (n + 1)^2 \cdot n$$
$$= \sum_{i=1}^{n} i^3 + (n + 1)^2 \cdot (1 + n)$$
$$= \sum_{i=1}^{n+1} i^3$$
$$\rightarrow P(n+1).$$

Therefore, we conclude that $P(n)$ holds $\forall n \in \mathbb{N}^+$. 
Problem 5. [13 points]
Suppose $G$ is a simple graph with $2n + 1$ vertices, such that each vertex has degree at least $n$. Prove that $G$ is connected if $n \geq 1$ (Hint: use a proof by contradiction).

Solution. Suppose by contradiction that a graph where each vertex has degree at least $n$ is not connected. Then the graph is composed of several connected components. Of these, there must exist a connected component, $G_i$, which contains at most $n$ nodes. (If not, then we would have at least two connected components with at least $n + 1$ nodes each, which would mean that $G$ would contain at least $2n + 2$ vertices, another contradiction.)

Each node in connected component $G_i$ has degree at least $n$. However, this is not possible, because each node could only have $n - 1$ edges at most, so we have a contradiction.

Therefore, $G$ must be connected.
Problem 6. [14 points]

(a) [10 pts] There are 5 people at a party. Each person shakes hands with at least 3 other people. Prove that it is always possible to find a subset of three people at the party such that they all shake hands with each other.

Solution.

Proof: (by contradiction)

Assume that there is no subset of 3 people who all shake hands with each other. Let our 5 people be named $A$, $B$, $C$, $D$, and $E$. Without loss of generality, assume $A$ shakes hands with $B$, $C$, and $D$. None of $B$, $C$, or $D$ can shake hands with each other since they all shake hands with $A$ and we assume that there is no group of 3 people who all shake hands with each other. $B$ must shake hands with at least 2 other people, but the only person left to for him to shake hands with is $E$. This is a contradiction, so there must be a subset of 3 people who have all shaken hands with each other.
(b) [4 pts] Now suppose there are 6 people at the party. Give an example where each person shakes hands with at least 3 other people, but for which no subset of 3 people have all shaken hands with each other. Draw your example as a 6-node graph. What do the nodes and edges represent in your graph?

**Solution.**

The nodes represent people, and the edges represent a handshake between two people.
Problem 7. [12 points]
Consider the graph in Figure 1 below representing the main campus buildings at a nearby university. In this graph, nodes denote buildings and edges are used to denote hallways that connect pairs of buildings.

(a) [3 pts] Is this graph bipartite? Provide a brief argument for your answer.
Solution. No. The graph contains an odd-length cycle, and therefore cannot be bipartite.

(b) [3 pts] Is it possible for someone to traverse every hallway exactly once in a single walkthrough while starting and ending at the same building? Provide a reason for your answer.
Solution. No. This is the equivalent of asking if the graph has an Euler tour, which is only true if all vertices have even degree.
(c) [6 pts] Ben Bitdiddle wants to install new WiFi routers in each of the buildings. He knows that if two buildings are linked by a hallway, then they require routers with different frequencies to prevent interference. Assume that the available frequencies are $A, B, C, D, E, \ldots$. Label each building in Figure 2 below with a frequency in a way that prevents interference and uses the minimum number of frequencies.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure2.png}
\caption{Label the graph above using the minimum number of frequencies and preventing interference.}
\end{figure}

**Solution.** Three frequencies are needed at most:

\[
\begin{array}{ccc}
A & B \\
A & B & C & A \\
C & A \\
\end{array}
\]
Problem 8. [18 points] A graph $G = (V, E)$ is said to be outerplanar if you can draw the graph in the plane so that each vertex is placed at a distinct point on the unit circle and so that when every edge is drawn as a straight line (e.g. a chord of the unit circle), there are no edge crossings. For example, look at the two graphs in Figure 3 below.

![Figure 3](image-url)

**Figure 3.** The graph on the left is an outerplanar graph. The graph on the right, $K_4$, is not an outerplanar graph.

Prove that for all integers $n \geq 2$, an $n$-node outerplanar graph can have at most $2n - 3$ edges.

**Solution.** There are several ways to prove this. Some of you tried to use the property that an outerplanar graph has at least one vertex with degree at most 2, but this property actually follows directly from the fact that an outerplanar graph has at most $2n - 3$ edges (not the other way around).

Let us instead directly induct on the number of nodes, using strong induction. Let $P(n)$ be the statement that an $n$-node outerplanar graph can have at most $2n - 3$ edges.

**Base Case:** $P(2)$.

A 2-node outerplanar graph can have at most 1 edge, which is equal to $2(2) - 3$, so our base case holds.

**Inductive Step:** Show that $P(2) \land P(3) \land \cdots \land P(n) \rightarrow P(n + 1)$.

Assume $P(2) \land P(3) \land \cdots \land P(n)$. Find an edge, $e$, on the $(n + 1)$-outerplanar graph that does not connect adjacent nodes (adjacent on the circle that can be drawn through the graph). If no such edge exists, then the graph can have at most $n + 1$ edges, and $\forall n > 2$, $n + 1 < 2(n + 1) - 3$ and we are done.

$e$ divides the circle into two sides. Consider the graph induced on one side of $e$ (which includes $e$) with $n_1$ nodes, and the graph induced on the other side of $e$ (which also includes $e$) with $n_2$ nodes, where $n_1, n_2 \leq n$ and $n_1 + n_2 = n + 3$ (the incident vertices of $e$ are repeated, which adds 2 to $n + 1$). Except for $e$, the graphs do not share any edges, and because they are subgraphs of an outerplanar graph, they themselves are also outerplanar.
As an example, consider the following figure. $e$ is marked in green, and the graph partitions are outlined in red.

By strong induction, the $n_1$-node outerplanar graph has at most $2n_1 - 3$ edges, and the $n_2$-node outerplanar graph has at most $2n_2 - 3$ edges. Then the original $(n + 1)$-node graph has

\[
\leq 2(n_1 + n_2) - 6 - 1 \text{ edges } (-1 \text{ because } e \text{ is repeated})
\]

\[
= 2(n + 3) - 7
\]

\[
= 2(n + 1) - 3
\]

which proves $P(n + 1)$.  □