1. (16 points) Circle T if the corresponding statement is True or F if it is False.

T  F  For any positive integer, n, GCD(n, 1) = 1.

T  F  Every positive integer is either prime or composite.

T  F  If \( a \equiv b \mod p \), then \( (a/p) = (b/p) \).

T  F  If \( a \) and \( b \) are positive integers, then \( a = b(a \operatorname{DIV} b) + (a \operatorname{MOD} b) \).

T  F  \( 1 + 3 + 3^2 + 3^3 + 3^4 + \ldots + 3^{33} = 3^{34} - 1 \).

T  F  Algorithms with \( O(n^3) \) are less efficient than those with \( O(3^n) \).

T  F  Any statement validated by the Weak Principle of Mathematical Induction cannot be validated by the Strong Principle of Mathematical Induction.

T  F  GCD(368, 60) = GCD(60, 8).

2. (8 points) Find GCD( 2^{35}2^{7}11^{1}13^{0}17^{5}19^{0}23^{1}29^{1}31^{2} , 2^{45}17^{0}11^{2}13^{4}17^{4}19^{3}23^{1}29^{0}31^{3} )

GCD = 2^{35}17^{0}11^{1}13^{0}17^{4}19^{0}23^{1}29^{0}31^{2}  
   equivalently, = 2^{35}11^{1}17^{4}23^{1}31^{2}

3. (8 points) List out the search intervals of the Binary Search algorithm to find 4 in the list:
   3 4 6 9 13 18 21 34 55 72 83 85 92 104 111 133

Pass 1: (3 4 6 9 13 18 21 34) (55 72 83 85 92 104 111 133)

Pass 2: (3 4 6 9) (13 18 21 34)

Pass 3: (3 4) (6 9)

Pass 4: (3) (4)
4. (10 points) List the next 5 terms of the sequence \( \{a_n\} \) that follows the Fibonacci relation with the initial conditions, \( a_0 = 2 \) and \( a_1 = 4 \).

\[
2, 4, (2+4), (2+4+2+4), (4+2+4+2+4+4+2+4), (2+4+4+2+4+4+2+4+4+2+4), ... \\
= 2, 4, 2+4 = 6, 4+6 = 10, 6+10 = 16, 10+16 = 26, 16+26 = 42, ...
\]

so the next 5 terms are 6, 10, 16, 26, 42.

5. (12 points) Write out the Division Algorithm and trace its steps to calculate \((44 \text{ MOD } 12)\).

\[
\text{PROCEDURE DIV ALG (INPUT N,D: INTEGER)} \\
\begin{align*}
\text{SET Q} & = 0 \\
\text{WHILE (N > D)} & \\
\text{SET Q} & = Q + 1 \\
\text{SET N} & = N - D \\
\text{ENDWHILE} \\
\text{OUTPUT (Q, N)}
\end{align*}
\]

Trace:

<table>
<thead>
<tr>
<th>Pass</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>N</td>
<td>44</td>
<td>32</td>
<td>20</td>
<td>8</td>
</tr>
<tr>
<td>D</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>

OUTPUT(3, 8).

6. (8 points) What set, \( S \), is defined by the Inductive Definition:

\[
1 \in S, \text{ and, if } n \in S, \text{ then } (5n) \in S.
\]

Iterations of \( S \): \( \{1\}, \{1, 5\}, \{1, 5, 5^2\}, \{1, 5, 5^2, 5^3, 5^4\}, \{1, 5, 5^2, 5^3, 5^4, 5^5, 5^6, 5^7, 5^8\}, \text{ etc.} \)

so, \( S \) is the set of powers of 5.

7. (8 points) Show \( n^{10} \) is the Big-Oh of the algorithm with complexity:

\[
(2n^3 + 3n^2)(n^7 + 6n^5) + [3n^5 + 2n^4].
\]

\[
(2n^3 + 3n^2)(n^7 + 6n^5) + [3n^5 + 2n^4] \\
\leq (2n^3 + 3n^3)(n^7 + 6n^7) + [3n^5 + 2n^5] \\
= (5n^3)(7n^7) + (5n^5) \\
= (35n^{10}) + (5n^5) \\
\leq (35n^{10}) + (5n^{10}) = 40n^{10}.
\]
8. (10 points) Prove ONE of the TWO Theorems below using Mathematical Induction.

Theorem 1: For all Natural numbers \( n \),
\[
\sum_{i=0}^{n} 7^i = \frac{7^{n+1} - 1}{6}.
\]

Theorem 2: If \( a_0 = 10, a_1 = 20, \) and \( a_2 = 30, \) then \( a_n = a_{n-1} + a_{n-2} + a_{n-3} \) is a multiple of 10, for all \( n > 2. \)

Theorem 1: Proof (Weak Induction):

\textbf{Basis Step:} Show true for \( n = 0. \) In this case, \(
\sum_{i=0}^{0} 7^i = 7^0 = 1\), and \( \frac{7^{0+1} - 1}{6} = \frac{7-1}{6} = \frac{6}{6} = 1 \), hence \( \sum_{i=0}^{n} 7^i = \frac{7^{n+1} - 1}{6} \), when \( n = 0. \)

\textbf{Induction Step:} Assume \( \sum_{i=0}^{k} 7^i = \frac{7^{k+1} - 1}{6} \) and show \( \sum_{i=0}^{k+1} 7^i = \frac{7^{k+2} - 1}{6}. \)

Now, \( \sum_{i=0}^{k+1} 7^i = \sum_{i=0}^{k} 7^i + \sum_{i=k+1}^{k+1} 7^i = \frac{7^{k+1} - 1}{6} + \frac{7^{k+1} - 1}{6} = \frac{7^{k+1} - 1 + 6(7^{k+1})}{6} = \frac{7^{k+1} - 1 + 6 \cdot 7}{6} = \frac{7^{k+1} - 1 + 42}{6} = \frac{7^{k+2} - 1}{6}. \)

Therefore \( \sum_{i=0}^{n} 7^i = \frac{7^{n+1} - 1}{6} \) for all Natural numbers, \( n. \) QED

Theorem 2: Proof (Strong Induction):

\textbf{Basis Step:} Show true for \( n = 3. \) Now, \( a_3 = a_2 + a_1 + a_0 = 30 + 20 + 10 = 60 = 10(6) \) and 6 is an Integer, hence \( a_3 \) is a multiple of 10. Thus the assertion is true for \( n = 3. \)

\textbf{Induction Step:} Assume \( a_4, a_5, a_6, \ldots, a_k \) are all multiples of 10. Show \( a_{k+1} \) is a multiple of 10. 

Now, \( a_{k+1} = a_k + a_{k-1} + a_{k-2}, \) but \( a_k, a_{k-1} \) and \( a_{k-2} \) are all multiples of 10 by the Inductive Hypotheses, hence there exist Integers, \( p, q, r, \) such that \( a_k = 10p, a_{k-1} = 10q, \) and \( a_{k-2} = 10r. \)

Thus, \( a_{k+1} = 10p + 10q + 10r = 10(p + q + r). \) Since \( p, q, r \) are Integers, we have that \( (p + q + r) \) is
an Integer, implying $a_{k+1}$ is a multiple of 10.

Therefore an is a multiple of 10 for all Integers $n > 2$. QED

9. (10 points) Prove ONE of the TWO Theorems below:

**Theorem 1:** If $a$, $b$, and $c$ are Integers, with $a = b + c$, then GCD($a$, $b$) = GCD($b$, $c$).

**Theorem 2:** If $a$, $b$, $c$, $d$, and $p$ are Integers with $a \equiv b \mod p$, and $c \equiv d \mod p$, then $(a + c) \equiv (b + d) \mod p$.

**Theorem 1:**

**Proof:** Assume $a$, $b$, and $c$ are Integers with $a = b + c$. We will show that GCD($a$, $b$) $\geq$ GCD($b$, $c$) and GCD($a$, $b$) $\leq$ GCD($b$, $c$), thus concluding that GCD($a$, $b$) = GCD($b$, $c$).

**Case 1:** (Show GCD($a$, $b$) $\leq$ GCD($b$, $c$)). Denote $X = \text{GCD}(a, b)$, and $Y = \text{GCD}(b, c)$. Since $X$ is the GCD($a$, $b$), $X$ is a common divisor of $a$ and $b$, hence, there are Integers $m$, $n$ with $a = mX$ and $b = nX$.

Now, $a = b + c$ implies $(mX) = (nX) + c$, so $c = (mX) - (nX) = (m - n)X$. Since $m, n$ are Integers, we have that $(m - n)$ is an Integer. Thus $X$ is an integer multiple of $c$, so it is a divisor of $c$. Since $X$ is also a divisor of $b$, it is a common divisor of $b$ and $c$, hence $X = \text{GCD}(a, b) \leq \text{GCD}(b, c)$.

**Case 2:** (Show GCD($b$, $c$) $\leq$ GCD($a$, $b$)). As above, denote $X = \text{GCD}(a, b)$, and $Y = \text{GCD}(b, c)$. Since $Y$ is the GCD($b$, $c$), $Y$ is a common divisor of $b$ and $c$, hence, there are Integers $p$, $q$ with $b = pY$ and $c = qY$.

Now, $a = b + c$ implies $a = (pY) + (qY)$, so $a = (p + q)Y$. Since $p, q$ are Integers, we have that $(p + q)$ is an Integer. Thus $Y$ is an integer multiple of $a$, so it is a divisor of $a$. Since $Y$ is also a divisor of $b$, it is a common divisor of $a$ and $b$, hence $Y = \text{GCD}(a, b) \leq \text{GCD}(a, b)$.

Therefore, GCD($a$, $b$) = GCD($b$, $c$). QED

**Theorem 2:**

**Proof:** Let $a$, $b$, $c$, $d$, and $p$ be Integers with $a \equiv b \mod p$, and $c \equiv d \mod p$. Thus, there exist Integers, $X$ and $Y$ with $(a - b) = pX$ and $(c - d) = pY$.

Now, $(a + c) - (b + d) = (a + c - b - d) = (a - b) + (c - d) = pX + pY = p(X + Y)$. Since $X$ and $Y$ are Integers, we see that $(X + Y)$ is an Integer, hence $(a + c) - (b + d)$ is an Integer multiple of $p$. 
Therefore, \((a + c) \equiv (b + d) \mod p\). QED

10. (10 points) Prove ONE of the TWO Theorems below by Contradiction or Contraposition.

**Theorem 1:** The set of Natural numbers is infinite.

**Theorem 2:** If \(n\) is an Integer and \(n^2\) is even, then \(n\) is even.

**Theorem 1:**
Proof: (Contradiction) Assume the set of Natural numbers is not infinite; that is, assume there is a largest Natural, say, \(Z\).

Now, since \(Z\) is a Natural number, \((Z + 1)\) is also a Natural number, but since \(Z\) is the largest Natural number, we have that \((Z + 1) < Z\). Subtracting \(Z\) from both sides yields \(1 < 0\), a contradiction.

Hence, \(Z\) cannot be the largest Natural number, therefore the set of Natural numbers is infinite.

**Theorem 2:**
Proof: (Contraposition) We will prove that assuming \(n\) is an Integer and \(n\) is odd, then \(n^2\) is odd.

Now, since \(n\) is odd, there is an Integer, \(X\), with \(n = 2X + 1\).

Thus, \(n^2 = (2X + 1)^2 = 4X^2 + 4X + 1 = 2(2X^2 + 2X) + 1\). However, since \(X\) is an Integer, it follows that \(2X^2 + 2X\) is an Integer.

Therefore \(n^2\) is an odd integer. QED