Name: ________________________________

- You may not use any reference materials during this exam.
- Electronic devices, including calculators, cell phones, mp3 players, and laptops are all prohibited.
- You may not use your own scratch paper. The exam has plenty and you can ask for more if needed.
- You may not leave the classroom once the exam has been distributed.
- Communicating with other students in any way is prohibited.

Academic Honesty: I understand that if I cheat on this exam in any way, I will receive the maximum possible penalty, including an F in this course.

Signature: ________________________________

<table>
<thead>
<tr>
<th>Problem</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>/20</td>
</tr>
<tr>
<td>2</td>
<td>/15</td>
</tr>
<tr>
<td>3</td>
<td>/15</td>
</tr>
<tr>
<td>4</td>
<td>/25</td>
</tr>
<tr>
<td>5</td>
<td>/20</td>
</tr>
<tr>
<td>6</td>
<td>/15</td>
</tr>
<tr>
<td>Total</td>
<td>/110</td>
</tr>
</tbody>
</table>
Basic Number Theory

(a) (3 points) What is $\phi(23)$?

(b) (3 points) What is $\phi(15)$?

(c) (3 points) What is $7^2 \mod 15$?

(d) (3 points) What is $7^{642} \mod 15$?

(e) (4 points) What is $7^{-1} \mod 15$?

(f) (4 points) Find integers $s$ and $t$ such that $15s + 23t = 1$. 
Induction

(15 points) Let \( x_0 = 1 \) and define \( x_n = \frac{1}{x_{n-1}} \). Prove by induction that, for all \( k \in \mathbb{N} \), \( x_{2k} > \frac{\sqrt{5} - 1}{2} \) and \( x_{2k+1} < \frac{\sqrt{5} - 1}{2} \).
Cardinality

(15 points) Indicate whether each set is finite, countably infinite, or uncountable.

(a) $\mathbb{N} \times \mathbb{Q}$

(b) $\prod_{n=0}^{\infty} \{0,1\}$

(c) $\{0,1\}^n$, where $n \in \mathbb{N}$

(d) $\bigcup_{n=0}^{\infty} \{0,1\}^n$

(e) $\mathbb{Q} \cup \bigcup_{n=0}^{\infty} \{0,1\}^n$
Analyzing the Euclidean Algorithm

(a) (7 points) Prove that if $b \leq a$, then $a \mod b < \frac{a}{2}$.

(b) (8 points) Assume computing $a \mod b$ takes 1 time unit. Let $T(a, b)$ be the amount of time it takes to compute $\gcd(a, b)$, when $b \leq a$. By using the fact that $\gcd(a, b) = \gcd(b, a \mod b)$, prove that $T(a, b) \leq 1 + T(b, a/2)$. 
(c) (10 points) Assume that for any $a > 0$, we can compute $gcd(a, 0)$ in 1 time unit. Prove by strong induction that, when $ab \neq 0$, $T(a, b) \leq 2 + \log_2 ab$. (Hint: Remember that $\log_2 \frac{x}{2} = \log_2 x - 1$).
Implementing Multiplication

Let $x_1x_0$ and $y_1y_0$ be 2-bit numbers, where $x_i$ is the $i$th bit of $x$ and $y_i$ is the $i$th bit of $y$. For example, if $x = 2$, then $x_1 = 1$ and $x_0 = 0$.

(a) (2 points) Since $x$ can each be represented using only 2 bits, what is the largest possible value for $x$?

(b) (2 points) Let $m = xy$. What’s the max possible value for $m$? How many bits do we need to represent $m$?

(c) (16 points) Derive boolean logic formulas for each bit of $m$. You can use $\land$, $\lor$, $\neg$, and $\oplus$ (exclusive-or) in your formulas.
Graph Theory

(15 points) Suppose an odd number of people attend a party. Prove that, no matter who shakes hands with whom, someone at the party must shake hands with an even number of people. (Hint: make a graph of who shakes hands; apply a theorem relating $|E|$ and the node degrees.)