1. You are given a fair balance, consisting of a pair of scales. Each time the balance is used, either the right scale will tip (if the weight on the right is strictly greater than the weight on the left), or the left scale will tip, or the two scales will be in balance (if the two weights are exactly equal). You are also given an infinite supply of two types of weights: small weights, each weighing \( m \) ounces, and large weights, each weighing \( n \) ounces. Finally, you also have a golden crown that weighs exactly \( x \) ounces, where \( x \) is a positive integer. Your goal is to determine the weight of the crown.

(a) Suppose that \( m = 100 \) and \( n = 441 \). Can you determine the weight of the crown? If yes, explain why. If not, explain why not.

(b) Now suppose that \( m = 6 \) and \( n = 9 \). Can you determine the weight of the crown? If yes, explain why. If not, explain why not.

(c) **Extra credit:** (5 points). Can the crown’s weight be determined if \( m = 6 \) and \( n = 88 \)?

2. Alice is a student in CSE20. Having learned about the RSA cryptosystem in class, she decides to set-up her own public key as follows. She chooses the primes \( p = 563 \) and \( q = 383 \), so that the modulus is \( N = 215629 \). She also chooses the encryption key \( e = 49 \). She posts the numbers \( N = 215629 \) and \( e = 49 \) to her website. Bob, who is in love with Alice, desires to send her messages every hour. To do so, he chooses his messages \( m \) such that \( \gcd(m, N) = 1 \) and encrypts them as follows: \( M = m^{49} \mod 215629 \), duly using the public key posted by Alice.

(a) Using the knowledge that \( N = 563 \cdot 383 \), compute a decryption key \( d \) for Alice, so that \( M^d = m \mod 215629 \). *(Hint: the Euclidean algorithm is helpful here.)*

A hacker Henry intercepts the encrypted messages. He does not want to bother factoring the modulus \( N = 215629 \). Instead, he mounts the following attack on Alice’s cryptosystem. Given the encrypted message \( M \), he encrypts it again to generate \( M_1 = M^{49} \mod 215629 \). He then encrypts \( M_1 \) again to generate \( M_2 = M_1^{49} \mod 215629 \). And so on. Thus Henry computes the sequence \( M_1, M_2, \ldots \), defined recursively by:

\[
M_{i+1} \overset{\text{def}}{=} M_i^{49} \mod 215629 \quad \text{for } i = 1, 2, \ldots
\]

At each step, Henry checks whether \( M_i = M \), where \( M \) is the original encrypted message. If this happens he is in luck, as we shall now see.

(b) Prove that no matter what message \( M = m^{49} \mod 215629 \) Bob sends to Alice, the hacker Henry will always observe that \( M_{10} = M \).

(c) Having observed that \( M_{10} = M \), Henry can now recover Bob’s message \( m \) from its encrypted version \( M \). How does he do that?

**Note:** In part (b), you might need to use a program that makes it possible to handle very large integers. Some examples are MATHEMATICA (or WOLFRAM ALPHA), MAPLE, and \texttt{bc} on Unix.

3. Prove with and without induction that \( 1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1 \)
4. We would like to prove by induction that \( \sum_{i=1}^{n} f(i) = n^2(n + 1) \). For which choice of \( f(i) \) will induction work?

   (0) \( 3i^2 - 2 \)
   (1) \( 2i^2 \)
   (2) \( 3i^3 - i \)
   (3) \( i(3i - 1) \)
   (4) \( 3i^3 - 7i \)

For full credit, you must not only indicate the correct answer, but also explain in detail how you arrived at this result.

5. This problem deals with the function

   \[ S(n) \overset{\text{def}}{=} \sum_{i=1}^{n} (-1)^{i+1} i^2 \]

   (a) Compute \( S(1), S(2), S(3), S(4), S(5) \) and, if you’d like, several more values of \( S(n) \).
   (b) Based on these results, guess a general formula for \( S(n) \).
   (c) Prove this formula by mathematical induction.

6. Prove by induction that for all integers \( n \geq 1 \), a \( 2^n \times 2^n \) grid with any one square missing can be tiled by 3-square L-shaped tiles. For example, here are tilings of three such grids:

```
<table>
<thead>
<tr>
<th>1</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
```

```
<table>
<thead>
<tr>
<th>4</th>
<th>4</th>
<th>3</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>5</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
```

```
<table>
<thead>
<tr>
<th>4</th>
<th>4</th>
<th>3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>5</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
```

where each number represents a tile and the black cell represents the missing square, which could appear anywhere in the \( 2^n \times 2^n \) grid.

7. Now, let us prove that all horses have the same color. We show by induction on \( n \) that in every set of \( n \) horses, all horses in the set have the same color.

   **Induction base:** Clearly, for every set of one horse, all horses in the set have the same color.

   **Induction hypothesis:** Suppose that in every set of \( k \) horses, all horses in the set have the same color.

   **Inductive step:** Let us consider an arbitrary set of \( k + 1 \) horses, and let us number these horses \( 1, 2, \ldots, k+1 \). By induction hypothesis, horses \( 1, 2, \ldots, k \) all have the same color, and horses \( 2, \ldots, k, k + 1 \) also all have the same color. But then horse \( k + 1 \) has the same color as horse \( k \), and therefore the same color as horses \( 1, 2, \ldots k - 1 \). Thus all horses \( 1, 2, \ldots k + 1 \) have the same color.

What is wrong with this argument?! Explain your answer in detail.