1. Let $G(c, e)$ be the predicate "Country c won a gold medal in event e" at the olympics. The propositional formulas below should use the predicate G and quantifiers over countries and events.

   (a) In the olympics, a gold medal is awarded in every event. Express that as a propositional formula.

   Solution: $\forall e\ \exists c\colon G(c, e)$.

   (b) One country was very successful. It won gold in all events. Express that as a propositional formula.

   Solution: $\exists c\ \forall e\colon G(c, e)$.

   (c) Show that (a) and (b) are not logically equivalent.
   (**Hint:** Construct an "olympic world" in which one is true and the other one is false.)

   Solution: Suppose Canada and USA are the only participating countries, curling and hockey are the only sports, Canada won gold in curling, and USA won gold in hockey. In these olympics (a) is true and (b) is false.

2. True or false? Justify your answer. There exists a 3 by 3 table of distinct numbers so that

   (a) after sorting its columns, the smallest and largest numbers are in the same column?

   Solution: True. Here is an example:

   $$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 9 & 8 & 7 \end{array}$$

   its columns are already sorted, and its smallest and largest entries are both in the first column.

   (b) after sorting its columns, the smallest and largest numbers are in the same row?

   Solution: False. We prove that they must be in distinct rows. The smallest number of the table is also smallest in its column. After sorting it must be in the first row. The largest number of the table is also largest in its column. After sorting it must be in the last row. Therefore the two are in different rows.

3. The sequence of numbers $a_0, a_1, a_2, \ldots$ is specified by $a_{n+1} = (a_n)^2 + a_{n-1}$ for $n \geq 1$, with $a_0 = 1$ and $a_1 = 1$.

   (a) Write 1 as an integer linear combination of a_3 and a_4. Show your work.

   Solution: We calculate $a_2 = 1^2 + 1 = 2$, $a_3 = 2^2 + 1 = 5$, and $a_4 = 5^2 + 2 = 27$. To express 1 as a combination of a_3 and a_4 we run extended Euclid's algorithm:

   $$\begin{aligned} E(27, 5) &= E(5, 2) & 27 &= 5 \cdot 5 + 2 \\ &= E(2, 1) & 5 &= 2 \cdot 2 + 1 \end{aligned}$$

   so that $1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (27 - 5 \cdot 5) = -2 \cdot 27 + 11 \cdot 5$.

   (b) Use induction to prove that 1 is an integer linear combination of a_n and a_{n-1} for every $n \geq 1$.

   Solution: Base case $n = 1$**:** $1 = 1 \cdot 1 + 0 \cdot a_0 = 1 \cdot a_1 + 0 \cdot a_0$.

   Inductive step: We assume 1 is a combination of a_n and a_{n-1}, namely $1 = s \cdot a_n + t \cdot a_{n-1}$ for some s and t. As $a_{n-1} = a_{n+1} - a_n^2$,

   $$1 = s \cdot a_n + t \cdot (a_{n+1} - a_n^2) = t \cdot a_{n+1} + (s - t \cdot a_n) \cdot a_n$$

   so 1 is also a combination of a_{n+1} and a_n.

4. Alice uses the one-time pad to message Bob. The modulus is $n = 37$.

   (a) If their secret key is $k = 20$ and Bob receives the encryption $c = 11$, what is Alice's message?

   Solution: To decrypt, Bob calculates $c - k \bmod 37 = 11 - 20 \bmod 37 = -9 \bmod 37 = 28$. This is Alice's message.

   (b) Now the secret key k is different. Eve observes the encryption $c = 32$ of Alice's message m. To make sure he got it right, Bob asks Alice to also encrypt $10m$. Eve observes $c' = 3$ as the encryption of $10m$ under the same secret key. Fill in the blanks and explain.

   Solution:

$$\underline{1} \cdot m + \underline{1} \cdot k \equiv \underline{32} \pmod{\underline{37}}$$
$$\underline{10} \cdot m + \underline{1} \cdot k \equiv \underline{3} \pmod{\underline{37}}$$

   To encrypt, Alice calculated $m + k$ to get 32 and $10m + k$ to get 3, both modulo 37.

   (c) Solve the equations in part (b) to find Alice's message.

   Solution: Subtracting the two we obtain $9m \equiv -29 \equiv 8 \pmod{37}$. To find the inverse of 9 we apply extended Euclid's algorithm to get $E(37, 9) = E(9, 1)$ as $37 = 4 \cdot 9 + 1$, so the inverse of 9 is -4, and m is $8 \cdot (-4) \equiv -32 \equiv 5 \pmod{37}$. The message is $m = 5$.

5. **BONUS.** You start with the sequence `1 2 3` $\cdots$ `30`. In every step you may choose five consecutive numbers and reverse their order. For example, `15 2 26 4 9` may be replaced by `9 4 26 2 15`. Can you eventually flip the whole sequence so that the numbers appear in reverse order from `30` to `1`?

   Solution: No. We prove that "the position of 1 is odd" is an invariant. Initially 1 is in position 1 which is odd. Now assume 1 is in odd position before a transition. If 1 is not among the reversed numbers, its position stays odd. Otherwise, if 1 was s slots away from the inversion pivot, its absolute position changes by $-2s$ (if it was to the right) or $2s$ (if it was to the left). The position of 1 therefore changes by an even amount so it stays odd.

   In the reverse ordering 1 is in position 30 which is even. As the invariant does not hold for this state it is unreachable.

   Alternative solution: No. We prove that "the number of inverted (out of order) pairs is even" is an invariant. Initially there are no inversions so the number of inverted pairs is even. In a transition, call R the set of five numbers that are reversed. The inversion status changes precisely for those pairs both of whose elements are in R. There are $4 + 3 + 2 + 1 = 10$ such pairs: The first element in R can be paired up with 4 others, the second one with 3 others, and so on.

   Before the transition, suppose there are r inverted pairs both of whose elements are in R, and s others. We know $r + s$ is even. After the transition, there will be $(10 - r) + s$ inversions. As $(10 - r) + s \equiv r + s \pmod 2$, the number of inverted pairs stays even.

   The state in which all numbers appear in reverse order has $29 + 28 + \cdots + 1 = 29 \cdot 30/2 = 29 \cdot 15$ inversions. This is a product of odd numbers so it is odd. Therefore this state cannot be reached.