1. **Proposition:** Every positive integer n can be written as a sum of distinct squares of positive integers. (For example, $45 = 2^2 + 4^2 + 5^2$.)

   (a) Show that the proposition is false.

   Solution: 2 is not a sum of distinct squares. The only possible representation as a sum of squares uses 1^2 twice.

   (b) Underline and explain the mistake in the following "proof".

   Proof. We prove the proposition by strong induction on n. The base case $n = 1$ holds because $1 = 1^2$. For the inductive step, assume that it is true for all numbers between 1 and $n - 1$. If n is the square of some number, then it is also true for n. If not, $m^2 < n < (m+1)^2$ for some number $m > 0$. By inductive hypothesis, the number $n - m^2$ is a sum of distinct squares $a_1^2 + \cdots + a_k^2$. Then $n = a_1^2 + \cdots + a_k^2 + m^2$ so n is also a sum of distinct squares. □

   Solution: It was never proved that m^2 is distinct from all of $a_1^2, \ldots, a_k^2$.

2. True or false? Justify your answer. Specify your proof method.

   (a) For all integers a, b, c, at least one of the three numbers $a + b$, $b + c$, $c + a$ is even.

   Solution: True. We prove it by contradiction. Suppose $a + b$, $b + c$, and $c + a$ are all odd. The sum of all three must then be odd. But the sum equals $2(a + b + c)$ which is an even number, a contradiction. This proof can also be formulated using modular arithmetic: Assuming $a + b \equiv 1$ and $b + c \equiv 1$ and $c + a \equiv 1$ modulo 2, adding the equations yields the conclusion

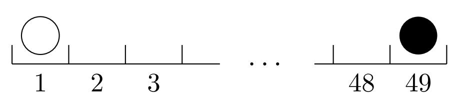
   $$0 = 0a + 0b + 0c \equiv 2a + 2b + 2c \equiv 1 + 1 + 1 \equiv 1 \pmod 2$$

   which is a contradiction.

   (b) For all integers a, b, c, at least one of the three numbers $a + b$, $b + c$, $c + a$ is odd.

   Solution: False. When $a = b = c = 0$ then all three numbers are zero therefore all are even.

3. A long ledge is divided into slots numbered from 1 to 49.



   A white ball and a black ball are placed in the first and last slot, respectively. In every step one of the balls is moved 5 slots to the left *or* 10 slots to the right of its current position.

   (a) Formulate this process as a state machine. Describe the states, start state, and transitions. (**Hint:** The state should describe the positions of both balls.)

   Solution: The states are ordered pairs of numbers (w, b) between 1 and 49 describing the white and black ball's slot respectively. The start state is $(1, 49)$. The transitions are

   $$(w, b) \to (w - 5, b) \text{ OR } (w + 10, b) \text{ OR } (w, b - 5) \text{ OR } (w, b + 10).$$

   (b) Fill in the two blanks so that the following predicate is an invariant. Provide a proof.

   The slot numbers of the black and white balls differ by 3 modulo 5.

Solution: In the start state, $49 - 1 = 48 \equiv 3 \pmod 5$ so the invariant holds. Now assume $b - w \equiv 3 \pmod 5$ in a given state. The transitions change the value of $b-w$ by $+5$, -10, -5, and -10 respectively. As all these numbers are 0 modulo 5 the value $b - w \pmod 5$ remains the same.

(c) Can the two balls ever occupy adjacent slots? Justify your answer.

Solution: No. If the balls occupy adjacent slots then $b - w$ equals to 1 or -1, that is 1 or 4 modulo 5. The invariant is not satisfied so such a state can never be reached.

4. Bob is waiting for a secret message from Alice. He publishes RSA modulus $n = 21$ and public key $e = 5$.

(a) Alice's message is $m = 8$. What is the ciphertext that she sends out? Show your calculations.

Solution: The ciphertext is $m^e \bmod n$, namely

$$8^5 \equiv 8 \cdot 8^4 \equiv 8 \cdot 64^2 \equiv 8 \cdot 1^2 = 8 \pmod{21}$$

because $64 = 3 \cdot 21 + 1 \equiv 1 \pmod{21}$.

(b) Alice sends another ciphertext $c = 2$ and this one is intercepted by Eve. What was Alice's message?

Solution: As n is the product of the two primes $p = 3$ and $q = 7$, Eve can recover the decryption key by solving for $ed \equiv 1 \pmod{(p-1)(q-1)}$, namely $5d \equiv 1 \pmod{12}$. Extended Euclid's algorithm gives

$$\begin{aligned} E(12,5) &= E(5,2) & \qquad 12 &= 2 \cdot 5 + 2 \\ &= E(2,1) & 5 &= 2 \cdot 2 + 1 \end{aligned}$$

from where $1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (12 - 2 \cdot 5) = -2 \cdot 12 + 5 \cdot 5$, so d equals 5. The ciphertext decrypts to $c^d \bmod n$, which equals $2^5 = 32 \equiv 11 \pmod{21}$. Alice's message was 11.

BONUS. What is

$$2^{2^{2^{2^{2^{2^{2}}}}}} \bmod 11?$$

By Fermat's little theorem, reducing the exponent modulo 10 does not change the answer. As the exponent is an even number and $10 = 2 \cdot 5$,

$$2^{2^{2^{2^{2^{2}}}}} \bmod 10 = 2 \cdot \left(2^{2^{2^{2^{2^{2}}}}}/2 \bmod 5\right) = 2 \cdot \left(2^{2^{2^{2^{2^{2}}}}-1} \bmod 5\right).$$

Using Fermat's little theorem again we find

$$2^{2^{2^{2^{2^{2}}}}-1} \equiv 2^{(2^{2^{2^{2^{2}}}}-1) \bmod 4} \equiv 2^{-1 \bmod 4} \equiv 2^3 \equiv 3 \pmod 5.$$

Therefore

$$2^{2^{2^{2^{2^{2^{2}}}}}} \equiv 2^{2^{2^{2^{2^{2^{2}}}}} \bmod 10} \equiv 2^{2 \cdot 3} = 64 \equiv 9 \pmod{11}.$$