Problem 7.1.

Until 2007, every published book was classified by a 10-digit ISBN number (nowadays replaced by a 13-digit number). The first 9 digits are decimal numbers and uniquely identify the book. The last (10th) digit is a control digit which is either a decimal number or the letter X. The purpose of the control digit is to detect eventual copying errors. It is calculated as follows:

$$x_{10} := \left(\sum_{i=1}^{9} i \cdot x_i\right) \ \%11, \tag{1}$$

where $x_1x_2\cdots x_9$ is the 9-digit identifier of the book. Recall that $n\%11$ is the remainder of the division of n by 11. If $x_{10} < 10$, then it is written as its decimal representation, otherwise it is replaced by the letter X. This way, $x_1x_2\cdots x_{10}$ has always length 10.

1. Show that x is a valid 10-digit ISBN number (commonly denoted as ISBN-10) if and only if

$$\left(\sum_{i=1}^{10} i \cdot x_i\right) \equiv 0 \mod 11 \tag{2}$$

   (If $x_{10} = X$, consider it as $x_{10} = 10$.)
2. Let $x = x_1 \cdots x_{10}$ be a valid ISBN-10 number, and y be a 10-digit number identical to x except at the ith digit where x_i is replaced with $y_i \neq x_i$. Show that y cannot be a valid ISBN-10 number.
3. Let y be a 10-digit number identical to x except in the ith and $(i+1)$th digits which are swapped:

$$\begin{cases} y_i = x_{i+1} \\ y_{i+1} = x_i \\ y_k = x_k \quad \text{if } k \neq i \text{ and } k \neq i+1 \end{cases}$$

   Show that if y is a valid ISBN-10 number, then $x_i = x_{i+1}$.

Problem 7.2.

Use modular arithmetic to compute the last digit of the number 347^{348}.

Problem 7.3.

Solve for $x \in \mathbb{Z}/7\mathbb{Z}$ and $y \in \mathbb{Z}/7\mathbb{Z}$:

$$\begin{cases} [2]_7 x + [5]_7 y = [5]_7 \\ [1]_7 x + [2]_7 y = [1]_7 \end{cases}$$

(Give the possible solutions in reduced form.)

Problem 7.4.

Do the extended Euclid algorithm by hand (or program it, if you prefer) to find

1. $g = \gcd(549, 174)$ and (u, v) such that $g = 549u + 174v$
2. $h = gcd(36548971, 24563)$ and (x, y) such that $h = 36548971x + 24563y$.

Problem 7.5.

Let a and m be integers and $m > 1$. Prove that for every $0 < a < m$, if a is not invertible modulo m, then there exists a number $0 < b < m$ such that $a \cdot b \equiv 0 \pmod{m}$. Is this b unique?
(Hint: start with an example, i.e., $a = 4$ and $m = 8$. For the general case, try to relate b to m and $\gcd(a, m)$.)

Problem 7.6.

Consider the following sequence of numbers:

$$11, 111, 1111, \ldots, 111111111, \ldots$$

Show that there are no squares inside the sequence. *(Hint: the square of an even number is an even number, why? What about odd numbers?).*