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 $x_1 x_2 \cdots x_9$ 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, $x_1 x_2 \cdots x_{10}$ 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 $x_{10} = 10$.)

Solution:

Equation (1) is equivalent to writing

$$[0]_{11} = \sum_{i=1}^{9} i[x_i]_{11} - [x_{10}]_{11} = \sum_{i=1}^{9} i[x_i]_{11} + 10[x_{10}]_{11} = \sum_{i=1}^{10} i[x_i]_{11}$$

which is in fact equation (2).

Relevant slides : 368 - 373

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.

Solution:

Since x is a valid ISBN-10 number, x satisfies equation (2)

$$\sum_{i=1}^{10} i \cdot [x_i]_{11} = [0]_{11}$$

After the change $x_i \to y_i$, the above sum is modified by $-i[x_i]_{11} + i[y_i]_{11} = i([y_i]_{11} - [x_i]_{11})$. Notice that by assumption, $y_i \neq x_i$ and $i \neq 0$. Neither i nor $([y_i]_{11} - [x_i]_{11})$ are multiples of 11, and since 11 is a prime number, $i([y_i]_{11} - [x_i]_{11})$ is also not a multiple of 11, that is, $i([y_i]_{11} - [x_i]_{11}) \bmod 11 \neq 0$. As a consequence, by replacing x_i with $y_i \neq x_i$, the sum is no longer equal to 0 modulo 11. This means that y cannot satisfy equation (2), which shows that y is not a valid ISBN-10 number.

Relevant slides : 368 - 373

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 $x_i = x_{i+1}$.

Solution:

Since both x and y are valid ISBN-10 numbers, they both satisfy equation (2). Taking the difference of the two, we obtain

$$\sum_{j=1}^{10} j \cdot [x_j - y_j]_{11} = [0]_{11}$$

All terms in the above sum are zero except for $j = i$ and $j = i + 1$, so

$$\begin{aligned} \sum_{j=1}^{10} j \cdot [x_j - y_j]_{11} &= i[x_i]_{11} + (i+1)[x_{i+1}]_{11} - i[x_{i+1}]_{11} - (i+1)[x_i]_{11} \\ &= [x_{i+1}]_{11} - [x_i]_{11} \end{aligned}$$

Therefore, we find

$$[x_{i+1}]_{11} - [x_i]_{11} = [0]_{11}$$

This implies that $[x_i]_{11} = [x_{i+1}]_{11}$ but $x_i, x_{i+1} \in \{0, \ldots, 10\}$, thus $x_i = x_{i+1}$.

Relevant slides : 368 - 373

Problem 7.2.

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

Solution:

The last digit can be found computing the class of $[347^{348}]_{10}$ (in the decimal system, the rest of the division of a number by 10 provides the last digit). We have that $[347^{348}]_{10} = [7^{348}]_{10} = [(7^2)^{174}]_{10} = [49^{174}]_{10} = [(-1)^{174}]_{10} = [1]_{10}$. Where, $[347^{348}]_{10} = [7^{348}]_{10}$ as $[347]_{10} = [340 + 7]_{10} = [7]_{10}$, and $[49^{174}]_{10} = [(-1)^{174}]_{10}$ follows from $[49]_{10} = [-1]_{10}$. Hence, the last digit is 1.

Relevant slides : 330, 384 - 385

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.)

Solution:

First, we find the conditions which x and y should satisfy. Note that we can replace 1 by $[1]_7$ etc. We eliminate x by multiplying the second equation with $[2]_7$ (i.e. $[3]_7$), and then subtracting:

$$\begin{array}{rrll} & [2]_7 x + [5]_7 y & = [5]_7 & \\ - & [1]_7 x + [2]_7 y & = [1]_7 & \times [2]_7 \\ \hline & ([5]_7 - [4]_7) y & = [5]_7 - [2]_7 & \\ & y & = [3]_7 & \end{array}$$

We can obtain x from the second equation, for example:

$$x = [1]_7 - [2]_7[3]_7 = [-5]_7 = [2]_7$$

Hence, $x = [2]_7$ and $y = [3]_7$.

Relevant slides : 382 - 393

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 $h = 36548971x + 24563y$.

Solution:

1. For part 1, we show the calculation for the algorithm by hand.

$\gcd(a,b)$	$a = bq + r$	q	$\tilde{u}$	$\tilde{v}$	$u = \tilde{v}$	$v = \tilde{u} - q\tilde{v}$
$\gcd(549, 174)$	$549 = 174 \times 3 + 27$	3			13	-41
$\gcd(174, 27)$	$174 = 27 \times 6 + 12$	6	-2	13	-2	13
$\gcd(27, 12)$	$27 = 12 \times 2 + 3$	2	1	-2	1	-2
$\gcd(12, 3)$	$12 = 3 \times 4 + 0$	4	0	1	0	1
$\gcd(3, 0) = 3$			1	0		

Also, recall that you can do sporadic checks to reduce errors. For example, take the third line: It must be true that $\gcd(27, 12) = 27u + 12v = 27 \times 1 + 12 \times (-2)$. Indeed, this is equal to 3, as it should.

And of course, you can easily verify the final answer, too: $549u + 174v = 549 \times 13 + 174 \times (-41)$ is again equal to 3, as claimed.

2. For part 2, it will be quite annoying to compute the solution by hand. We can, however, program the solution. An example python program computing the required values of x and y is provided on the final page of the solutions; the values of h, x, y are 1, 6673, and -9929214 respectively.

Relevant slides : 409 - 416

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 $a \cdot b \equiv 0 \,(\text{mod} m)$. 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 $\gcd(a, m)$.)

Solution:

Let d be any divisor of both a and m. Then $b = \frac{m}{d}$ and $c = \frac{a}{d}$ are integers, and $a \cdot b = a \cdot \frac{m}{d} = \frac{a}{d} \cdot m = c \cdot m \equiv 0 \pmod m$. Furthermore, if $1 < d < m$ then $1 < b < m$. Note that if a is not invertible modulo m, then $1 < \gcd(a, m) < m$, and for every divisor $d \neq 1$ of $\gcd(a, m)$ we can find the corresponding b. In general this b is not unique, as every multiple of it (which is smaller than m) will satisfy the modular equality. For example if $a = 4$, $m = 8$ we can choose $b = 2$, $b = 4$ or $b = 6$.

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?).*

Solution:

Starting from the hint, if n is an even number it can be written as $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ which is even. Since in our sequence the numbers are all odd, they can only be squares of odd numbers. If a number n is odd it can be written as $n = 2k + 1$ for some $k \in \mathbb{Z}$. Hence, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2+k)+1 = 4j+1$ with $j = k^2+k$. We have that in this case $[n^2]_4 = [1]_4$. Going back to our sequence; each number $11 \ldots 11$ can be written as $11 \ldots 08 + 3$. Consequently $[11 \ldots 11]_4 = [11 \ldots 08+3]_4 = [3]_4$ (4 divides $11 \ldots 08$ because the last two digits are 08 and 4 divides 8). Since $[3]_4 \neq [1]_4$ we can conclude that no number in the sequence is a square.

Relevant slides : 384 - 385

```python
def euclidsub(a, b, qs):
    q = a//b
    r = a % b
    qs.append(q)
    if r == 0:
        us = [1]
        vs = [0]
        counter = 1
        return counter, qs, us, vs
    counter, qs, us, vs = euclidsub(b, r, qs)
    u = vs[-1]
    v = us[-1] - qs[-counter]*u
    us.append(u)
    vs.append(v)
    counter += 1
    return counter, qs, us, vs


def euclid(a, b):
    qs = []
    steps, qs, us, vs = euclidsub(a, b, qs)
    u = vs[-1]
    v = us[-1] - qs[-steps]*u
    return u, v
```