Danmarks Tekniske Universitet

DTU

Home assignment 4

Authors

Martin Moos Hansen - s203822
Jacopo Ceccuti - s215158
Mads Yar - s193992

Group 11

November 24, 2022

1 Exercise 4.1

a) We have to show the following holds by using induction:

$$10^n \equiv 1^n \pmod 9$$

The first thing to determine, when using induction, is the base case. This is done by setting n = 0. Thus, the following occurs:

$$10^0 \equiv 1^0 \pmod 9$$
$$1 \equiv 1 \pmod 9$$

It can now be seen that the base case is correct since 1 is equal to 1. In other words, 1 is congruent with itself, hence the relation holds for n = 0. Furthermore, before moving onwards to the induction step, recall the useful property: 10 mod 9 $\equiv$ 1 (mod 9) as dividing 10 by 9 leaves a remainder of 1. Now, for the induction step, assume that it holds for n, that is:

$$10^n \equiv 1^n \pmod 9 \tag{1}$$

Now recall that 10 mod 9 $\equiv$ 1 (mod 9):

$$10^n \cdot 10 \equiv 1^n \cdot 10 \pmod 9 \tag{2}$$
$$10^{n+1} \equiv 1^n \cdot 1 \pmod 9 \tag{3}$$
$$10^{n+1} \equiv 1^{n+1} \pmod 9 \tag{4}$$

Now, since the (n+1)th case is true whenever the nth case is true, and the 0th case is true, then the relation must hold for all $n \in \mathbb{N}$.

b) Recall that every base 10 represented number can be described as follows:

$$k = \sum_{i=0}^{n} d_i \cdot 10^i \tag{5}$$

Where d_i is the digit at the i'th position in the base-10 number (d_0 is the rightmost digit), and n denotes the number of digits in the number minus 1. Now apply the modulo of 9 to that equation:

$$k \equiv \sum_{i=0}^{n} d_i \cdot 10^i \equiv \sum_{i=0}^{n} d_i \cdot 1^i \equiv \sum_{i=0}^{n} d_i \equiv \alpha \pmod 9 \tag{6}$$

The substitution of 10^i with 1^i and 1^i with 1 occurs in accordance with Lemma 5.4 part 2. From Part 1 of Exercise 4.1, we showed that any multiple of 10 can be reduced to 1 in mod 9, as such, the 10 multiplier disappears from the sum, yielding the digit sum from the original base-10 representation.

2 Exercise 4.2

a) Recall, that the machine only accepts coins of type 2-krone and 5-krone. As such, the total weight must be describable by $59 \cdot x + 92 \cdot y = 7229$, where $x \in \mathbb{N} \wedge y \in \mathbb{N}$ as the value must be some sum of 2-krones and 5-krones. Now, take the mod 92 of the system: $59 \cdot x + 92 \cdot y \equiv 7229 \pmod{92}$. Using the hint from the exercise, it can be seen that the $92 \cdot y$ component should dissapear (as it has 92 as a factor) yielding the following relation:

$$59 \cdot x \equiv 7229 \pmod{92} \tag{7}$$

As can be seen, this is the same relation as the one presented in the exercise. Thus, since the congruence equation is derived from the fundamentals of what describe the situation in the question, the congruence relation must hold.

b) Recall, when taking the modulo of a number (for instance a mod z) the returned value should be the remainder of the integer division: $\frac{a}{z}$. When finding the remainder of 7229 when divided by 92, this yields 53. In fact, it can be shown that 7229 is a part of the 53rd residue class of 92, as: $7229 = 53 + 92 \cdot 78$. Hence, it must be the case that $59 \cdot x \equiv 53 \pmod{92}$ is equivalent to: $59 \cdot x \equiv 7229 \pmod{92}$.

c) To solve this equation, it can be seen that:

$$x \equiv 53 \cdot 59^{-1} \pmod{92} \tag{8}$$

Hence, the modular inverse of 59 must be found. It can be found by finding a solution to the following congruence relation:

$$59 \cdot a \equiv 1 \pmod{92} \tag{9}$$

A solution to this equation can be found using the extended gcd method, that is, compute the extended gcd for gcd(92, 59):

k	r_k	q_k	s_k	t_k
0	92	-	1	0
1	59	-	0	1
2	33	1	1	-1
3	26	1	-1	2
4	7	1	2	-3
5	5	3	-7	11
6	2	1	9	-14
7	1	2	-25	39
8	0	2	59	-92

From the above, the element t_{k-1} should yield the inverse modulo value for 59, which is in this case: $t_7 = 39$. Plugging this into the original equation regarding x:

$$x \equiv 53 \cdot 59^{-1} \equiv 53 \cdot 39 \equiv 43 \pmod{92} \tag{10}$$

Now, since this is modular arithmetic, this means there are infinitely many solutions for x in this case, the only restriction being, that they must come from the 43rd residue class of mod 92, that is, the following is the solution space for x:

$$x = 43 + 92 \cdot b \text{ where: } b \in \mathbb{Z} \tag{11}$$

Verifying this claim, the value 43 is plugged back into the original equation:

$$59 \cdot 43 = 2537 = 53 + 27 \cdot 92 \equiv 53 \pmod{92} \tag{12}$$

As can be seen it holds, hence it would appear that the above is correct.

d) Since the modulo is the remainder after the division, this means that the congruence equation from previously must hold to let x "remove" the remainder after taking as many y coins as possible. This allows for a trial and error approach to determine the possible solution space (since we know that there may be a positive amount of each coin):

$$7229 - 59 \cdot 43 = 4692 \tag{13}$$

$$7229 - 59 \cdot (43 + 92) = -736 \tag{14}$$

As can be seen, the only acceptable x value from the set is 43, as the next value in line results in a negative sum, which is not possible with positive coinage values. Hence, solving for y:

$$y = \frac{7229 - 59 \cdot 43}{92} = 51 \tag{15}$$

Thus the set (x, y) = (43, 51) is the only solution to the system.

3 Exercise 4.3

a) In order to find the set of solutions for x in the system of congruence relations we first have to simplify the second one dividing both sides by 118. Then we will get:

$$\begin{cases} x \equiv 250 \mod 439 \\ x \equiv 5 \mod 1121 \end{cases}$$

Before we can use the Chinese reminder theorem we have to check that $gcd(n_1, n_2) = 1$. This can be done using Euclid's algorithm:

k	r_k	q_k
0	1121	-
1	439	-
2	243	2
3	196	1
4	47	1
5	8	4
6	7	5
7	1	1
8	0	7

Table 1: Euclid's algorithm for the $gcd(n_1, n_2)$

It is clear that it is the case that $gcd(n_1, n_2) = 1$, thus we can use the Chinese remainder theorem.
To use the Chinese remainder theorem we need to evaluate the value for the multiplicative inverses $u_1 = n_1^{-1} \mod n_2$ and $u_2 = n_2^{-1} \mod n_1$, together with the values:

- $n_1 = 439$
- $n_2 = 1121$
- $b_1 = 250$
- $b_2 = 5$

To find the two missing values for the multiplicative inverses we can use theorem 5.6 from the textbook; it requires us to find a t that fulfills the relation $t \cdot a \equiv 1 \mod n$. This can be easily done computing the extended Euclid's algorithm for $gcd(n_1, n_2)$ and $gcd(n_2, n_1)$ in the following two tables:

k	r_k	q_k	s_k	t_k
0	1121	-	1	0
1	439	-	0	1
2	243	2	1	-2
3	196	1	1	3
4	47	1	2	-5
5	8	4	-9	23
6	7	5	47	-120
7	1	1	-56	143
8	0	7	-	-

Table 2: Euclid's algorithm for u_1

k	r_k	q_k	s_k	t_k
0	439	-	1	0
1	1121	-	0	1
2	439	0	1	0
3	243	2	-2	1
4	196	1	3	-1
5	47	1	-5	2
6	8	4	23	-9
7	7	5	-120	47
8	1	1	143	-56
9	0	7	-	-

Table 3: Euclid's algorithm for u_2

As we can see in table 2 the value of $u_1 = 143$. To find out the value of u_2 we need to get the value of t given (in red) by the algorithm in table 3 and make it positive adding a whole "period", thus it becomes $u_2 = -56 + 439 = 383$. We can now proceed to state the solutions which are the same as the congruence equation:

$$x \equiv u_1 n_1 b_2 + u_2 n_2 b_1 \mod n_1 n_2$$

$$x \equiv 143 \cdot 439 \cdot 5 + 383 \cdot 1121 \cdot 250 \mod 439 \cdot 1121$$

Which is equal to:

$$x \equiv 107649635 \mod 492119$$

The set of solutions for x can be written in the form: $107649635 + 492119\mathbb{Z}$

Which simplifies to:

$$367693 + 492119\mathbb{Z} \tag{16}$$