Session 20: Modular arithmetic

Discrete Mathematics

Escuela Técnica Superior de Ingeniería Informática (UPV)

1 Introduction

In this session we are going to introduce two operations, sum and product, in the set of congruence classes modulo m (for any natural number $m > 1$), $\mathbb{Z}_m$. These will give rise to arithmetic properties in $\mathbb{Z}_m$ that considerably differ from the the properties of usual arithmetic with natural (and real) numbers.

2 Sum and product in $\mathbb{Z}_m$

Consider a natural number $m > 1$ and its associated set of congruence classes modulo m:

$$\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

If $\overline{a}$ and $\overline{b}$ are two elements of $\mathbb{Z}_m$, then the **sum** and **product** of $\overline{a}$ and $\overline{b}$ is defined as follows:

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

For example, for $m = 8$, we have that $\overline{5} + \overline{7}$ is $\overline{12}$, which is equal to $\overline{4}$ (it is strongly convenient to take the "main representative" of each congruence class; in this case is 4, the remainder of the division $12 \div 8$). Therefore:

$$\overline{5} + \overline{7} = \overline{4}.$$

Another example (for $m = 5$): $\overline{-7} + \overline{14} = \overline{7}$, which is $\overline{2}$. Therefore, in $\mathbb{Z}_5$:

$$\overline{-7} + \overline{14} = \overline{2}.$$

The definition of the sum does not depend on the chosen representatives of the classes. In the above example, for the class $\overline{-7}$, one could take a different representative; say, for example, -2. But this does not affect to the sum: $\overline{-2} + \overline{14} = \overline{12} = \overline{2}$. We will omit the proof of this fact here.

For the product consider, for example, the classes $\overline{5}$ and $\overline{-2}$ in $\mathbb{Z}_8$. Then

$$\overline{5} \cdot (\overline{-2}) = \overline{-10} = \overline{6}.$$

As in the case of the sum, the product does not depend on the chosen representatives.

We can construct a table with double input with all the possible results of the sum in $\mathbb{Z}_m$ (and also for the product). This kind of tables are known as the **Cayley table** of the operation.

Example 1. These are the Cayley tables of the sum and the product in $\mathbb{Z}_4$. Every "black class" is equal to the sum (or product) of the "blue class" associated to its row and that associated to its column.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

3 Properties

The sum and the product in $\mathbb{Z}_m$ satisfy the following properties (The proofs are very easy and we omit them):

Properties of sum and product:

- The sum and the product in $\mathbb{Z}_m$ are commutative and associative.
- The product is distributive respect to the sum.
- $\overline{0}$ and $\overline{1}$ are identity elements with respect to sum and the product, respectively.
- Every element of $\mathbb{Z}_m$ has a symmetric element respect to the sum (also known as **opposite**). In particular, the opposite of $\overline{a}$ is $\overline{-a}$ because $\overline{a} + \overline{-a} = \overline{0}$.

Every element of $\mathbb{Z}_m$ has a symmetric element with respect to the sum. However, with respect to the product:

- The element 0 has not symmetric element with respect to the product.
- Not every non-zero element has symmetric element with respect to the product. For example, in the case of $\mathbb{Z}_4$, looking at the Cayley table you can see that there is not $x \in \mathbb{Z}_4$ such that $2 \cdot \overline{x} = \overline{1}$ and, then, $\overline{2}$ has not symmetric element.

If an element $\overline{a}$ of $\mathbb{Z}_m$ has symmetric with respect to the product then it is called **invertible** and its symmetric element (denoted by $\overline{a}^{-1}$) is called **inverse** of $\overline{a}$.

It can be proved that both identity elements are unique, the opposite of any element is unique and the inverse of an invertible element is also unique.

Example 2. In the case of $\mathbb{Z}_4$, looking at the Cayley tables we have that the invertible elements of $\mathbb{Z}_4$ are $\overline{1}$ and $\overline{3}$. Moreover:

$$\overline{1}^{-1} = \overline{1}, \quad \text{and} \quad \overline{3}^{-1} = \overline{3} \ \text{ because } \overline{3} \cdot \overline{3} = \overline{1}$$

The next result characterizes which are the invertible elements of $\mathbb{Z}_m$:

Theorem 1. Let $m > 1$ be a natural number. A class $\overline{a}$ in $\mathbb{Z}$ is **invertible** if and only if

$$GCD(a, m) = 1,$$

that is, if and only if a and m are relatively primes (that is, if $GCD(a, m) = 1$).

Proof. $\Rightarrow$ To prove the direct implication, assume that $\overline{a}$ is invertible. Then there exists $\overline{b} \in \mathbb{Z}_m$ such that $\overline{a} \cdot \overline{b} = \overline{1}$. This means that $ab \equiv 1 \ (mod\ m)$, that is, $ab - 1$ is a multiple of m. Then, there exists an integer number k such that $ab - 1 = km$, that is,

$$ab - km = 1.$$

Let us see that the unique positive common divisor of a and m is 1 (this will prove that $GCD(a, m) = 1$):

Let x be a positive common divisor of a and m. Then there exist integers s_1 and s_2 such that $a = s_1 x$ and $m = s_2 x$. Replacing a and m in the equality above we obtain:

$$s_1 bx - ks_2 x = 1,$$

that is,

$$(s_1 b - ks_2)x = 1.$$

Since $s_1 b - ks_2$ and x are both integers whose product is 1, then both must be equal to 1 or to -1. Since x is positive, both must be equal to 1; in particular, $x = 1$.

$\Leftarrow$ To prove the converse implication, assume that $GCD(a, m) = 1$. Then, considering a Bézout Identity of a and m, there exist integers x and y such that

$$ax + my = 1.$$

Then, the congruence class (modulo m) of the left-hand-side of this equality coincides with the congruence class of the right-hand-side:

$$\overline{ax + my} = \overline{1}.$$

But $\overline{ax+my} = \overline{ax} + \overline{my} = \overline{ax} = \overline{a} \cdot \overline{x}$, because my is a multiple of m and, then, its class is $\overline{0}$. Then we have

$$\overline{a} \cdot \overline{x} = \overline{1}.$$

This means that $\overline{x}$ is the inverse of $\overline{a}$, that is:

$$\overline{a}^{-1} = \overline{x}.$$

□

Notice that the proof of the converse implication of the above theorem gives a method to compute the inverse of an invertible element a of $\mathbb{Z}_m$:

Method to compute the inverse of $\overline{a}$ in $\mathbb{Z}_m$ (provided that $GCD(a,m) = 1$):

- Compute a Bézout Identity for a and m: $ax + my = 1$.
- Then $\overline{a}^{-1} = \overline{x}$, where x is the coefficient of a.

This is shown in the following example:

Example 3. We are going to prove that $\overline{11}$ is invertible in $\mathbb{Z}_{27}$ and we'll find its inverse.
Applying the Euclidean Algorithm to 11 and 27 we obtain, on the one hand, that $\gcd(27, 11) = 1$ (and, therefore, by the above theorem, $\overline{11}$ is invertible in $\mathbb{Z}_{27}$. On the other hand, we can obtain the following Bézout Identity:

$$5 \cdot 11 - 2 \cdot 27 = 1 \tag{1}$$

Then: $\overline{11}^{-1} = \overline{5}$ in $\mathbb{Z}_{27}$ because, from Equation (1):

$$\overline{5} \cdot \overline{11} + \overline{-2} \cdot \overline{27} = \overline{1}$$

and, since $\overline{27} = \overline{0}$:

$$\overline{5} \cdot \overline{11} = \overline{1}.$$

4 Solving linear congruence equations

In the previous section we have analyzed the problem of finding the inverse (if there exists) of an element $\overline{a}$ of $\mathbb{Z}_m$, that is, the problem of solving the following equation in $\mathbb{Z}_m$ (if there exists a solution):

$$\overline{a} \cdot \overline{x} = \overline{1}.$$

We will deal with the more general problem of solving any linear equation of first order in $\mathbb{Z}_m$, that is, any equation in $\mathbb{Z}_m$ of the form:

$$\overline{a} \cdot \overline{x} = \overline{b}, \tag{2}$$

where $\overline{a}, \overline{b} \in \mathbb{Z}_m \setminus \{\overline{0}\}$, and $\overline{x}$ is an unknown that represents a class of $\mathbb{Z}_m$.

The next proposition will show that these equations can also be written in the "equivalent" form:

$$a \cdot x \equiv b \pmod{m}.$$

Notice that this equation is defined in $\mathbb{Z}$, that is, to solve it, we need to find all the **integers** x such that ax is congruent to b modulo m (that is, $ax - b$ is multiple of m). However, equation (2) is defined in $\mathbb{Z}_m$, that is, to solve it, we need to find all the **classes** $\overline{x}$ in $\mathbb{Z}_m$ satisfying the equality.

Proposition 1. If the equation
$$a \cdot x \equiv b \pmod{m}$$
has solution, then its solutions are unions of solutions $\overline{x} \in \mathbb{Z}_m$ of the equation

$$\overline{a} \cdot \overline{x} = \overline{b}.$$

Proof. Let x_0 be a solution of the equation $a \cdot x \equiv b \pmod{m}$. This means that ax and b are in the same congruence class in $\mathbb{Z}_m$ and, therefore, $\overline{ax_0} = \overline{b}$. Then $\overline{a} \cdot \overline{x_0} = \overline{b}$, that is, the class $\overline{x_0} \in \mathbb{Z}_m$ is a solution of the equation $\overline{a} \cdot \overline{x} = \overline{b}$.

Now, we are going to prove that **every integer** in the class $\overline{x_0}$ is also a solution of the equation $\overline{a} \cdot \overline{x} = \overline{b}$:

Let $y \in \overline{x_0}$. Then $y \equiv x_0 \pmod{m}$ and, therefore, $y = x_0 + k \cdot m$ for some integer k. Replacing x by y in the equation $a \cdot x \equiv b \pmod{m}$ we have:

$$a(x_0 + km) \equiv b \pmod{m},$$

and this is true because $a(x_0 + km) - b = ax_0 - b + akm$ is a multiple of m (notice that $ax_0 - b$ is a multiple of m because x_0 is a solution of the equation $a \cdot x \equiv b \pmod{m}$).

Hence we have proved that, if x_0 is a solution of the equation $a \cdot x \equiv b \pmod{m}$ then every element in its class $\overline{x_0}$ is also a solution. Then the solution set of $a \cdot x \equiv b \pmod{m}$ is a union of solutions of (2).

□

The previous proposition means that, to solve the equation $a \cdot x \equiv b \pmod{m}$, one can solve the equation
$$\overline{a} \cdot \overline{x} = \overline{b}$$
in $\mathbb{Z}_m$ and take the union of its solutions. Then, essentially, both equations are "equivalent".

Example 4. Let us consider the equation

$$2x \equiv 6 \ (mod\ 8).$$

By the above proposition, this is equivalent to solve the equation

$$\overline{2} \cdot \overline{x} = \overline{6}$$

in $\mathbb{Z}_8$. Since 8 is a small number, we can compute directly the solutions of this last equation by checking it for every class in $\mathbb{Z}_8$:

$\overline{2} \cdot \overline{0} = \overline{6}$ is false.

$\overline{2} \cdot \overline{1} = \overline{6}$ is false.

$\overline{2} \cdot \overline{2} = \overline{6}$ is false.

$\overline{2} \cdot \overline{3} = \overline{6}$ is true.

$\overline{2} \cdot \overline{8} = \overline{6}$ is false.

$\overline{2} \cdot \overline{5} = \overline{6}$ is false.

$\overline{2} \cdot \overline{6} = \overline{6}$ is false.

$\overline{2} \cdot \overline{7} = \overline{6}$ is true.

Therefore the second equation has two solutions: $\overline{3}$ and $\overline{7}$. Using the proposition we conclude that the solutions of the initial equation are those integers in the union $\overline{3} \cup \overline{7}$. In other words, the solution set is

$$\{3 + 8k \mid k \in \mathbb{Z}\} \cup \{7 + 8k \mid k \in \mathbb{Z}\}.$$

In the previous example we have solved the equation $\overline{2} \cdot \overline{x} = \overline{6}$ in $\mathbb{Z}_8$ by checking it for every class of $\mathbb{Z}_8$. When the modulo and coefficients are big numbers, this " brute force" method is not efficient.

The following theorem (that we admit without proof) provides a practical method to solve any linear congruence equation of the form $\overline{a} \cdot \overline{x} = \overline{b}$ in $\mathbb{Z}_m$:

Proposition 2. Consider a linear congruence equation $\overline{a} \cdot \overline{x} = \overline{b}$ in $\mathbb{Z}_m$. Set

$$d = GCD(a, m).$$

Then:

(a) The equation has solution/s if and only if d divides b.

(b) If $d = 1$ then the equation has exactly one solution, which is $\overline{tb} \in \mathbb{Z}_m$, where t is a representative of the class $\overline{a}^{-1} \in \mathbb{Z}_m$.

(c) If the equation has solution/s and $d > 1$, it has exactly d solutions which are the following **classes of** $\mathbb{Z}_m$:

$$\overline{s},\ \overline{s + \frac{m}{d}},\ \overline{s + 2 \cdot \frac{m}{d}},\ \ldots,\ \overline{s + (d-1) \cdot \frac{m}{d}},$$

where s is the main representative of the (unique) solution $\overline{s} \in \mathbb{Z}_{\frac{m}{d}}$ of the equation

$$\overline{\frac{a}{d}} \cdot \overline{x} = \overline{\frac{b}{d}}, \text{ in } \mathbb{Z}_{\frac{m}{d}}$$

(that corresponds to Case (b) because $GCD(a/d, m/d) = 1$).

We will apply this theorem in the exercises.