1 Congruences in $\mathbb{Z}$ and Modular Arithmetic

Recall the notion of a function $f : S_1 \longrightarrow S_2$ between two sets S_1 and S_2: k is a rule which assigns to any element of S_1 a unique element of S_2. (Here, I am assuming that the domain of k is S_1.) k can be given by a formula as in calculus, or, for small sets, it can be represented by arrows pointing from elements of S_1 to elements of S_2.

In this section, we will be interested in a special type of functions called binary operations. Recall first that $S \times S$ denotes the Cartesian product of the set S with itself, that is, the set of all pairs (s_1, s_2) of elements with $s_1, s_2 \in S$.

Definition 1.1. *A binary operation on a set S is a function $f : S \times S \longrightarrow S$.*

Examples: 1) $S = \mathbb{Z}$, $f(a, b) = a + b$, so k is just the usual addition. $\mathbb{Z}$ could be replaced by $\mathbb{Q}$ or $\mathbb{R}$.

2) $S = \mathbb{Z}$, $f(a, b) = ab$, the usual product. Again, we could replace $\mathbb{Z}$ by $\mathbb{Q}$ or $\mathbb{R}$.

These two examples are very familiar to you and very natural. It is possible to create all sorts of strange examples of binary operation.

3) Suppose that $S = \{a, b, c, d\}$ is just a set with four elements. One way to specify what is $f(s_1, s_2)$ for each pair $(s_1, s_2) \in S \times S$ is to construct a table:

k	a	b	c	d
a	$f(a,a)$	$f(a,b)$	$f(a,c)$	$f(a,d)$
b	$f(b,a)$	$f(b,b)$	$f(b,c)$	$f(b,d)$
c	$f(c,a)$	$f(c,b)$	$f(c,c)$	$f(c,d)$
d	$f(d,a)$	$f(d,b)$	$f(d,c)$	$f(d,d)$

We can choose arbitrarily what each entry should be. For instance, we could define k using the following table:

k	a	b	c	d
a	d	c	a	b
b	c	a	d	a
c	a	d	c	c
d	a	d	d	b

Later, we will want the binary operation k to satisfy properties called associativity, distributivity and commutativity: it will then be necessary to be more careful in the way that k is defined.

Let $m \in \mathbb{N}, m \geqslant 2$. Let me introduce a new finite set, denoted $\mathbb{Z}_m$, which contains n elements denoted $[0], [1], [2], \ldots, [n-1]$.

There are two useful binary operations defined on $\mathbb{Z}_m$ and they are called addition and multiplication (or product). They are defined in the following way. Take $[a], [b] \in \mathbb{Z}_m$ and

set $f([a],[b]) = [r]$ where r is the remainder of $a+b$ upon division by m: $a+b = qm+r$ with $0 \leqslant r < m-1$. Instead of $f([a],[b])$, we will use the more suggestive notation $[a] \oplus [b]$, so $f([a],[b]) = [a] \oplus [b] = [r]$.

Similarly, the product $g : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$ of $[a]$ and $[b]$ is given by $g([a],[b]) = [\widetilde{r}]$ where $\widetilde{r}$ is the remainder of ab upon division by m: $ab = qm + \widetilde{r}$ with $0 \leqslant \widetilde{r} < m-1$. We will also use the more suggestive notation $[a] \odot [b]$ for multiplication, so $g([a],[b]) = [a] \odot [b] = [\widetilde{r}]$.

Examples: 1) $m = 18$, $[7] \oplus [16] = [5]$ because $7 + 16 = 23 = 18 \cdot 1 + 5$, so the remainder is 5.

2) $m = 67$, $[35] + [48] = [16]$ because $35 + 48 = 83 = 67 \cdot 1 + 16$.

3) $m = 12$ In this case, there is a concrete way to illustrate the addition procedure. Think of $[a]$ as representing the a^{th} hour on a circular clock. (So $[0]$ is either noon or midnight.) To find $[a] + [b]$, imagine that the time right now is a : 00 (am or pm, it doesn't matter). Then $[a] + [b]$ is the time it will be in b hours.

For instance, if $a = 5$ and $b = 9$, to find $[a] + [b]$, imagine it is now 5:00. What time will it be in 9 hours? It will be 2:00. Therefore, $[5] + [9] = [2]$. Similarly, to find $[5] + [11]$, let's pretend that it's 11:00. Five hours later, it will be 4:00, so $[5] + [11] = [4]$.

If it helps you to perform addition in $\mathbb{Z}_m$, you can imagine a clock with m different hours. Arithmetic in $\mathbb{Z}_m$ is sometimes called clock arithmetic.

4) $m = 5$. Since this is a small value of m, it is possible to give the full addition table for $\mathbb{Z}_5$.

$\oplus$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

5) $[2] \odot [4] = [3]$ in $\mathbb{Z}_5$ and $[6] \odot [9] = [4]$ in $\mathbb{Z}_{10}$.

6) The first few rows of the multiplication table of $\mathbb{Z}_7$ are:

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Equivalence relations

The elements $[0], [1], [2], \ldots$ of $\mathbb{Z}_m$ are actually sets of integers. More precisely, $[k]$ is the set of all integers with remainder k upon division by m, so $[k] = \{qm + k : q \in \mathbb{Z}\}$. For instance,

$$[0] = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\},$$
$$[1] = \{\ldots, -3m+1, -2m+1, -m+1, 1, m+1, 2m+1, 3m+1, \ldots\},$$
$$[2] = \{\ldots, -3m+2, -2m+2, -m+2, 2, m+2, 2m+2, 3m+2, \ldots\}, \text{ etc.}$$

Why do we consider these subsets of $\mathbb{Z}$? Why these and not some other subsets? What is special about them? To answer these questions, we need the notions of equivalence relation and of equivalence class.

I will now give you the precise definition of a relation and of an equivalence relation. This may appear very abstract to you, but fortunately there are some concrete examples that illustrate these concepts.

Definition 1.2. *Let X be a set. A relation on X is any subset R of $X \times X$.*

This may seem to be very strange, but here is the meaning of this. If $(x, y) \in R$ for two elements $x, y \in X$, we say that x and y are in relation and write $x \sim y$. If $(x, y) \notin R$, then x and y are not in relation and we write $x \not\sim y$.

Definition 1.3. *A relation on a set X is called an equivalence relation if it satisfies the following properties:*

1. *It is reflexive: $x \sim x$ for every $x \in X$;*
2. *It is symmetric: If $x \sim y$, then $y \sim x$;*
3. *It is transitive: If $x \sim y$ and $y \sim z$, then $x \sim z$.*

If $x \sim y$ under an equivalence relation, then we say that x is equivalent to y or that x and y are equivalent.

If this definition appears very abstruse, don't worry. Hopefully, it will become more understandable after looking at some examples.

Examples:

1) Let $X = \mathbb{R}$ and let $R = \{(x, x), (x, -x) \in \mathbb{R}^2 : x \in \mathbb{R}\}$. In other words, $x \sim y$ (x is equivalent to y) exactly when $|x| = |y|$.

2) Let $X = \mathbb{R}^2$. Instead of expressing R as a subset of $\mathbb{R}^2 \times \mathbb{R}^2 = \mathbb{R}^4$, it is simpler to say exactly when two points in the plane are equivalent: $(x, y) \sim (u, v)$ if and only if $x = u$. Let's check the three defining conditions of an equivalence relation.

1. $(x, y) \sim (x, y)$ since the first entries of both pairs are the same.
2. If $(x, y) \sim (u, v)$, then $x = u$, so $u = x$ and $(u, v) \sim (x, y)$.
3. If $(x, y) \sim (u, v)$ and $(u, v) \sim (w, z)$, then $x = u$ and $u = w$, so $x = w$ and $(x, y) \sim (w, z)$.

3) This is an example of a relation which is not an equivalence relation. Let X be a group of people. Declare x to be related to y if x and y are friends. This relation is not transitive since a friend of a friend is not always a friend.

4) Suppose that X is the set of students in the class. If x and y are two students, we declare x and y to be in relation if x was born the same month as y.
1) $x \sim x$ means that x was born the same month as himself or herself, which is a tautology.
2) If $x \sim y$, then x was born the same month as y, so y was also born the same month as x, hence $y \sim x$.
3) If $x \sim y$ and $y \sim z$, then x was born the same month as y and y was born the same month as z, hence x was born the same month as z, so $x \sim z$. This shows that if $x \sim y$ and $y \sim z$, then $x \sim z$.

5) Let $X = \mathbb{R}^2$. $(x, y) \sim (u, v)$ if and only if the distance between (x, y) and the origin $(0, 0)$ is the same as the distance between (u, v) and the origin. In other words, $(x, y) \sim (u, v)$ if and only if $(x^2+y^2)^{\frac{1}{2}} = (u^2+v^2)^{\frac{1}{2}}$. Let's check the three defining conditions of an equivalence relation.

1. $(x, y) \sim (x, y)$ since $(x^2 + y^2)^{\frac{1}{2}} = (x^2 + y^2)^{\frac{1}{2}}$.
2. If $(x, y) \sim (u, v)$, then $(x^2 + y^2)^{\frac{1}{2}} = (u^2 + v^2)^{\frac{1}{2}}$, so $(u^2 + v^2)^{\frac{1}{2}} = (x^2 + y^2)^{\frac{1}{2}}$ and $(u, v) \sim (x, y)$.
3. If $(x, y) \sim (u, v)$ and $(u, v) \sim (w, z)$, then $(x^2 + y^2)^{\frac{1}{2}} = (u^2 + v^2)^{\frac{1}{2}}$ and $(u^2 + v^2)^{\frac{1}{2}} = (w^2 + z^2)^{\frac{1}{2}}$, so $(x^2 + y^2)^{\frac{1}{2}} = (w^2 + z^2)^{\frac{1}{2}}$ and $(x, y) \sim (w, z)$.

6) This is the most important example for us. Let $X = \mathbb{Z}, m \in \mathbb{N}, m \neq 0$ and define $a \sim b$ if and only if $a - b$ is divisible by m. Since it is so important, let us take a minute to check that this defines an equivalence relation. We have to verify that the three defining conditions of an equivalence relation hold.
1) Reflexive: $a \sim a$ since $a - a = 0$ and 0 is divisible by m.
2) Symmetric: if $a \sim b$, then m divides $a - b$, so m divides also $b - a$, hence $b \sim a$.
3) Transitive: if $a \sim b$ and $b \sim c$, then m divides $a - b$ and $b - c$, so m divides $(a - b) + (b - c)$. Therefore m divides $a - c$, so $a \sim c$.

An equivalence relation on a set X is the same as a partition of X into disjoint subsets. Before I state this fact, we need one definition.

Definition 1.4. *Let $\sim$ be an equivalence relation on a set X. If $x \in X$, the equivalence class of x, denoted $[x]$, is the set of all elements in X that are equivalent to x. In mathematical symbols, $[x] = \{y \in X : y \sim x\}$.*

If $\sim$ is an equivalence relation on a set X, then we can find elements $x_i \in X$ for $i \in I$ in some indexing set, such that $X = \bigcup_{i \in I} [x_i]$ and $[x_i] \cap [x_j] = \phi$ if $i \neq j$. Here, I can be infinite, even uncountable.

Theorem 1.5. *The set X is a disjoint union of equivalence classes. In other words, equivalence classes form a partition of X.*

Let us return to the examples above (except example 3) to see what are the equivalence classes and what is the partition of X induced by the equivalence relation.

Examples: 1) $[0] = \{0\}$ and, if $x \neq 0$, then $[x] = \{x, -x\}$ since, if $|y| = |x|$, then $y = x$ or $y = -x$.

2) Fix $(x, y) \in \mathbb{R}^2$. The points equivalent to (x, y) are all those of the form $(x, v), v \in \mathbb{R}$, that is, $[(x, y)] = \{(x, v) \in \mathbb{R}^2 : v \in \mathbb{R}\}$. The equivalence class $[(x, y)]$ is thus the vertical line passing through (x, y). The plane $\mathbb{R}^2$ is the disjoint union of all these vertical lines.

4) If x is a student in the class, then $[x]$ is the set of all students born the same month as x. The set x of all students in the class can thus be divided into 12 disjoint subsets (the equivalence classes), one for each month of the year. The equivalence class labelled "January" consists of all the students born in January, etc. (In this case, some of these subsets may be empty if no students were born on a given month.)

5) If $(x^2 + y^2)^{\frac{1}{2}} = (u^2 + v^2)^{\frac{1}{2}}$, then (x, y) and (u, v) are on the same circle centered at the origin. The partition of X is thus as the disjoint union of the circles centered at the origin of radius r for any $r \geqslant 0$. (The circle of radius 0 reduces to the origin $(0, 0)$.)

6) Fix $a \in \mathbb{Z}$. If $b \sim a$, then $m \mid (b - a)$, so there exists $k \in \mathbb{Z}$ such that $b - a = mk$, that is $b = a + nk$. Therefore, $[a] = \{a + mk : k \in \mathbb{Z}\} = \{\ldots, a - 2m, a - m, a, a + m, a + 2m, \ldots\}$.

In this case, the partition of $\mathbb{Z}$ is finite: $\mathbb{Z} = \bigcup_{i=0}^{m-1} [i]$. (This will be proved later.)

For instance, if $m = 11$ and $a = 3$, then $[a] = \{\ldots, -30, -19, -8, 3, 14, 25, 36, \ldots\}$; if instead $a = 7$, then $[7] = \{\ldots, -26, -15, -4, 7, 18, 29, 40, \ldots\}$.

$[a]$ is thus a set called an equivalence class, or, in this case, the congruence class of a modulo n. The addition $\oplus$ and multiplication $\odot$ on $\mathbb{Z}_m$ are thus binary operations on subsets of $\mathbb{Z}$.

Why should we care about $\mathbb{Z}_m$? From the point of view of an algebraist, $\mathbb{Z}_m$ provides a very interesting example of a ring (the subject of the next section); in particular, if p is a prime number, $\mathbb{Z}_p$ is a finite field (more about fields later). A number theorist may

be interested in studying integral solutions of equations and it is natural to consider the reduction modulo a prime of the equation in question. Even applied mathematicians should be interested in $\mathbb{Z}_m$ because these rings play a role in coding theory. There is a course dedicated to this subject, MATH 422, and a good part of the course is about linear algebra over finite fields like $\mathbb{Z}_p$.

The following notation is standard: if $m \in \mathbb{Z}, m \neq 0$, we write $a \equiv b \pmod{m}$ if $m \mid (a-b)$. In other words, a is congruent to b modulo m if m divides $a - b$. When working with the congruence relation (which is the most important one in this course), it is much more common to write $\equiv$ instead of $\sim$.

Examples: $44 \equiv 11 \pmod{33}$, $126 \equiv 14 \pmod{16}$, since $126 - 14 = 112 = 7 \cdot 16$, so $16 \mid (126 - 4)$.

Since $\equiv$ is an equivalence relation, it has the following properties, which we have already checked.

Theorem 1.6. *Let $m \in \mathbb{N}, m \geqslant 1$. For all $a, b \in \mathbb{Z}$,*

1. *$a \equiv a \pmod{m}$;*
2. *if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$;*
3. *if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$;*

When I defined $\mathbb{Z}_m$, I said that it consisted of the m equivalence classes $[0], [1], \ldots, [m-1]$. Now, by the definition of equivalence class given above, we can talk about $[a]$ for any $a \in \mathbb{Z}$. The following theorem reconciles these two facts.

Theorem 1.7. *Let $m \in \mathbb{N}, m \geqslant 1$. For $a \in \mathbb{Z}$, let $[a]$ be the equivalence class of a with respect to the equivalence relation $\equiv$; in other words, $[a]$ is the congruence class of a:*

$$[a] = \{b \in \mathbb{Z} : b \equiv a \pmod{m}\} = \{b \in \mathbb{Z} : m \mid (b - a)\} = \{a + km : k \in \mathbb{Z}\}.$$

Then $[a] = [r]$ where r is the remainder when a is divided by m.

Proof. By the division algorithm, there exist $q, r \in \mathbb{Z}$ such that $a = qm + r$ with $0 \leqslant r < m$. We have to show that $[a] = [r]$: when proving the equality of two sets, one trick that often works is to show that the first set is contained in the second one, and the second set is also contained in the first one. In our case, this means that we should prove that $[a] \subset [r]$ and $[r] \subset [a]$, for this implies that $[a] = [r]$.

Let $b \in [a]$, so that $b \equiv a \pmod{m}$, hence $m \mid (b - a)$, say $b - a = km$ with $k \in \mathbb{Z}$. Then

$$b - r = b - (a - qm) = b - a + qm = km + qm = (k + q)m.$$

This means that $m \mid (b-r)$, so $b \equiv r \pmod{m}$ and $b \in [r]$. This argument shows that $[a] \subset [r]$.

The proof that $[r] \subset [a]$ is entirely similar, but let's do it in detail. Choose $c \in [r]$, so that $c \equiv r \pmod{m}$, that is, $m \mid (c-r)$. Write $c - r = lm$ for some $l \in \mathbb{Z}$. It follows that

$$c - a = c - (qm + r) = c - r - qm = lm - qm = (l - q)m,$$

hence $m \mid (c-a)$, so $c \equiv a \pmod{m}$ and $c \in [a]$. Since c was an arbitrary element of $[r]$, it must be the case that $[r] \subset [a]$.

In conclusion, since $[a] \subset [r]$ and $[r] \subset [a]$, we must have $[a] = [r]$. □

Examples: 1) $m = 12$, $a = 40$. Then $40 = 12 \cdot 3 + 4$, so $r = 4$ and $[40] = [4]$. We can verify this directly. $[40]$ is the equivalence class (or congruence class) of 40 modulo 12, so, by definition,

$$\begin{aligned} [40] &= \{b \in \mathbb{Z} : b \equiv 40 \pmod{12}\} = \{b \in \mathbb{Z} : 12 \mid (b - 40)\} \\ &= \{b \in \mathbb{Z} : b - 40 = 12k \text{ for some } k \in \mathbb{Z}\} \\ &= \{40 + 12k : k \in \mathbb{Z}\} = \{\ldots, -32, -20, -8, 4, 16, 28, 40, 52, 64, 76, \ldots\}. \end{aligned}$$

We can also say that $[40] = [4] = [16] = [28] = [-8] = [-20] = [-32]$, etc., because all these numbers leave a remainder of 4 when divided by 12.

2) $m = 7$. What are the integers $a \in \mathbb{Z}$ such that $[a] = [5]$? $[a] = [5]$ if and only if $7 \mid (a - 5)$, which is equivalent to $a - 5 = 7k$ for some $k \in \mathbb{Z}$. Therefore, a is of the form $a = 7k + 5$, that is, the remainder of a upon division by 7 is 5, so a belongs to the set $\{\ldots, -30, -23, -16, -9, -2, 5, 12, 19, 26, 33, \ldots\}$.

Theorem 1.8. *There are exactly m distinct congruence classes modulo m:* $[0], [1], \ldots, [m-1]$.

Proof. The previous theorem implies that any congruence class $[a]$ is equal to one among $[0], [1], \ldots, [m-1]$. We only have to see that these classes are all distinct. (We already know that equivalence classes which are distinct are also disjoint.) Suppose that $0 \leqslant r_1, r_2 < m$ and that $[r_1] = [r_2]$; we have to see that $r_1 = r_2$.

$[r_1] = [r_2]$ implies that $m \mid (r_1 - r_2)$, so $r_1 = r_2 + km$ for some $k \in \mathbb{Z}$. Since $0 \leqslant r_1, r_2 < m$, the only possibility is $k = 0$, so $r_1 = r_2$. □

The set $\mathbb{Z}_m$ is thus the set of all equivalence classes under the equivalence relation $\equiv \pmod{m}$.

Theorem 1.9. $[a] = [b]$ *in* $\mathbb{Z}_m$ *if and only if* $a \equiv b \pmod{m}$.

Theorem 1.10. *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then*

1. $a + c \equiv b + d \pmod{m}$;

2. $ac \equiv bd \pmod{m}$.

Here are some examples which show how to apply this theorem.

1) If $a \equiv 2 \pmod{11}$ and $b \equiv 5 \pmod{11}$, what is $17a^2 + 9b^2$ congruent to modulo 11?

$$17a^2 + 9b^2 \equiv 6a^2 + 9c^2 \equiv 6 \cdot 2^2 + 9 \cdot 5^2 \equiv 24 + 9 \cdot 3 \equiv 2 + 27 \equiv 29 \equiv 7 \pmod{11}.$$

2) What is the remainder of $27 \cdot 12 \cdot 5 \cdot 41$ when divided by 16?

$$27 \cdot 12 \cdot 5 \cdot 41 \equiv 11 \cdot 12 \cdot 5 \cdot 9 \equiv (-5) \cdot (-4) \cdot 5 \cdot 9 \equiv 20 \cdot 45 \equiv 4 \cdot (-3) \equiv -12 \equiv 4 \pmod{16}.$$

Therefore, the remainder of $27 \cdot 12 \cdot 5 \cdot 41$ when divided by 16 is 4.

3) If $a \equiv 7 \pmod{9}$ and $b \equiv 4 \pmod{9}$, what is the remainder of $12a^3b - 8ab^2$ when divided by 9?

$$\begin{aligned} 12a^3b - 8ab^2 &\equiv 3 \cdot 7^3 \cdot 4 - 8 \cdot 7 \cdot 4^2 \equiv 3 \cdot (-2)^3 \cdot 4 - (-1) \cdot (-2) \cdot 16 \\ &\equiv 3 \cdot (-8) \cdot 4 - 2 \cdot 7 \equiv 12 - 14 \equiv -2 \equiv 7 \pmod{9}. \end{aligned}$$

The previous theorem can be rephrased in the more abstract context of congruence classes in $\mathbb{Z}_m$. Indeed, $a \equiv b \pmod{m}$ is the same as $[a] = [b]$ by Theorem 1.9, and $c \equiv d \pmod{m}$ is the same as $[c] = [d]$. Therefore, the theorem says that $[a + c] = [b + d]$ and $[ac] = [bd]$ if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

The addition and the multiplication operations on $\mathbb{Z}_m$ have been defined before. The rules I gave you allowed you to compute $[a] \oplus [c]$ when $0 \leqslant a, c \leqslant m - 1$. However, we have just seen that $[a] = [a + km]$ for any $k \in \mathbb{Z}$. A natural question is now: given arbitrary $a, c \in \mathbb{Z}$, what is the sum $[a] \oplus [c]$? The answer is given by the same formula as before: divide $a + c$ by m and find the remainder r, so $a + c = qm + r$ with $0 \leqslant r \leqslant m - 1$, and set $[a] \oplus [c] = [r]$. The product $[a] \odot [c]$ is obtained similarly: dividing ac by m with remainder $\widetilde{r}$ means that $a \odot c = qm + \widetilde{r}$ with $0 \leqslant \widetilde{r} \leqslant m - 1$, and we set $[a] \odot [c] = [\widetilde{r}]$.

There is a more subtle question that we haven't considered yet: we know that it's possible to have $[a] = [b]$ for different $a, b \in \mathbb{Z}$. If we also have $[c] = [d]$ for possibly different $c, d \in \mathbb{Z}$, is it still true that $[a] \oplus [c] = [b] \oplus [d]$ and $[a] \odot [c] = [b] \odot [d]$? The answer is yes.

Examples: 1) $m = 20, a = 17, c = 54$. Then $[17] \oplus [54] = [17 + 54] = [71] = [11]$ since $71 = 20 \cdot 3 + 11$; this could also be computed in the following way using theorem 1.9: $[17] \oplus [54] = [17] \oplus [14] = [-3] \oplus [14] = [-3 + 14] = [11]$.

$[17] \odot [54] = [918] = [18]$ since $918 = 20 \cdot 45 + 18$, but it is simpler to compute it in the following way: $[17] \odot [54] = [-3] \odot [-6] = [(-3)(-6)] = [18]$.

2) $m = 13, a = 34, c = 21$. Then $[34] \oplus [21] = [55] = [3]$, which could also be computed as: $[34] \oplus [21] = [8] \oplus [8] = [16] = [3]$.

$[34] \odot [21] = [714] = [12]$ since $714 = 54 \cdot 13 + 12$, but it is simpler to compute it in the following way: $[34] \odot [21] = [8] \odot [8] = [-5] \odot [-5] = [(-5)(-5)] = [25] = [12]$.

Here is the reason why $[a] \oplus [c] = [b] \oplus [d]$ and $[a] \odot [c] = [b] \odot [d]$ if $[a] = [b]$ and $[c] = [d]$ for possibly different $a, b, c, d \in \mathbb{Z}$. Since $[a] = [b]$, there exists a $k \in \mathbb{Z}$ such that $a - b = km$; since $[c] = [d]$, there exists an $l \in \mathbb{Z}$ such that $c - d = lm$. Therefore, if $a + c = qm + r$, then

$$b + d = a - km + c - lm = a + c - (k + l)m = qm - (k + l)m + r = (q - k - l)m + r.$$

This implies that $[b] \oplus [d] = [r] = [a] \oplus [c]$.

The same argument works for the product: if $ac = qm + \widetilde{r}$, then

$$\begin{aligned} bd &= (a - km)(c - lm) = ac - alm - ckm + klm^2 = qm + \widetilde{r} + (klm - al - ck)m \\ &= (q + klm - al - ck)m + \widetilde{r}, \end{aligned}$$

so the remainder upon dividing bd by m is also $\widetilde{r}$, hence $[b] \odot [d] = [\widetilde{r}] = [a] \odot [c]$.

Finally, observe that, if r is the remainder of $a + c$ upon division by m, then $[r] = [a + c]$. Therefore, we can simply write $[a] \oplus [c] = [a + c]$. Similarly, if r is the remainder of ac upon division by m, then $[r] = [ac]$, so we can just write $[a] \odot [c] = [ac]$. When doing computations, sometimes it's easier to just use $[a] \oplus [c] = [a + c]$, sometimes it's preferable to write $[a] \oplus [c] = [r]$ with r the remainder of $a + c$ after division by m.

Let us continue to analyze the addition and the multiplication on $\mathbb{Z}_m$. The binary operations $\oplus$ and $\odot$ have a lot of properties in common with the addition and multiplication in $\mathbb{Z}$. These properties will reappear again in the more general setting of chapter 3 when we will study rings.

Addition in $\mathbb{Z}$ is a binary operation, that is, given two integers a and b, $a + b$ is the sum of these two numbers. If $c \in \mathbb{Z}$, what is then the meaning of $a + b + c$? There are two interpretations, both of which give the same answer: $a + b + c = (a + b) + c$ and also $a + b + c = a + (b + c)$: recall that parentheses tell you what is the order of priority for binary operations, so $(a + b) + c$ means that you should first compute $a + b$ and add the result to c. Similarly, $a + (b + c)$ means compute $b + c$ and add the result with a. The fact that $(a + b) + c = a + (b + c)$ is called the associativity property of addition: you have used it all the time, although you probably did not know that it had a name. The same can be said about associativity of multiplication in $\mathbb{Z}, \mathbb{Q}$ or $\mathbb{R}$. This property of addition is trivial in the case of $\mathbb{Z}$ and it will hold also in the other rings that we will encounter in this course; however, there exist rings in which associativity does not hold, for instance, the ring of octonions and Lie algebras.

Theorem 1.11. *For any $[a], [b], [c] \in \mathbb{Z}_m$, the following equalities hold:*

1. *Associativity of $\oplus$:* $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$;

2. *Commutativity of* $\oplus$: $[a] \oplus [b] = [b] \oplus [a]$;
3. *Existence of an identity element for* $\oplus$: $[a] \oplus [0] = [a] = [0] \oplus [a]$;
4. *Associativity of* $\odot$: $[a] \odot ([b] \odot [c]) = ([a] \odot [b]) \odot [c]$;
5. *Commutativity of* $\odot$: $[a] \odot [b] = [b] \odot [a]$;
6. *Existence of an identity element for* $\odot$: $[a] \odot [1] = [a] = [1] \odot [a]$;
7. *Distributivity of* $\odot$ *over* $\oplus$: $[a] \odot ([b] \oplus [c]) = ([a] \odot [b]) \oplus ([a] \odot [c])$ *and* $([a] \oplus [b]) \odot [c] = ([a] \odot [c]) \oplus ([b] \odot [c])$;

Remark: multiplication is not always commutative. For instance, matrix multiplication is not commutative: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, but if we change the order of multiplication, we get $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

Proof. I will give the proof of a couple of these properties; you will have to prove two more in the homework. Associativity is the most fundamental one, but let us start with commutativity since it's easier.

$$\begin{aligned} [a] \oplus [b] &= [a + b] \text{ by definition of } \oplus \\ &= [b + a] \text{ by commutativity of } + \text{ in } \mathbb{Z} \\ &= [b] \oplus [a] \text{ by definition of } \oplus \end{aligned}$$

The associativity in $\mathbb{Z}_m$ also follows from the associativity in $\mathbb{Z}$:

$$\begin{aligned} [a] \oplus ([b] \oplus [c]) &= [a] \oplus [b + c] \text{ by definition of } \oplus \\ &= [a + (b + c)] \text{ by definition of } \oplus \\ &= [(a + b) + c] \text{ by associativity of } + \text{ in } \mathbb{Z} \\ &= [a + b] \oplus [c] \text{ by definition of } \oplus \\ &= ([a] \oplus [b]) \oplus [c] \text{ by definition of } \oplus. \end{aligned}$$

The proof of the commutativity and the associativity of $\odot$ is entirely similar. □

When p is a prime number, $\mathbb{Z}_p$ is what we will call later a field. What differentiates it from $\mathbb{Z}_m$ when m is composite is the content of the following theorem.

Theorem 1.12. *Let* $p \in \mathbb{N}$ *be a prime number. If* $a \in \mathbb{Z}$ *and* $a \not\equiv 0 \pmod{p}$*, then there exists* $s \in \mathbb{Z}$ *such that* $sa \equiv 1 \pmod{p}$*. This is the same as saying that there exists* $s \in \mathbb{Z}$ *such that* $[s] \odot [a] = [1]$ *in* $\mathbb{Z}_p$*.*

Proof. Since $a \not\equiv 0 \pmod{p}$, a is not divisible by p, therefore, $(a, p) = 1$. What can you say about a, p and (a, p)? What is a relation between them? By Theorem 1.6 in these lecture notes, there exist $s, t \in \mathbb{Z}$ such that $sa + tp = 1$. Therefore, $sa \equiv 1 \pmod{p}$. □

This theorem will be very useful for solving congruence equations. Note that s is not unique: actually, s could be replaced by any $\widetilde{s} \in \mathbb{Z}$ such that $s \equiv \widetilde{s} \pmod{p}$.

Example: If $p = 7$ and $a = 5$, then $s = 3$ since $3 \cdot 5 \equiv 1 \pmod{7}$. If $a = 32$, then $s = 2$: one way to see this is to notice that $32 \equiv 4 \pmod{7}$, hence $2 \cdot 32 \equiv 2 \cdot 4 \equiv 1 \pmod{7}$.

Recall that one goal is to learn how to solve basic (systems of) congruence equations and equations in $\mathbb{Z}_m$.

Let us start with a very basic example: find all the solutions of $x \equiv 4 \pmod{14}$. The set of solutions consists of all the numbers with remainder 4 when divided by 14. Therefore, the set of all solutions is $\{\ldots, -24, -10, 4, 18, 32, \ldots, \}$. The answer is the same to the question of finding all the solutions of $x \equiv -24 \pmod{14}$ or $x \equiv 18 \pmod{14}$.

A linear congruence equation is an equation of the form $ax \equiv b \pmod{m}$. Such an equation does not always have a solution. For instance, consider the equation $2x \equiv 5 \pmod{6}$. Can this equation have a solution with $x \in \mathbb{Z}$? Suppose that x is a solution; then $6 \mid (2x-5)$, so there exists $k \in \mathbb{Z}$ such that $2x - 5 = 6k$. This implies that $5 = 2x - 6k = 2(x - 3k)$: this is a contradiction because 5 is odd. Therefore, no solution exists with $x \in \mathbb{Z}$.

One case which is easier is when m is equal to a positive prime number p. The equation $ax \equiv b \pmod{p}$ always has a solution except when a is a multiple of p but not b. Indeed, suppose that $a \not\equiv 0 \pmod{p}$. By the previous theorem, there exists $s \in \mathbb{Z}$ such that $sa \equiv 1 \pmod{p}$. Therefore,

$$ax \equiv b \pmod{p} \iff sax \equiv sb \pmod{p} \iff x \equiv sb \pmod{p}.$$

Therefore, the set of solutions of $ax \equiv b \pmod{p}$ consists of all the integers $x \in \mathbb{Z}$ such that $x \equiv sb \pmod{p}$, so the set of solutions is $\{\ldots, sb - 2p, sb - p, sb, sb + p, sb + 2p, \ldots\}$.

Example: Solve $5x \equiv 11 \pmod{7}$.

We have to find s such that $5s \equiv 1 \pmod{7}$. When the values are small, it should not be difficult to find such a s by simple trial and error. What multiples of 5 is congruent to 1 modulo 7? The smallest one is 15 and $15 = 5 \cdot 3$, so we can take $s = 3$. Therefore,

$$5x \equiv 11 \pmod{7} \iff 3 \cdot 5x \equiv 3 \cdot 11 \pmod{7} \iff x \equiv 5 \pmod{7}.$$

The set of solutions of $5x \equiv 11 \pmod{7}$ is $\{\ldots, -9, -2, 5, 12, 19, \ldots\} = \{5 + 7k \in \mathbb{Z} : k \in \mathbb{Z}\}$.

We can also interpret this in $\mathbb{Z}_p$. In this context, the paragraph preceding the previous example can be summarized in the following theorem.

Theorem 1.13. *Let p be a (positive) prime number. For any $[a] \neq [0]$ and any $[b] \in \mathbb{Z}_p$, the equation $[a] \odot x = [b]$ has a unique solution in $\mathbb{Z}_p$.*

Here, x is a variable which can take values in $\mathbb{Z}_p$, so $x = [y]$ for some $y \in \mathbb{Z}$. (It is enough to consider $0 \leqslant y \leqslant p-1$.) The equation $[a] \odot x = [b]$ is thus equivalent to $[a] \odot [y] = [b]$, which is the same as $[ay] = [b]$, which is true if and only if $ay \equiv b \pmod{p}$ by Theorem 1.9. Therefore, we see that the unique solution of $[a] \odot x = [b]$ is given by $x = [sb]$ where $s \in \mathbb{Z}$ is such that $sa \equiv 1 \pmod{p}$.

Example: Solve $[7] \odot x = [12]$ in $\mathbb{Z}_{17}$.

We have to find $[s]$ such that $[s] \odot [7] = [1]$.

$$[s] \odot [7] = [1] \iff [7s] = [1] \iff 7s \equiv 1 \pmod{17}.$$

We need one solution of the previous congruence equation: trying small multiples of 7, we find that $s = 5$ is a solution since $7 \cdot 5 = 35 = 2 \cdot 17 + 1$. Therefore, the solution of $[7] \odot x = [12]$ in $\mathbb{Z}_{17}$ is $x = [5 \cdot 12] = [60] = [9]$ since $60 = 17 \cdot 3 + 9$.

The previous theorem can be generalized to any $m \in \mathbb{N}, m \geqslant 1$ under an extra condition. Suppose that $(a, m) = 1$ and we want to solve $ax \equiv b \pmod{m}$. Since $(a, m) = 1$, there exist $s, t \in \mathbb{Z}$ such that $sa + tm = 1$. Therefore, $sa \equiv 1 \pmod{m}$, hence

$$ax \equiv b \pmod{m} \iff sax \equiv sb \pmod{m} \iff x \equiv sb \pmod{m}.$$

This means that the set of solutions of $ax \equiv b \pmod{m}$ is $\{\ldots, sb - 2m, sb - m, sb, sb + m, sb + 2m, \ldots\}$, which equals $\{sb + km : k \in \mathbb{Z}\}$.

Example: $m = 14, a = 9, b = 7$, so we have to solve $9x \equiv 7 \pmod{14}$. $(9, 14) = 1$, so now we need to find s, t such that $9s + 14t = 1$. In general, this can be done using the Euclidean algorithm, but in this specific case, since 9 and 14 are rather small numbers, it is possible to find directly the values $s = -3$ and $t = 2$. Therefore, $-3 \cdot 9 \equiv 1 \pmod{14}$, so

$$9x \equiv 7 \pmod{14} \Leftrightarrow -3 \cdot 9x \equiv -3 \cdot 7 \pmod{14} \Leftrightarrow x \equiv -21 \pmod{14} \Leftrightarrow x \equiv 7 \pmod{14}.$$

Therefore, the set of all solutions of the congruence equation $9x \equiv 7 \pmod{14}$ is the set $\{\ldots, -21, -7, 7, 21, 35, \ldots\}$, which equals $\{7 + 14k \in \mathbb{Z} : k \in \mathbb{Z}\}$.

We can rephrase all this in terms of $\mathbb{Z}_m$.

Theorem 1.14. *Suppose that $m \in \mathbb{N}, m > 1, a \in \mathbb{Z}$ and $(a, m) = 1$. Then the equation $[a] \odot x = [b]$ has a unique solution in $\mathbb{Z}_m$.*

Example: Solve $[9] \odot x = [6]$ in $\mathbb{Z}_{16}$.

We have to find $s, t \in \mathbb{Z}$ such that $9s + 16t = 1$. $s = 9, t = -5$ is a good choice since $9 \cdot 9 - 16 \cdot 5 = 81 - 80 = 1$. Therefore,

$$[9] \odot x = [6] \Leftrightarrow [9] \odot [9] \odot x = [9] \odot [6] \Leftrightarrow x = [54] \Leftrightarrow x = [6].$$

In general, we can use the following theorem to solve linear congruence equations.

Theorem 1.15. *Let $a, b, m \in \mathbb{Z}, m > 1$ and set $d = (a, m)$. Then*

1. *The equation $[a] \odot x = [b]$ has solutions in $\mathbb{Z}_m$ if and only if $d \mid b$.*
2. *If $d \mid b$, then the equation $[a] \odot x = [b]$ has d distinct solutions in $\mathbb{Z}_m$.*

Examples: 1) Find all the solutions in $\mathbb{Z}_{65}$ of $[25] \odot x = [10]$.

Here, $m = 65, a = 25, b = 10$ and $d = (65, 25) = 5$. Since $5 \mid 10$, this equation has five distinct solutions in $\mathbb{Z}_{65}$. How can we find them? The language of congruences is useful here. Suppose that $x = [y]$.

$$\begin{aligned} [25] \odot x = [10] &\iff 25y \equiv 10 \pmod{65} \iff 65 \mid (25y - 10) \\ &\iff \text{there exists } k \in \mathbb{Z} \text{ such that } 25y - 10 = 65k \\ &\iff 5y - 2 = 13k \iff 5y \equiv 2 \pmod{13}. \end{aligned}$$

Since $8 \cdot 5 \equiv 40 \equiv 1 \pmod{13}$,

$$5y \equiv 2 \pmod{13} \iff 40y \equiv 8 \cdot 2 \pmod{13} \iff y \equiv 3 \pmod{13}.$$

Therefore, the set of all solutions of the congruence equation $5y \equiv 2 \pmod{13}$ is the set $\{\ldots, -23, -10, 3, 16, 29, \ldots\}$.

It follows that the solutions of the initial equation $[25] \odot x = [10]$ with $x \in \mathbb{Z}_{65}$ are thus given by $x = [3], [16], [29], [42], [55]$ (give y the values in the previous set which are $\geqslant 0$ and < 65). There are indeed five solutions.

In general, it can be proved that if $d \mid b$, where $d = (a, b)$, then the equation $[a] \odot x = [b]$ in $\mathbb{Z}_m$ has solutions given by $x = [y + k\frac{m}{d}]$ for $k = 0, 1, \ldots, d - 1$ where y is a solution of $\frac{a}{d}y \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

2) Find all the solutions of the congruence equation: $36x \equiv 27 \pmod{45}$.

$$\begin{aligned} 36x \equiv 27 \pmod{45} &\iff 45 \mid (36x - 27) \\ &\iff 36x - 27 = 45k \text{ for some } k \in \mathbb{Z} \\ &\iff 4x - 3 = 5k \Leftrightarrow 4x \equiv 3 \pmod{5} \\ &\iff -x \equiv 3 \pmod{5} \\ &\iff x \equiv -3 \equiv 2 \pmod{5}. \end{aligned}$$

Therefore, the set of solutions is $\{\ldots, -13, -8, -3, 2, 7, 12, \ldots\}$.

As you've seen in linear algebra, it may be necessary to consider not only just one equation, but many equations at once. This is what is meant by a system of equations (of congruence equations in this course). The main theorem that we will need is called the Chinese Remainder Theorem because it was known centuries ago to Chinese mathematicians.

Theorem 1.16 (Chinese Remainder Theorem)**.** *Suppose that* $m, m' \in \mathbb{N}, m, m' > 1$ *and* $\gcd(m, m') = 1$*. For any integers* $b, b' \in \mathbb{Z}$*, the system of congruence equations*

$$\begin{aligned} x &\equiv b \pmod{m} \\ x &\equiv b' \pmod{m'} \end{aligned}$$

has a solution. Let x_0 *be a solution. Then,* x *is another solution of the system if and only if* $x \equiv x_0 \pmod{mm'}$*.*

The general procedure to find one solution of a system of two equations is to use the first equation to express x in terms of b and m and then substitute into the second one. Solving this second equation then leads to a solution x_0 for the system and the Chinese Remainder Theorem tells us what are all the others. A couple of examples will help make this clearer.

Examples: 1) Find all the solutions of

$$\begin{aligned} x &\equiv 3 \pmod{11} \\ x &\equiv 4 \pmod{17} \end{aligned}$$

Note that 11 and 17 are relatively prime since they are actually distinct prime numbers. If $x \equiv 3 \pmod{11}$, then $x = 3 + 11y$ for some $y \in \mathbb{Z}$. Let's substitute this into the second equation to obtain

$$3 + 11y \equiv 4 \pmod{17}.$$

This is equivalent to $11y \equiv 1 \pmod{17}$. Finding y is like finding s in the problems above. Let's find s and t such that $11s + 17t = 1$. Trying some small values lead to the solution $s = -3$ and $t = 2$, so we can take $y = -3$.

Therefore $x = 3 + 11 \cdot (-3) = -30$, so this is a solution of both equations. (This is the x_0 in the Chinese Remainder Theorem.) Any other solution of the system is a solution of $x \equiv -30 \pmod{187}$ according to the Chinese Remainder Theorem since $11 \cdot 17 = 187$. In conclusion, the set of all solutions of the system of equations is $\{-30 + 187k : k \in \mathbb{Z}\}$.

2) Solve the following system:

$$\begin{aligned} 7x &\equiv 5 \pmod{9} \\ x &\equiv -3 \pmod{16} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

Using that $4 \cdot 7 \equiv 1 \pmod{9}$ and $4 \cdot 5 \equiv 20 \equiv 2 \pmod{9}$, we see that this system is equivalent to the following one:

$$\begin{aligned} x &\equiv 2 \pmod{9} \\ x &\equiv -3 \pmod{16} \\ x &\equiv 3 \pmod{5}. \end{aligned}$$

Note that $(9, 16) = 1$, so we can apply the Chinese Remainder theorem. If $x \equiv 2 \pmod 9$, then $x = 2 + 9y$ for some $y \in \mathbb{Z}$, so we substitute this into the second equation to obtain

$$2 + 9y \equiv -3 \pmod{16},$$

which simplifies to $9y \equiv -5 \pmod{16}$. We need to find s and t such that $9s + 16t = 1$. One possibility is $s = -7$ and $t = 4$ since $9 \cdot (-7) + 16 \cdot 4 = -63 + 64 = 1$. Therefore,

$$9y \equiv -5 \pmod{16} \Leftrightarrow (-7) \cdot 9y \equiv (-7) \cdot (-5) \pmod{16} \Leftrightarrow y \equiv 35 \pmod{16} \Leftrightarrow y \equiv 3 \pmod{16}.$$

One choice for y is thus $y = 3$, so a solution of the first two equation is given by $x = 2 + 9 \cdot 3 = 29$. By the Chinese Remainder Theorem, any other solution x of the first two equations satisfies $x \equiv 29 \pmod{144}$ because $9 \cdot 16 = 144$.

The initial system of three congruence equations is thus equivalent to the following system of two congruence equations:

$$\begin{aligned} x &\equiv 29 \pmod{144} \\ x &\equiv 3 \pmod 5. \end{aligned}$$

We can proceed in the same way as before. From $x \equiv 29 \pmod{144}$, we can write $x = 29 + 144l$ for some integer $l \in \mathbb{Z}$, and we substitute this into $x \equiv 3 \pmod 5$ to obtain

$$29 + 144l \equiv 3 \pmod 5.$$

This congruence equation is equivalent to $144l \equiv -26 \pmod 5$. Observe that $144 \equiv -1 \pmod 5$ and $-26 \ -1 (\mathrm{mod}\, 5)$, so the congruence equation $144l \equiv -26 \pmod 5$ is equivalent to $-l \equiv -1 \pmod 5$. One solution is $l = 1$, so we obtain that $x = 29 + 144 = 173$ is one solution of the system

$$\begin{aligned} x &\equiv 29 \pmod{144} \\ x &\equiv 3 \pmod 5. \end{aligned}$$

By the Chinese Remainder Theorem, any other solution x of this system satisfies $x \equiv 173 \pmod{720}$ because $720 = 144 \cdot 5$.

In conclusion, the set of solutions of the initial system of three equations is $\{173 + 720k : k \in \mathbb{Z}\}$.