Congruences on the integers

Definition. Let n be a positive integer. Integers a and b are said to be *congruent modulo* n if $a - b$ is a multiple of n. We use the notation $a \equiv b \pmod{n}$ to indicate that a and b are congruent modulo n.

For example, $13 \equiv 20 \pmod{7}$, and $22 \equiv 92 \equiv -8 \pmod{10}$.

It is straightforward to show that congruence modulo n is an equivalence relation. Firstly, if a is any integer then $a - a = 0$, which is a multiple of n (since $0 = 0 \times n$). So $a \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$; that is, congruence modulo n is reflexive. Secondly, if $a, b \in \mathbb{Z}$ are such that $a \equiv b \pmod{n}$ then there exists an integer k such $a - b = kn$, and this implies that $b - a = (-k)n$, which is also a multiple of n. Thus $b \equiv a \pmod{n}$ whenever $a \equiv b \pmod{n}$: the relation is symmetric. Finally, suppose that a, b, $c \in \mathbb{Z}$ are such that $a \equiv b$ and $b \equiv c \pmod{n}$. Then $a - b = kn$ and $b - c = ln$ for some integers k and l. Adding these equations gives

$$a - c = (a - b) + (b - c) = kn + ln = (k + l)n,$$

a multiple of n; so $a \equiv c \pmod{n}$. We have shown that $a \equiv c$ whenever $a \equiv b$ and $b \equiv c$; that is, the relation is also transitive. Since it is reflexive, symmetric and transitive, by definition it is an equivalence relation.

The equivalence classes for the congruence modulo n relation are called *congruence classes (modulo n)*. If $n = 4$ then there are four congruence classes:

$$\begin{aligned}
\mathscr{C}_0 &= \{\ldots, -8, -4, 0, 4, 8, 12, \ldots\},\\
\mathscr{C}_1 &= \{\ldots, -7, -3, 1, 5, 9, 13, \ldots\},\\
\mathscr{C}_2 &= \{\ldots, -6, -2, 2, 6, 10, 14, \ldots\},\\
\mathscr{C}_3 &= \{\ldots, -5, -1, 3, 7, 11, 15, \ldots\}.
\end{aligned}$$

Here $\mathscr{C}_0$ consists of all integers that are multiples of 4, $\mathscr{C}_1$ consists of all integers that one more than multiples of 4, $\mathscr{C}_2$ consists of all integers that two more than multiples of 4, and $\mathscr{C}_3$ consists of all integers that three more than multiples of 4. Observe that if you add any integer in the class $\mathscr{C}_2$ to any integer in the class $\mathscr{C}_3$ then the answer is always in the class $\mathscr{C}_1$. Similarly, adding something in $\mathscr{C}_3$ to something in $\mathscr{C}_1$ always gives something in $\mathscr{C}_0$, and a similar result holds for the sum of an element of $\mathscr{C}_i$ and an element of $\mathscr{C}_j$ for any choice of i and j. It is thus natural to define "addition" of these congruence classes by the rule that

$$\mathscr{C}_i + \mathscr{C}_j = \mathscr{C}_k$$

if and only if

$$a + b \in \mathscr{C}_k \text{ for all } a \in \mathscr{C}_i \text{ and } b \in \mathscr{C}_j.$$

This gives us the following addition table:

	$\mathscr{C}_0$	$\mathscr{C}_1$	$\mathscr{C}_2$	$\mathscr{C}_3$
$\mathscr{C}_0$	$\mathscr{C}_0$	$\mathscr{C}_1$	$\mathscr{C}_2$	$\mathscr{C}_3$
$\mathscr{C}_1$	$\mathscr{C}_1$	$\mathscr{C}_2$	$\mathscr{C}_3$	$\mathscr{C}_0$
$\mathscr{C}_2$	$\mathscr{C}_2$	$\mathscr{C}_3$	$\mathscr{C}_0$	$\mathscr{C}_1$
$\mathscr{C}_3$	$\mathscr{C}_3$	$\mathscr{C}_0$	$\mathscr{C}_1$	$\mathscr{C}_2$

You should recognise this table: it is just like the multiplication table for a cyclic group of order 4.

In the above example, we started with the set of all integers and introduced an equivalence relation that divided the integers up into four equivalence classes. We then considered these classes as objects in their own right, forming a set with four elements. This is really the whole point of equivalence relations. Effectively, one "identifies" things that are equivalent, so that a whole class of objects is thought of as being one single object. This can be a great simplification, because it reduces the number of different objects under discussion. These new objects, which comprise many old objects rolled into one (so to speak), are the elements of a new set, which is called the *quotient* of the original set by the equivalence relation.

Definition. If $\sim$ is an equivalence relation on a set S, then the set of all equivalence classes is called the *quotient of S by $\sim$*, written as $S/\!\sim$).

With this notation, if $\equiv$ is the relation of congruence modulo 4 on $\mathbb{Z}$ then

$$\mathbb{Z}/\!\equiv \;=\; \{\mathscr{C}_0, \mathscr{C}_1, \mathscr{C}_2, \mathscr{C}_3\}.$$

We shall in fact use the notation $\mathbb{Z}/(4)$ rather than $\mathbb{Z}/\!\equiv$. More generally, we shall use $\mathbb{Z}/(n)$ for the quotient of $\mathbb{Z}$ by the equivalence relation congruence modulo n.

Recall that $\mathbb{Z}$ is a group under addition. Let n be a fixed positive integer, and define $n\mathbb{Z} = \{\, nk \mid k \in \mathbb{Z} \,\}$, the set of all integers that are multiples of n. It is easily checked that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Indeed, if a, $b \in n\mathbb{Z}$ then $a = nk$ and $b = nl$ for some k, $l \in \mathbb{Z}$, and it follows that $a+b = n(k+l) \in n\mathbb{Z}$. Thus (SG1) holds. Since $0 = n\times 0 \in n\mathbb{Z}$, (SG2) holds. And if $a \in n\mathbb{Z}$ then $a = nk$ for some k, from which it follows that $-a = n(-k) \in n\mathbb{Z}$; so (SG3) holds too. Since (SG1),(SG2) and (SG3) all hold, $n\mathbb{Z}$ is a subgroup.

We saw in Week 8 that the cosets of any subgroup of any group can be viewed as equivalence classes, in the following manner. If H is a subgroup of G then the relation on G given by

$$x \sim y \text{ if and only if } x = yh \text{ for some } h \in H \tag{1}$$

is an equivalence relation. The equivalence classes are the left cosets gH (where $g \in G$).† Since $x = yh$ if and only if $h = y^{-1}x$, the definition (1) gives

$$x \sim y \text{ if and only if } y^{-1}x \in H.$$

If G is Abelian and the group operation is written as addition this becomes

$$x \sim y \text{ if and only if } x - y \in H,$$

and the cosets are written as $g + H$ rather than gH.

† In the notes for Week 8 we discussed right cosets rather than left cosets, but the two cases are totally analogous. Note also that the distinction between right cosets and left cosets disappears when dealing with an Abelian group.

In the case $G = \mathbb{Z}$ and $H = n\mathbb{Z}$ then the equivalence relation obtained by the above construction is precisely congruence modulo n, and the cosets $i + n\mathbb{Z}$ (for $i \in \mathbb{Z}$) are the congruence classes of $\mathbb{Z}$ modulo n. There are exactly n of these:

$$\begin{aligned} n\mathbb{Z} &= \{\dots, -2n, -n, 0, n, 2n, \dots\}, \\ 1 + n\mathbb{Z} &= \{\dots, 1-2n, 1-n, 1, 1+n, 1+2n, \dots\}, \\ 2 + n\mathbb{Z} &= \{\dots, 2-2n, 2-n, 2, 2+n, 2+2n, \dots\}, \\ &\vdots \\ (n-1) + n\mathbb{Z} &= \{\dots, -1-n, -1, n-1, 2n-1, 3n-1, \dots\}. \end{aligned}$$

In contexts where the value of n is fixed, we often use the shorter notation $\overline{i}$ for the coset $i + n\mathbb{Z}$. Adopting this convention, the quotient set $\mathbb{Z}/(n)$ is given by

$$\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}.$$

We can define addition on $\mathbb{Z}/(n)$ by exactly the same rule that we used for $\mathbb{Z}/(4)$; that is,

$$\overline{i} + \overline{j} = \overline{k}$$

if and only if

$$a + b \in \overline{k} \text{ for all } a \in \overline{i} \text{ and } b \in \overline{j}.$$

It is now very easy to see that $\mathbb{Z}/(n)$ is a group under this operation: indeed, addition is given by the table

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\dots$	$\overline{n-2}$	$\overline{n-1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\dots$	$\overline{n-2}$	$\overline{n-1}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\dots$	$\overline{n-1}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\dots$	$\overline{0}$	$\overline{1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
$\overline{n-2}$	$\overline{n-2}$	$\overline{n-1}$	$\overline{0}$	$\dots$	$\overline{n-4}$	$\overline{n-3}$
$\overline{n-1}$	$\overline{n-1}$	$\overline{0}$	$\overline{1}$	$\dots$	$\overline{n-3}$	$\overline{n-2}$

which we recognise as corresponding to a cyclic group of order n. The element $\overline{1}$ is a generator, since its sequence of multiples

$$\overline{0}, \quad \overline{1}, \quad \overline{1} + \overline{1} = \overline{2}, \quad \overline{1} + \overline{1} + \overline{1} = \overline{3}, \quad \dots$$

runs through all the elements of $\mathbb{Z}/(n)$.

Definition. The group $\mathbb{Z}/(n)$ constructed above is called the *group of integers modulo n*.