

MATHEMATICAL OLYMPIADS LECTURE NOTES

Congruences

Equivalence Relations

Often in mathematics a concept is borne out of generalising ideas that are well understood. For example, the Principle of Mathematical Induction generalises the following two properties of the natural numbers \mathbb{N} :

- there is a *first* natural number: 1; and
- each natural number n has a *successor*: $n + 1$.

The concept of an *equivalence relation* generalises the notion of *equality*. The essential properties of $=$ are *reflexivity*, *symmetry* and *transitivity* (which we define below), and these are the properties of $=$ we take to define the only slightly more general concept of an *equivalence relation*. Note that $=$ always has a meaning relative to some set – we may be saying two integers are equal, in which case $=$ has a meaning relative to the set \mathbb{Z} .

Definition. An *equivalence relation* \sim on a set S is a relation that has, for any $x, y, z \in S$, the following three properties:

- \sim is *reflexive*: $x \sim x$;
- \sim is *symmetric*: if $x \sim y$ then $y \sim x$; and
- \sim is *transitive*: if $x \sim y$ and $y \sim z$ then $x \sim z$.

Examples.

1. Notice that $=$ on the set \mathbb{R} is an equivalence relation.
2. Let S be the set of all triangles. Write $\triangle ABC \parallel \triangle DEF$, if $\triangle ABC$ is similar to $\triangle DEF$. Then \parallel is an equivalence relation. (Sometimes \sim is used here, rather than \parallel ; but we need \sim for the more general concept.)
Note: Two right-angled triangles are similar if and only if a pair of corresponding acute angles are equal (this is the basis of *trigonometry*).

At this point, the concept of an *equivalence relation* may appear trivial. Let's explore some non-examples.

Non-examples.


1. \neq on the set \mathbb{R} is *not* an equivalence relation, since \neq is *not reflexive* (i.e. $x \neq x$ is *false* for any $x \in \mathbb{R}$) and \neq is (in general) *not transitive* (e.g. $3 \neq 5$ and $5 \neq 3$, but $3 = 3$). On the other hand, \neq is *symmetric* (whenever $x \neq y$, we also have $y \neq x$).

2. $>$ on the set \mathbb{R} is *not* an equivalence relation, since $>$ is *not reflexive* (i.e. $x > x$ is *false* for any $x \in \mathbb{R}$) and $>$ is *not symmetric* (i.e. $x > y$ does *not imply* that $y > x$). However, $>$ is *transitive* (whenever $x > y$ and $y > z$, we also have $x > z$).

Note: The concept of an *order* relation generalises $>$; and a *partial order* relation generalises \geq .

Now that we know what an *equivalence relation* is, we can focus on the property which makes this concept so important:


An *equivalence relation* \sim defined on a set S , partitions the set into disjoint subsets called *equivalence classes*. From each *equivalence class* we can select one element, called a *representative*. The *equivalence class* with *representative* r is precisely all elements $s \in S$ such that $r \sim s$.

 Above, we defined $=$ to be *equality* on the set \mathbb{Z} . The *equivalence classes* here are not too interesting since each *equivalence class* has precisely one element. Suppose we define a set $E(\mathbb{Z})$ which contains all *expressions* that can be built up using the operations $+$ and \times and elements of \mathbb{Z} , e.g. $2 + 3$, $2 + 3 \times 5$ are two elements of $E(\mathbb{Z})$. Take $=$ to be what you would expect on $E(\mathbb{Z})$; now the *equivalence classes* on $E(\mathbb{Z})$ with respect to $=$ are more interesting. In fact, the *representatives* of the *equivalence classes* of $E(\mathbb{Z})$ can simply be taken to be the elements of \mathbb{Z} , e.g.

the equivalence class for 1 contains $1, 2 + -1, -1 \times -1, \dots$

and in general

the equivalence class for $n \in \mathbb{Z}$ contains all those expressions e of $E(\mathbb{Z})$ such that $n = e$.

 Let us return to one of the examples of an *equivalence relation*: \parallel . Below is a proof that \parallel is an *equivalence relation* on the set of all triangles, where **(AAA)** (acronym for **Angle-Angle-Angle**) represents the *similarity* theorem that states:

if corresponding angles of two triangles are *equal* then the triangles are *similar*.

- (i) \parallel is *reflexive*: For any $\triangle ABC \in S$,

$$\angle A = \angle A, \quad \angle B = \angle B, \quad \angle C = \angle C,$$

and so by **(AAA)**, $\triangle ABC \parallel \triangle ABC$.

- (ii) \parallel is *symmetric*: Suppose $\triangle ABC \parallel \triangle DEF$. Then

$$\begin{aligned} \angle A = \angle D, \quad \angle B = \angle E, \quad \angle C = \angle F. \\ \therefore \angle D = \angle A, \quad \angle E = \angle B, \quad \angle F = \angle C, \end{aligned}$$

and so by **(AAA)**, $\triangle DEF \parallel \triangle ABC$.

- (iii) \parallel is *transitive*: Suppose $\triangle ABC \parallel \triangle DEF$ and $\triangle DEF \parallel \triangle GHI$. Then

$$\begin{aligned} \angle A = \angle D, \quad \angle B = \angle E, \quad \angle C = \angle F, \\ \text{and } \angle D = \angle G, \quad \angle E = \angle H, \quad \angle F = \angle I, \\ \therefore \angle A = \angle G, \quad \angle B = \angle H, \quad \angle C = \angle I \end{aligned}$$

and so by **(AAA)**, $\triangle ABC \parallel \triangle GHI$.

Thus, since \parallel is *reflexive*, *symmetric* and *transitive*, we have that \parallel is an *equivalence relation* on the set of all triangles.

(Observe that each property of \parallel was proved via the corresponding property of $=$.)

Exercises.

1. Let S be the set of all triangles. Write $\triangle ABC \cong \triangle DEF$, if $\triangle ABC$ is *congruent* to $\triangle DEF$. Show that \cong is an equivalence relation on S .
(*Hint:* Model your proof on the one above that shows \parallel is an equivalence relation. Replace **(AAA)** with a convenient congruence property.)

Congruence modulo m

Suppose $m \in \mathbb{N}$. Then for two integers a, b we say:

a is congruent to b modulo m

(written: $a \equiv b \pmod{m}$)

if and only if

a and b give the same *remainder* on division by m ,

(in which case: $m \mid a - b$).

The reason that \equiv looks so much like $=$, is that like $=$ on \mathbb{Z} , *congruence modulo m* is an *equivalence relation* on \mathbb{Z} .

Exercises.

2. Check *congruence modulo m* , where $m \in \mathbb{N}$, is an *equivalence relation* on \mathbb{Z} .

The first question one should ask, given an *equivalence relation* on a set, is: *What are the equivalence classes?*

It is reasonably clear that every $n \in \mathbb{Z}$ can be written as

$$n = km + r,$$

for some $k \in \mathbb{Z}$ and some integer r satisfying $0 \leq r < m$. If we denote by \bar{r} all those integers $n \in \mathbb{Z}$ that give *remainder r* on division by m , then the *equivalence classes* modulo m are precisely:

$$\bar{0}, \bar{1}, \dots, \overline{m-1}.$$

Note: It is important to realise that there are an *infinite* number of ways of labelling each *equivalence class*, since each class has an *infinite* number of *representatives*, e.g.

$$\begin{aligned}\bar{0} &= \overline{-m} = \overline{m} = \overline{2m} = \dots \\ \bar{1} &= \overline{-m+1} = \overline{m+1} = \overline{2m+1} = \dots \\ &\vdots \\ \overline{m-1} &= \overline{-1} = \overline{2m-1} = \dots\end{aligned}$$

In some sense, the *equivalence classes* modulo m “simplify” \mathbb{Z} . Can we still recover many of the properties of \mathbb{Z} ? The answer is: a resounding *yes!* and it is because of this that *congruence modulo m* is worthy of further investigation.

Number Laws

Let's define the following number laws relative to a set S , on which operations $+$ (addition) and \cdot (multiplication) are defined.

- P1** (*closure* under $+$): if $x, y \in S$ then $x + y \in S$.
- P2** (*commutativity* of $+$): $x + y = y + x$ for all $x, y \in S$.
- P3** (*associativity* of $+$): $(x + y) + z = x + (y + z)$ for all $x, y, z \in S$.
- P4** (*identity* element for $+$): there is an *additive identity* element 0 (*zero*), which has the property that $x + 0 = x$ for all $x \in S$.
- P5** (*inverse* elements under $+$): each $x \in S$ has an *additive inverse* element $-x$, which has the property that $x + (-x) = 0$.
- M1** (*closure* under $.$): if $x, y \in S$ then $x.y \in S$.
- M2** (*commutativity* of $.$): $x.y = y.x$ for all $x, y \in S$.
- M3** (*associativity* of $.$): $(x.y).z = x.(y.z)$ for all $x, y, z \in S$.
- M4** (*identity* element for $.$): there is a *multiplicative identity* element 1 (*one*), which has the property that $x.1 = x$ for all $x \in S$.
- M5** (*inverse* elements under $.$): each *non-zero* $x \in S$ has a *multiplicative inverse* element (or *reciprocal*) $\frac{1}{x}$, which has the property that $x.\frac{1}{x} = 1$.
- D1** (*distribution* of $.$ over $+$): $x.(y + z) = x.y + x.z$ for all $x, y, z \in S$.
- C1** (*Cancellation law* for $+$): if $x + y = z + y$ then $x = z$.
- C2** (*Cancellation law* for $.$): if $x.y = z.y$ and $y \neq 0$ then $x = z$.

The sets of numbers that you are familiar with are the *natural numbers* \mathbb{N} , the *integers* \mathbb{Z} , the *rational numbers* \mathbb{Q} and the *real numbers* \mathbb{R} . Let us investigate which of the *Number Laws* are satisfied by each of these sets.

By definition, $\mathbb{N} = \{1, 2, 3, \dots\}$. It is easy (but a little tedious) to check that the only *Number Laws* above that *fail* for \mathbb{N} are **P4**, **P5** and **M5**.

Now $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ contains \mathbb{N} and enough extra elements so that **P4** and **P5** *succeed*. One can check that the only *Number Law* above that *fails* for \mathbb{Z} is **M5**.

In a similar fashion, $\mathbb{Q} = \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$ contains \mathbb{Z} and enough extra elements so that **M5** *succeeds*. One can check that *none* of the above *Number Laws* *fail* for \mathbb{Q} .

How does \mathbb{R} fit into this? Well ... there are other properties that numbers may satisfy, and \mathbb{R} contains \mathbb{Q} and a lot of other elements so that the additional properties are satisfied along with the *Number Laws* above. By the way, a set S that satisfies *all* of the *Number Laws* above is called a *field*; and a set S that satisfies the same *Number Laws* that \mathbb{Z} satisfies is called a *ring*.

Now can we recover some of the *Number Laws* when we consider not \mathbb{Z} , but the set of equivalence classes *modulo* m , where $m \in \mathbb{N}$? Indeed we can, but we have to re-interpret our notions of $+$, $.$ and $=$. Writing

$$\bar{x} + \bar{y} = \overline{x + y}$$

means

When an element of the class \bar{x} is added to an element of the class \bar{y} one obtains an element of the class *that contains* $x + y$.

And writing

$$\overline{x \cdot y} = \overline{x} \cdot \overline{y}$$

means

When an element of the class \overline{x} is multiplied by an element of the class \overline{y} one obtains an element of the class *that contains* $x \cdot y$.

Exercises.


3. Check that the same *Number Laws* satisfied by \mathbb{Z} are satisfied by the set of *equivalence classes* modulo m , where $m \in \mathbb{N}$.
4. (*Harder*) Show that *all* the *Number Laws* are satisfied by the set of *equivalence classes* modulo m , *if and only if* m is a prime.

Finally, note that if \overline{x} and \overline{y} are *equivalence classes* modulo m then

$$\overline{x} = \overline{y}$$

says *exactly* the same thing as

$$x \equiv y \pmod{m}.$$

 Incidentally, you will be familiar with a number of other properties of \mathbb{Z} that are not among the *Number Laws* above. Each of the following *laws* follows from those *Number Laws* above, where $x, y, z \in S$.

X1 $-(-x) = x$.

X2 $0 \cdot x = 0$.

X3 $-1 \cdot x = -x$.

Exercises (Hard).

5. Prove each of **X1**, **X2** and **X3**.

Hints

- (i) **X1** follows from **P5** and **P2**.
 - (ii) **X2** follows from **C1**, **P4**, **M4** and **D1**.
 - (iii) **X3** follows from **C1**, **P5**, **X2**, **D1** and **M4**.
6. Prove **C1** follows from **P5**, **P3** and **P4**. (Thus, **C1** may be deduced from other *Number Laws* satisfied by \mathbb{Z} , but **C1** cannot be deduced from other *Number Laws* that are satisfied by \mathbb{N} .)
 7. Prove **C2** follows from **M5**, **M3** and **M4**. (Of course, \mathbb{Z} does not satisfy **M5**. So **C2** cannot be deduced from other *Number Laws* satisfied by \mathbb{Z} .)

Of course, this means that **X1**, **X2** and **X3** are also satisfied by the set of *equivalence classes* modulo m .

Problems.

1. Show that: if the sum of the digits of a natural number N is divisible by 3 then $3 \mid N$.
2. Prove that for every integer n :
 - (i) $3 \mid n^3 - n$;
 - (ii) $5 \mid n^5 - n$;
 - (iii) $7 \mid n^7 - n$;
 - (iv) $11 \mid n^{11} - n$;
 - (v) $13 \mid n^{13} - n$.
3. Show that $n^9 - n$ is not necessarily divisible by 9.
4. Prove the following:
 - (i) $3^{6n} - 2^{6n}$ is divisible by 35, for every positive integer n ;
 - (ii) $n^5 - 5n^3 + 4n$ is divisible by 120, for every integer n ;
 - (iii) for all integers m and n , $mn(m^{60} - n^{60})$ is divisible by 56 786 730.
Hint: $56\,786\,730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$.
 - (iv) Prove that $n^2 + 3n + 5$ is never divisible by 121 for any positive integer n .
 - (v) What is the final digit of $(\dots(((7^7)^7)^7)\dots^7)$.
There are 1001 7s in the formula.
 - (vi) What is the final digit of $7^{7^{7^{\dots^7}}}$.
There are 1001 7s in the formula.