MA294 Lecture

Timothy Kohl

Boston University

June 30,2025

Modular Arithmetic

We recall the definition of 'equivalence'.

Definition

An equivalence relation $\sim$ on a set S is an association between pairs of elements of S that satisfies the following properties:

- $a \sim a$ for all $a \in S$ (reflexivity)
- $a \sim b$ implies $b \sim a$ (symmetry)
- $a \sim b$ and $b \sim c$ implies $a \sim c$ (transitivity)

The word 'association' may seem a bit nebulous so here is a more formal definition.

An equivalence relation $\sim$ on a set S is a subset $R \subseteq S \times S$ such that

- $(a, a) \in R$ for all $a \in S$ (reflexivity)
- $(a, b) \in R$ implies $(b, a) \in R$ (symmetry)
- $(a, b) \in R$ and $(b, c) \in R$ implies $(a, c) \in R$ (transitivity)

and sometimes one writes aRb instead of $a \sim b$.

An equivalence relation gives rise to a *partition* of the set.

Definition

Given an equivalence relation $\sim$ on a set S and $a \in S$, the equivalence class of a is the set

$$[a] = \{b \in S \mid a \sim b\}$$

i.e. the set of all those elements equivalent to a.

Note: $[a] \subseteq S$ and that $a \in [a]$ of course.

FACTS:

Proposition

If $a_1 \sim a_2$ then $[a_1] = [a_2]$ and vice-versa.

Proof.

Well, if $a_1 \sim a_2$ then if $b \sim a_1$ then, by transitivity $b \sim a_2$ so $[a_1] \subseteq [a_2]$.

Since $a_1 \sim a_2$ implies $a_2 \sim a_1$ then if $b \sim a_2$ (i.e. $b \in [a_2]$) then $b \sim a_1$ (again by transitivity).

So $b \in [a_1]$ and therefore $[a_2] \subseteq [a_1]$ so $[a_1] = [a_2]$.

If $[a_1] = [a_2]$ then, since $a_1 \in [a_1]$ we have that $a_1 \in [a_2]$ so $a_1 \sim a_2$. □

Proposition

For $a_1, a_2 \in S$, either $[a_1] = [a_2]$ or $[a_1] \cap [a_2] = \emptyset$.

Proof.

Suppose $[a_1] \cap [a_2] \neq \emptyset$ then if $x \in [a_1] \cap [a_2]$ we have $x \sim a_1$ and $x \sim a_2$.

Thus $a_1 \sim x$ and $x \sim a_2$ so, by transitivity, $a_1 \sim a_2$ which, by the previous fact, implies that $[a_1] = [a_2]$. □

Proposition

If $\sim$ is an equivalence relation defined on a set S then S is the union of the distinct equivalence classes with respect to $\sim$.

Proof.

The basic point is that if $a \in S$ then $a \in [a]$ so every element of S belongs to an equivalence class.

And the only other observation to make is that, by the above facts, two distinct elements of S give rise to equivalence classes that are either identical, or disjoint, as sets. □

Note, if $a \sim b$ for *all* $a, b \in S$ then there is only one equivalence class, namely $[a] = S$ for *any* $a \in S$.

On the other hand, one can define $a \sim b$ only if $a = b$, in which case each $a \in S$ determines its own equivalence class, namely $[a] = \{a\}$, the set consisting of a by itself.

Modular Arithmetic

The principle example of an equivalence relation is that which gives rise to what is known as *modular arithmetic*.

Definition

Let $S = \mathbb{Z}$ (the integers) and pick $m > 1$ a fixed integer (called the **modulus**) and define an equivalence relation $\equiv$ on $\mathbb{Z}$ as follows:

$$a \equiv b\ (mod\ \ m)$$

if m divides $a - b$, written $m|a-b$.

Equivalently, $a - b = km$ for some integer k. (k can be positive or negative!)

We also use the terminology 'a is congruent to b mod m'.

Proposition

$a \equiv b \ (mod \ \ m)$ is an equivalence relation on $\mathbb{Z}$

Proof.

If $a \in \mathbb{Z}$ then $a \equiv a \ (mod \ \ m)$ since $a - a = 0 = 0 \cdot m$. (i.e. $k = 0$)

If $a \equiv b \ (mod \ \ m)$ then $a - b = km$, so the question is whether $b \equiv a$, but this is indeed the case since $b - a = -(a - b) = -km = (-k)m$ so $b - a$ is a multiple of m.

If $a \equiv b \ (mod \ \ m)$ and $b \equiv c \ (mod \ \ m)$ then $a - b = k_1 m$ for some k_1 and $b - c = k_2 m$ for some k_2 and so
$a - c = (a - b) + (b - c) = k_1 m + k_2 m = (k_1 + k_2)m$ and so
$a \equiv c \ (mod \ \ m)$. □

Examples:

- $5 \equiv 2 \ (mod \ 3)$

- $-1 \equiv 5 \ (mod \ 6)$

- $2 \equiv 0 \ (mod \ 2)$

- $-2 \equiv -5 \ (mod \ 3)$

Note, we don't usually let $m = 1$ as then $a \equiv b \ (mod \ 1)$ would hold for *all* integers a, b which wouldn't be terribly interesting.

The equivalence classes of $\mathbb{Z}$ with respect to congruence mod m can be understood by means of the Division Algorithm.

Proposition

(The Division Algorithm) Given an integer a and divisor m, there exists unique integers q, r such that

$$a = qm + r$$

where $0 \leq r < m$. (q=quotient, r=remainder)

Example: $a = 23$, $m = 5$ yields $23 = 4 \cdot 5 + 3$ and observe, as a consequence, that $23 \equiv 3\ (mod\ 5)$ which is no accident since $a = qm + r$ implies $a \equiv r\ (mod\ m)$.

Back to $m = 3$, consider the equivalence classes under $\equiv$ mod 3.

- [0]={...,-9,-6,-3,0,3,6,9,...}
- [1]={...,-8,-5,-2,1,4,7,10,...}
- [2]={...,-7,-4,-1,2,5,8,11,...}

The reason for this is that if $m = 3$, given $a \in \mathbb{Z}$ one has

$$a = 3 \cdot q + r$$

where $0 \leq r < 3$, i.e. $r = 0, 1, 2$.

That is, dividing a number by 3 leaves a particular (<u>unique</u>) remainder.

The key point to observe is that, for $a \in \mathbb{Z}$, and a fixed modulus $m > 1$ then $a \equiv r \ (mod \ m)$ for *exactly one* $r \in \{0, 1, \ldots, m-1\}$, i.e. $a \in [r]$ uniquely.

Example: $m = 2$

$$a \equiv 0 \ (mod \ 2) \text{ only if } 2|a, \text{ i.e. } a \text{ is even}$$
$$a \equiv 1 \ (mod \ 2) \text{ only if } a = 2k+1, \text{ i.e. } a \text{ is odd}$$

So $\mathbb{Z} = [0] \cup [1]$ which is the natural division of integers into even versus odd numbers.

Note of course that for a given m one may have $[a_1] = [a_2]$ for distinct a_1,a_2.
i.e. Under $\equiv$ mod 2 for example

$$\begin{aligned}[0] = [2] = [-2] = [4] = [-4] = \ldots \text{ etc.}\\ [1] = [3] = [-1] = [5] = [-3] = \ldots \text{ etc.}\end{aligned}$$

But, again, given $m > 1$, a given $a \in \mathbb{Z}$ lies in exactly one $[r]$ for $0 \leq r \leq m - 1$.

For example, for $m = 10$, one has $a = d_n d_{n-1} \cdots d_1 d_0$ (where the d_i are the digits of a) namely

$$a = d_n \cdot 10^n + d_{n-1} \cdot 10^{n-1} + \cdots + d_1 \cdot 10 + d_0$$

yields the fact that $a \equiv d_0$ $(mod\ 10)$.

For a given modulus m we can utilize the properties of congruence, to define an 'arithmetic' of congruences, based on the following properties of $\equiv$.

Theorem

Given a fixed modulus $m > 1$, if $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$ then
(i) $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$
(ii) $a_1 b_1 \equiv a_2 b_2 \pmod{m}$
namely that addition and multiplication are 'compatible' with $\equiv$.

Proof.

If $a_1 - a_2 = km$ and $b_1 - b_2 = lm$ then

$$\begin{array}{r}
(a_1 - a_2) + (b_1 - b_2) = (k + l)m \\
\downarrow \\
(a_1 + b_1) - (a_2 + b_2) = (k + l)m \\
\downarrow \\
a_1 + b_1 \equiv a_2 + b_2 \ (mod \ \ m)
\end{array}$$

Similarly, $a_1 b_1 = (a_2 + km)(b_2 + lm) = a_2 b_2 + a_2 lm + b_2 km + kmlm$ implies that $a_1 b_1 \equiv a_2 b_2$. □

Another consequence of this is the following.

Proposition

If $a \equiv b \ (mod \ \ m)$ *then*

$$a^n \equiv b^n \ (mod \ \ m)$$

for any $n \geq 1$*.*

Proof.

This is basically an application of the previous theorem, in particular $a \equiv b \ (mod \ \ m)$ and $a \equiv b \ (mod \ \ m)$ (multiplied on both sides) yields $a \cdot a \equiv b \cdot b \ (mod \ \ m)$, namely $a^2 \equiv b^2 \ (mod \ \ m)$ and we can repeat this as often as we like for larger exponents. □

Here is a neat application of this fact.
Prove that the last digit of 2^{30} is 4.

The basic bit of information we need is that digit $'d' \in \{0, \ldots, 9\}$ such that $2^{30} \equiv d\ (mod\ 10)$.

We note that $2^2 = 4$ so $2^2 \equiv 4\ (mod\ 10)$ which implies that $(2^2)^2 \equiv 4^2\ (mod\ 10)$, and since $4^2 = 16$, and $16 \equiv 6\ (mod\ 10)$ then $2^4 \equiv 6\ (mod\ 10)$ and so $2^5 \equiv 12\ (mod\ 10)$ where, of course $12 \equiv 2\ (mod\ 10)$, and so

$$2^5 \equiv 2\ (mod\ 10)$$

which implies $(2^5)^6 \equiv 2^6\ (mod\ 10)$, that is $2^{30} \equiv 2^6\ (mod\ 10)$ and since $2^6 = 64$ then $2^6 \equiv 4\ (mod\ 10)$ and therefore $2^{30} \equiv 4\ (mod\ 10)$.

That is, the last digit is 4, and indeed $2^{30} = 1,073,741,824$.
Exercise: Repeat this for the number 2^{2023}.

$\mathbb{Z}_m$ the integers mod m - "$\mathbb{Z}$ mod m"

Recall that for a given modulus $m > 1$ that any integer a is congruent to exactly one $r \in \{0, \ldots, m-1\}$ because, by the division algorithm

$$a = q \cdot m + r$$

for unique q, r, where $r \in \{0, 1, \ldots, m-1\}$.

With this and the arithmetic properties of $\equiv$ we just proved, one can define a system of numbers that is based on the integers $\mathbb{Z}$ but is finite in size.

Definition

The set of integers mod m denoted $\mathbb{Z}_m$ is the set of distinct equivalence classes

$$\{[0],[1],\ldots,[m-1]\}$$

with respect to the equivalence relation of congruence mod m.

For example $\mathbb{Z}_3 = \{[0],[1],[2]\}$ since $\mathbb{Z} = [0]\cup[1]\cup[2]$.

Bear in mind that we are treating these infinite sets $[a]$ as though they are individual entities, which they are since each equivalence class is different than another,but we can treat $\mathbb{Z}_m$ as a finite set since there are only finitely many equivalence classes in $\mathbb{Z}_m$.

Later on we will take this even further by dropping the '[]' around the $[r]$.

The facts we proved earlier show how the congruence relation is 'compatible' with addition and multiplication.

With this in mind we define the following addition and multiplication operations on the set $\mathbb{Z}_m$.

Definition

If $[x], [y] \in \mathbb{Z}_m$ then $[x] + [y] = [x + y]$ and $[x] \cdot [y] = [xy]$.

The key fact(s) to be verified is that this operation is 'closed' namely that $[x] + [y] \in \mathbb{Z}_m$ and $[x] \cdot [y] \in \mathbb{Z}_m$.

In lieu of a formal proof, let us consider some examples which illustrate this very clearly.

Example: $\mathbb{Z}_5 = \{[0],[1],[2],[3],[4]\}$.

$[2]+[4]=[2+4]=[6]=[1]$ since $6 \equiv 1\ (mod\ 5)$

$[4]+[1]=[4+1]=[5]=[0]$

$[2]+[2]=[2+2]=[4]$

$[2]+[0]=[2+0]=[2]$

$[2]\cdot[4]=[2\cdot 4]=[8]=[3]$ since $8 \equiv 3\ (mod\ 5)$

$[3]\cdot[1]=[3\cdot 1]=[3]$

$[2]\cdot[3]=[2\cdot 3]=[6]=[1]$

For simplicity, it's easier to write $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ and compute $a + b$ and $a \cdot b$ mod m by computing the appropriate remainders 'mod m'.

Ex: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

- $2 + 3 = 5$
- $4 + 3 = 1$
- $5 \cdot 2 = 4$
- $3 \cdot 3 = 3$ (Yes, this can happen.)

Theorem

In $\mathbb{Z}_m$ the operations $+$ and $\cdot$ follow the following rules.
Let $a, b, c \in \mathbb{Z}_m$

- *(1)* $a + b = b + a$ *[Commutativity]*
- *(2)* $a \cdot b = b \cdot a$ *[Commutativity]*
- *(3)* $(a + b) + c = a + (b + c)$ *[Associativity]*
- *(4)* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *[Associativity]*
- *(5)* $a + 0 = a$ *[Additive Identity]*
- *(6)* $a \cdot 1 = a$ *[Multiplicative Identity]*
- *(7)* $a(b + c) = ab + ac$ *[Distributive Law]*
- *(8) For each* $a \in \mathbb{Z}_m$*, there exists* $b \in \mathbb{Z}_m$ *such that* $a + b = 0$*.* *[Additive Inverses]*

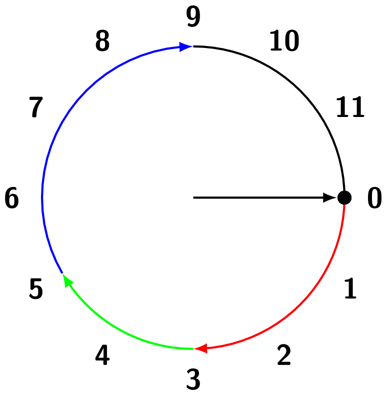
Proof.

(Sketch) (5),(6) If $[a] \in \mathbb{Z}_m$ then $[a] + [0] = [a + 0] = [a]$, and similarly $[a] \cdot [1] = [a \cdot 1] = [a]$.

(8) If $a \in \mathbb{Z}_m$ then if we let $b = m - a$ then $b \in \mathbb{Z}_m$ and obviously $[a] + [b] = [a] + [m - a] = [a + m - a] = [m] = [0]$ in $\mathbb{Z}_m$.

So, for we may define $-a$ to be $m - a$ and observe that $a + (-a) = 0$. □

As to the associativity of addition, $(a + b) + c = a + (b + c)$ we invoke an image which really conveys why the parentheses don't matter.



Here, if we represent a number in $\mathbb{Z}_{12}$ as clockwise rotation, and the sum of two numbers as the composition of two rotations then it's clear why, for example $(3 + 2) + 4 = 3 + (2 + 4) = 3 + 2 + 4 = 9$.