MA294 Lecture

Timothy Kohl

Boston University

January 18, 2024

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 $a_1 \sim a_2$. $\square$

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 $[a_1] = [a_2]$. $\square$

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. $\square$

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

$a \equiv b \pmod{m}$ is an equivalence relation on $\mathbb{Z}$

Proof.

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

If $a \equiv b \pmod{m}$ 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 $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ 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
$a \equiv c \pmod{m}$. $\square$

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 $0 \le r < m$. (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

$$[0] = [2] = [-2] = [4] = [-4] = \dots \text{ etc.}$$
$$[1] = [3] = [-1] = [5] = [-3] = \dots \text{ etc.}$$

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

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

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

Another consequence of this is the following.

Proposition

If $a \equiv b \pmod{m}$ *then*

$$a^n \equiv b^n \pmod{m}$$

for any $n \geq 1$.

Proof.

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

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}.