Jan26

Monday, January 25, 2021 9:06 PM

Def^n $m \in \mathbb{N}$ $a \in \mathbb{Z}$.

Then $a = mq + r$ for unique q, r w/ $0 \le r < |a|$.

Then call r the residue of a modulo m.

Lemma $m \in \mathbb{Z},$ $a, b \in \mathbb{Z}$. a, b have the same residue mod m

$$\iff m \mid (a-b)$$ ←

Def^n

If a, b are as in the Lemma, the we write

$$a \equiv b \mod m.$$

"a is congruent to b modulo m"

Impt Exercise

① Prove Lemma.

② Prove $\equiv \mod m$ is an equivalence relation on $\mathbb{Z}$.

What are the equivalence classes?

$a \in \mathbb{Z}$.

$$[a] = \overline{a} = \{ b \mid m \text{ divides } a-b \}$$

Notation

$km = a-b$

$a = b + km$

$$= \{a, a \pm m, a \pm 2m, ---- \}$$

Def^n

$$\mathbb{Z}/m\mathbb{Z} = \{ \overline{a} \mid a \in \mathbb{Z} \}$$

Ex $m=2$ $\mathbb{Z}/m\mathbb{Z} = \{ \{\text{even \#s}\}, \{\text{odd \#s}\} \}$.

Lemma $a, b \in \mathbb{Z}$. $m \in \mathbb{N}$.

$$[\underline{a}] = [\underline{b}] \iff \underline{a} \equiv \underline{b} \mod m.$$

Pf/ $[a] = [b] \ni b$

$\implies a \equiv b \mod m$.

Rmk True for any equivalence relation.

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

for any $c \in \mathbb{Z}$.

$c \in [a]$

$\iff c \equiv a \equiv b$

$\iff c \in [b]$

$\implies [a] = [b]$.

$\emptyset$

Observation

There is a surjective function

$$\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

$$a \longmapsto [a].$$

Not injective

$$[a] = [a+m].$$

Def$^{\underline{n}}$

A choice of an element in an equivalence class is called a representative element.

Example $\mathbb{Z}/2\mathbb{Z} = \{\text{evens}, \text{odds}\}$

3 is a representative of the odds.

Observation

$m \in \mathbb{N}$. $a \in \mathbb{Z}$. r be the reside of a mod m.

* Then r is a representative of $[a]$. $\leftarrow$ ($a = mq + r$ so $a - r$ divisible by m)

* $[a] = [r]$. $\longleftrightarrow$ $r \in [a]$

Also $r \in \{0, 1, 2, \ldots, m-1\}$.

So $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], [2], \ldots [m-1]\}$.

Claim These are all distinct.

Pf/ $0 \le r_1 \le r_2 < m$

Suppose $[r_1] = [r_2]$.

$\Longrightarrow m \mid r_2 - r_1$

But $0 \le (r_2 - r_1) < m$

so $r_2 - r_1 = 0 \Longrightarrow r_2 = r_1$ ∅

Upshot

Represent $\mathbb{Z}/m\mathbb{Z}$ by the integers between 0 & $m-1$.

Example

$(\mathbb{Z}/12\mathbb{Z}) = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{11}\}$.

"Clock arithmetic".

"count in circles"

$$\begin{array}{ccccc} 1, 2, \dots, & 12, & 13, & 14, & \dots \\ & \| & \| & \| & \\ & 0 & 1 & 2 & \end{array}$$

3 hrs after 11 is 2.

$$\boxed{3 + 11 = 2} \quad ?$$

$$\overline{3} + \overline{11} = \overline{14} = \overline{2}$$

But $14 \equiv 2 \mod 12$

In this way we define a notion of + & × on $\mathbb{Z}/m\mathbb{Z}$.

Lemma $a, a', b, b' \in \mathbb{Z}$.

$a \equiv a' \bmod m$ $\qquad [a] = [a']$

$b \equiv b' \bmod m.$ $\qquad [b] = [b']$

Then $(a+b) \equiv (a'+b') \bmod m$ $\qquad [a+b] = [a'+b']$

$(a \cdot b) \equiv (a' \cdot b') \bmod m.$ $\qquad [ab] = [a'b'].$

Proof

Exercise.

Def^{n} Define $+ : (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \longrightarrow \mathbb{Z}/m\mathbb{Z}$

$\times : (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \longrightarrow \mathbb{Z}/m\mathbb{Z}$

as follows.

$$[a] + [b] = [a+b]$$

$$[a] \times [b] = [ab].$$

Remark This is well defined b/c of Lemma.

Suppose $a \equiv a' \bmod m.$ but $a \neq a'.$

Then $[a] = [a'] \leftarrow$

But... need $[a] + [b] = [a'] + [b]$

even though $a+b \neq a'+b$.

Lemma $\Longrightarrow$ $[a+b] = [a'+b]$

Phew

Example

$$\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

$2 \equiv 8 \mod 6$

$\bar{2} = \bar{8}$

* $\bar{2} \cdot \bar{5} = \overline{2 \cdot 5}$

$= \overline{10}$

$= \bar{4}$

$\bar{8} \cdot \bar{5} = \overline{8 \cdot 5}$

$= \overline{40}$

$= \bar{4}$

Phew.

$40 = 36 + 4$

$\Longrightarrow 40 \equiv 4$

* Zero divisors

$$\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$$

* Don't necessarily have division:

$\bar{2}x = \bar{3}$ $\quad$ $(2x \equiv 3 \mod 6)$.

No solution

Multiples of 2

$$\bar{2},\ \bar{4},\ \underset{\bar{0}}{\underset{\shortparallel}{\bar{6}}},\ \underset{\bar{2}}{\underset{\shortparallel}{\bar{8}}},\ \underset{\bar{4}}{\underset{\shortparallel}{\overline{10}}},\ \underset{\bar{0}}{\underset{\shortparallel}{\overline{12}}},\ \underset{\bar{2}}{\underset{\shortparallel}{\overline{14}}},\ \ldots$$

* But sometimes you do.....

$\bar{5}x = \bar{1}$ $\quad$ $(5x = 1 \mod 6)$.

$$5 \times 5 = 25 \equiv 1 \mod 6$$

$$\bar{5} \cdot \bar{5} = \bar{1}$$

$\rightsquigarrow$ "Mod 6, $\frac{\bar{1}}{\bar{5}} = \bar{5}$"

Dividing by 5 is multiplying by 5.

$$\bar{5} x = \bar{3}$$

$$\begin{array}{l} \bar{5} \cdot \bar{5} \cdot x = \bar{5} \cdot \bar{3} = \overline{15} = \bar{3} \\ \quad \| \\ \overline{25}\, x \\ \quad \| \\ \bar{1}\, x \\ \quad \| \\ x \end{array}$$

Indeed $\bar{5} \cdot \bar{3} = \overline{15} = \bar{3}$ ✓

Exercise

Compute $\frac{1}{2}$ modulo 5.

Def$^{\underline{n}}$

If $\bar{a} x = \bar{1}$ has a solution mod m, we say a has a multiplicative inverse modulo m.

Call the solution $\bar{a}^{-1}$. (or $[a]^{-1}$).

↑ the solution?

← equiv to $\bar{a}x = \bar{1}$ has a soln.

Prop $ax \equiv 1 \mod m$ has a solution in $\mathbb{Z}$ $\Longleftrightarrow$ $\gcd(a, m) = 1$.

Proof $\gcd(a, m) \Longrightarrow \exists\, u, v$ s.t.

$$au + mv = 1$$

So $x = u$ is a solution.

bc $au = 1 - mv \equiv 1 \mod m$.

Conversely $ax \equiv 1 \mod m$ has a solution.

$$ax - 1 = km$$

o $ax + km = 1$

$g = \gcd(a, m)$

$$\left.\begin{array}{l} g \mid ax \\ g \mid km \end{array}\right\} \Longrightarrow g \mid (ax + km) = 1$$

so $g = 1$.

Summarize (The following are equivalent).

1) $[a] = \bar{a}$ has a multiplicative inverse in $\mathbb{Z}/m\mathbb{Z}$.
2) $\bar{a}x = \bar{1}$ has a solution in $\mathbb{Z}/m\mathbb{Z}$

3) $ax \equiv 1 \mod m$ has a solution in $\mathbb{Z}$

4) $\gcd(a, m) = 1$.

Corollary

All nonzero elements of $\mathbb{Z}/m\mathbb{Z}$ have multiplicative inverses $\iff$ m is prime.

Observe If p prime & $\gcd(a,p) \neq 1$

$\implies p \mid a$

$\implies [a] = [0]$.

Exercise

- p prime. $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}$ nonzero, so is $\bar{a} \cdot \bar{b}$.
- Give an example to show false if p composite.

Remark we will see:

- $(\mathbb{Z}/m\mathbb{Z}, +, \times)$ is a ring.
- $\mathbb{Q}$ is a field b/c divide by anything except 0.

we will see $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ is a field.

Def^n The multiplicative group of $\mathbb{Z}/m\mathbb{Z}$ is defined to be

$$(\mathbb{Z}/m\mathbb{Z})^{\times} = \{\bar{a} \in \mathbb{Z}/m\mathbb{Z} \mid \bar{a}x = \bar{1} \text{ has a soln}\}$$

$$= \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,m) = 1\}$$

Groups

History

① Number Theory.

Lagrange/Euler/FLittle

* The $(p-1)$st power of a nonmult of p is one more than a mult of p.

* If a not divisible by 2 or 5, then the last 2 digits of a^{40} are 0 & 1.

Structure of the group

1) $(\mathbb{Z}/p\mathbb{Z})^{\times}$

2) $(\mathbb{Z}/100\mathbb{Z})^{\times}$

② Geometry & topology.

(crypto)

(AG)

Solutions to cubic equations (curves) satisfy some sort of addition law. This law pinned down geometry of this curve.

$\Longrightarrow$ Elliptic Curves.

③ Algebra

$ax^2+bx+c=0$

2 solns $\quad x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$

↑ symmetry.
swap + − .

Similar formulas for cubic & quartic polynomials } More complicated ($+, \times, -, \div, \sqrt[n]{\ }$) ★
↗ Still symmetric..

Observation Galois

- * Operations in ★ only allow for certain types of symmetries to arise.
- * Deg 5 polys whose solutions have more complicated symmetry.
- * These symmetries have mult law pinning them down.

---

3 shadows of a deeper & more abstract idea.

So... what is a group.

Defⁿ

Let G be a set. A binary operation on G is a function $*: G \times G \to G$.

Rmk we write $a*b$ rather than $*(a,b)$.

Fundamental Def^n

A group $(G,*)$ is a set G w/ a binary operation $*$ satisfying:

Associativity ① $(a*b)*c = a*(b*c)$ $\forall a,b,c \in G$

Identity. ② There exists some $e \in G$ s.t. $a*e = e*a = a$ $\forall a \in G$.

Inverse. ③ $\forall a \in G$, $\exists$ $b \in G$. s.t. $\underline{a*b} = \underline{b*a} = e$.

Observations

① Did not assert $a*b = b*a$. will not always hold.

② We did not assert uniqueness of inverse & identity. will always hold.

It turns out that the inverse & identity will be unique. This is a consequence of def^n of group, highlighting the strength & structure of these axioms.

③ We write G for $(G, *)$ sometimes.

Proposition: (Uniqueness of identity & inverse).

Let G be a group. Then

① The identity of G is unique.

② $a \in G$, then the inverse of a is unique. We can write it as a^{-1}.

Pf/ $e_1, e_2 \in G$ are both identities

①

$$e_1 \underset{\substack{\uparrow \\ e_2 \text{ identity}}}{=} e_1 * e_2 \underset{\substack{\uparrow \\ e_1 \\ \text{identity}}}{=} e_2.$$

✓

② b, c both inverses of $a \in G$.

want $b = c$

$$\begin{aligned} b &= b * e && \text{(identity)} \\ &= b * (a * c) && \text{(c an inv).} \\ &= (b * a) * c && \text{(assoc.} \\ &= e * c && \text{(b an inv)} \end{aligned}$$

$= c$ cid). ⊘

Impt never changed order.

Corollary

Suppose G a gp. $a, b \in G$.

If $a * b = e$ then

1) $b = a^{-1}$

2) $a = b^{-1}$

Pf/ Exercise.

Hint Show $b * a$ also e.
Then apply prop. ⊘