Lecture 23

Wednesday, March 4, 2015 8:00 AM

Modular Arithmetic

Assume we know about $\mathbb{Z}$.

For integers n, m

Say n divides m, and write $n \mid m$, when $\exists k \in \mathbb{Z}$ s.t. $m = n \cdot k$.

Fix $n \in \mathbb{N}$. Define a relation $\sim_n$ on $\mathbb{Z}$ s.t.

$$a \sim_n b \iff n \mid a - b$$

e.g. $5 \sim_2 3$ b/c $5 - 3 = 2$ and $2 \mid 2$ b/c $2 = 2 \cdot 1$.

$7 \sim_{10} 337$ b/c ~~$337 - 7 = 330$~~ $7 - 337 = -330$ and $10 \mid 330$ (330)

b/c $-330 = 10 \cdot (-33)$.

Claim $\sim_n$ is an equivalence relation.

If Reflexive: Is $a \sim_n a$? $a - a = 0$ and

$n \mid 0$ b/c $0 = n \cdot 0$ so $a \sim_n a$.

Symmetric: Suppose $a \sim_n b$ in which case $a - b = n \cdot k$ for some $k \in \mathbb{Z}$. Then $b - a = -(a - b) = -n \cdot k = n \cdot (-k)$ and $-k \in \mathbb{Z}$ so $n \mid b - a$ and thus $b \sim_n a$.

Transitive Suppose $a \tilde{\equiv}_n b$, $b \tilde{\equiv}_n c$ with $k, l \in \mathbb{Z}$ s.t.

$a - b = n \cdot k$, $b - c = n \cdot l$. Adding these,

$$(a-b) + (b-c) = nk + nl$$

$$a - c = n \cdot (k+l).$$

Since $k+l \in \mathbb{Z}$, get $n \mid a-c$ so $a \tilde{\equiv}_n c$. □

$\tilde{\equiv}_n$ partitions $\mathbb{Z}$ into equivalence classes.

What are the equivalence classes?

Write $[a] = [a]_n$ for the equiv class (under $\tilde{\equiv}_n$) of a, i.e.,

$$[a] = \{ b \in \mathbb{Z} \mid b \tilde{\equiv}_n a \}$$

$$= \{ b \in \mathbb{Z} \mid n \mid b-a \}$$

$$= \{ b \in \mathbb{Z} \mid b - a = n \cdot k \text{ for some } k \in \mathbb{Z} \}$$

$$= \{ b \in \mathbb{Z} \mid b = a + nk \text{ for some } k \in \mathbb{Z} \}$$

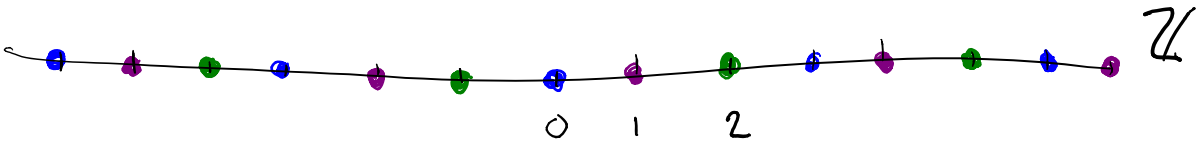
$$= \{ a + nk \mid k \in \mathbb{Z} \}$$

$\equiv = x_i$

$\equiv = \equiv = X_i$

Thus $1 = \equiv$

$n=3$



$[0]_3 = \{0+3\cdot k \mid k\in\mathbb{Z}\}$
$= \{3k \mid k\in\mathbb{Z}\}$

$[1]_3 = \{1+3k \mid k\in\mathbb{Z}\}$

$[2]_3 = \{2+3k \mid k\in\mathbb{Z}\}$

Observe $[0]\cup[1]\cup[2] = \mathbb{Z}$

and $[i]\cap[j] = \emptyset$
if $i\neq j$ for $i,j\in\{0,1,2\}$.

In fact, $[i]_n \cap [j]_n = \begin{cases} \emptyset & i \not\sim_n j \\ [i]_n = [j]_n & i \sim_n j \end{cases}$

Write $\mathbb{Z}/n\mathbb{Z}$ for $\mathbb{Z}/\sim_n$, i.e., the set of mod n equivalence classes.

Preferred names for these $\{[0]_n, [1]_n, \ldots, [n-1]_n\}$

(If we go further, get $[0]_n = [n]_n$ b/c $0 \sim_n n$
(b/c $n-0 = n = n\cdot 1$).)

Notation The relation $a \sim_n b$ is usually written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv b \ (n).$$

Read this as "a is congruent to b mod(ulo) n."

Arithmetic If $a \sim_n a'$, $b \sim_n b'$, then

$$a+b \sim_n a'+b' \quad \& \quad a \cdot b \sim_n a' \cdot b'.$$

This allows us to define

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

$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

e.g. In $\mathbb{Z}/3\mathbb{Z}$,

$$[1]+[1] = [1+1] = [2]$$

$$[1]+[2] = [1+2] = [3] = [0]$$

$$[2]\cdot[2] = [2\cdot 2] = [4] = [1]$$

(b/c $4-1=3$ is divisible by 3)

Thm $+, \cdot$ are comm & assoc on $\mathbb{Z}/n\mathbb{Z}$.
They have additive identity $[0]$, mult id $[1]$
$\mathbb{Z}/n\mathbb{Z}$ has additive inverses: $-[a] = [-a] = [n-a]$.

$[a] + [n-a] = [a+n-a] = [n] = [0]$, the add id.

Thus $[n-a] = -[a]$ & $[a] = -[n-a]$.

subtraction in $\mathbb{Z}$ — additive inverse

Thm ct'd • distributes over + in $\mathbb{Z}/n\mathbb{Z}$.

$$([a]+[b])\cdot[c] = ([a][c]) + ([b][c])$$

Note $(R, +, \cdot)$ satisfying these properties is called a commutative ring.

Field = commutative ring in which $1 \neq 0$ & multiplicative inverses of nonzero elts exist.

Is $\mathbb{Z}/5\mathbb{Z}$ a field? $[0] \neq [1]$ so only have to check mult inverses of nonzero elts, i.e.

for $[a] \in \mathbb{Z}/5\mathbb{Z}$ need $[b] \in \mathbb{Z}/5\mathbb{Z}$ s.t. $[a][b] = [1]$.

·	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

$8 \equiv 3 \ (5)$?

$8-3 = 5$ a mult. of 5 ✓

$\Rightarrow \mathbb{Z}/5\mathbb{Z}$ is a field!

Experiment Fix a prime p.

Take any $[a] \in \mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}$.

Take powers of $[a]$.

When is $[a]^r = [1]$

$\rightsquigarrow$ Fermat's little theorem.

FLT