Math 4460

3/8/23

Today – integers mod n

Mon – back at school
review for test
new stuff if time

Weds – Test $\underline{1}$
Calculator is fine

Theorem: Let $n \in \mathbb{Z}$ with $n \geq 2$.
Let $x, y \in \mathbb{Z}$.

(1) Either $\overline{x} \cap \overline{y} = \emptyset$ or $\overline{x} = \overline{y}$.

(2) $\overline{x} = \overline{y}$
iff $x \equiv y \pmod{n}$
iff $x \in \overline{y}$ ← (or $y \in \overline{x}$)

(3) A complete set of distinct equivalence classes modulo n is given by $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$.
That is, if $z \in \mathbb{Z}$ then $\overline{z} = \overline{r}$ for a unique integer r with $0 \leq r \leq n-1$.

Moreover, r is the remainder when you divide z by n.

Ex: $n = 3$

$\overline{10} = \overline{1}$

$z = 10$

$$\begin{array}{r} 3 \\ 3 \overline{)\,10} \\ \underline{-9} \\ 1 \end{array}$$

$\boxed{r}$

$z = 10,\ n = 3$
$10 = 3 \cdot 3 + 1$

proof: ① and ② are in the HW.

Let's prove ③

Let $z \in \mathbb{Z}$.

By the division algorithm

$$z = qn + r$$

where $q, r \in \mathbb{Z}$ and $\boxed{0 \le \underbrace{r \le n-1}_{r<n}.}$

Then, $z - r = nq$.

Thus, $n \mid (z-r)$.

So, $z \equiv r \pmod{n}$.

By part ② this implies $\boxed{\overline{z} = \overline{r}.}$

Thus, $\overline{z} \in \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$

ie $\overline{z}$ is one of $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$.

All we have to show is that none of $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ are equal, they are all distinct.

Suppose $0 \leq a \leq b \leq n-1$ with $\overline{a} = \overline{b}$.

We will show that this implies that $a=b$.

Since $a \leq b \leq n-1$ we have

subtract by a

$$0 \leq b-a \leq \underbrace{n-1-a}_{\leq n-1}$$

Thus, $\boxed{0 \leq b-a \leq n-1}$

Since $\overline{a} = \overline{b}$, by part 2 of this theorem, this tells us that $a \equiv b \pmod{n}$.

So, $\boxed{n \mid (b-a)}$.

The only way we can have $0 \leq b-a < n$ and $n \mid (b-a)$ is if $b-a=0$.

Thm from topic 1

Thus, $a=b$.

$\blacksquare$

<u>Def</u>: Let $n \in \mathbb{Z}$ with $n \geq 2$.

Define

$$\mathbb{Z}_n = \{ \overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1} \}$$

$\mathbb{Z}_n$ is called the <u>set of integers modulo n.</u>

Ex: $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

and so on...

We want to define $+$ and $\cdot$ in $\mathbb{Z}_n$.

What if we just define it this way?

$$\bar{a} + \bar{b} = \overline{a+b}$$

$$\bar{a} \cdot \bar{b} = \overline{ab}$$

But is this definition well-defined?

What do we mean by this question?

Consider $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.

Using the proposed definition

$$\overline{1} + \overline{2} = \overline{1+2} = \overline{3} = \overline{0}$$

From thm

$3 \equiv 0 \pmod 3$
so
$\overline{3} = \overline{0}$ in $\mathbb{Z}_3$

There are an infinite number of ways to describe $\overline{1}$ and $\overline{2}$. If we redescribe them do we get the same answer?

For example, $\overline{1} = \overline{4}$ in $\mathbb{Z}_3$ because $1 \equiv 4 \pmod 3$ and $\overline{2} = \overline{-10}$ because $2 \equiv -10 \pmod 3$. And

$$\underbrace{\overline{4} + \overline{-10}}_{\text{this better be the same as } \overline{1}+\overline{2}} = \overline{4-10} = \overline{-6} = \overline{0}$$

$\boxed{-6 \equiv 0 \pmod 3}$

We get the same answer in this case.

Theorem (Addition and multiplication in $\mathbb{Z}_n$ are well-defined)

Let $n \in \mathbb{Z}$ with $n \geq 2$.
Given $x, y \in \mathbb{Z}$, the operations

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

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

are well-defined in $\mathbb{Z}_n$.

need to show this step

proof: Let $a, b, c, d \in \mathbb{Z}$.
Suppose $\overline{a} = \overline{b}$ and $\overline{c} = \overline{d}$.
We want to show that

$$\overline{a} + \overline{c} = \overline{a+c} = \overline{b+d} = \overline{b} + \overline{d}$$

and $\overline{a} \cdot \overline{c} = \overline{ac} = \overline{bd} = \overline{b} \cdot \overline{d}$.

Since $\overline{a} = \overline{b}$ and $\overline{c} = \overline{d}$ we know
$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

previous thm from today

By a theorem in class this implies that
$(a+c) \equiv (b+d) \pmod{n}$ and $ac \equiv bd \pmod{n}$.
But then $\overline{a+c} = \overline{b+d}$ and $\overline{ac} = \overline{bd}$. $\blacksquare$

Ex: $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

Let's do some calculations in $\mathbb{Z}_7$.

$$\bar{5} + \bar{6} = \overline{5+6} = \overline{11} = \bar{4}$$

$$\boxed{11 \equiv 4 \pmod{7}}$$

$$(\bar{5} \cdot \bar{6}) \cdot \bar{4} = \overline{30} \cdot \bar{4} = \overline{120} = \bar{1}$$

remainder

$$\boxed{\begin{array}{r} 17 \\ 7\overline{)120} \\ -7 \\ \hline 50 \\ -49 \\ \hline 1 \end{array}}$$

$$\bar{6}^8 = \overline{1{,}679{,}616} = \bar{1}$$

$$\boxed{\begin{array}{l} 239945 \\ 7\overline{)1679616} \\ -14 \\ \hline \;27 \\ -21 \\ \hline \;69 \\ -63 \\ \hline \;66 \end{array}}$$

Another idea:

$$\overline{6}^8 = \overline{6}^2 \cdot \overline{6}^2 \cdot \overline{6}^2 \cdot \overline{6}^2$$

$$= \overline{36} \cdot \overline{36} \cdot \overline{36} \cdot \overline{36}$$

$$= \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{1} = \overline{1}$$

$\overline{36} = \overline{1}$

$36 \equiv 1 \pmod 7$

$$\begin{array}{r} 5 \\ 7 \overline{)36} \\ -35 \\ \hline 1 \end{array}$$

$$\begin{array}{r} -63 \\ \hline 31 \\ -28 \\ \hline 36 \\ -35 \\ \hline 1 \end{array}$$