new schedule

M	W
10/7	10/9
class workshop review	Test 1
M 11/4	W 11/6
class Workshop review	Test 2

9/23

Monday

Recall

If $\sim$ is an equivalence relation on S, then $S/_{\sim}$ is the set of equivalence classes for $\sim$

$\mathbb{Z}_n$ is the set of equivalence classes for the equivalence relation modulo n. $\Big\}$ $\mathbb{Z}_n = \mathbb{Z}/_{\equiv}$

Ex: $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ and given any $x \in \mathbb{Z}$ either $\overline{x} = \overline{0}$ or $\overline{x} = \overline{1}$ or $\overline{x} = \overline{2}$

...s an equivalence
...n on S, then
... is the set of
...alence classes for $\sim$

... of equivalence
...e equivalence
n.

$\mathbb{Z}_n = \mathbb{Z}/\equiv$

$\ldots, \bar{2}\}$ and given any $x \in \mathbb{Z}$
either $\bar{x} = \bar{0}$ or $\bar{x} = \bar{1}$
or $\bar{x} = \bar{2}$

For example,
take $x = 32$.

$$\begin{array}{r} 10 \\ 3\,\overline{)\,32} \\ -30 \\ \hline 2 \end{array}$$

the remainder
is the equivalence
class we
want

$32 = 3(10) + 2$

$32 - 2 = 3(10)$

$3 \mid (32 - 2)$

So, $32 \equiv 2 \pmod 3$

So, $\overline{32} = \bar{2}$.

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

Then,

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

Furthermore, if $0 \leq x \leq y \leq n-1$ and $\overline{x} = \overline{y}$, then $x = y$.

This part says that none of $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ are equal. They are all distinct.

Ex: $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

and none of these elements are equal

Proof of theorem

Let $S = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

Let's show that $S = \mathbb{Z}_n$.

We know $S \subseteq \mathbb{Z}_n$ because S consists of equivalence classes.

Now let's show that $\mathbb{Z}_n \subseteq S$.

Recall that

$$\mathbb{Z}_n = \{\overline{x} \mid x \in \mathbb{Z}\}.$$

Let $\overline{x} \in \mathbb{Z}_n$ where $x \in \mathbb{Z}$.

By the division algorithm there exist $q, r \in \mathbb{Z}$ with $x = qn + r$ and $0 \leq r < n$.

So, $x - r = qn$.

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

Hence $x \equiv r \pmod{n}$.

So, $\overline{x} = \overline{r}$.

$\boxed{\text{Ex:}}$

$n = 3$

$x = 32$

$32 = 10 \cdot 3 + 2$

$x = qn + r$

So, $\overline{32} = \overline{2}$

Since $0 \le r \le n-1$ and $\overline{x} = \overline{r}$

we have $\overline{x} \in S$.

Therefore, $\mathbb{Z}_n = S = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Now we prove the furthermore part of the theorem.

Suppose $0 \le x \le y \le n-1$ and $\overline{x} = \overline{y}$

where $x, y \in \mathbb{Z}$.

We want to show that $x = y$.

Since $\overline{x} = \overline{y}$ we know by the super-duper equivalence class theorem that

$x \equiv y \pmod{n}$.

So, $\boxed{n \mid (y-x).}$

Using $0 \leq x \leq y \leq n-1$ we get $-x \leq 0 \leq y-x \leq n-1-x$,

Note that $n-1-x < n$.

So,

$$\boxed{0 \leq y-x < n.}$$

Since $n \mid (y-x)$ we have

$nq = (y-x)$ for some $q \in \mathbb{Z}$.

Note that $q \geq 0$ since $n \geq 2$ and $y-x \geq 0$.

<u>Goal:</u> Show $q = 0$.

Suppose to the contrary that $q > 0$.
Then,

$$\underbrace{0 \le y-x < n}_{\text{known}} \underset{\boxed{\text{since } q \ge 1}}{\le} nq \underset{\boxed{\text{known}}}{=} y-x.$$

But then

$$y-x < y-x.$$

Contradiction.

So, $q=0$ and $y-x=nq=0$. Thus, $y=x$. $\blacksquare$

Ex:

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

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

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

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

$\vdots \qquad \vdots$

Unsolved math problem

Given an integer m can we express m in the form

$$m = x^3 + y^3 + z^3$$

where $x, y, z \in \mathbb{Z}$?

Ex:

$m = 0$

$0 = 0^3 + 0^3 + 0^3$

Ex: $m = 1$

$1 = 1^3 + (-1)^3 + 1^3$

Ex: $m = 2$

$2 = 0^3 + 1^3 + 1^3$

Ex: There are no solutions to

$4 = x^3 + y^3 + z^3$

$+0^3$

$+1^3$

Ex: $m=2$

$$2=0^3+1^3+1^3$$

Ex: There are no solutions to

$$4=x^3+y^3+z^3$$

Recently (2019)

$$33=x^3+y^3+z^3$$

and

$$42=x^3+y^3+z^3$$

were solved.

$$33=8866128975287528^3+(-8778405442862239)^3+(-2736111468807040)^3$$

It can be shown that if $m \equiv 4 \pmod 9$ or $m \equiv 5 \pmod 9$ then there do not exist $x,y,z \in \mathbb{Z}$ with

$$m=x^3+y^3+z^3.$$

Theorem: Let $n, a, b, c, d \in \mathbb{Z}$ with $n \geq 2$.
If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

$$(a+c) \equiv (b+d) \pmod{n}$$

and $ac \equiv bd \pmod{n}$.

Proof: Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.
Then $n \mid (a-b)$ and $n \mid (c-d)$.

So, $nk = a - b$ and $n\ell = c - d$ where $k, \ell \in \mathbb{Z}$

Then

$$(a+c)-(b+d) = (a-b)+(c-d) = nk + n\ell = n[k+\ell].$$

Since $k+\ell \in \mathbb{Z}$ we get that $n \mid [(a+c)-(b+d)]$

So, $(a+c) \equiv (b+d) \bmod n$.

Also,

$$ac-bd = a(\underbrace{n\ell+d}_{c}) - (\underbrace{a-nk}_{b})d$$

$$= an\ell + ad - ad + nkd$$

$$= n[a\ell + kd].$$

Since $a\ell+kd \in \mathbb{Z}$ we get that $n \mid (ac-bd)$.

So, $ac \equiv bd \pmod{n}$. $\blacksquare$