Weds
1/29

Week 2

$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$

is the set of integers.

Def 1: Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say that a divides b if there exists $k \in \mathbb{Z}$ where $b = ak$. If such a k exists then we write

a

a

of

If

the

doe

Wr

$\ldots\}$

$).$

$k.$

rite

$a \mid b$ and say that a is a <u>factor</u> or <u>divisor</u> of b.

If there is no such k then we say that a <u>does not divide</u> b and write $a \nmid b$.

$\boxed{\text{Ex 2}}$ $2 \mid 8$ since

$$8 = (2)\underbrace{(4)}_{k}$$

$\boxed{\text{Ex 3}}$ $3 \nmid 7$

since there is no integer k with $7 = 3k$ [You'd need $k = \frac{7}{3}$ which isn't an integer.]

Theorem 4 (Division Algorithm)

Let $a,b \in \mathbb{Z}$ with $b>0$ then there exists unique $q,r \in \mathbb{Z}$ with $a=bq+r$ and $0 \leq r < b$.

Ex 5

$a=133$

$b=21$

$$\begin{array}{r} 6 \leftarrow q \\ 21\overline{)133} \\ -126 \\ \hline 7 \leftarrow r \end{array}$$

$$\begin{array}{ccccc} 133 & = & (21) & (6) & +7 \\ a & = & b & q & +r \end{array}$$

and $0 \leq 7 < 21$

$0 \leq r < b$

Def 6

Let $a,b,$

$n \geq 2$. W

a is congr

if $n|(a-$

9

r

$+7$

$+r$

and

$0 \leq 7 < 21$

$0 \leq r < b$

Def 6

Let $a, b, n \in \mathbb{Z}$ with $n \geq 2$. We say that a is congruent to b modulo n if $n \mid (a-b)$. If this is so then we write $a \equiv b \pmod{n}$. If $n \nmid (a-b)$ then we write $a \not\equiv b \pmod{n}$.

Ex 7:

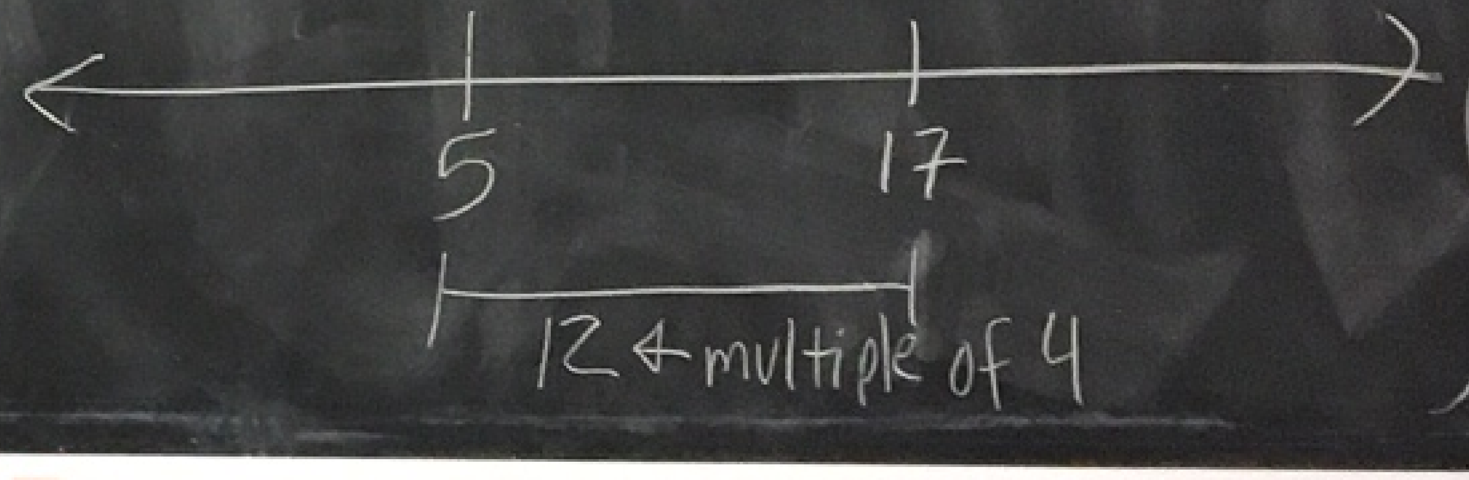
$n = 4$

$a = 5$

$b = 17$

$$\underbrace{5-17}_{a-b} = -12 = \underbrace{4(-3)}_{n(-3)}$$

So, $4 \mid (5-17)$. So, $5 \equiv 17 \pmod{4}$



$\boxed{5-17=4(-3)}$

Ex 8: $n = 4$

$4 \mid (-4-8)$

$-4 \equiv 8 \pmod{4}$

$-7 \equiv -3 \pmod{4}$

$0 \equiv 8 \pmod{4}$

$4 \mid (0-8)$

mod 4 breaks the integers into 4 classes of numbers

Thm 9 Let $a,b,n \in \mathbb{Z}$ with $n \geqslant 2$. Then $a \equiv b \pmod{n}$ iff there exists $k \in \mathbb{Z}$ with $a-b=nk$.

Ex 10: Let $x \in \mathbb{Z}$ and $n=4$. By the division algorithm there exist unique $q,r \in \mathbb{Z}$ with $x=4q+r$ and $0 \leq r < 4$. So,

$$x=4q+0 \ \boxed{\text{or}}\ x=4q+1 \ \boxed{\text{or}}\ x=4q+2 \ \boxed{\text{or}}\ x=4q+3.$$

That is, $x-0=4q \ \boxed{\text{or}}\ x-1=4q \ \boxed{\text{or}}\ x-2=4q \ \boxed{\text{or}}\ x-3=4q.$

So, $x \equiv 0 \pmod{4} \ \boxed{\text{or}}\ x \equiv 1 \pmod{4} \ \boxed{\text{or}}\ x \equiv 2 \pmod{4} \ \boxed{\text{or}}\ x \equiv 3 \pmod{4}.$

Thm 11 Let $x, n \in \mathbb{Z}$ with $n \geq 2$. Then x is congruent to exactly one of

$$0, 1, 2, \ldots, n-1.$$