Math 321

4.1 $x|y$ is $x \cdot n = y \quad n \in \mathbb{Z}$

$a = d \cdot q + r \qquad 0 \le r < d$

dividend = divisor · quotient + remainder

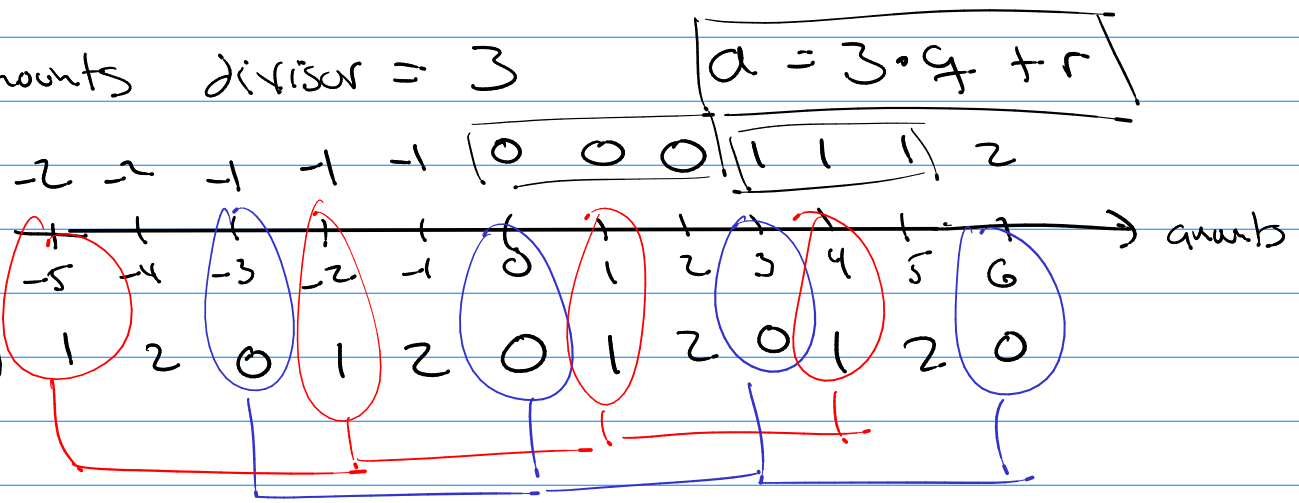
$q = a \text{ div } d$

$r = a \bmod d$

ex amounts divisor = 3 $\boxed{a = 3 \cdot q + r}$

div

mod



$\{ \ldots, -6, -3, 0, 3, 6, \ldots \}$ ← all congruent.

$\{ \ldots, -5, -2, 1, 4, 7, \ldots \}$

$\{ \ldots, -4, -1, 2, 5, 8, \ldots \}$

Congruence

Notation: $a \equiv b \pmod m$ or $a \underset{m}{\equiv} b$

def: $m \mid (a-b)$

Th^m $a \underset{m}{\equiv} b$ the following are equivalent

Def ① $m \mid (a-b)$ "a, b are a multiple of m apart"

② $a \bmod m = b \bmod m$ "equal remainders"

③ $a = b + km, \quad k \in \mathbb{Z}$

Ex under mod 3

$\{\ldots, -6, -3, 0, 3, 6, \ldots\} \ldots \underset{3}{\equiv} -6 \underset{3}{\equiv} -3 \underset{3}{\equiv} 0 \underset{3}{\equiv} 3 \underset{3}{\equiv} \ldots$

$\{\ldots, -5, -2, 1, 4, 7, \ldots\} \quad \ldots \underset{3}{\equiv} -2 \underset{3}{\equiv} 1 \underset{3}{\equiv} 4 \underset{3}{\equiv} 7 \underset{3}{\equiv} \ldots$

$\{\ldots, -4, -1, 2, 5, 8, \ldots\} \ldots \underset{3}{\equiv} -4 \underset{3}{\equiv} -1 \underset{3}{\equiv} 2 \underset{3}{\equiv} 5 \underset{3}{\equiv} 8 \underset{3}{\equiv} \ldots$

#15 $(a \bmod m = b \bmod m) \rightarrow a \underset{m}{\equiv} b$

Def: $m \mid (a-b) \equiv (m \cdot k = (a-b))$ ← Def

Pf assume $a \bmod m = b \bmod m$

① $a = mq_1 + r_1$ ② $b = mq_2 + r_2$

know $r_1 = r_2$ ←

$\rightarrow \quad a - b = (mq_1 + r_1) - (mq_2 + r_2)$

$= mq_1 - mq_2 + r_1 - r_2 = 0$ b/c they are equal

$= mq_1 - mq_2 = m(q_1 - q_2)$

(50) $n \mid (a-b)$ so $a \equiv_n b$ ✓

We know properties of equality.

→ properties of congruence ... mod 5

$a \equiv_n b \qquad c \equiv_n d$

(1) $a + c \equiv_n b + d$

(2) $a \cdot c \equiv_n b \cdot d$

(2c) mod 5

$\ldots -5 \equiv_5 0 \equiv_5 5 \equiv_5 10 \ldots$

$\ldots -4 \equiv_5 1 \equiv_5 6 \equiv_5 11 \ldots$

$2 \equiv_5 7 \equiv 12 \ldots$

$3 \equiv 8 \equiv 13$

$-1 \equiv 4 \equiv 9 \equiv 14$

$3 \cdot x + 1 \equiv_5 14$

$3x + 1 \equiv_5 4$

$3x \equiv_5 3$ bc $1 \equiv_5 6$

$2 \cdot 3x \equiv_5 2 \cdot 2$

$6x \equiv_5 4$

$x \equiv_5 4$ $\{\ldots, -6, -1, 4, 9, 13, \ldots\}$

Corollary

$$(a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n$$

$$(a \cdot b) \bmod n = (a \bmod n)(b \bmod n) \bmod n$$

Ex $\left(4^{1001} + 10^{10^{10}}\right) \bmod 3 = (1+1) \bmod 3$

$4 \equiv 1 \pmod 3$, $10 \equiv 1 \pmod 3$

$= \boxed{2}$

$4^{1001} \bmod 15 = 4 \bmod 15 = \boxed{4}$

$16 \equiv_{15} 1$

Numbers and their representations

$\boxed{1231} = 1 \cdot 1000 + 2 \cdot 100 + 3 \cdot 10 + 1$

positional representation $= 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 1 \cdot 10^0$

any base $n = a_k b^k + \cdots + a_2 b^2 + a_1 b + a_0$

$= \boxed{(a_k, \ldots, a_2, a_1, a_0)_b}$

$$(1,3,7,0,2)_9 = 1\cdot 9^4 + 3\cdot 9^3 + 7\cdot 9^2 + 0\cdot 9^1 + 2$$

(15) $(1,2,3,1)_{10}$

Note: try to do base 10 $+, *$ for several problems.