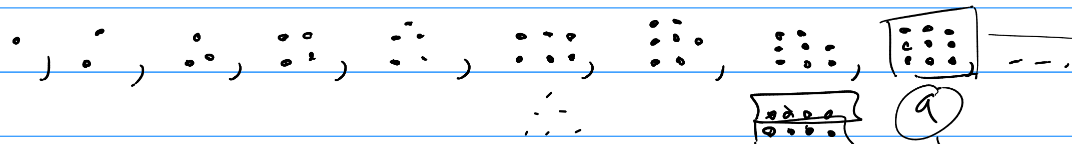
Math 321

Ch 4 Number theory (Study of $\mathbb{Z}^+$ extended to $\mathbb{Z}$)

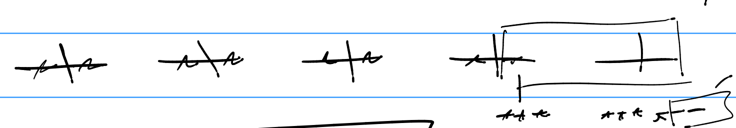


9 — figure representation of a number

Unary (tally) 16 — sixteen ~~||||~~ ~~||||~~ ~~||||~~ |

Applications: ① Metric of value (How much?)

② Sharing: egyptian fractions $\frac{5}{7} = 5\left(\frac{1}{7}\right)$



$\frac{1}{6} + \frac{1}{6}$

$\frac{1}{12}$

$\frac{5}{7} = \boxed{\frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \frac{1}{84}}$

$= \frac{1}{7} + \frac{1}{7} + \frac{1}{7} + \frac{1}{7} + \frac{1}{7}$

$7(12)$

$7(10+2)$

4.1 Sharing $\boxed{\text{Divisibility}}$

Q can b objects be shared by a people fairly?

Def $\boxed{a \mid b}$ says $\boxed{a \cdot c = b}$ c is an integer.

"a divides b"

"a is a factor of b"

"b is a multiple of a"

ex $\quad 4 \mid -20 \quad$ b/c $\quad 4 \cdot (-5) = -20$

if not true use $a \nmid b$

ex $\quad 4 \nmid -21 \quad$ b/c $\quad 4 \cdot (\ ) = -21$ $\quad$ no integer k

---

Thm ① $a \mid b \wedge a \mid c \rightarrow a \mid (b+c)$ $\quad$? $a \cdot (\ ) = b+c$

pf $\quad a \cdot k_1 = b \wedge a \cdot k_2 = c \rightarrow b+c = ak_1 + ak_2$
$= a(k_1 + k_2)$ ☒

② $a \mid b \rightarrow \forall c,\ a \mid (b \cdot c)$

$b \cdot c$ " $\underbrace{b+b+b+\dots+b}_{c \text{ times}}$

③ $a \mid b \wedge b \mid c \rightarrow a \mid c$

pf $\quad a \cdot k_1 = b \wedge b \cdot k_2 = c \rightarrow a \cdot k_1 \cdot k_2 = c \rightarrow a \mid c$ ☒

Doing the sharing ..

Division Algorithm $\quad a \in \mathbb{Z},\ d \in \mathbb{Z}^+ \quad a = d \cdot q + r$
$0 \le r < d$

ex $\quad$ 7 cats $\quad$ 2 pirates $\quad 2 \nmid 7$

$|||||||\ = (|||) + (|||) + (|)$ $\quad \boxed{7 = 2 \cdot 3 + 1}$

$a \in \mathbb{Z}$ $\quad d \in \mathbb{Z}^+$ $\quad \boxed{a = dq + r}$ $\quad 0 \le r < d$

$a \equiv$ dividend $\quad q \equiv$ quotient

$d \equiv$ divisor $\quad r \equiv$ remainder

$$q = a \text{ div } d = \text{div}(a, d)$$
$$r = a \text{ mod } d = \text{mod}(a, d)$$

$21 and 4 people

$$21 = 4(5) + (1)$$
$$21 \text{ div } 4 = 5$$
$$21 \text{ mod } 4 = 1$$

-$21 bill and 4 people

$$-21 = 4(-6) + (3)$$
$$-21 \text{ div } 4 = -6$$
$$-21 \text{ mod } 4 = 3$$

Modulus

ex mod 3 →

	-4	-3	-2	-1	0	1	2	3	4
...	2	0	1	2	0	1	2	0	1

Congruence $\quad a \equiv b \pmod{m}$ $\qquad a \underset{m}{\equiv} b$

iff Def ① $m \mid (a-b)$ &

thm ② $a \text{ mod } m = b \text{ mod } m$

③ $a = b + m \cdot k \qquad k \in \mathbb{Z}$

ex (under mod 7) $\ldots \underset{7}{\equiv} -9 \underset{7}{\equiv} -2 \underset{7}{\equiv} 5 \underset{7}{\equiv} 12 \underset{7}{\equiv} 19 \underset{7}{\equiv} \ldots$

Thm $a \underset{m}{\equiv} b$, $c \underset{m}{\equiv} d$

① $a + c \underset{m}{\equiv} b + d$

② $ac \underset{m}{\equiv} bd$ $\qquad -2 \underset{7}{\equiv} 5 \underset{7}{\equiv} 12 \underset{7}{\equiv} 19 \underset{7}{\equiv} 26 \underset{7}{\equiv} 33 \equiv 40$

ex Solve $\overset{5}{\cancel{33}}x + \overset{5}{\cancel{26}} \underset{7}{\equiv} 4$

$5x + 5 \underset{7}{\equiv} 4$

Applied to $a \bmod m$

① $(a+b) \bmod m = (a \bmod m + b \bmod m) \bmod m$

② $(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

ex $(123 + 7^3)^{1001} \bmod 6$ $\qquad 123 \underset{6}{\equiv} 3$

$(3 + 1^3)^{1001} \bmod 6$ $\qquad 7 \underset{6}{\equiv} 1$

$4^{1001} \bmod 6$

$16 \underset{6}{\equiv} 2$

$4 \cdot 4^{1000} \bmod 6$

$4 \cdot (4^2)^{500} \bmod 6 = 4 \cdot 2^{500} \bmod 6$

$16 \underset{6}{\equiv} 2$

4.2 n is an integer $\qquad$ base 10, base 2, base b representations.

123