Math 321

Number Theory

- $\cdot \equiv$ reason
- $\cdot\cdot \equiv$ female / opinion
- $\therefore \equiv$ harmony / 1st true male

$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$

$\frac{a}{b}$ is a rational $\rightarrow$ $a \cdot \frac{1}{b}$

$\boxed{\text{Division}}$

8 sticks and 3 people

$\underset{P_1}{||} + \underset{P_2}{||} + \underset{P_3}{||} + \underbrace{||}_{\text{remainders}}$

$$8 = 3 \cdot 2 + 2$$

$p, T \in \mathbb{Z}$, $p \neq 0$

$p \mid T$ reads "p divides T"

if there is a $c \in \mathbb{Z}$ such that $p \cdot c = T$

def: p and c are factors of T

T is a multiple of p and c.

if no such c exists $p \nmid T$

ex

$3 \mid 12$ why? $3 \cdot 4 = 12$

$-4 \mid 16$ why? $(-4)(-4) = 16$

$5 \mid -15$ why? $(5)(-3) = -15$

$2 \nmid 13$

$3 \nmid 13$

$s \mid 9$ rewrite as $\exists t (s \cdot t = 9)$

Diophantine Equations.

→ only consider integers as possible solutions.

ex $a^2 + b^2 = c^2 \quad (a, b, c \in \mathbb{Z}^+)$

$\boxed{a \cdot c = b}$ ✓ $\quad a \mid b$

$a \cdot m + b \cdot n = N$

Thm: $a, b, c \in \mathbb{Z}$ then

① $a \mid b \wedge a \mid c \rightarrow a \mid (b+c)$

pf: $a \mid b \rightarrow \boxed{a \cdot k = b}$ for some k

$a \mid c \rightarrow \boxed{a \cdot l = c}$ for some l

So $(b+c) = (a \cdot k + a \cdot l) = a \cdot (k+l)$

$\rightarrow$ by def $a \mid (b+c)$

Def: $\boxed{\square \mid \triangle} \Leftrightarrow \exists z \in \mathbb{Z} \; \boxed{\square \cdot z = \triangle}$

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

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

pf: $a \cdot k = b \wedge b \cdot l = c$

$\rightarrow (a \cdot k) \cdot l = c$

$a \cdot (kl) = c \xrightarrow{\text{by def.}} a \mid c$

Corollary $a, b, c \in \mathbb{Z} \wedge a \mid b \wedge a \mid c$

$\rightarrow \forall m \in \mathbb{Z}\, \forall n \in \mathbb{Z}\, (a \mid mb + nc)$

Note: $a \mid mb + nc$

can be rewritten by the def. as

$a \cdot k = (mb + nc)$ for some $k \in \mathbb{Z}$

$a \mid b$ means $b = a \cdot c + 0$

nothing left.

but what about left overs?

Division Algorithm

$a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$, $r \in \mathbb{Z}$, $0 \le r < d$

$$\exists! q \, \exists! r \, (a = d \cdot \boxed{q} + \boxed{r})$$

from 1st example: $8 = 3 \cdot 2 + 2$

$$16 = 5 \cdot 3 + 1$$

$$-16 = 5 \cdot (-4) + 4$$

Names: $q \equiv$ quotient $\qquad r \equiv$ remainder ✓

$d \equiv$ divisor $\qquad a \equiv$ dividend

$$\boxed{q = a \text{ div } d}$$

$$\boxed{r = a \bmod d}$$

Modulus:

$a \equiv b \pmod{p}$

① $a \mid (b-c)$

② $a \bmod p = b \bmod p$

③ $a = b + K \cdot p$