Integers

divisibility
modulor arithmetic
prime numbers
interpers & algoritms

$a, b \in \mathbb{Z}$, $a \neq 0$

$a \mid b$ if there exists an integer c s.t.

$b = a.c$ or equivalently b/a is an integer.

$a \mid b$: a divides b $\qquad 3 \mid 12$

$a \nmid b$: $\qquad 5 \nmid 12$

- $a \mid b$ and $a \mid c \rightarrow a \mid b+c$

$b = a.t_1 \qquad a+b = a.t_1 + a.t_2$

$c = a.t_2 \qquad = a(t_1 + t_2)$

- $a \mid b \rightarrow a \mid b.c$
- $\underset{2}{a} \mid \underset{6}{b}$ and $\underset{6}{b} \mid \underset{30}{c}$ then $\underset{2}{a} \mid \underset{30}{c}$ $\left(\begin{array}{ll} b = a.t_1 & c = a.t_1.t_2 \\ c = b.t_2 & \end{array} \right.$

Thm $\forall\, a, d \in \mathbb{Z}$, $d > 0$ $\exists$ unique $q, r \in \mathbb{Z}$

s.t. $0 \leq r < d$ and

$$\underbrace{a}_{\text{dividend}} = \underbrace{d}_{\text{divisor}} . \underbrace{q}_{\text{quotient}} + \underbrace{r}_{\text{remainder}}$$

$q = a \text{ div } d$ (integer part)

$r = a \bmod d$

proof (1) existence $a > 0$

$q.d \leq a < (q+1).d$ $\qquad r = a - q.d$

$a = q.d + r \qquad 0 \leq r < d$

(2) uniqueness proof by contradiction

$a = q_1 \cdot d + r_1$ $a = q_2 \cdot d + r_2$

$\rightsquigarrow q_1 d + r_1 = q_2 d + r_2$

$\rightsquigarrow (q_1 - q_2) d = r_2 - r_1$

$\underbrace{\underbrace{|q_1 - q_2|}_{>0} d}_{\geq d} = \underbrace{|r_2 - r_1|}_{< d}$ $0 \leq r_1 < d$ $0 \leq r_2 < d$

$\perp$

ex 123, 12 $123 = 12 \times \underbrace{10}_{\text{quotient}} + \underbrace{3}_{\text{remainder}}$

$-15, 6$ $-15 = -3 \times 6 + \underbrace{3}_{\text{remainder}}$

Def $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}_+$
a is congruent to b modulo m if $m \mid a-b$

$a \equiv b \pmod m$

$11 \equiv 5 \pmod 6$ $6 \mid 6$ $6 \mid (11-5)$

$11 \equiv 17 \pmod 6$ $6 \mid 6$ $6 \mid \underbrace{11-17}_{-6}$

$11 \not\equiv 3 \pmod 6$

Thm $a \equiv b \pmod m$ iff $\exists\, k \in \mathbb{Z}_+$ s.t. $a = b + k.m$

$m \mid a - b$ $a - b = m.k \Rightarrow a = b + k.m$

Thm $m \in \mathbb{Z}_+$ If $a \equiv b \pmod m$ and $c \equiv d \pmod m$

$a + c \equiv b + d \pmod m$

$a.c \equiv b.d \pmod m$

Proof $m \mid a-b$ $\qquad a-b = m \cdot t_1$

$m \mid c-d$ $\qquad c-d = m \cdot t_2$

$$a+c-(b+d) = m.(t_1+t_2)$$

$$m \mid (a+c)-(b+d)$$

$$a+c \equiv b+d \pmod m$$

$b \equiv a \pmod m$ $\quad m \mid b-a$

$a \equiv b \pmod m$ $\quad m \mid a-b$

remainder $\boxed{a \bmod m} = b$

function, it gives remainder

$b \in \{0, \ldots, m-1\}$

$a \operatorname{div} m = \lfloor a/m \rfloor$

quotient

$3 \equiv 8 \pmod 5$

$3 \equiv 13 \pmod 5$

$13 \bmod 5 = 3$

$8 \bmod 5 = 3$

$3 \bmod 5 = 3$

0, 1, 2, 3, 4

$\mathbb{Z}_m$: non-negative integers less than m

$\{0, 1, \ldots, m-1\}$

arithmetic operations on $\mathbb{Z}_m$

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

$$a \cdot_m b = (a.b) \bmod m$$

$$11 +_{12} 23 = 10$$

$$11 +_{14} 7 = 4$$

$$9 \cdot_{10} 7 = 3$$

$3 \bmod 5 \neq 8$

$3 \equiv 8 \pmod 5$

$8 \equiv 3 \pmod 5$

$8 \bmod 5 = 3$