

Teorema: le operazioni $+$ e \cdot in \mathbb{Z} sono compatibili con \sim_n cioè

$$\text{se } a \sim_n b \quad a' \sim_n b' \Rightarrow a+a' \sim_n b+b' \\ a \cdot a' \sim_n b \cdot b'$$

dimostrazione: (per $+$)

$$a \sim_n b \Rightarrow a-b = kn$$

$$a' \sim_n b' \Rightarrow \underline{a'-b' = hn}$$

$$a+a'-b-b' = kn+hn$$

$$(a+a')-(b+b') = (k+h)n$$

$$\Rightarrow a+a' \sim_n b+b'$$

Def: $+_n: \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ è

$$([a]_n, [b]_n) \mapsto [a+b]_n =: [a]_n +_n [b]_n$$

$\cdot: \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ è

$$([a]_n, [b]_n) \mapsto [a \cdot b]_n =: [a]_n \cdot_n [b]_n$$

es $\forall_n \quad \mathbb{Z}_2 = \{[0]_2, [1]_2\}$

$$[0] + [0] = [0+0] = [0]$$

$$[0] + [1] = [0+1] = [1]$$

$$[1] + [0] = [1+0] = [1]$$

$$[1] + [1] = [1+1] = [2] = [0]$$

$$(\mathbb{Z}_3, \cdot) \quad [0] \cdot [0] = [0 \cdot 0] = [0]$$

$$[0] \cdot [1] = [0 \cdot 1] = [0]$$

$$[0] \cdot [2] = [0]$$

$$[1] \cdot [1] = [1]$$

$$[1] \cdot [2] = [2]$$

$$[2] \cdot [2] = [4] = [1]$$

Oss: Il prodotto e la somma in \mathbb{Z}_n sono definiti "usando" il \cdot e la somma in \mathbb{Z}

\Rightarrow sono associativi e commutativi

$$([a] \cdot [b] = [a \cdot b]) \sim [b \cdot a] = [b] \cdot [a]$$

\downarrow
sum

$\cdot_n, +_n$ sono commutativi e associativi

$$(\mathbb{Z}_3, +_3)$$

$+_3$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

osservazione $[0]$ è l'elemento neutro di $+_n$
ogni elemento ha un inverso

In generale l'inverso in $+_n$ di $[a]_n$ è la classe $[-a]_n$

es l'inverso di $+_3$ di $[1]_3$ è $[-1]_3$
 $-1 \sim_3 2 \quad -1-2 = -3$

osservazione $[1]_n$ è il neutro di \cdot_n

Proprietà $(\mathbb{Z}_n, +_n, \cdot_n)$ è anello

$(\mathbb{Z}_n, +_n)$ è un gruppo \checkmark

(\mathbb{Z}_n, \cdot_n) è monoide \checkmark

$$\rightarrow [a]_n \cdot_n ([b]_n + [c]_n) = [a \cdot (b+c)]_n =$$

\uparrow in \mathbb{Z} vale distributiva

$$= [a \cdot b + a \cdot c] = [a \cdot b]_n + [a \cdot c]_n$$

Def: Sia $(A, +, \cdot)$ un anello. Diciamo che $a \in A$
 $a \neq 0_A$ è DIVISORE DELLO ZERO & $\exists b \neq 0, b \in A$
 t.c. $a \cdot b = 0$

Prop: $\forall a \in A \quad a \cdot 0_A = 0_A \cdot a = 0$
 se $a \neq 0$ è un divisore dello zero \Rightarrow
 a non ammette inverso moltiplicativo
 (cioè non esiste $a^{-1} \mid a \cdot a^{-1} = 1$)

Corollario: se A ha dei divisori dello zero \rightarrow
 $(A, +, \cdot)$ non è campo

Teorema: $(\mathbb{Z}_n, +_n, \cdot_n)$ è campo & è solo se
 n è un numero primo

es $(\mathbb{Z}_3, +_3, \cdot_3)$ è campo

$$\rightarrow [1] \cdot [1] = [1]$$

(quindi $[1]$ è inverso di $[1]$)

$$[2] \cdot [2] = [1]$$

(quindi $[2]$ è inverso di $[2]$)

$(\mathbb{Z}_5, +_5, \cdot_5)$

$$\rightarrow [2]_5 \cdot [3]_5 = [6]_5 = [1]_5$$

($[2]_5$ è inverso di $[3]_5$)

es se $n=4$

$[2]_4$ è divisore dello zero $[2]_4 \neq 0$

$$\underset{\neq 0}{[2]_4} \cdot \underset{\neq 0}{[2]_4} = [2 \cdot 2]_4 = [4]_4 = [0]_4$$

Mostro che non ha inverso

$$[2] \cdot [0] = [0] \neq [1]$$

$$[2] \cdot [1] = [2] \neq [1]$$

$$[2] \cdot [2] = [4] = [0] \neq [1]$$

$$[2] \cdot [3] = [6] = [2] \neq [1]$$

Se n non è primo $n = p \cdot q$ $p \neq 1, n$, $q \neq 1, n$

$\Rightarrow [p], [q]$ sono divisori dello zero $[p], [q] \neq 0$

$$[p \cdot q] = [n]_n = [0]$$

INTERI, DIVISIBILITÀ

$\mathbb{N} = \{ \text{numeri interi non negativi} \}$

$\mathbb{Z} = \{ \text{numeri interi} \}$

$(\mathbb{Z}, +, \cdot)$ è quello $(\mathbb{N}, +)$ è un monoid, ma non gruppo

— è operazione in \mathbb{Z} (ma non in \mathbb{N})

: non è operazione in \mathbb{Z}

Def: Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Se esiste $q \in \mathbb{Z}$ t.c.
 $a = b \cdot q$ diciamo:

.) a è divisibile per b

.) a è multiplo di b

.) b divide a o $b | a$

.) b è fattore di a

Es $2 | 12$ $-2 | 12$ $2 | -12$ $-2 | -12$

$2 \nmid 13$

\hookrightarrow non divide

$$\overset{a}{13} : \overset{b}{2} = \overset{q}{6} \text{ con resto } \overset{r}{1} \rightsquigarrow \overset{b}{2} \cdot \overset{q}{6} + \overset{r}{1} = \overset{a}{13}$$

Teorema: Siano $a, b \in \mathbb{Z}$ $b \neq 0 \Rightarrow$ esistono unici $q, r \in \mathbb{Z}$ tali che:

$$\textcircled{1} \quad a = b \cdot q + r$$

$$\textcircled{2} \quad 0 \leq r < |b|$$

- Chiamiamo q quoziente della divisione e r resto della divisione di a per b

Dim: Mostro unicità.

Suppongo che esistano q_1, r_1, q_2, r_2 t.c.

$$\textcircled{1} \quad a = bq_1 + r_1, \quad a = bq_2 + r_2$$

$$\textcircled{2} \quad 0 \leq r_1 < |b|, \quad 0 \leq r_2 < |b|$$

Voglio mostrare che $q_1 = q_2$ e $r_1 = r_2$

$$\begin{array}{r} a = bq_1 + r_1 \\ - \\ a = bq_2 + r_2 \\ \hline \end{array}$$

$$0 = b(q_1 - q_2) + r_1 - r_2 \Rightarrow |r_1 - r_2| = |b(q_1 - q_2)| = |b| |q_1 - q_2|$$

$$\text{ma } |r_1 - r_2| < |b| \quad \text{e} \quad |r_1 - r_2| = |b| |q_1 - q_2| \quad \rightarrow \quad |q_1 - q_2| < 1$$

$$\Rightarrow |q_1 - q_2| = 0 \Rightarrow q_1 = q_2$$

$$|r_1 - r_2| = |b| |q_1 - q_2| = |b| \cdot 0 = 0 \Rightarrow r_1 = r_2$$

Mostro esistenza solo per $a \geq 0 \quad b > 0$

Se $a > 0$ e $a < b \Rightarrow a = b \cdot 0 + a$

cioè scelgo $q=0 \quad r=a < b$

ho trovato q e r

Posso assumere $a > b$

(mostro per induzione)

Primo passo $a=0$ la proprietà è vera

$$q=r=0 \quad a=b \cdot q + r$$

$$0 = b \cdot 0 + r$$

Suppongo vera la proprietà per $a' < a$

la dimostro per a

se è vera per $a' \Rightarrow \exists q', r' \text{ t.c.}$

$$\textcircled{1} \quad a' = q' b + r'$$

$$\textcircled{2} \quad 0 \leq r' < |b|$$

suppongo $a > b \quad a-b > 0 \quad a-b < a$

pongo $|a' = a-b|$ so che $\exists q', r' \text{ t.c.}$

$$a' = b q' + r' \quad 0 \leq r' < b$$

$$a-b = b q' + r' \quad 0 \leq r' < b$$

$$a = b + b q' + r' = b(q'+1) + r'$$

$$\text{pongo } q = q' + 1 \quad r = r'$$

$$0 \leq r = r' < b$$

$\Rightarrow q$ e r esistono

$$\text{es } a=31 \quad b=5 \Rightarrow q=6 \quad r=1$$

$$a=31 \quad b=-5 \Rightarrow q=-6 \quad r=1$$

$$a=-31 \quad b=5 \Rightarrow q=-7 \quad r=4$$

$$"-6-1"$$

$$\begin{aligned} & q \cdot (-1) \\ & (-1)q - 1 \end{aligned}$$

✓ $q(-1)$

Algoritmo per trovare q e r

$$a \geq 0 \quad b \geq 0$$

- ⊙ Pongo $a_0 := a$

- Se $a_0 < b \Rightarrow q_0 = 0 \quad r_0 = a_0 \rightarrow \text{termina}$
altrimenti ($a_0 > b$) $a_0 - b =: a_1$

- ② se $a_1 < b \Rightarrow q_1 = 0 \quad r_1 = a_1 \rightarrow \text{termine}$
 altrimenti $a_2 := a_1 - b$

Se $a_2 < b \leadsto q_2 = 0 \quad r_2 = a_2 \rightarrow \text{termina}$
altrimenti ...

$$a_{i+1} := a_i - b$$

Dopo n passi

$$a_n < b \quad a_n := a_{n-1} - b = (a_{n-2} - b) - b$$
$$\qquad\qquad\qquad |$$
$$\qquad\qquad\qquad = a_0 - nb$$

\Rightarrow Quando $a - nb < b$ l'algoritmo termina

$q = n = \#$ passi dopo cui l'algoritmo termina
e $\pi = a - nb$

Oss: In \mathbb{Z}_n non si fa!

↓
cioè non si fa unicità

Pero in \mathbb{Z}_n la classe di equivalenza è il resto della divisione

$a \in \mathbb{Z}$ voglio capire chi è $[a]_n$

$$a: n \rightarrow \mathbb{Z} \quad \exists g, r \text{ t.c. } a = n \cdot g + r \quad 0 \leq r < n$$

$$\mathbb{Z}_n = \{ [0], [1], \dots, [n-1] \} \ni [r]$$

$$\begin{aligned} a = nq + r \quad [a]_n &= [nq + r]_n = [nq]_n + [r]_n \\ &= [n]_n [q]_n + [r]_n \\ &\stackrel{0}{=} \cdot [q]_n + [r]_n = [r]_n \end{aligned}$$

$$\text{es } [16]_5 = [1]_5$$

$$[31]_5 = [1]_5 \quad [-31]_5 = [4]_5$$

Def: Siano $a, b \in \mathbb{Z} - \{0\}$. Si dice **MASSIMO COMUNE DIVISORE** fra a e b il numero $d \in \mathbb{Z}$ t.c.

① $d|a \quad d|b$

② se $t \in \mathbb{Z} - \{0\}$ è t.c. $t|a \quad t|b \Rightarrow t|d$

scriviamo $d = \text{MCD}(a, b)$

Teorema (algoritmo divisioni successive)

Per ogni coppia di interi non nulli $a, b \in \mathbb{Z} - \{0\}$ esiste un massimo comune divisore d

ed esistono $x, y \in \mathbb{Z}$ t.c.

$$d = a \cdot x + b \cdot y$$

Def: Due numeri $a, b \in \mathbb{Z} - \{0\}$ si dicono **COPRIMI** o primi fra loro se $\text{MCD}(a, b) = \pm 1$

Oss: Se a e b sono coprimi $\Rightarrow 1 = ax + by$
 \downarrow
 d del teorema

Def.: Siano $a, b \in \mathbb{Z} - \{0\}$. Si chiama MINIMO COMUNE MULTIPLO di a e b l'intero n t.c.

① $a \mid n, b \mid n$

② $\forall k$ t.c. $a \mid k, b \mid k \Rightarrow n \mid k$

Considero $(\mathbb{R}[x], +, \cdot)$ anello di polinomi

Teorema: Siano $a(x), b(x) \in \mathbb{R}[x]$ polinomi $b(x) \neq 0$

\Rightarrow esistono unici $q(x), r(x)$ t.c.

$$a(x) = b(x) \cdot q(x) + r(x), \quad 0 \leq \deg r(x) < \deg b(x)$$

$\underbrace{\hspace{1.5cm}}$
grado di $r(x)$

$\Rightarrow q(x)$ è detto quoziente, $r(x)$ resto

Diciamo che $b(x)$ divide $a(x)$ se $\exists q(x)$ t.c.

$$a(x) = b(x)q(x) \quad \text{cioè se } r(x) = 0$$

Teorema: Dato $a(x), b(x) \in \mathbb{R}[x] - \{0\}$ esiste
e massimo comune divisore $d(x)$

ed esistono $\alpha(x), \beta(x)$ t.c.

$$d(x) = \alpha(x) \cdot a(x) + \beta(x) \cdot b(x)$$

Teorema di Ruffini:

Siano $a(x), b(x) \in \mathbb{R}[x]$, e sia $b(x) = x - \xi, \xi \in \mathbb{R}$

\Rightarrow il resto della divisione $a(x) : (x - \xi)$ è
 $a(x) : b(x)$

$a(\xi)$ (è un numero perché $\deg b(x) = 1$ e
 $0 \leq \deg r(x) < \deg b(x) = 1 \Rightarrow \deg r(x) = 0$)

infatti $a(x) = b(x) \cdot q(x) + r(x)$

$$a(x) = (x - \xi) q(x) + r(x)$$

pongo $x = \xi$

$$a(\xi) = \underbrace{(\xi - \xi)}_0 q(\xi) + r(\xi)$$

$$a(\xi) = \underbrace{r(\xi)}_{\text{è un numero}} = r_0$$

$$r(x) = r_0$$

Corollario: $a(x)$ è divisibile per $(x - \xi)$
 se e solo se $a(\xi) = 0$

es $x^2 + x - 2$ $x^3 - x^2 + x - 1$ $x^5 + 7$

sono divisibili per $x - 1$? per $x - 2$?
 $\xi = 1$ $\xi = 2$

$$x^2 + x - 2 = a(x) \quad a(1) = 1 + 1 - 2 = 0 \quad \text{Sì}$$

$$x^3 - x^2 + x - 1 = a(x) \quad a(1) = 1 - 1 + 1 - 1 = 0 \quad \text{Sì}$$

$$x^5 + 7 = a(x) \quad a(1) = 1 + 7 = 8 \neq 0 \quad \text{No}$$