Aritmetica (I parte)

È lo studio delle proprietà dell'insieme dei numeri interi relativi:

$$\mathbb{Z} = \{ \dots -3, -2, -1, 0, 1, 2, 3, \dots \}$$

rispetto alle operazioni di addizione e moltiplicazione.

Addizione:

associativa	$\forall x, y, z \in \mathbb{Z}$	$(x+y)+z = x+(y+z)$
elemento neutro	$\exists\, 0 \in \mathbb{Z}$ t.c. $\forall x \in \mathbb{Z}$	$x+0 = x = 0+x$
opposto	$\forall x \in \mathbb{Z}\ \exists -x \in \mathbb{Z}$ t.c.	$x+(-x) = 0 = (-x)+x$
commutativa	$\forall x, y \in \mathbb{Z}$	$x+y = y+x$

$(\mathbb{Z}, +, 0)$ è un gruppo abeliano

$\mathbb{Z}$ è "generato additivamente" da 1: cioè $2 = 1+1$, $3 = 1+1+1$, $\dots$, $n = \underbrace{1+1+\dots+1}_{n \text{ volte}}$ $(n>0)$

-1 è l'opposto di 1, $-3 = -1-1-1$ $\qquad 0 = 1-1$

Moltiplicazione:

associativa	$\forall x, y, z \in \mathbb{Z}$	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$
el. neutro	$\exists\, 1 \in \mathbb{Z}$ t.c. $\forall x \in \mathbb{Z}$	$x \cdot 1 = x = 1 \cdot x$
commutativa	$\forall x, y \in \mathbb{Z}$	$x \cdot y = y \cdot x$

$(\mathbb{Z}, \cdot, 1)$ è un monoide commutativo

Gli inversi non sono garantiti. Solo ± 1 sono invertibili.

Per generare $\mathbb{Z}$ moltiplicativamente abbiamo bisogno di tutti i numeri primi, oltre che $0, \pm 1$.

Proprietà che lega $+, \cdot$: distributiva : $\forall x, y, z \in \mathbb{Z} \quad x \cdot (y+z) = x \cdot y + x \cdot z$

Una struttura come $(\mathbb{Z}, +, \cdot, 0, 1)$ con le proprietà descritte si chiama anello commutativo unitario.

Divisibilità

Def : Dati $a, b \in \mathbb{Z}$ diciamo che "a divide b", scritto $a \mid b$ se $\exists k \in \mathbb{Z}$ t.c.

$$b = a \cdot k$$

Es : $2 \mid 6$ perché $\underset{b}{6} = \underset{a}{2} \cdot \underset{k}{3}$ $\qquad -4 \mid 12$ perché $12 = (-4) \cdot \underset{k}{(-3)}$

$6 \nmid 9$ perché non esiste $k \in \mathbb{Z}$ t.c. $9 = 6 \cdot k$

Proprietà : $\forall n \in \mathbb{Z} \quad \pm 1 \mid n$ perché $n = 1 \cdot n$ e $n = (-1) \cdot (-n)$

$\forall n \in \mathbb{Z} \quad n \mid 0$ perché $0 = n \cdot 0$

Prop: Siano $a,b,k \in \mathbb{Z}$.

1) Se $k|a \wedge k|b$ allora $k|(a+b)$
2) Se $k|a \wedge k|(a+b)$ allora $k|b$

Dim: 1) Sia k t.c. $k|a$ e $k|b$, allora $a = k \cdot \alpha$, $b = k \cdot \beta$ per qualche valore $\alpha, \beta \in \mathbb{Z}$.
Ma allora $a+b = k\alpha + k\beta = k(\alpha+\beta) \Rightarrow k|(a+b)$.

2) Sia k t.c. $k|a$ e $k|(a+b)$, allora $a = k\alpha$, $a+b = k \cdot \sigma$ per qualche $\alpha, \sigma \in \mathbb{Z}$.
Ma allora $b = (a+b) - a = k \cdot \sigma - k\alpha = k(\sigma - \alpha) \Rightarrow k|b$.

Dato un certo $n \in \mathbb{Z}$, denotiamo $D_n = \{d \in \mathbb{Z} \text{ t.c. } d|n\}$ l'insieme dei divisori di n.

Oss: se $n=0$, allora $D_0 = \mathbb{Z}$

se $n \neq 0$, allora D_n è <u>finito</u> (se $d|n \Rightarrow |d| \leq |n|$) e <u>non vuoto</u> ($\pm 1 | n$)

Domanda: Dati $a,b \in \mathbb{Z}$, $(a,b) \neq (0,0)$, chi è $MCD(a,b)$?

$$MCD(a,b) = \max(D_a \cap D_b)$$ questo valore esiste sempre ed è ≥ 1.

Ci sono vari modi per calcolarlo:
- usando la definizione
- usando le fattorizzazioni in prodotto di primi
- usando l'algoritmo euclideo.

Divisione euclidea

Teorema: Dati $a, b \in \mathbb{Z}$ $(b \neq 0)$, esistono unici due numeri $q, r \in \mathbb{Z}$ t.c.

$$a = bq + r \qquad e \qquad 0 \leq r < |b|$$

q si chiama quoziente ed r resto.

Dim: Esistenza. Ci concentriamo sul caso $a \geq 0$, $b > 0$.

Procediamo per induzione su a.

Passo base: se $a = 0$ $\quad 0 = 0 \cdot b + 0 \quad (q = r = 0)$

Ipotesi induttiva: $\forall \alpha < a \ \exists q', r'$ t.c. $\alpha = b \cdot q' + r'$ e $0 \leq r' < b$.

Se $a < b \Rightarrow a = b \cdot 0 + a \quad (q = 0, r = a)$

Se $a \geq b \Rightarrow a - b \geq 0$ e poniamo $\alpha = a - b$, ovviamente $\alpha < a$ perciò posso usare l'ipotesi induttiva, cioè $\exists q', r'$ t.c. $\alpha = b \cdot q' + r'$ e $0 \leq r' < b$

cioè $\quad a - b = b \cdot q' + r' \Rightarrow a = b + b \cdot q' + r' = b(1 + q') + r' \quad (q = 1 + q', r = r')$

1) Se $a \geq 0, b < 0$, allora $-b > 0$, posso applicare il ragionamento precedente alla coppia $\underbrace{a}_{\geq 0}, \underbrace{-b}_{> 0}$

Cioè $\exists q', r'$ t.c. $\begin{cases} a = (-b) \cdot q' + r' \\ 0 \leq r' < -b \end{cases}$, ma allora $a = b \cdot (-q') + r' \quad (q = -q', r = r')$

2) Se $a<0$, $b>0$, allora possiamo applicare il ragionamento alla coppia $\underbrace{-a}_{>0}, \underbrace{b}_{>0}$, cioè
$\exists q', r' \in \mathbb{Z}$ $(0 \leq r' < b)$ t.c. $-a = b \cdot q' + r' \Rightarrow a = -bq' - r' = b(-q') - r'$

se $r' = 0$ $\quad a = b \cdot (-q')$ $\qquad (q = -q', \ r = 0)$

se $r' > 0$ $\quad a = b \cdot (-q') - r' = b(-q') - b + b - r' = b(-q'-1) + \underbrace{(b - r')}_{>0}$ $\qquad (q = -q'-1, \ r = b - r')$

3) se $a<0$, $b<0$, allora $-a>0$, $-b>0$ $\Rightarrow \exists q', r' \in \mathbb{Z}$ $(0 \leq r' < -b)$ t.c. $-a = (-b) \cdot q' + r'$

$\Rightarrow a = b \cdot q' - r'$

Se $r' = 0 \Rightarrow a = bq'$ $\qquad (q = q', \ r = 0)$

se $r' > 0 \Rightarrow a = b \cdot q' - r' = bq' - b + b - r' = b \cdot (q'-1) + \underbrace{(b - r')}_{>0}$. $\qquad (q = q'-1, \ r = b - r')$

<u>Unicità</u>: Siano (q,r) e (q', r') due coppie che soddisfano le ipotesi, allora

$$\begin{cases} a = b \cdot q + r \\ a = b \cdot q' + r' \end{cases} \qquad \text{possiamo supporre } r \geq r'$$

allora
$$a - a = bq + r - bq' - r'$$
$$0 = bq - bq' + r - r'$$
$$0 = b(q - q') + r - r'$$

$0 \leq r, r' < |b|$

$b(q' - q) = r - r' \quad \Longrightarrow \quad b \mid (r - r') \Longrightarrow r - r' = 0 \Rightarrow r = r'$

Di conseguenza $b(q' - q) = 0 \xRightarrow{b \neq 0} q' - q = 0 \Rightarrow q' = q$ $\qquad \boxtimes$