

Pre-corso

giovedì 2 settembre 2021 09:34

Buonoh!

fgaluppi@units.it

beozchia@units.it

NUMERI NATURALI

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

Ordine : $\leq$ oppure $<$

ossia

- riflessiva $m \leq m \quad \forall m \in \mathbb{N}$
- antisimmetrica $\forall x, y \in \mathbb{N}$

se $x \leq y$ e $y \leq x$,
allora $x = y$.

- transitiva se $x \leq y$ e $y \leq z$
allora $x \leq z$.

Questo è un ordine totale :

$\forall a, b \in \mathbb{N}$, $a \leq b$ oppure $b \leq a$.

PRINCIPIO DEL MINIMO

Ogni sottoinsieme non vuoto di $\mathbb{N}$ ha un elemento minimo.

$\forall S \subseteq \mathbb{N}$, se $S \neq \emptyset$ allora
 $\exists m \in S$ tale che $m \leq x \forall x \in S$.

OPERAZIONI

Su $\mathbb{N}$ c'è un $+$
 e c'è un $\cdot$

1) associative $(a+b)+c = a+(b+c)$
 $(ab) \cdot c = a \cdot (bc)$

2) commutative $a+b = b+a$
 $ab = ba$

3) elemento neutro $a+0 = 0+a = a$
 $a \cdot 1 = 1 \cdot a = a$

• $\mathbb{N}$ è distributivo / distributive

4) distributivita' / associativita'

$$a(b+c) = ab+ac$$

$$(b+c)a = ba+ca$$

5) cancellazione

$$a+c = b+c \Rightarrow a=b$$

$$ac = bc$$

$$\Rightarrow a=b$$

$\forall a, b, c \in \mathbb{N}$
(se $c \neq 0$)

6) $a \leq b \Rightarrow a+c \leq b+c$

e

$$ac \leq b \cdot c$$

Definizione: $a^b = \underbrace{a \cdot \dots \cdot a}_{b \text{ volte}}$

7) $a \leq b \Rightarrow a^c \leq b^c$

Definizione: a è divisore di b ($a|b$)

(oppure b è multiplo di a) se

$$\exists n \in \mathbb{N} \text{ tale che } a \cdot n = b.$$

a è primo se gli unici
divisori di a sono a e 1
 $a \neq 1 \Rightarrow a \neq 1$

(1 non è primo :.)

"essere divisore" è una relazione d'ordine in $\mathbb{N}$?

• $a \mid a \ \forall a \in \mathbb{N}$? 

perché $a = a \cdot 1$

• $a \mid b$ e $b \mid c \stackrel{?}{\Rightarrow} a \mid c$ 

perché $ma = b$

$mb = c$

$\Rightarrow c = m \cdot b = m \cdot m \cdot a$
 $= (mm) \cdot a$

• se $a \mid b$ e $b \mid a$, è vero che $a = b$? 

DIVISIONE EUCLIDEA

(divisione con resto)

$\forall a, b \in \mathbb{N}$ con $b \neq 0 \ \exists ! q, r \in \mathbb{N}$

tali che

- $a = b \cdot q + r$

- $0 \leq r < b$

$$25 = 6 \cdot 4 + 1$$

$$= 5 \cdot 4 + \underline{\underline{5}} \quad \times$$

$$a = 25$$

$$b = 4$$

TEOREMA (EUCLIDE) Esistono infiniti numeri primi.

dim Voglio dimostrare che $\forall N \in \mathbb{N}$
 $\exists p \in \mathbb{N}$ primo tale che $p > N$.

Dato N , consideriamo

$$a = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (N-1) \cdot N + 1 > N$$

Se a è primo, abbiamo finito

~~Se a non è primo, osservo che~~

- $2 \nmid a$, perché a è
(multiplo di 2) + 1

- $3 \nmid a$, _____

⋮

• $N \neq a$,

Se a non è primo, ogni suo
 divisore primo p deve essere
 $> N$. Ho trovato il numero primo
 assoluto

PROBLEMI APERTI

- ogni numero pari maggiore di 2
 è la somma di due numeri
 primi

$$4 = 2 + 2$$

$$6 = 3 + 3$$

$$8 = 3 + 5$$

$$10 = 5 + 5$$

⋮

(Congettura di Goldbach)

- due numeri primi p e q sono
 gemelli se $q = p + 2$

$$(5, 7)$$

$$11, 13$$

$$17, 19$$

⋮

$$29, 31$$

⋮

Ce ne sono infinite?

"essere divisore di" è un ordine
su $\mathbb{N}$. È un ordine totale?

NO!

2 non è multiplo di 3

3 ————— 2.

SCOMPOSIZIONE IN FATTORI PRIMI

Ogni numero naturale maggiore
di 1 si può scrivere **in**
modo unico come prodotto di
numeri primi.

Esempio:

$$A = \{ 1, 5, 9, 13, 17, 21, \dots \}$$

$$= \{ 4m+1 \mid m \in \mathbb{N} \}$$

a è divisore di b (in A)

se $\exists c \in A$ t.c. $a \cdot c = b$.

p è primo (in A) se i suoi unici

divisori in A sono 1 e p .

21 è primo in A o anche 9 e 49

$$441 = 440 + 1 \in A$$

$$441 = 21 \cdot 21$$

$$441 = 9 \cdot 49$$

ha due decomp
in fattori primi
(in A)

Def $a, b \in \mathbb{N}$

1) a e b sono primi tra loro se
l'unico divisore di entrambi è 1.

2) il minimo comune multiplo
di a e b è il più piccolo
multiplo di entrambi

$$\text{mcm}(a, b) = \min \{ n \in \mathbb{N} / a | n \text{ e } b | n \}$$

$\neq \emptyset$ perché
c'è ab

3) il massimo comun divisore
è il più grande divisore di
entrambi.

$$\text{MCD}(a, b) = \max \{ m \in \mathbb{N} / m | a \text{ e } m | b \}$$