NUMERI PRIMI E TEOREMA FONDAMENTALE DELL'ARITMETICA

(Cazzola, pag 105)

Definizione (numero primo)

Chiamiamo numero PRIMO ogni $n \in \mathbb{N}$ tale che

1) $n \geq 2$
2) n è divisibile SOLO per 1 e per se stesso.

OSS: a) 1 non è un numero primo, ma soddisfa la condizione 2)

b) Non dobbiamo dimenticare la parola SOLO, poiché tutti i numeri $n \in \mathbb{N}$ sono divisibili per 1 e per n!!!

ESEMPI: 2 (è l'unico numero primo pari)

3

5

7

⋮

CRIVELLO DI ERATOSTENE

Come individuare i numeri primi minori e uguali a un certo intero $n_0 \in \mathbb{N}$?

Es. $n_0 = 30$

$\cancel{1}$ 2 3 $\cancel{4}$ 5 $\cancel{6}$ 7 $\cancel{8}$ $\cancel{9}$ $\cancel{10}$ 11 $\cancel{12}$ 13
$\cancel{14}$ $\cancel{15}$ $\cancel{16}$ 17 $\cancel{18}$ 19 $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ 23 $\cancel{24}$
$\cancel{25}$ $\cancel{26}$ $\cancel{27}$ $\cancel{28}$ 29 $\cancel{30}$

Come capire se un numero $p \in \mathbb{N}$ è primo?

Se $p \geq 2$ non è primo, allora

$p = a \cdot b$ con $1 < a < p$
$1 < b < p$

(abbiamo visto il 21/3)

Inoltre, almeno uno tra a e b deve verificare $a \leq \sqrt{p}$ (oppure $b \leq \sqrt{p}$)

infatti, se fossero entrambi $> \sqrt{p}$

avremmo $\quad a \cdot b > \sqrt{p} \cdot \sqrt{p} = p \quad$ <u>assurdo</u>

Quindi p non è primo $\Rightarrow$ $\exists$ un divisore di p minore o uguale a $\sqrt{p}$ (condizione <u>NECESSARIA</u>)

<u>ES</u>: $\quad p = 341 \qquad \underbrace{18}_{} < \sqrt{p} < 19$

Basta testare i divisori ≤ 18

<u>OSS</u>: $\quad n = 252$

252	2
126	2
63	3
21	3
7	7
1	

$$252 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7 =$$
$$= 2^2 \cdot 3^2 \cdot 7$$

TEOREMA (Fondamentale dell'aritmetica)

Sia $a \in \mathbb{N}$, $\underline{\underline{a \geq 2}}$.

Allora a può essere scritto come prodotto di numeri primi (eventualmente ripetuti).

Tale decomposizione è essenzialmente unica, nel senso che due decomposizioni possono differire solo per l'ordine dei fattori.

OSS: Abbiamo già visto nel passato un teorema di decomposizione dei numeri naturali: teorema di decomposizione in base $b \geq 2$

$$\underline{\underline{\forall a \in \mathbb{N}}} \qquad a = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$$

Qui stiamo dicendo che !!!

$$\forall a \geq 2 \qquad a = \overbrace{q_1 \cdot q_2 \cdot \dots \cdot q_N}^{\text{prodotto !!!}}$$

q_j sono primi

e N è univocamente definito

i fattori $q_1, q_2, \dots, q_N$ sono univocamente definiti

<u>OSS</u>: Poichè è un risultato che deve essere valido $\forall n \in \mathbb{N}$ dobbiamo <u>DIMOSTRARLO</u> non bastano gli esempi!

Servono 2 ingredienti:

→ PRINCIPIO DI INDUZIONE

→ PROPRIETÀ DI EUCLIDE (che utilizza il teorema di Bézout)

<u>Richiami</u>:

<u>PRINCIPIO DI INDUZIONE</u>: permette di dimostrare proposizioni del tipo

$$\forall n \geq n_0 \quad P(n)$$

in questo modo

a) $P(n_0)$ è vera

b) $P(n) \rightarrow P(n+1) \qquad \forall n \geq n_0$

<u>OPPURE</u> (in modo equivalente)

a) $P(n_0)$ è vera.

b) $P(k)$ vera $\quad \forall \; n_0 \leq k \leq n$

$\longrightarrow P(n+1)$

TEOREMA (Proprietà di Euclide)
Se p primo divide a.b, allora p divide a oppure divide b

OSS 1) 7 divide 35.5   7 divide 35

6 divide $28.3 = 7.2^2.3 = 7.2.6$
6 non è primo ed è $6 = 2.3$

2) La proprietà di Euclide si generalizza al prodotto di N fattori $(N \geq 2)$
Se p primo che divide $\underbrace{a_1 \cdot a_2 \cdot \dots \cdot a_N}_{\text{prodotto}}$

allora p divide almeno uno dei fattori a_j.

dim (proprietà di Euclide)
Se a oppure b sono nulli è ovvio.
Supponiamo $a \neq 0$, $b \neq 0$.
Supponiamo che p non divida a.
Dimostriamo che allora p divide b

Poiché p (primo) non divide a,
si ha che $MCD(a,p)=1$ e
per Bézout

$$1 = ma - np \qquad (\text{oppure } 1 = np - ma)$$

moltiplichiamo per b

$$b = m\underbrace{ab}_{} - n\underbrace{p}_{}b$$

p divide ab

e quindi p divide b.

DIMOSTRAZIONE (teorema fondam. dell'aritmetica)

La dimostrazione si divide in

- Esistenza della decomposizione (fattorizzazione)
- Unicità della fattorizzazione.

Entrambe sono dimostrazioni per induzione

ESISTENZA:

mostriamo che $\forall a \geq 2 \quad a \in \mathbb{N}$
esiste una fattorizzazione di a in

fattori primi $(p(a))$

Per induzione su $a \geq 2$

- $P(2)$ 2 ammette una fattorizzazione
  $2 = 2$ (è primo!!)

- Sia ora $a \geq 3$
  Supponiamo (per induzione) che
  $\forall \quad 2 \leq k \leq a-1 \qquad p(k)$ sia vera
  cioè k abbia una fattorizzazione in fattori primi e deduciamo
  $p(a)$ cioè a ha una fattorizzazione in fattori primi.

Sia quindi $a \geq 3$.
Ci sono 2 possibilità

- a è primo e quindi $a = a$
  e una fattorizzazione esiste
- a non è primo, allora
  $$a = b \cdot c \qquad \text{con}$$
  $$1 < b < a$$
  $$1 < c < a$$

Ho per ipotesi di induzione poiché

$2 \leq b < a \qquad b = p_1 \cdots p_N \qquad p_j$ primi

$2 \leq c < a \qquad c = q_1 \cdots q_M \qquad q_j$ primi

e quindi

$$a = b \cdot c = p_1 \cdot p_2 \cdots \cdot p_N \cdot q_1 \cdot q_2 \cdots \cdot q_M$$

quindi a ha una fattorizzazione in fattori primi.

<u>UNICITÀ</u>:

$\underline{\forall N \geq 1}$ se a ha una decomposizione in N fattori, allora tale decomposizione è unica.

$P(N)$

Dimostriamo per induzione su N.

$P(1)$: se a ha una decomposizione di 1 fattore, allora la decomposizione è unica.

<u>VERO</u>, poiché <u>a è primo</u>.

<u>ora</u> supponiamo $P(N)$ vera $\quad N \geq 1$

e deduciamo $P(N+1)$, cioè

supponiamo che se a si fattorizza in N fattori, la fattorizzazione è unica e deduciamo che se a si fattorizza in $N+1$ fattori, la fattorizzazione è unica.

Sia quindi $a = p_1 \cdot p_2 \cdots \cdot p_N \cdot p_{N+1}$ $\quad$ p_j primi

e supponiamo che

$$a = q_1 \cdot q_2 \cdots \cdot q_M \quad \text{con } q_j \text{ primi}$$

dimostriamo che $N+1 = M$

$$p_j = q_j \quad 1 \le j \le N+1$$

Si ha $p_1 \cdot p_2 \cdots \cdot p_{N+1} = q_1 \cdot q_2 \cdots \cdot q_M$

poiché p_1 (primo) divide $q_1 \cdot q_2 \cdots \cdot q_M$ allora (proprietà di Euclide) p_1 divide almeno uno dei fattori $q_1, q_2, \dots, q_m$

possiamo supporre che p_1 divida q_1

ma poiché anche q_1 è primo, allora

$$\boxed{p_1 = q_1}$$

$$\cancel{p_1} \cdot p_2 \cdots \cdot p_{N+1} = \cancel{p_1} \cdot q_2 \cdots \cdot q_M$$

(legge di cancellazione del prodotto)
da cui

$$\underbrace{p_2 \cdot p_3 \cdot \dots \cdot p_{N+1}}_{\text{sono } N \text{ fattori}} = q_2 \cdot q_3 \cdot \dots \cdot q_m$$

per ipotesi di induzione la fattorizzazione in N fattori è <u>unica</u>, quindi

$$N+1 = m$$

$$q_j = p_j \qquad 1 \leq j \leq N+1$$

—— o ——

<u>Domanda</u>: perché 1 non è un numero primo? Se 1 fosse un numero primo, allora esisterebbero <u>infinite</u> fattorizzazioni diverse per ogni numero naturale

$$a = p_1 \cdot p_2 \cdot p_3 \cdots \cdot p_N \cdot 1 \cdot 1 \cdot 1 \cdot \dots$$

e quindi l'<u>unicità</u> nel teorema fondamentale dell'aritmetica non sarebbe più valida.

OSS: Se nella fattorizzazione compare più volte uno stesso fattore, allora si scrive come potenza

$$a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n} \qquad k_j \geq 1$$

$$252 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7 = 2^2 \cdot 3^2 \cdot 7$$

TEOREMA (Euclide)

I numeri primi sono infiniti.

dim: per assurdo, supponiamo che esista solo un numero <u>finito</u> di numeri primi $p_1, p_2, \dots, p_N$.

Consideriamo ora il numero seguente

$$q = (p_1 \cdot p_2 \cdot p_3 \cdots p_N) + 1 \qquad \in \mathbb{N}$$

Si ha $q > p_j \quad \forall\, 1 \leq j \leq N$ e quindi q <u>non</u> è primo tuttavia (per il teorema fondamentale dell'aritmetica) q è divisibile per almeno un numero primo, ma

$$q = p_1 \cdot p_2 \cdot \ldots \cdot p_N + 1$$

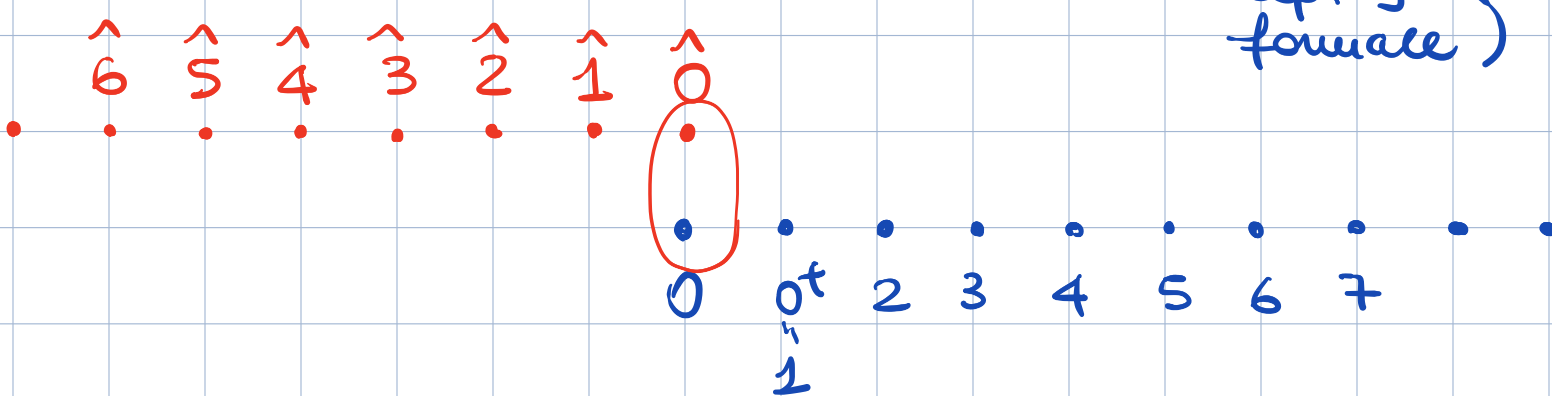
è la scrittura della divisione euclidea di q per ognuno dei numeri $p_1, p_2, \ldots, p_N$ e il resto è sempre 1, quindi la divisione non è mai esatta

ASSURDO.

— o —

NUMERI INTERI (RELATIVI)

(Cazzola cap. 4 informale
cap. 9 formale)



Introduciamo una seconda copia di $\mathbb{N}$ $\{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \ldots\}$, identifichiamo $0 = \hat{0}$

e consideriamo l'insieme unione

$\mathbb{Z} = \{ \ldots, \hat{3}, \hat{2}, \hat{1}, 0, 1, 2, 3, \ldots \}$

<u>Notazione:</u> $\mathbb{Z}^- = \{ \ldots, \hat{3}, \hat{2}, \hat{1} \}$

$\mathbb{Z}^+ = \{ 1, 2, 3, \ldots \} = \mathbb{N} \setminus \{0\}$

$\mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+$

(<u>per ora</u> non c'è ordinamento !!!)

Dobbiamo definire in $\mathbb{Z}$ somma e prodotto in modo che

- siano una <u>estensione</u> delle leggi di somma e prodotto in $\mathbb{N}$
- valgano le stesse proprietà

<u>Ricordo che</u> (in $\mathbb{N}$)

$$\begin{cases} n + 0 = n & \forall n \in \mathbb{N} \\ (n + m^+) = (n + m)^+ & \forall n, m \in \mathbb{N} \end{cases}$$

$$\begin{cases} n \cdot 0 = 0 & \forall n \in \mathbb{N} \\ n \cdot m^+ = n \cdot m + n & \forall n, m \in \mathbb{N} \end{cases}$$

e valeranno le proprietà

1) associativa per somma e prodotto

2) commutativa ———

3) esiste $0 \in \mathbb{N}$: $\quad 0+n = n+0 = n \quad \forall n$

4) esiste $1 \in \mathbb{N}$: $\quad 1 \cdot n = n \cdot 1 = n \quad \forall n$

5) distributiva $\quad (n+m) \cdot p = np + mp$

6) legge cancell. somma

$$n+p = n+q \Longrightarrow p=q$$
$$\forall n, p, q \in \mathbb{N}$$

7) cancellaz prodotto

$$n \cdot p = n \cdot q \Longrightarrow p=q$$
$$\forall n, p, q \in \mathbb{N}, \quad n \neq 0$$

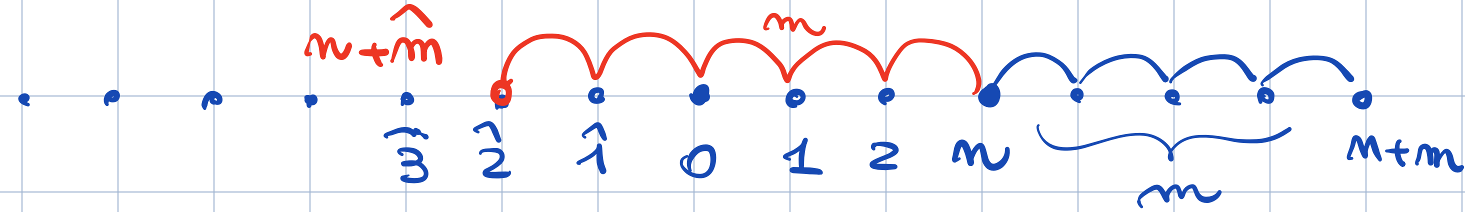
8) $n+m = 0 \Longleftrightarrow n = m = 0$

9) $n \cdot m = 0 \longrightarrow n=0$ oppure $m=0$

10) $n \cdot 0 = 0 \cdot n = 0 \quad \forall n \in \mathbb{N}$

11) $n \cdot m = 1 \Longleftrightarrow n = m = 1$

Nelle definizioni di somma e prodotto in $\mathbb{Z}$ vogliamo mantenere <u>tutte</u> le proprietà tranne quelle sottolineate in rosso.



$n+m \quad , \quad n, m \in \mathbb{N}$

sommare in $\mathbb{N}$ "significa" <u>spostarsi a destra</u>

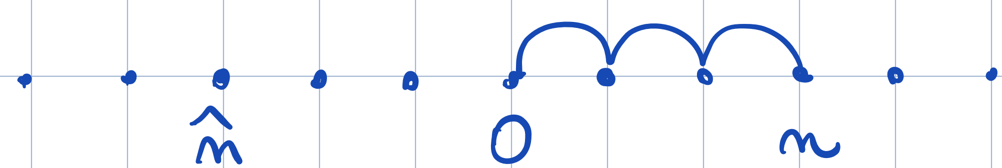
<u>Definiamo</u> $n+\hat{m}$ l'elemento che si trova <u>spostandosi</u> a <u>sinistra</u> di m posizioni

<u>In generale</u> $\forall a \in \mathbb{Z}$

$a+n$ sposta a destra di n posizioni

$a+\hat{n}$ sposta a sinistra di n posizioni

<u>Bisognerebbe</u> mostrare che questa definizione preserva le proprietà sopra richiamate



<u>OSS. FONDAMENTALE</u> $n+\hat{n}=0$ $\quad \forall n \neq 0$

$\hat{n}+n=0$

Non vale più la legge di annullamento della somma.

<u>Definizione</u>: Dato $a \in \mathbb{Z}$ chiamiamo <u>opposto di a</u> l'elemento $b \in \mathbb{Z}$ tale che $a + b = 0$

<u>OSS</u>: 1) l'opposto è unico, per la legge di cancellazione della somma:

$$0 = a + b = a + c \implies b = c$$

2) Se $a = n \in \mathbb{N}$ allora $b = \hat{n}$

Se $a = \hat{n}$ allora $b = n$

<u>Notazione</u>: D'ora in poi denoteremo $\hat{n} = -n$

<u>Per ora</u>: $(-n)$ è l'opposto di n

$$n + (-n) = 0$$

Non abbiamo ancora definito la sottrazione !!