

LA TEOREMA FONDAMENTALE DELL'ARITMETICA

Teorema 10.5 Ogni numero naturale $n \geq 2$ può essere fattorizzato in numeri primi, ovvero può essere scritto come prodotto di un certo numero finito di numeri primi p_1, \dots, p_a , eventualmente ripetuti: $n = p_1 \cdots p_a$.

Tale fattorizzazione è unica a meno di riordinamento. Più precisamente, se q_1, \dots, q_b sono numeri primi, eventualmente ripetuti, tali $n = q_1 \cdots q_b$, allora $a = b$ ed esiste una bijezione $\varphi: \{1, \dots, b\} \xrightarrow[i]{\quad} \{1, \dots, a\}$ t.c. $q_i = p_{\varphi(i)}$ per ogni $i \in \{1, \dots, b\}$.

DIM. ESISTENZA Procediamo per induzione (shiftata in 2) di 2^a forma per $n \geq 2$.

BASE DELL'INDUZIONE ($n=2$) E' suff. osservare che $n=2$ e' un numero primo.

Dunque basta porre $a_1 := 1$ e $p_1 := 2$: $n = 2 = p_1$. Ciò prova la base dell'induz.

PASSO INDUTTIVO ($n > 2$, $2 \leq k < n \Rightarrow n$) Sia $n > 2$. Supponiamo che l'asserito si sia ipot

$\forall k \in \mathbb{N}$ t.c. $2 \leq k < n$, ovvero supponiamo che ogni $k \in \mathbb{N}$ compreso fra 2 e $n-1$

(inclusi) si possa fattorizzare in numeri ^{primi} (IPOTESI INDUTTIVA).

Dobbiamo provare che anche n si può fattorizzare in numeri ^{primi}. Se n e' un numero primo, allora

e' suff. porre $a_1 := 1$ e $p_1 := n$: $n = p_1$. Supponiamo che n non sia un numero

primo. Allora $\exists d_1, d_2 \in \mathbb{N}$ t.c. $2 \leq d_1 < n$, $2 \leq d_2 < n$ e $n = d_1 d_2$.

Grazie all'ip. ind., d_1 e d_2 ammettono una fattorizzazione in numeri primi:

$$\underline{d_1 = p_1 \cdots p_a}, \underline{d_2 = p_{a+1} \cdots p_b} \quad \text{per qualche } p_1, \dots, p_a, p_{a+1}, \dots, p_b \text{ primi, eventualmente ripetuti.}$$

segue che:

$$n = \boxed{d_1 d_2} = \boxed{p_1 \cdots p_a} \boxed{p_{a+1} \cdots p_b}$$

Dunque n ammette una fattorizzazione in numeri primi. Il passo induuttivo è stato fatto.

Dunque, grazie al principio di induz. di 2^a forma (shiftata in $n=2$), ogni $n \geq 2$ possiede una fattorizzazione in numeri primi.

UNICITA' Supponiamo che esista $n \in \mathbb{N}$ con $n > 2$ che ammette due fattorizzazioni:

$$p_1 \cdots p_a = n = q_1 \cdots q_b$$

per qualche $a, b \in \mathbb{N}$ con $a > 0$ e $b > 0$, e $p_1, \dots, p_a, q_1, \dots, q_b$ numeri primi, event.

Ripet. A meno di scambiare a con b , possiamo supporre che $a \leq b$.

Proveremo l'unicità delle fattorizzazioni di n , a meno di riordinamento, procedendo per induz. di 1^a forma su $a \geq 1$.

BASE DELL'INDUZ. ($a=1$) Sia $p_1 = q_1 \cdots q_b$ per qualche p_1, q_1, \dots, q_b numeri primi.

Osserviamo che $p_1 | p_1 = q_1 \cdots q_b$, ovvero $p_1 | q_1 \cdots q_b$. Grazie all'esercizio 10.1, p_1 divide

almeno uno dei q_i . A meno di voler dire gli indici $\{1, \dots, b\}$, possiamo supporre $p_1 | q_1$.

Vale: $p_1 \mid q_1$. Osserviamo che q_1 è un numero ^{primo} (dunque possiede solo i divisori banali $\cancel{1}, \cancel{q_1}$) e $p_1 \geq 2$. Segue che $p_1 = q_1$.

Se $b \geq 2$, allora $p_1 = q_1 q_2 \cdots q_b = p_1 q_2 \cdots q_b \Rightarrow \cancel{p_1} = \cancel{p_1} q_2 \cdots q_b \Rightarrow 1 = q_2 \cdots q_b \geq 2$

ASSURDO. Ciò dimostra che $b=1$, ovvero $p_1 = q_1$. La base dell'induz. è dimostrata.

PASSO INDUTTIVO ($\alpha \Rightarrow \alpha+1$) Sia $\alpha \geq 1$. Supponiamo l'asserzione (di unicita') vero per

α , ovvero se $p_1 \cdots p_\alpha = q_1 \cdots q_b$ con $\alpha \leq b$, $p_1, \dots, p_\alpha, q_1, \dots, q_b$ primi, allora $\alpha = b$

e, sotto di riordinando degli indici, $p_i = q_i$. Utilizzando l'IP. INDUTTIVO.

Dovrò provare l'asserzione (di unicita') per $\alpha+1$.

Sia $p_1 \cdots p_{\alpha+1} = q_1 \cdots q_b$ t.c. $\underline{\alpha+1 \leq b}$, $p_1, \dots, p_{\alpha+1}, q_1, \dots, q_b$ numeri primi.

Vale: $p_{\alpha+1} \mid p_1 \cdots \cdots p_{\alpha+1} = q_1 \cdots q_b \Rightarrow p_{\alpha+1} \mid q_1 \cdots q_b \stackrel{\text{es. 10.1}}{\Rightarrow} p_{\alpha+1} \mid q_i$ per qualche $i \in \{1, \dots, b\}$

A meno di riordinare gli indici $\{1, \dots, b\}$, possiamo supporre che $p_{a+1} | q_b \Rightarrow \underline{p_{a+1} = q_b}$

Segue che $p_1 \cdots p_a p_{a+1} = q_1 \cdots q_{b-1} q_b = q_1 \cdots q_{b-1} p_{a+1} \Rightarrow p_1 \cdots p_a \cancel{p_{a+1}} = q_1 \cdots q_{b-1} \cancel{p_{a+1}}$

$$\Rightarrow \underline{p_1 \cdots p_a = q_1 \cdots q_{b-1}} \quad e \quad a \leq b-1 \quad (\Leftrightarrow a+1 \leq b)$$

\Downarrow IP. IND.

$$\underline{a = b-1} \quad e, \text{ a meno di riord.}, \quad \underline{p_i = q_i \quad \forall i \in \{1, \dots, a\}}$$

\Downarrow

$$a+1 = b \quad e \quad p_i = q_i \quad \forall i \in \{1, \dots, a, a+1\}$$

Il passo indukt. è stato fatto. Dunque, grazie al princ. di induz. di 1^a forma, la fattor. è

unica e non dividibile per $n \geq 2$. \square

Collobo 1D.6 L'insieme dei numeri primi è infinito.

DIM. Supponiamo per assurdo che $\{p_1, \dots, p_m\}$ sia l'insieme di tutti i numeri primi per qualche $m \in \mathbb{N}, m > 0$). Definiamo $n \in \mathbb{N}$:

$$n := 1 + p_1 \cdots p_m.$$

Osserviamo che $n \geq 1 + 2 \geq 2$. Grazie al teorema fondamentale dell'aritmetica, n ammette una fattoriz. in numeri primi. (cioè è assurdo infatti, $\forall i \in \{1, \dots, m\}$, $p_i \nmid n$).

Infatti, vale:

$$\begin{cases} n = (p_1 \cdots p_{i-1} p_{i+1} \cdots p_m) p_i + 1 \\ 0 \leq 1 < 2 \leq p_i \end{cases} \Rightarrow \begin{array}{l} \text{il resto della divisione di } n \text{ per } p_i \\ \text{è } 1 \neq 0 \Rightarrow p_i \nmid n \end{array}$$

$\Rightarrow n$ NON AMMETTE ALCUNA FATTORIZ. IN NUMERO PRIMO \Rightarrow ASSURDO. \blacksquare l'ins. dei numeri primi non è finito.

CONGRUENZA MODULO n , INTERI MODULO n (p. 28)

DEF. 11.1 Fissiamo $n \in \mathbb{Z}$. Detti $a, b \in \mathbb{Z}$, diciamo che $a \equiv b$ CONGRUO A b MODULO n ,

in simboli $a \equiv b \pmod{n}$, se $n \mid (a-b)$.

SI

ESEMPIO • $2 \equiv 16 \pmod{7} \stackrel{\text{det.}}{\Leftrightarrow} 7 \mid (2-16) \Leftrightarrow 7 \mid -14$ vera $-14 = (-2)7$.

• $14 \stackrel{?}{\equiv} 4 \pmod{3} \stackrel{\text{det.}}{\Leftrightarrow} 3 \mid 14-4 \Leftrightarrow 3 \mid 10$ NO

$14 \not\equiv 4 \pmod{3}$.

Proposizione 11.2 Fissiamo $n \in \mathbb{Z}$. Siano $a, b, c \in \mathbb{Z}$. Vengono le seguenti aff.:

(1) (Prop. RIFLESSIVA) $a \equiv a \pmod{n}$.

(2) (Prop. SIMMETRICA) Se $a \equiv b \pmod{n}$, allora $b \equiv a \pmod{n}$.

(3) (Prop. TRANSITIVA) Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, allora $a \equiv c \pmod{n}$.

DIM. (1) Dato provare che $a \equiv b \pmod{n}$, ovvero $n \mid a - b$ e visto che $a - b = 0 \Leftrightarrow n \mid 0$

(2) Supp. che $a \equiv b \pmod{n}$, ovvero $n \mid a - b \Leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } a - b = kn$

$$b \equiv a \pmod{n} \Leftrightarrow n \mid b - a \Leftrightarrow \frac{-(a - b)}{b - a} = \frac{-kn}{(-k)n}$$

(3) Supponiamo che $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$. Vale:

$$\begin{aligned} & \bullet a \equiv b \pmod{n} \Leftrightarrow n \mid a - b \Leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } a - b = kn \\ & \bullet b \equiv c \pmod{n} \Leftrightarrow n \mid b - c \Leftrightarrow \exists h \in \mathbb{Z} \text{ t.c. } b - c = hn \end{aligned} \quad \Rightarrow (a - b) + (b - c) = kn + hn = (k+h)n$$

Segue che $n \mid a - c$, ovvero $a \equiv c \pmod{n}$. \blacksquare

DEF. 11.3 Sia X un insieme non vuoto e sia R una relazione binaria su X (ovvero $R \subseteq X \times X$). Diciamo che R è una relazione di equivalenza su X se possiede le seguenti tre proprietà:

(1) Prop. riflessiva $\forall x \in X, x R x$ (cioè $(x, x) \in R$).

(2) Prop. simmetrica $\forall x, y \in X, (x R y \Rightarrow y R x)$.

(3) Prop. transitiva $\forall x, y, z \in X, (x R y \wedge y R z) \Rightarrow x R z.$

OSSERVAZIONE 11.5 Abbiamo provato nella Prop. 11.2 che, se $X = \mathbb{Z}$ e R è la relazione di congruenza mod m , allora R è una relazione di equivalenza su \mathbb{Z} .