Questo fascicolo contiene la dimostrazione di tre importanti teoremi, precisamente!

Teorema 1

Ogni numero naturale $n > 1$ ammette una fattorizzazione in numeri primi.

Teorema 2

I numeri primi sono infiniti.

Teorema 3 (teorema fondamentale dell'Aritmetica)

La fattorizzazione prima di un numero naturale $n > 1$ è unica, a meno dell'ordine dei fattori.

←

La dimostrazione del teorema 3 è facoltativa (contrariamente a quando ho scritto sul programma). I teoremi 1 e 2 sono obbligatori.

Dimostreremo ora tre importanti risultati riguardanti i numeri primi, precisamente i tre teoremi seguenti.

Teorema 1

Ogni numero naturale $n > 1$ ammette una fattorizzazione in numeri primi.

Teorema 2 (Euclide, 300 a. C. circa)

I numeri primi sono infiniti.

Teorema 3 (teorema fondamentale dell'Aritmetica)

La fattorizzazione prima di un numero naturale $n > 1$ è unica, a meno dell'ordine dei fattori.

Cominciamo dimostrando il teorema 1.

Dimostrazione teorema 1

Come prima cosa osserviamo che il risultato è evidentemente vero per i primi naturali, infatti

$$2, 3, 4 = 2.2, 5, 6 = 2.3, 7, 8 = 2.2.2, 9 = 3.3 \ldots$$

Ragioniamo allora per induzione supponendo il teorema vero per tutti i naturali $k < n$ e

dimostriamo che allora è vero anche per n. (2)
Infatti, se n è primo non c'è niente da dimostrare (la fattorizzazione è ridotta ad un solo fattore). Se n non è primo, allora $n = a \cdot b$ con $1 < a, b < n$: per ipotesi induttiva il teorema vale sia per a che per b, cioè $a = p_1 p_2 \dots p_r$, $b = q_1 \dots q_s$, e, sostituendo in $n = a \cdot b$, si ottiene

$$n = (p_1 p_2 \dots p_r)(q_1 \dots q_s)$$

che è la fattorizzazione prima richiesta.
Ciò dimostra il teorema 1.

Un problema che ci si pone immediatamente è se i numeri primi siano infiniti o no.
La risposta è stata data da Euclide (nel 300 a.C. circa) che ha dimostrato il teorema 2.
Dimostriamo il teorema 2, cioè che i numeri primi sono infiniti.

Dimostrazione del teorema 2

Ragioniamo per assurdo, supponendo che esista solo un numero finito di primi, e che P sia il massimo primo. Consideriamo il numero

(1) $$n = (2 \cdot 3 \cdot 5 \cdot 7 \cdot \dots \cdot P) + 1$$

dove, a destra di (1), compare il prodotto di tutti i primi più uno.

Per il precedente teorema 1 il numero n o è primo o è rappresentabile come prodotto di primi. Consideriamo ora le due possibilità.

I° caso: n è primo.

Dato che $n > P$ si ha immediatamente un assurdo.

II° caso: n non è primo.

Dato che n non è primo, per il teorema 1 il numero n è rappresentabile come prodotto di primi, diciamo

$$(2) \quad n = q_1 q_2 \cdots q_s$$

Da (1) e (2) segue

$$(3) \quad n = q_1 q_2 \cdots q_s = (2.3.5.7 \ldots . P) + 1$$

Ma l'eguaglianza (3) è assurda, infatti dalla (3) si ottiene, per differenza e raccogliendo q_1,

$$(4) \quad q_1 \left(q_2 \cdots q_s - \frac{2.3.5 \ldots P}{q_1} \right) = 1$$

dove $\frac{2.3.5 \ldots .P}{q_1}$ è intero (infatti q_1 è primo e nel prodotto fino a P compaiono tutti i primi).

Ma la ④ è assurda, infatti implica $q_1 | 1$. ④
Quindi i due casi possibili portano entrambi ad un assurdo, e ciò dimostra il teorema 2.

Osservazione

Il ragionamento di Euclide dimostra che, data una famiglia finita $p_1, p_2, \dots, p_k$ di primi, il numero $n = (p_1 p_2 \cdots p_k) + 1$ o è esso stesso primo, o nella sua fattorizzazione prima compariono solo primi $q_1, q_2, \dots, q_s$ non appartenenti alla famiglia.

Considerate i seguenti esempi:

$n = 2 \cdot 3 + 1 = 7$ è primo
$n = 2 \cdot 3 \cdot 5 + 1 = 31$ è primo
$n = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ è primo → $n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ è primo

$n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = (59)(509)$

$n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 510\,511 = (19)(97)(277)$

(gli ultimi due numeri sono composti e, a destra tra parentesi, ne è riportata la fattorizzazione prima).

Passiamo ora alla dimostrazione del teorema 3. Premettiamo un importante lemma:

Lemma di Euclide

Se un numero primo p divide un prodotto $a \cdot b$ allora divide uno almeno dei fattori.

Dimostrazione

Possiamo riformulare il lemma in modo equivalente dicendo che

$$(5) \quad \begin{cases} p \mid (a \cdot b) \\ p \nmid a \end{cases} \Longrightarrow p \mid b$$

(cioè se p divide il prodotto $a \cdot b$ e non divide a allora divide b).

La dimostrazione di (5) è basata sull'identità di Bézout. Infatti da $p \nmid a$ segue $(a, p) = 1$ e quindi esistono due interi $\lambda, \mu \in \mathbb{Z}$ tali che

$$(6) \quad \lambda p + \mu a = 1$$

Dalla (6) segue, moltiplicando per b,

$$7) \quad \lambda p b + \mu a b = b$$

Ma, per ipotesi, si ha $p \mid (a \cdot b)$ e quindi il numero a sinistra di (7) è multiplo di p,

infatti

(8) $p\left(\lambda b + \mu\cdot\left(\frac{a\cdot b}{p}\right)\right) = b$

da cui segue $p \mid b$.

Ciò prova l'implicazione (5) e quindi il lemma.

Possiamo ora dimostrare il

Teorema fondamentale dell'Aritmetica

La fattorizzazione prima di ogni numero naturale $n > 1$ è unica, a meno dell'ordine dei fattori.

Dimostrazione

Ragioniamo per induzione, basandoci sul lemma di Euclide.

Si verifica facilmente che il teorema è vero per i primi numeri naturali, infatti

$2, 3, 4 = 2.2, 5, 6 = 2.3, 7, 8 = 2.2.2, 9 = 3.3$

$10 = 2.5, 11, 12 = 2.2.3, - - - -$

Quindi supponiamo vero il teorema per ogni naturale $k < n$ e dimostriamo che allora vale anche per n. Se n è primo non c'è nulla da dimostrare. Supponiamo allora che n sia com=

e siano

(9) $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$

due fattorizzazioni di n (sia i p_i, $i=1,\dots,r$ che i q_j, $j=1,\dots,s$ sono primi).

Vedremo ora che il lemma di Euclide implica che p_1 deve coincidere con uno dei primi q_h a destra di (9). Infatti dalla (9) segue

(10) $p_1 \mid q_1 (q_2 \cdots q_s)$

e dunque $p_1 \mid q_1$ e quindi $p_1 = q_1$, poiché sono entrambi primi, e la proprietà è dimostrata, oppure $p_1 \nmid q_1$ ma allora

(11) $p_1 \mid q_2 (q_3 \cdots q_s)$

Dalla (11) segue $p_1 \mid q_2$ e quindi $p_1 = q_2$, poiché sono entrambi primi, e la proprietà è dimostrata, oppure $p_1 \nmid q_2$ ma allora

12) $p_1 \mid q_3 (q_4 \cdots q_s)$

Il ragionamento può, evidentemente, essere iterato, ottenendo che $p_1 \mid q_j$ per un certo $j \le s-2$, e quindi $p_1 = q_j$, oppure si termina dicendo che

(13) $p_1 \mid q_{s-1} \cdot (q_s)$

da cui segue $p_1 \mid q_{s-1}$ oppure $p_1 \mid q_s$, e quindi p_1 è uguale ad uno dei due.

In ogni caso p_1 compare nella fattorizzazione di destra di (9), diciamo $p_1 = q_j$ per un certo j con $1 \le j \le s$, e quindi può essere cancellato da entrambe le fattorizzazioni, ottenendo

(14) $$\frac{n}{p_1} = p_2 \cdots p_r = q_1 q_2 \cdots q_{j-1} q_{j+1} \cdots q_s$$

Ma $\frac{n}{p_1} = k < n$ e quindi, per ipotesi induttiva, le due fattorizzazioni in (14) devono coincidere: di conseguenza coincidono anche quelle in (9). Ciò prova il teorema.