IL TEOREMA FONDAMENTALE DELL'ARITMETICA: DIMOSTRAZIONE VELOCE.

PH. ELLIA

Indice

Introduzione

Scopo di questi appunti è di presentare una dimostrazione elementare del Teorema Fondamentale dell'Aritmetica secondo il quale ogni numero intero ammette una fattorizzazione, essenzialmente unica, come prodotto di numeri primi.

La dimostrazione proposta è così elementare che potrebbe (anzi dovrebbe) essere insegnata al liceo.

1. Divisori di un numero.

Ci occuperemo esclusivamente di numeri naturali positivi ("numeri" nel seguito) cioè degli elementi di $\mathbb{N} = \{0, 1, 2, 3, ..., n, ...\}$.

Definizione 1.1. *Il numero $a \in \mathbb{N}^*$ divide il numero $n \in \mathbb{N}$ se esiste $b \in \mathbb{N}$ tale che: $n = ab$.*

Osservare che non si può dividere per zero. Se a divide n si nota $a \mid n$ (a divide n). Ogni numero n ha sempre due divisori banali: 1 e se stesso: $n = 1.n$.

Più generalmente abbiamo la divisione euclidea:

Date: 8 Ottobre 2012.

Proposizione 1.2. *Dati due numeri a, b, $a \neq 0$, esiste un'unica coppia di numeri (q, r) tale che: $b = aq + r$ con $0 \leq r < a$.*

Proof. Mostriamo prima l'esistenza. Se $a > b$ basta prendere $q = 0$, $r = b$. Se $a \leq b$, si considera $b - a$ al posto di b: se $a > b - a$, allora $b = a + (b - a)$ ($q = 1$, $r = b - a$); se $a \leq b - a$, si considera $b - 2a$ e si ripete il ragionamento. A un certo punto si avrà: $a > b - qa$ e quindi $b = qa + r$, $0 \leq r < a$ (con $r = b - qa$).

Mostriamo adesso l'unicità: se $b = aq + r = aq' + r'$ con, diciamo, $q > q'$, allora $r < r'$ e: $a(q - q') = r' - r$, ma $a(q - q') \geq a$ mentre $r' - r < a$: assurdo. Questo mostra l'unicità. □

Quindi $a \mid b$ se e solo se il resto nella divisione euclidea di b per a è zero.

Nel seguito useremo il Principio del Minimo (che può essere preso come un assioma):

Principio del minimo: *Se $X \subset \mathbb{N}$ è un sottinsieme non vuoto, allora X ha un elemento* minimo*, cioè esiste $m \in X$ tale che: $\forall x \in X, m \leq x$.*

Finalmente l'ultima definizione:

Definizione 1.3. *Un numero $n \in \mathbb{N}$ è* primo *se $n > 1$ e se gli unici divisori di n sono quelli banali (cioè 1 e n).*

Quindi i numeri primi minori o uguali a 20 sono: $2, 3, 5, 7, 11, 13, 17, 19$.

Osservazione 1.4. *Risulta dalla definizione che se $n > 1$ non è primo allora esiste d, $1 < d < n$ con $d \mid n$.*

Il numero 1 (unità) non viene considerato primo perché 1 divide ogni numero ($n = 1.n$).

2. Il Teorema Fondamentale dell'Aritmetica.

Abbiamo subito la parte "facile" del teorema:

Lemma 2.1. *Ogni numero $n > 1$ si scrive come un prodotto di numeri primi.*

Dimostrazione. Sia $S \subset \mathbb{N}$ l'insieme dei numeri che non si possono scrivere come un prodotto di numeri primi. Se S è non vuoto, ammette un elemento minimo, m. Il numero m non è primo, quindi: $m = dn$, con $1 < d \leq n < m$.

In particolare $d \notin S$ e $n \notin S$. Quindi d e n si scrivono come un prodotto di numeri primi: $d = p_1...p_r$, $n = q_1..q_t$. Pertanto $m = dn = p_1...p_r q_1...q_t$ si scrive come un prodotto di numeri primi: assurdo (perché $m \in S$). Quindi $S = \emptyset$. □

Per completare la dimostrazione ci serve il seguente:

Lemma 2.2. *Sia p un numero primo e siano a, b degli interi. Se $0 < a < p$ e se $0 < b < p$, allora $p \nmid ab$ (p non divide ab).*

Dimostrazione. Supponiamo $p \mid ab$, dunque $S_a = \{n \in \mathbb{N} \mid 0 < n < p \text{ e } p \mid an\}$ è non vuoto ($b \in S_a$). Sia c l'elemento minimo di S_a. Quindi $0 < c < p$, $p \mid ac$ e se $0 < n < c, p \nmid an$.

Facciamo la divisione euclidea di p per c: $p = mc + r$, $0 \leq r < c$. Abbiamo $r > 0$, infatti altrimenti si avrebbe $p = mc$ e siccome p è primo, $c = p$ o $c = 1$. Il primo caso è impossibile ($c < p$) e se fosse $c = 1$, si avrebbe $p \mid a$, ma questo è impossibile perché $a < p$.

Abbiamo quindi $0 < r = p - mc < c$ $(*)$. Adesso siccome p divide ac, abbiamo $p \mid mac$, abbiamo anche (ovviamente) $p \mid ap$. Quindi p divide la differenza $ap - mac$: $p \mid ap - amc = a(p - mc)$, ma questo è assurdo perché $p - mc < c$ (cf $(*)$) e c è l'elemento minimo di S_a. Quindi $S_a = \emptyset$ e $p \nmid ab$. □

Osservazione 2.3. *Abbiamo $6 \mid 3.4 = 12$. Riprendiamo la dimostrazione precedente con $a = 3, b = 4$. Viene $c = 2$ e $6 = 3.2 + 0$, cioè con le notazioni precedenti $r = 0$ e (giustamente) non si può concludere ad un assurdo. Quindi l'ipotesi p primo serve per mostrare $r > 0$.*

Da questo risultato otteniamo facilmente il lemma seguente (chiamato certe volte *Lemma di Gauss* (uno dei tanti!)):

Lemma 2.4. *Sia p un numero primo, se $p \mid ab$, allora $p \mid a$ o $p \mid b$.*

Dimostrazione. Basta mostrare la contrapposta cioè:

se $p \nmid a$ e $p \nmid b$, allora $p \nmid ab$.

Per la divisione euclidea, se $p \nmid a$: $a = mp + r$, $0 < r < p$. Nello stesso modo se $p \nmid b$, $b = np + s$, $0 < s < p$. Adesso:

$$ab = (mp + r)(np + s) = p(mnp + sm + rn) + rs$$

Vediamo che se $p \mid ab$, allora $p \mid rs$, ma questo è impossibile per il Lemma 2.2. □

Osservazione 2.5. *Abbiamo* $6 \mid 3.4 = 12$*, ma* 6 *non divide né* 3 *né* 4*. Se "spezziamo"* 6 *in numeri primi:* $6 = 2.3$*, vediamo che il* 2 *va a dividere* 4 *e il* 3 *il* 3*. Un numero primo non si può "spezzare" e quindi deve entrare in uno dei fattori.*

Questo enunciato si può generalizzare:

Lemma 2.6. *Sia* p *un numero primo. Se* p *divide un prodotto di* n *numeri, allora* p *divide uno dei fattori. In simboli: se* $p \mid a_1...a_n$*, allora esiste* i*,* $1 \leq i \leq n$*, tale che* $p \mid a_i$*.*

Dimostrazione. Abbiamo $p \mid a_1.(a_2...a_n)$. Per il Lemma 2.4: $p \mid a_1$ o $p \mid a_2...a_n$. Se $p \mid a_1$ abbiamo finito, altrimenti $p \mid a_2.(a_3...a_n)$. Quindi, sempre per il Lemma 2.4, $p \mid a_2$ o $p \mid a_3.(a_4...a_n)$. Vediamo che dopo al più n passi, avremo trovato un a_i divisibile per p. □

Possiamo finalmente dimostrare il nostro teorema:

Teorema 2.7. (Teorema Fondamentale dell'Aritmetica)
Ogni intero $n > 1$ *si scrive come un prodotto di numeri primi:*

$$n = p_1...p_r$$

Inoltre, a meno dell'ordine dei fattori, questa fattorizzazione è unica, cioè se $n = p_1...p_r = q_1...q_s$*, (*$p_i$ *e* q_j *numeri primi), allora* $r = s$ *e (dopo eventuale riordino degli indici):* $p_i = q_i, \forall i$*.*

Dimostrazione. Abbiamo già visto (Lemma 2.1) l'esistenza della fattorizzazione, rimane da mostrare l'unicità. Sia dunque $n = p_1...p_r = q_1...q_s$. Per il Lemma 2.6 p_1 divide uno dei q_j. Riordinando semmai gli indici possiamo assumere $p_1 \mid q_1$, siccome p_1 e q_1 sono primi questo implica $p_1 = q_1$. Abbiamo quindi $p_2...p_r = q_2...q_s$. Se $r < s$, procedendo in questo modo si arriverà a: $1 = q_{r+1}...q_s$: assurdo, quindi $r = s$ e, a meno di un riordino degli indici, $p_i = q_i, \forall i$. □

Osservazione 2.8. *Nella fattorizzazione possono esserci fattori ripetuti, in questo caso, di solito, si usa la notazione esponenziale (p^r), si può anche convenire di scrivere i fattori in ordine crescente ($p_1 < p_2 < ... < p_r$), seguendo queste convenzioni la fattorizzazione si scrive: $n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_r^{\alpha_r}$ $(*)$, $p_i \neq p_j$ se $i \neq j$ e $p_1 < p_2 < ... < p_r$. Con queste convenzioni la fattorizzazione $(*)$ è unica.*

Per esempio: $180 = 2^2.3^2.5$.

3. L'insieme dei numeri primi è infinito.

La dimostrazione classica (che risale ad Euclide) del fatto che l'insieme, $\mathcal{P}$, dei numeri primi è infinito è una dimostrazione per assurdo: se $\mathcal{P}$ è finito, $\mathcal{P} = \{2 = p_1, p_2, ..., p_r\}$, consideriamo il numero $N := (p_1...p_r) + 1$. Abbiamo visto (Lemma 2.1) che ogni numero > 1 si scrive come un prodotto di primi, quindi in particolare ogni numero > 1 ammette un divisore primo. Pertanto esiste i tale che $p_i \mid N$, ma questo è impossibile perché:

$$\frac{N}{p_i} = \frac{p_1...p_i...p_r}{p_i} + \frac{1}{p_i}$$

non è intero ($1/p_i \notin \mathbb{N}$). Quindi $\mathcal{P}$ è infinito.

Un'altra dimostrazione (dovuta a Hermite), più diretta, è la seguente. Intanto osserviamo il seguente:

Lemma 3.1. *Sia $n > 1$ un intero e sia $Div(n) = \{1 = d_0, d_1, ..., d_r = n\}$ l'insieme dei suoi divisori, con $1 < d_1 < d_2 < ... < d_{r-1} < n$. Allora d_1 è primo.*

Dimostrazione. Se d_1 non è primo esiste d, $1 < d < d_1$ tale che $d \mid d_1$ (Osservazione 1.4), ma da $d \mid d_1$ e $d_1 \mid n$, segue $d \mid n$, contro la definizione di d_1. □

Consideriamo adesso il numero $n! := 1.2.3...n$ (n fattoriale). Il più piccolo divisore di $N := n! + 1$ è $> n$: infatti se $k \leq n$, $k \nmid n! + 1$ perché:

$$\frac{N}{k} = \frac{1.2.3...k...n}{k} + \frac{1}{k}$$

e $1/k \notin \mathbb{N}$. Quindi d_1 il più piccolo divisore > 1 di N verifica $d_1 > n$. Per il Lemma 3.1, segue che: $\forall n \in \mathbb{N}$, $\exists p$, p primo con $p > n$. Pertanto $\mathcal{P}$ è infinito.

Ci sono tante altre dimostrazioni del fatto che $\mathcal{P}$ è infinito, alcune (come quella di Hermite) sono delle variazioni sul tema sviluppato da Euclide, ma altre no...

4. Commenti.

Passiamo adesso in rassegna gli strumenti usati.

(1) La divisione euclidea e le proprietà di base della divisione (per esempio: $a \mid b$ e $b \mid c$ implica $a \mid c$). Questo non dovrebbe presentare alcun problema.
(2) Il principio del minimo: il principio, da prendere come un assioma, è così "evidente" intuitivamente che non dovrebbe porre problemi. Osserviamo che questo *principio* è equivalente al *principio di induzione* (Osservazione 4.1).
(3) La dimostrazione per assurdo viene usata varie volte (lemma 2.1, Lemma 2.2, ecc...). Lo studente deve avere presente che se partendo da una premessa, P, si arriva ad una contraddizione, allora P è falsa, cioè nonP è vera (=dimostrata).
(4) La dimostrazione per contrapposizione, ossia $(p \Rightarrow q) \Leftrightarrow (non\, q \Rightarrow non\, p)$ (lemma 2.4). La dimostrazione per contrapposizione non deve essere confusa con una dimostrazione per assurdo: si nega la tesi, cioè si considera $non\, q$, ma non c'è nessuna contraddizione, nessun assurdo nella dimostrazione di $non\, q \Rightarrow non\, p$.
(5) Le dimostrazioni del Lemma 2.6 e del teorema 2.7 sarebbero più limpide con un ragionamento per induzione, ma trattandosi di induzioni "finite" (o "discesa"), le formulazioni del testo non dovrebbero porre (troppi) problemi.

Osservazione 4.1. *Vediamo velocemente, una volta preso per buono gli assiomi di base e la nozione di (buon) ordine su* $\mathbb{N}$*, l'equivalenza tra il principio del minimo e il principio di induzione. Ricordiamo:*

Principio di induzione: *Sia* $X \subset \mathbb{N}$ *un insieme tale che:*

- $0 \in X$
- $n \in X \Rightarrow n+1 \in X$

allora $X = \mathbb{N}$.

Il principio del minimo $\Rightarrow$ il principio di induzione

Sia $X \subset \mathbb{N}$ tale che $0 \in X$ e che verifica $n \in X \Rightarrow n+1 \in X$. Dobbiamo mostrare che $X = \mathbb{N}$. Consideriamo $Z := \mathbb{N} \setminus X$. Se Z è non vuoto, ammette un più piccolo elemento, n_0. Abbiamo $n_0 > 0$, perché $0 \in X$. Quindi $n_0 - 1$ è un intero e $n_0 - 1 \notin Z$, cioè $n_0 - 1 \in X$. Per il principio di induzione $(n_0 - 1) + 1 = n_0 \in X$: assurdo, quindi $Z = \emptyset$ e $X = \mathbb{N}$.

Il principio di induzione $\Rightarrow$ il principio del minimo

Sia $X \subset \mathbb{N}$ un insieme che non ammette nessun elemento minimo e sia $Z = \mathbb{N} \setminus X$. Abbiamo $0 \in Z$ (perché se $0 \in X$, allora $\forall x \in X, 0 \leq x$ e X ha un elemento minimo). Sia $n \in Z$, se mostriamo che $n+1 \in Z$, allora abbiamo finito. Infatti per il principio di induzione si avrà $Z = \mathbb{N}$, ossia $X = \emptyset$.

Mostriamo $n \in Z \Rightarrow n+1 \in Z$ per induzione su n. Per ipotesi di induzione $k \in Z$ se $k \leq n$, ossia $k \notin X$ se $k \leq n$. Se fosse $n+1 \in X$, allora $n+1$ sarebbe un elemento minimo di X (perché $x \in X \Rightarrow x \geq n+1$), ma X non ha nessun elemento minimo, quindi $n+1 \notin X$, cioè $n+1 \in Z$.

Dipartimento di Matematica, 35 via Machiavelli, 44100 Ferrara
E-mail address: phe@unife.it