Politecnico di Milano
Corso di Analisi e Geometria 1

Federico Lastaria
federico.lastaria@polimi.it

Il teorema sulla esistenza di infiniti numeri primi
17 Settembre 2018

1 La classica dimostrazione di Euclide

Definizione 1.1. *Un numero intero maggiore di 1 si dice un numero* primo *se è divisibile soltanto per se stesso e per 1.*

Ad esempio, $2, 3, 5, 7, 11, 13, 17, 19, 23, 29,$ sono numeri primi.

Teorema 1.2 (Teorema di Fattorizzazione Unica, o Teorema Fondamentale dell'Aritmetica)**.** *Ogni numero naturale n maggiore di 1 si può esprimere come prodotto di numeri primi in modo unico (a meno dell'ordine dei fattori).*

Ad esempio, 60 si scrive come: $60 = 2 \cdot 2 \cdot 3 \cdot 5$.

Per la dimostrazione (non difficile) del Teorema Fondamentale dell'Aritmetica, si veda ([1], pag.3).

Teorema 1.3 (Euclide, *Elementi,* circa 300 a.C.)**.** *Esistono infiniti numeri primi.*

La formulazione originaria di Euclide (*Elementi*, libro IX, Proposizione 20) è la seguente:

"I numeri primi sono più numerosi di qualunque assegnata quantità di numeri primi."

Dimostrazione. Sia assegnata una qualunque quantità di numeri primi. Per fissare le idee, chiamiamo (seguendo Euclide) questi numeri primi a, b, c. (Dovremmi dire: $p_1, p_2, ..., p_k$, ma non cambia niente). Dico che esiste un numero primo che *non è uguale a nessuno dei numeri assegnati* a, b, c. Ragioniamo in questo modo: moltiplichiamo tra loro i numeri assgnati a, b, c, e sommiamo 1. Cioè, consideriamo il numero $abc + 1$. Ci sono due casi possibili: o il numero $abc + 1$ è primo, o non lo è. Se è primo, abbiamo finito, perché abbiamo trovato un numero primo ($abc + 1$, appunto) che è sicuramente diverso da ciascuno dei numeri assegnati a, b, c (è piu grande di ciascuno di essi). Supponiamo allora che $abc + 1$ non sia primo. Per il Teorema Fondamentale dell'Aritmetica 1.2, ogni numero intero maggiore di 1 si fattorizza (in modo unico) come prodotto di numeri primi; quindi esiste un numero primo, chiamiamolo d, che divide $abc + 1$. Dico che questo numero primo d è *diverso da ciascuno* dei numeri primi a, b, c. Infatti, supponiamo, per assurdo, che d sia uguale ad a. Poiché d divide $abc+1$ e divide abc (essendo $d = a$), divide anche la differenza tra $abc+1$ e abc, cioè divide 1. Assurdo, perché nessun numero primo divide 1. Abbiamo quindi dimostrato che esiste sempre

un numero primo che è diverso da ciascuno dei numeri primi a, b, c, e questo è quanto si doveva dimostrare. □

Riferimenti bibliografici

[1] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Fourth Edition, Oxford (1960). Disponibile al sito:

https://archive.org/details/AnIntroductionToTheTheoryOfNumbers-4thEd-G.h.HardyE.m.Wright