Dimostrazione che i numeri primi sono infiniti

Fausto Vezzaro

sitofausto@gmail.com

Svilupperemo la dimostrazione in 6 passaggi numerati.

1. Per prima cosa dimostriamo una cosa che ci servirà in seguito nella dimostrazione: qualsiasi numero naturale maggiore di 1 o è primo o è divisibile per un numero primo. Ipotizzare che ciò sia falso è come ipotizzare che

$$\exists x \in \mathbb{N}(x \neq 1, x \notin \mathbb{P}) : (\nexists k \in \mathbb{P} : \frac{x}{k} \in \mathbb{N}) \tag{1}$$

   dove ho denotato con $\mathbb{P}$ l'insieme dei numeri primi. A parole, ipotizzare che non sia vero ciò che stiamo dimostrando, significa ipotizzare che esista un numero che non è primo e che è divisibile solo per numeri non primi. Sia α il più piccolo numero naturale con questa proprietà. I divisori di α, in quanto non primi, devono a loro volta possedere divisori, alcuni dei quali possono essere primi perché α è il più piccolo numero divisibile solo per numeri non primi. Ma il divisore di un divisore è divisore, quindi α deve possedere divisori primi. Siamo giunti a una contraddizione, quindi abbiamo dimostrato per assurdo la tesi.

2. Supponiamo per assurdo che la tesi che ci proponiamo di dimostrare sia falsa, e che dunque esista solo un numero finito di numeri primi. Allora è possibile calcolare il prodotto di tutti i numeri primi (che sarà un numero intero ben definito, visto che si tratta di eseguire un numero finito di moltiplicazioni). Chiameremo N tale prodotto. È chiaro che ogni numero primo n è più piccolo di N e che N è divisibile per ogni numero primo.

3. Consideriamo il numero $M = N + 1$. Dato che tutti i numeri primi sono più piccoli di N, ed M è maggiore di N, M non può essere primo. Allora in base al punto 1 deve esistere un numero primo k tale che $\frac{M}{k} = m$ con m intero. Scriviamo allora

$$M = km \tag{2}$$

4. Anche N è divisibile per k (è divisibile per ogni numero primo!), per cui esiste un numero h (non necessariamente primo) tale che

$$N = kh \tag{3}$$

5. Ma $M = N + 1$. Sostituendo nella 2 e sfruttando la 3 si trova

$$k(m-h) = 1 \qquad \Rightarrow \qquad m - h = \frac{1}{k} \tag{4}$$

6. Il numero $n - h$ è intero perché differenza di interi, mentre $\frac{1}{k}$ non è intero perché $k > 1$ (k è primo, vedi punto 1). L'equazione 4 costituisce dunque una contraddizione: un numero intero non può essere uguale a un numero non intero. Siamo giunti a un assurdo, quindi l'ipotesi dalla quale siamo partiti (esiste un numero finito di numeri primi) è falsa. La dimostrazione è così terminata.