Università degli Studi di Cagliari
Corso di Laurea Triennale in Matematica

Dimostrazione Topologica dell'Infinità dei Numeri Primi

Relatore
Prof. Andrea Loi

Candidato
Andrea Carta

27 Febbraio 2018

Introduzione

In questa tesi daremo una dimostrazione topologica dell'infinità dell'insieme dei numeri primi.
Analizzando in dettaglio l'approccio di Furstenberg, il quale utilizza concetti base della topologia, come spazi topologici, insiemi aperti e insiemi chiusi.

Definizione

- Sia X un insieme non vuoto, una famiglia $\mathcal{T}$ di sottoinsiemi di X è una ***topologia*** in X se e solo se soddisfa i seguenti assiomi:

  Top 1) X,Ø appartengono a $\mathcal{T}$

  Top 2) La unione di un qualsiasi numero di insiemi in $\mathcal{T}$ appartiene a $\mathcal{T}$

  Top 3) La intersezione di un numero finito di insiemi in $\mathcal{T}$ appartiene a $\mathcal{T}$

Definizione

- Gli elementi di $\mathcal{T}$ si chiamano ***insiemi aperti***, e la coppia $(X, \mathcal{T})$ si dice che è uno ***spazio topologico***. I complementari degli insiemi aperti si dicono ***insiemi chiusi***.

Definizione

Sia $\mathbb{Z}$ l'insieme dei numeri interi, e per qualsiasi coppia di numeri interi a e b, con $b > 0$, sia

$$N_{a,b} \equiv \{a + \mathrm{n}b : \mathrm{n} \in \mathbb{Z}\} = \{a, a \pm b, a \pm 2b, \dots\}.$$

La nostra topologia Ƭ sarà quindi definita come

$\mathcal{T} = \{ \mathbb{Z} \} \cup \{ \emptyset \} \cup \{ \mathrm{E} \subseteq \mathbb{Z} : \forall a \in \mathrm{E}$ *esiste* $\mathrm{b} \in \mathbb{Z}$ $\mathrm{b}>0$ t.c $N_{a,b} \subseteq \mathrm{E}\}$

Lemma 1

La coppia ($\mathbb{Z}$,T) è uno spazio topologico.

Dimostrazione

Top 1. $\mathbb{Z}$,Ø ∈ T per definizione.

Top 2. Sia $\{E_i$ i ∈ I$\}$ ∈ T, e sia $a \in \bigcup_{i\in I} E_i$. Allora $a \in E_{i_0}$ per qualche i_0 ∈ I.
Poiché E_{i_0} ∈ T allora esiste b ∈ $\mathbb{Z}$ b>0 t.ale che $N_{a,b} \subseteq E_{i_0} \subseteq \bigcup_{i\in I} E_i$
Quindi $\bigcup_{i\in I} E_i$ ∈ T

Top 3. Supponiamo adesso che E_1, E_2 ∈ T e che $a \in (E_1 \cap E_2)$, Allora esistono $b_1, b_2 \in \mathbb{Z}$ $b_1, b_2 > 0$ tali che $N_{a,b_1} \subseteq E_1$ e $N_{a,b_2} \subseteq E_2$,
Sia $x \in N_{a,b_1 b_2}$, allora per qualche $n \in \mathbb{Z}$ abbiamo che

$$x = a + n(b_1 b_2) = a + (nb_2)\, b_1 = a + (nb_1)\, b_2$$

Allora $x \in N_{a,b_1}$ e $x \in N_{a,b_2} \Rightarrow x \in E_1$ e $x \in E_2 \Rightarrow x \in (E_1 \cap E_2)$, quindi $N_{a,b_1 b_2} \subseteq (E_1 \cap E_2)$.

Lemma 2

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$$

Dimostrazione

$\{N_{a+i,b}\}_{i=0,1,2,\dots,b-1}$ forma una partizione di $\mathbb{Z}$.

Ricoprimento: Sia $x \in \mathbb{Z}$. Allora, per il teorema di divisione euclidea, esistono unici q e r tali che

$$x - a = qb + r \qquad \text{con} \qquad 0 \leq r < b$$

da cui $x = a + r + qb$, ossia $x \in N_{a+r,b}$ e quindi $x \in \bigcup_{i=0}^{b-1} N_{a+i,b}$

Intersezione disgiunta: Siano $i,j = 0, 1, 2,\dots, b-1$. tali che $i \neq j$ e supponiamo per assurdo che esista $x \in N_{a+i,b} \cap N_{a+j,b}$. Allora $x = a + i + kb = a + j + hb$, da cui, supponendo senza perdere di generalità che $j < i$, otteniamo

$$i - j = (h - k)b$$

Ma $0 < i - j \leq b - 1 - j < b$ e quindi $i - j$ non può essere multiplo di b; da qui segue che $h = k$ e, in ultima analisi $i = j$, che è in contraddizione. Segue che $N_{a+i,b} \cap N_{a+j,b} = \emptyset$ se $i \neq j$

Lemma 3

L'insieme $N_{a,b}$ è sia aperto che chiuso.

Dimostrazione

L'insieme $N_{a,b}$ non è vuoto poiché a $\in N_{a,b}$.

Sia $x \in N_{a,b}$, cioè $x = a + nb$ per qualche $n \in \mathbb{Z}$. Per qualunque $y \in N_{x,b}$ abbiamo che

$$y = x + mb = (a + nb) + mb = a + (m + n)b$$

e questo implica che $y \in N_{a,b}$. Allora $N_{x,b} \subseteq N_{a,b}$ quindi è aperto.

Dato che

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$$

Allora, $N_{a,b}$ è chiuso.

Lemma 4

Qualunque insieme aperto non vuoto è infinito.

Dimostrazione

Questa è una conseguenza diretta della definizione di insieme aperto visto che $N_{a,b}$ è infinito e $N_{a,b} \subseteq E$

Lemma 5

$$\mathbb{Z} \setminus \{-1,1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}$$

Dimostrazione

Sia $x \in \mathbb{Z} \setminus \{-1, 1\}$ allora x ha un divisore primo q, cioè $x = mq$ per qualche intero m. Questo implica che $x \in N_{0,q}$ cioè che $x \in \bigcup_{p \in \mathbb{P}} N_{0,p}$. Allora

$$\mathbb{Z} \setminus \{-1, 1\} \subseteq \bigcup_{p \in \mathbb{P}} N_{0,p}$$

Viceversa, sia $x \in \bigcup_{p \in \mathbb{P}} N_{0,p}$ allora $x \in N_{0,q}$ per un certo $q \in \mathbb{P}$ quindi $x = mq$ questo implica che x ha un divisore primo e che quindi $x \in \mathbb{Z} \setminus \{-1, 1\}$. Allora

$$\bigcup_{p \in \mathbb{P}} N_{0,p} \subseteq \mathbb{Z} \setminus \{-1, 1\}$$

Teorema

L'insieme $\mathbb{P}$ è infinito.

Dimostrazione

Supponiamo per assurdo che $\mathbb{P}$ sia finito, allora il lato sinistro di

$$\mathbb{Z} \setminus \{-1,1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}$$

sarebbe un chiuso poiché è unione finita di insiemi chiusi. Quindi {-1,1} è aperto, ma questa è una contraddizione perché tutti gli aperti non vuoti devono essere infiniti. Per tanto esistono infiniti numeri primi.