

LA CONGETTURA DEI NUMERI PRIMI GEMELLI

di Salvatore Ingala

Introduzione

Due numeri primi consecutivi sono detti gemelli quando la loro differenza è pari a 2. Si congettura che esistano infinite coppie di numeri primi gemelli.

Lemma 1. Dati i e k interi, se $i < k < 2i$, allora k non è divisibile per i .

Il primo multiplo di i è il suo doppio, ossia $2i$, per cui k non è multiplo di i .

Lemma 2. Dati a , b ed n interi, se a è multiplo di n e b non è divisibile per n , allora $a + b$ non è divisibile per n .

Infatti $\frac{a+b}{n} = \frac{a}{n} + \frac{b}{n}$, in cui $\frac{b}{n}$ non è una divisione esatta.

1. Progressioni numeriche a ragione variabile

Ai fini della dimostrazione è necessario l'utilizzo delle progressioni numeriche. Si tratterà tuttavia di un particolare tipo di progressioni, differenti da quelle aritmetiche perché la ragione cambia costantemente e in modo ciclico. Indicheremo con $S.i\{d_1; d_2; d_3... d_n\}$ una progressione con i come primo elemento e avente come ragioni rispettivamente $d_1, d_2, d_3... d_n$. Dato che la ragione cambia in modo ciclico, d_{n+m} (con d_n ultima ragione del ciclo e $m \in N$) è uguale a d_n .

Indicando con P_n l' $(n+1)$ -esimo elemento, P_0 è uguale ad i e P_n è uguale a $P_{n-1} + d_n$.

Ovviamente in una progressione di questo tipo non valgono le regole di una progressione aritmetica a ragione costante.

1.1. Progressioni di numeri primi

Escludendo dall'insieme dei numeri naturali i multipli dei primi n numeri primi, si ottengono progressioni con alcune particolari proprietà, la cui analisi è essenziale per la dimostrazione della congettura.

Partiamo togliendo i multipli di 2. L'inizio della progressione sarà 3:

S.3 {2}

La progressione ha cioè 3 come inizio e 2 come ragione, in questo caso costante. L'insieme degli elementi della progressione sarà dunque formato da tutti gli elementi dispari maggiori o uguali a 3. Togliendo anche i multipli di 3, si ottiene la seguente progressione:

S.5 {2; 2+2}

In questo caso abbiamo due diverse ragioni: 2 e 4 (che per comodità scriviamo 2+2). Chiamiamo ogni "2" *componente* della progressione. Ogni ragione sarà formata da una o più componenti. Cerchiamo adesso un metodo per derivare la progressione S.7 sulla base della progressione S.5, escludendo anche i multipli di 5.

Poiché i e la somma delle ragioni sono primi tra loro, ripetiamo i volte l'insieme delle ragioni:

S.5 {2; 2+2; 2; 2+2; 2; 2+2; 2; 2+2; 2; 2+2}

Dato che l'inizio della progressione è 5, ovviamente divisibile per se stesso, i componenti divisibili per 5 saranno quelli la cui posizione è divisibile per 5:

S.5 {2; 2+2; 2; 2+2; 2; 2+2; 2; 2+2; 2; 2+2}

Il primo caso possiamo tralasciarlo, dato che basta considerare i componenti finali delle varie ragioni, i quali vanno invece sommati all'elemento successivo:

S.5 {2; 2+2; 2; 2+2; 2; 2+2; 2+2+2; 2; 2+2+

L'ultima ragione va sommata alla ragione successiva, che trattandosi di progressioni cicliche sarà uguale alla prima; contemporaneamente dobbiamo cambiare l'inizio della progressione, che non sarà più 5 ma sarà $i + d_1$, ovvero $5 + 2 = 7$, e di conseguenza spostare il primo elemento all'ultimo. Avremo perciò:

S.7 {2+2; 2; 2+2; 2; 2+2; 2+2+2; 2; 2+2+2}

Osserviamo che in tutti i casi visti finora la somma delle ragioni è uguale al prodotto di tutti i numeri primi inferiori ad i , e come conseguenza diretta del metodo utilizzato per la derivazione delle progressioni (ovvero la ripetizione delle ragioni per un numero di volte pari ad i) possiamo affermare che per induzione questa proprietà continuerà ad essere valida anche per tutte le progressioni successive.

Per poter giustificare l'utilizzazione di questo sistema di derivazione delle progressioni da progressioni precedenti è necessario dimostrare che $i + d_1$ è il numero primo consecutivo di i .

Poiché esiste almeno un numero primo tra i e $2i$ (Chebyshev) e l'insieme dei numeri primi maggiori di i è un sottoinsieme della progressione, possiamo dedurre che $i + d_1 < 2i$ e di conseguenza che $d_1 < i$. Inoltre, essendo $i + d_1$ minore di $2i$ non sarà divisibile per i (lemma 1) né per nessun numero primo inferiore di i in quanto se così fosse non potrebbe essere membro della progressione. Da ciò deduciamo che $i + d_1$ è il numero primo consecutivo di i .

Riassumendo, le progressioni appena analizzate hanno le seguenti proprietà:

1. gli elementi della progressione non sono divisibili per nessun numero minore di i ;
2. i è un numero primo; $i + d_1$ è il numero primo consecutivo di i ;
3. $d_1 < i$;
4. la somma delle ragioni è uguale al prodotto p di tutti i numeri primi minori di i . Il numero di componenti è invece dato da $\frac{p}{2}$;

2. “Dimostrazione” della congettura

Alla luce delle proprietà delle progressioni di numeri primi viste finora, dimostreremo adesso che tra $S.i$ e $S.(i+d_1)$, ovvero tra due progressioni successive, continuerà ad essere presente almeno una ragione uguale a 2, ossia avente una sola componente.

Per creare $S.(i+d_1)$, il primo passo, come abbiamo visto, è quello di ripetere i volte le ragioni di $S.i$. Quindi da:

$$S.i \{d_1; d_2; d_3 \dots d_n\}$$

passeremo a:

$$S.i \{ \underbrace{d_1; d_2; d_3 \dots d_n}_{1^\circ \text{ gruppo}}; \underbrace{d_{n+1}; d_{n+2}; d_{n+3} \dots d_{n+n}}_{2^\circ \text{ gruppo}}; \underbrace{d_{2n+1}; d_{2n+2}; d_{2n+3} \dots d_{2n+n}}_{3^\circ \text{ gruppo}}; \dots; \underbrace{d_{in+1}; d_{in+2}; d_{in+3} \dots d_{in+n}}_{i\text{-esimo gruppo}} \}$$

Avremo cioè i gruppi di ragioni che si ripetono, e ogni gruppo sarà formato da un numero di componenti pari al prodotto p di tutti i numeri primi minori di i diviso per 2. Dato che i non compare tra i fattori di p , è chiaro che p non è divisibile per i .

Sia d_k (con $1 \leq k \leq n$) una qualunque componente pari a 2, e P_k il $(k+1)$ -esimo elemento della progressione.

Se P_k e P_{k-1} non sono divisibili per i , allora (conseguentemente al metodo utilizzato per la derivazione delle progressioni) la ragione d_k sarà presente anche nella progressione successiva.

Lemma 3. Se P_k è divisibile per i , allora P_{k+n} e P_{k+2n} non sono divisibili per i . Infatti P_{k+n} è uguale a $P_k + p$, e, dato che p non è divisibile per i , $P_k + p$ non è divisibile per i per il lemma 2. Analogamente P_{k+2n} è uguale a $P_k + 2p$, non divisibile per i per il lemma 2.

Si hanno le seguenti possibilità:

- P_k e P_{k-1} non sono divisibili per i . In questo caso la ragione d_k (uguale a 2) sarà presente anche nella progressione successiva.
- P_k e P_{k-1} sono entrambi divisibili per i . Allora per il lemma 3 P_{k+n} e P_{k+n-1} non sono divisibili per i , per cui la ragione d_{k+n} (uguale a 2) sarà presente anche nella progressione successiva.
- P_k è divisibile per i e P_{k-1} non è divisibile per i . In questo caso P_{k+n} e P_{k+2n} non sono divisibili per i per il lemma 3. Se P_{k+n-1} non è divisibile per i , allora la ragione d_{k+n} (uguale a 2) sarà presente anche nella progressione successiva; se P_{k+n-1} è divisibile per i , allora P_{k+2n-1} non è divisibile per i per il lemma 3, per cui la ragione d_{k+2n} (uguale a 2) sarà presente anche nella progressione successiva;
- P_k non è divisibile per i e P_{k-1} è divisibile per i . Per il lemma 3 sappiamo che P_{k+n-1} e P_{k+2n-1} non sono divisibili per i . Se P_{k+n} non è divisibile per i , allora la ragione d_{k+n} (uguale a 2) sarà presente nella progressione successiva; se P_{k+n} è divisibile per i , allora P_{k+2n} non è divisibile per i per il lemma 3, per cui la ragione d_{k+2n} (uguale a 2) sarà presente nella progressione successiva;

In tutti i casi, dunque, nella progressione successiva sarà presente almeno una ragione uguale a 2.

3. Conclusioni

Le congetture riguardanti i numeri primi sono notoriamente tra le più resistenti agli “attacchi” dei matematici che tentano di dimostrarle. Questo perché l’irregolare distribuzione dei numeri primi non permette di trovare una regola di formazione per sapere, ad esempio, l’ n -esimo numero primo.

Alla luce di questa dimostrazione, a mio parere, non restano incertezze (da un punto di vista puramente euristico) sulla veridicità della congettura, anche se una dimostrazione oggettivamente certa appare ancora lontana.

Con questo scritto mi proponevo di suggerire un possibile approccio alla congettura dei primi gemelli.