TEOREMA FONDAMENTALE DEI NUMERI PRIMI

dal libro di Filippo Giordano "Origine e funzione dei numeri primi" in vetrina sul sito internet www.ilmiolibro.it

Enunciato

Sia n un numero naturale qualsiasi. Per qualsiasi n^2 esistono sempre due numeri primi p_1 e p_2 tali che $n^2 - n < p_1 < n^2$ e $n^2 < p_2 < n^2 + n$.
Ne segue che tra n^2 e $(n+1)^2$ esistono sempre almeno due numeri primi.

Definizioni

iT (insieme Triangolare) : insieme di numeri naturali consecutivi compresi tra 1 e n-1 (estremi inclusi): (1, 2, 3, … n-1).
iMa (insieme multiplo, a) : insieme di elementi compresi fra $n(n-1)$ ed n^2, estremi esclusi.
iMb (insieme multiplo, b) : insieme di elementi compresi fra n^2 e $n(n+1)$, estremi esclusi.

Proprietà 1

Qualsiasi valore si attribuisca a n il numero degli elementi dell'insieme *iMa* è sempre uguale al numero degli elementi dell'insieme *iMb* e ciascuno di essi, a sua volta, ha un numero di elementi uguale a quelli dell'insieme *iT*.

Esempio 1
Sia $n = 3$;

iT = { 1, 2 }
iMa = { 7, 8 }
iMb = {10,11 }

Esempio 2
Sia $n = 4$;

iT = { 1, 2, 3 };
iMa = { 13, 14, 15};
iMb = {17, 18, 19 }.

Considerata l'alternanza della parità con la disparità nella successione dei numeri naturali si ha che, partendo da 1, per ogni quantità pari di elementi consecutivi si ha lo stesso numero di elementi pari e dispari; per ogni quantità dispari di elementi consecutivi, nell'insieme c'è prevalenza di una unità dei dispari.

Proprietà 2

Poiché *iT* contiene n-1 elementi, *iT* ha un numero di elementi pari se n è dispari mentre ha un numero di elementi dispari se n è pari. Conseguentemente, *iMa* e *iMb* , che hanno lo stesso numero di elementi di *iT* , hanno un numero di elementi dispari se n è pari mentre hanno un numero di elementi pari se n è dispari.

Esempio 3
Sia n = 5

iT = { 1, 2, 3, 4 } (4 elementi);
iMa = { 21, 22, 23, 24 } (“),
iMb = { 26, 27, 28, 29 } (“).

Esempio 4
Sia *n* = 6

iT = { 1, 2, 3, 4, 5 } (5 elementi);
iMa = { 31, 32, 33, 34, 35 } (“)
iMb = {37, 38, 39, 40, 41 } (“).

Proprietà 3

All’interno della simmetria del numero complessivo di elementi di ciascun insieme *iT, iMa e iMb*, è simmetrico anche il numero di elementi pari e dispari di ciascun insieme. Infatti, quando *n* è dispari l’insieme degli elementi è pari e allora il numero degli elementi dispari è uguale al numero degli elementi pari; invece quando *n* è pari il numero degli elementi di ciascun insieme è dispari, con prevalenza di elementi dispari.

Esempio 5
Sia *n* = 7

iT = {1, 2, 3, 4, 5, 6 } (6 elementi, di cui tre dispari e tre pari);
iMa = { 43, 44, 45, 46, 47, 48 } (“ “ “ “);
iMb = { 50, 51, 52, 53, 54, 55 } (“ “ “ “).

Esempio 6
Sia *n* = 8

iT = { 1, 2, 3, 4, 5, 6, 7 } (7 elementi, di cui quattro dispari e tre pari);
iMa = {57, 58, 59, 60, 61, 62, 63} (“ “ “);
iMb = {65, 66, 67, 68, 69, 70, 71} (“ “ “).

Formule

a) La somma dei valori degli elementi dello *iT* è data dalla formula di Gauss,
   $\boldsymbol{n(n\text{-}1)/2}$.
b) La somma dei valori degli elementi dell'insieme *iMa* è data dalla formula,
   $\boldsymbol{n(n\text{-}1)^2 + n(n\text{-}1)/2}$
c) La somma dei valori degli elementi dell'insieme *iMb* è data dalla formula
   $\mathbf{(n\text{-}1)n^2 + n(n\text{-}1)/2}$.

Esempio 7
Sia $n = 9$
Somma degli elementi **iT** : $\boldsymbol{n(n\text{-}1)/2}$ = 9 x 8 : 2 = 36;
Somma degli elementi **iMa** : $\boldsymbol{n(n\text{-}1)^2 + n(n\text{-}1)/2}$ = (9 x 8 x 8) + (9 x 8 : 2) =
576 + 36 = 612;
Somma degli elementi **iMb** : $\boldsymbol{(n\text{-}1)n^2 + n(n\text{-}1)/2}$ = (8 x 9 x 9) + (9 x 8 : 2) =
648 + 36 = 684.

Esempio 8
Sia $n = 10$

Somma degli elementi **iT** : $\mathbf{n(n\text{-}1)/2}$ = 10 x 9 : 2 = 45;
Somma degli elementi **iMa** : $\mathbf{n(n\text{-}1)^2 + n(n\text{-}1)/2}$ = (10 x 9 x 9) +
+ (10 x 9:2) = 810 + 45 = 855;
Somma degli elementi **iMb** : $\mathbf{(n\text{-}1)n^2 + n(n\text{-}1)/2}$ = (9 x 10 x 10) +
+ (10 x 9:2) = 900 + 45 = 945;

Le formule sopra riportate sono facilmente comprensibili.
La b), per esempio, si deduce in modo naturale dalla struttura stessa dei singoli addendi che così si presentano :

n (n-1) +1
n (n-1) +2
n (n-1) +3
n (n-1) +4
n (n-1) +5
n (n-1) +6
……………

La somma di n-1 di tali addendi, (proprietà 2) dà come risultato la formula su riportata.
Analogo discorso per l'altra formula.

Osservazioni

a) La somma dei valori degli elementi dell'insieme *iMa* è sempre divisibile per la somma dei valori degli elementi *iT* e il risultato è dato dalla formula 2n-1.
b) La somma dei valori degli elementi dell'insieme *iMb* è sempre divisibile per la somma dei valori degli elementi *iT* e il risultato è dato dalla formula 2n +1. (vedere pag. 25)

Esempio 9

Sia n = 9

$$9(9-1)^2+\frac{9(9-1)}{2}=\frac{9(9-1)}{2}(2\cdot 9-1)$$

Il secondo membro dell'uguaglianza mette in chiaro la divisibilità per (2 x 9 -1)

c) Per lo stesso valore di *n*, la somma dei valori degli elementi dispari degli iMa e iMb è sempre divisibile per la somma dei valori degli elementi dispari iT.

Infatti, tenendo conto del fatto che la somma di n numeri consecutivi dispari corrisponde a n^2, l'affermazione precedente resta così giustificata:

se n è pari si ha

$$n(n-1)\frac{n}{2}+\left(\frac{n}{2}\right)^2=\frac{n}{2}\left[n(n-1)+\frac{n}{2}\right]=\frac{n}{2}\left(n^2-\frac{n}{2}\right)=\frac{n}{2}\frac{2n^2-n}{2}=\frac{n^2}{4}(2n-1) \quad ;$$

se n è dispari si ha

$$n(n-1)\frac{n-1}{2}+\left(\frac{n-1}{2}\right)^2=\frac{n-1}{2}\left[n(n-1)+\frac{n-1}{2}\right]=\frac{n-1}{2}\frac{(2n+1)(n-1)}{2}=\frac{(n-1)^2}{4}(2n+1);$$

anche in questo caso è evidente la divisibilità di cui si parlava.

Esempio 10
Sia n = 15

211 + 213 + 215 + 217 + 219 + 221 + 223 = 1519 (somma dei valori degli elementi dispari iMa)

1+ 3+ 5+ 7 + 9+ 11+ 13 = 49 (somma degli elementi dispari di iT)

1519 : 49 = 31 (2 x 15+1)

Ricordando che, per ogni numero naturale *n* , si dicono *banali* i divisori 1 e *n*, e *non banali* tutti gli altri , si ha :

Proprietà 4

Ciascun elemento sia dell'insieme *iMa* che sia dell'insieme *iMb,* essendo compreso fra due multipli consecutivi di *n,* di cui uno corrispondente a n^2 (rispettivamente fra $(n-1)n$ e n^2 e fra n^2 e $n(n+1)$), ha sempre come propri divisori un numero inferiore ad *n* e un numero superiore ad *n,* con la peculiarità che, complessivamente, sia **tutti gli elementi dell'insieme *iMa* che tutti gli elementi dell'insieme *iMb* presentano, sempre e sistematicamente, fra i propri divisori minori di n, tutti gli elementi dell'insieme iT, compreso il divisore *banale 1;*** se, inoltre, in uno o più elementi *iMa* o *iMb* confluiscono diversi divisori minori di *n, ciò causa* una molteplice presenza di altri elementi iMa o iMb con gli stessi divisori minori di *n,* compreso il divisore *banale 1*.

Esempio 11

Sia *n* = 11

elementi di *iMa*, divisore massimo, minore di *n*

111……………………….. 3
112……………………….. 8
113……………………….. **1**
114……………………….. 6
115………………………. 5
116………………………. 4
117………………………. 9
118………………………. 2
119………………………. 7
120 ……………………… 10

Tutti gli elementi di iMa hanno un divisore minore di n = 11, fra loro diversi. Tutti i naturali minori di n sono presenti e nessuno è ripetuto.

Esempio 12
Sia *n* = 11

<u>elementi di *iMb*,</u>   <u>divisore massimo,minore di *n*</u>

122 ………………………… 2
123 ………………………… 3
124 ………………………… 4
125 ………………………… 5
126 ………………………… 6, 7, 9
127 ………………………… **1**
128 ………………………… 8
129 ………………………… 3
130 ……………………….. 10
131 ……………………….. **1**

Si noti che tutti gli elementi di iMb hanno almeno un divisore minore di n = 11. Tutti i naturali minori di n = 11 sono presenti. Su un elemento iMb (126) confluiscono tre divisori minori di n (6, 7, 9) di cui due (6 e 9) sono multipli del 3. Tale concomitanza dei due multipli del 3 è causa stessa della ripetizione del 3 al suo naturale passo successivo (elemento iMb 129). A sua volta la confluenza del fattore 7 è causa della ripetizione del divisore banale 1 presente due volte (elementi 127 e 131).

Proprietà 5

Per ogni valore di n elevato al quadrato c'è una ricorsiva uguaglianza fra gli elementi iT, (i cui valori sono rappresentati dalla prima colonna verticale) e i corrispondenti elementi di iMa, secondo lo schema quadratico seguente che ne ripercorre i primi valori e che, per induzione facilmente verificabile, si può estendere all'infinito.
Le formule che consentono di individuare i divisori degli iMa.
(omissis)

Proprietà 6

Per ogni valore di n elevato al quadrato c'è una ricorsiva uguaglianza fra gli elementi iT, (i cui valori sono rappresentati dalla prima colonna verticale) e i corrispondenti elementi di iMb, secondo lo schema quadratico seguente che ne ripercorre i primi valori e che, per induzione facilmente verificabile, si può estendere all'infinito.

Le formule che consentono di individuare i divisori degli iMb.
(omissis)

Conclusioni:

divisibilità di iMa e iMb

Se, per assurdo, un qualsiasi *insieme multiplo a (iMa)* oppure un qualsiasi *insieme multiplo b (iMb)* non avesse al proprio interno alcun elemento con l'unico divisore banale 1 allora la rispondenza biunivoca con gli elementi iT dovrebbe fare a meno dell'elemento 1 dello insieme Triangolare (iT), ma ciò, essendo il numero 1 parte minima indispensabile dello insieme iT, causerebbe:

1) la non divisibilità della somma dei valori degli elementi di iMa e/o iMb per la somma dei valori degli elementi di It;
2) la non divisibilità della somma dei valori dei soli elementi dispari iMa e/o iMb per la somma dei valori dei soli elementi dispari di It;

e quindi una imperfezione dentro un sistema perfetto.

Invece:
Per ogni valore attribuito ad *n*, ciascun elemento dello iT (insieme triangolare), essendo ciascuno di valore inferiore a *n*, troverà identificazione col fattore -di pari valore- di un suo multiplo in almeno uno degli elementi dello *insieme Multiplo a* (iMa) ed –inoltre- troverà altra identificazione col fattore -di pari valore- di un suo multiplo in almeno uno degli elementi dello *insieme Multiplo b* (iMb). Infatti, ciascun elemento iT, partendo dalla propria postazione naturale e procedendo con passo adeguato al proprio valore, giungerà in ciascuno degli insiemi iMa e iMb, trovando negli elementi dei due insiemi, i propri multipli con fattore minore di *n* identico all'elemento iT.
Successivamente, se vi è la capienza, troverà altri propri multipli con fattore minore di n, a loro volta multipli dello elemento iT, ma loro stessi identici ad altro elemento iT minore di n, oppure ritroverà sé stesso perché nel precedente suo multiplo sono contemporaneamente confluiti diversi suoi multipli con fattori minori di n, primi fra loro. Allora è evidente che, essendo il numero degli elementi iT, iMa, iMb, tutti uguali a n-1 ed essendo i fattori non banali sempre uguali a n-2 (mancando il banale 1), sia Ima che iMb conserveranno alla fine del processo almeno un elemento non fattorizzabile, se non banalmente, e quindi primo.
Inoltre, poiché gli **insiemi multipli a** e gli **insiemi multipli b** sono infiniti e poiché i numeri primi sono elementi di tali insiemi, si deduce che i numeri primi sono infiniti.
C.v.d.

FUNDAMENTAL THEOREM OF PRIME NUMBERS