ALGORITMI PER LA CONGETTURA DI GOLDBACH – G(N) REALE

Napoli 31-10-07
Aggiornato il 07-01-2008

BIOGRAFIA

Rosario Turco è un ingegnere elettronico, laureato all'Università Federico II di Napoli, che lavora dal 1990 in società del gruppo Telecom Italia.

Le sue competenze professionali sono in ambito delle architettetture hw/sw Object Oriented (OOA/OOP, AOP, SOA, Virtualization) e in generale "Java 2 Enterprise Edition". Ha lavorato molti anni nella progettazione e sviluppo di sistemi informatici su piattaforme Windows/Unix/Linux e con linguaggi Java, C, C++.

Negli ultimi anni si sta particolarmente interessando alla crittografia e alla Teoria dei Numeri.

Sommario

Nel seguito viene affrontata la congettura di Goldbach e, nell'ambito della congettura forte, viene percorsa ogni strada per la sua dimostrazione. Si giunge, infine, ad una dimostrazione convincente attraverso una rappresentazione algebrica.

Viene presentato un possibile utilizzo pratico della congettura stessa. Inoltre vengono presentati due algoritmi, uno in linguaggio C relativo alla dimostrazione del calcolo dei composti su di un reticolo quadrato di numeri dispari a partire da 3, ed un secondo algoritmo funzionale con WinHugs (standard Haskell) per il calcolo sia di tutte le soluzioni di Goldbach che dell'ultima soluzione di Goldbach (interessante per i numeri gemelli).

L'algoritmo in C è un algoritmo inedito, ideato dall'autore, per il calcolo del G(N) reale a partire dal reticolo quadrato dei numeri dispari maggiori di 2.

CONGETTURA "DEBOLE" DI GOLDBACH

La congettura debole di Christian Goldbach o "Problema dei tre numeri primi" afferma che: "*Ogni numero naturale dispari maggiore di 5 si può scrivere come somma di tre numeri primi*".

Un'altra versione della stessa congettura dice: "*Ogni numero naturale dispari maggiore di 7 si può scrivere come somma di tre numeri dispari*".

Lehonard Eulero arrivò ad una variante detta Congettura forte di Goldbach.

CONGETTURA "FORTE" DI GOLDBACH

La congettura forte di Goldbach o "Problema binario" è dovuta a Eulero: "*Se n è un numero naturale intero pari e maggiore di 2, allora si possono trovare due numeri primi la cui somma restituisce il numero pari*".

Nota: Lo stesso numero primo può essere usato anche due volte nella somma es: 3+3 ma la somma 5+3 e quella 3+5 vanno considerata una sola volta.

Osservazione 1

Esiste più di una soluzione, il cui numero G(N) è dipendente dal numero di primi minori del numero pari in gioco, in ogni caso il tutto dipendente da N.

Osservazione 2

Risolvere la congettura forte significa anche risolvere la congettura debole; difatti banalmente se ogni numero pari > 4 è la somma di due numeri primi dispari (solo il 2 è un numero primo pari), se si aggiunge 3 al numero pari > 4 questo produrrà numeri dispari > 7.

ANALISI CONGETTURA FORTE DI GOLDBACH

Detto *∏(N) il numero di numeri primi p minori di N (escludendo l'1)*, si ottiene ad esempio per i numeri pari fino a 32 la tabella di seguito proposta.

Numero pari N	Numero soluzioni G(N)	Spazio delle soluzioni della somma dei numeri primi a+b	∏(N)
4	1	2+2	2:(2,3)
6	1	3+3	3:(2,3,5)
8	1	3+5;	4:(2,3,5,7)
10	2	3+7; 5+5	4:(2,3,5,7)
12	1	5+7	5 (2,3,5,7,11)
14	2	3+11;7+7	6:(2,3,5,7,11,13)
16	2	3+13;5+11	7:(2,3,5,7,11,13)
18	2	5+13;7+11	7:(2,3,5,7,11,13,17)
20	2	3+17;7+13	8:(2,3,5,7,11,13,17,19)
22	3	3+19;5+17;11+11	8:(2,3,5,7,11,13,17,19)
24	3	5+19;7+17;11+13	9:(2,3,5,7,11,13,17,19,23)
26	3	3+23; 7+19;13+13	9:(2,3,5,7,11,13,17,19,23)
28	2	5+23;11+17	9:(2,3,5,7,11,13,17,19,23)
30	3	7+23;11+19;13+17	10:(2,3,5,7,11,13,17,19,23,29)
32	2	3+29;13+19	11:(2,3,5,7,11,13,17,19,23,29,31)
34	4	3+31;5+29;11+23;17+17	11:(2,3,5,7,11,13,17,19,23,29,31)
36	4	5+31;7+29;13+23;17+19	11:(2,3,5,7,11,13,17,19,23,29,31)

Osservazione 3

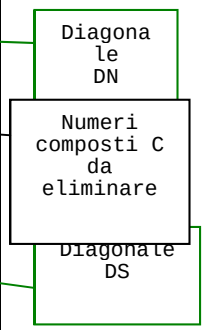
Il numero di soluzioni G(N) cresce con ∏(N); inoltre varia in maniera diversa e sembra che non sia mai nullo, ma può essere G(N)=0 ?.

Nel 1975 Vaughan e Montgomery, con l'ipotesi generalizzata di Riemann (GRH) asserivano che non è vero che esistono sempre soluzioni, ma che possono esistere dei casi per cui non è vero. Sul sito è presentato anche il loro lavoro. Avevano torto o ragione? La loro dimostrazione è basata sul fatto che l'ipotesi di Riemann sia vera.

Una soluzione grafica è costituita dal reticolo completo delle somme dei numeri naturali DISPARI a partire da 3, come nella figura successiva.

Reticolo quadrato delle somme dei numeri naturali DISPARI a partire da 3

	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35
3	**6**	8	10	12	14	16	18	**20**	22	24	26	28	30	32	34	36	38
5	8	**10**	12	14	16	18	**20**	22	24	26	28	30	32	34	36	38	40
7	10	12	**14**	16	18	**20**	22	24	26	28	30	32	34	36	38	40	42
9	12	14	16	**18**	**20**	22	24	26	28	30	32	34	36	38	40	42	44
11	14	16	18	**20**	**22**	24	26	28	30	32	34	36	38	40	42	44	46
13	16	18	**20**	22	24	**26**	28	30	32	34	36	38	40	42	44	46	48
15	18	**20**	22	24	26	28	**30**	32	34	36	38	40	42	44	46	48	50
17	**20**	22	24	26	28	30	32	**34**	36	38	40	42	44	46	48	50	52
19	22	24	26	28	30	32	34	36	**38**	40	42	44	46	48	50	52	54
21	24	26	28	30	32	34	36	38	40	**42**	44	46	48	50	52	54	56
23	26	28	30	32	34	36	38	40	42	44	**46**	48	50	52	54	56	58
25	28	30	32	34	36	38	40	42	44	46	48	**50**	52	54	56	58	60
27	30	32	34	36	38	40	42	44	46	48	50	52	**54**	56	58	60	62
29	32	34	36	38	40	42	44	46	48	50	52	54	56	**58**	60	62	64
31	34	36	38	40	42	44	46	48	50	52	54	56	58	60	**62**	64	66



33	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64	**66**	68
35	38	40	42	44	46	48	50	52	54	56	58	60	62	64	66	68	70

L'eleganza del reticolo quadrato è che mette subito in mostra delle semplici proprietà delle somme di Goldbach:

- considerando le righe del reticolo, se si prende un numero N pari interno al reticolo associato a N-3 della riga (esempio 20 associato a 17), il numero N, si ripete nella "diagonale DN" (DN = Diagonale del numero pari) fino alla colonna del reticolo dove è presente N-3 (17 nell'esempio), per (N-4)/2 volte (8 volte). In altri termini il numero di elementi nella diagonale è:

  (5) DN = (N-4)/2

- Tutti i numeri pari sono presenti G(N) volte in un sottoreticolo triangolare esteso all'infinito e individuato dalla "diagonale di simmetria DS" dove p+q=N e p=q=N/2.
- Le somme che rispettano la congettura di Goldbach sono quelle che fanno riferimento a numeri dispari primi; per cui occorre eliminare, come in un crivello di Eratostene, i composti (multipli dei dispari) presenti in numero C (es: 9, 15, 21) eliminando righe e colonne. Per cui rimangono DN-C somme pari poiché i reticoli sono simmetrici rispetto alla diagonale di simmetria, vanno considerate una sola volta le somme del tipo 3+5 e 5+3; per cui il reticolo da considerare contenente le soluzioni è triangolare. Quindi vanno cancellati nell'esempio tutti i numeri sotto la diagonale che partono dal 6 e arriva a 42. Il reticolo rimanente è quello delle soluzioni di Goldbach dove:

  (6) G(N)=(DN-C)/2

Nel seguito percorreremo le varie strade per comprendere il problema.

Considerazioni e dimostrazione classica

Nel caso di Goldbach è sempre rimasto un dubbio cruciale. L'andamento generale è vero, ma esiste un N per cui G(N)=0 localmente?

Prima di arrivare ad una nostra dimostrazione, che non percorre la strada delle ipotesi di Vaughan e Montgomery, esamineremo il percorso classico delle dimostrazioni e vedremo che non è sufficiente. Certamente il dubbio sulla veridicità o falsità della congettura di Goldbach si eliminerà definitivamente solo nel momento in cui sarà possibile accettare o confutare il lavoro di Vaughan e Montgomery.

Proposizione diretta

Come si potrebbe dimostrare il tutto diversamente? Premettiamo che dati due numeri dispari p e q, la cui somma p+q=N, N è sempre un numero pari e maggiore del singolo p e q.

Un numero dispari è sempre scrivibile come 2n+1 per assioma. Anche i primi sono dispari ad eccezione del 2.

Nel caso particolare p=q=2n+1 si ha p+q=(2n+1)+(2n+1)=4n+2 anch'esso numero pari e posizionato sulla diagonale DS.

Ora tutti i numeri primi, ad eccezione del 2, sono dispari e la loro somma p+q=(2n+1)+(2m+1)=2n+2m+2 è ancora un numero pari, poiché 2n è pari qualunque sia n,

così pure 2m ed il termine 2, pari per definizione. Un numero è difatti considerato pari se è n mod 2= 0, ovvero se il resto della divisione è nullo.

Finora abbiamo anche compreso che la probabilità che non esistano due numeri primi che diano come somma il numero N pari >2 diminuisce al diminuire del valore di N, però tale probabilità non si annulla, perché esiste almeno un numero primo che sommato a sé stesso da il numero N (es: 2+2=4, 3+3=6, 5+5=10, 7+7=14 etc).

La sorte, tra l'altro, ha voluto che nei primi 21 numeri naturali ci siano almeno 8 numeri primi: 2,3,5,7,11,13,17,19. Che succede se eliminiamo un paio di numeri primi, ad esempio 3 e 5?

In figura il reticolo quadrato risultante.

Reticolo quadrato delle somme dei numeri naturali DISPARI a partire da 7

	7	9	11	13	15	17	19	21
7	14	16	18	20	22	24	26	28
9	16	18	20	22	24	26	28	30
11	18	20	22	24	26	28	30	32
13	20	22	24	26	28	30	32	34
15	22	24	26	28	30	32	34	36
17	24	26	28	30	32	34	36	38
19	26	28	30	32	34	36	38	40
21	28	30	32	34	36	38	40	42

Si nota subito che eliminando 3 e 5 spariscono le somme dei numeri pari 6, 8, 10, 12; quindi se si eliminano k primi dal reticolo, spariscono le prime 2k somme. Mentre i rimanenti pari riducono il loro numero di soluzioni. Ad esempio il 14 è ottenibile solo come 7+7 mentre prima disponeva anche di 3+11.

La probabilità, invece, di trovare somme con numeri primi aumenta all'aumentare di N, perché aumenta $\prod(N)$ e in tal caso aumentano anche le soluzioni di Goldbach.

Il "nocciolo del problema" è di verificare che per un numero pari maggiore di 2 esistono sempre due numeri dispari entrambi primi, la cui somma dia il numero pari. L'avverbio "sempre".

Proposizione inversa

Analizziamo la proposizione inversa della congettura, invertendo ipotesi e tesi: "la somma di due numeri dispari e primi maggiori di 2 (unico numero primo pari) da sempre un numero pari maggiore di 2" è vera; il fatto che i numeri devono essere primi rappresenta la condizione necessaria e sufficiente (tra dispari e primi) della proposizione inversa della congettura forte di Goldbach. In altri termini la proposizione inversa è vera. Di fatti l'insieme dei numeri primi, escluso il 2, è incluso nell'insieme dei numeri dispari. La condizione è necessaria e sufficiente perché si ricade nell'assioma. Mentre il solo fatto che "i numeri siano dispari" è una condizione necessaria ma non sufficiente, perché sommando due numeri dispari non primi e maggiori di 2 oppure sommando un numero dispari con un numero primo entrambi maggiori di 2 si ottiene un numero pari maggiore di 2. Questo punto significa anche che "un numero pari maggiore di 2" è solo una condizione necessaria ma non sufficiente della congettura forte di Goldbach per poter dire che esistono due numeri primi la cui somma dia il numero pari.

Proposizione contraria

La “proposizione contraria” della congettura, ottenuta negando ipotesi e tesi è falsa:”Ogni numero dispari non è somma di due numeri primi”. Basta pensare a p=7 e q=2 e che 7+2=9.

Proposizione contronominale
La proposizione contronominale, negando ipotesi e tesi e invertendole tra loro, dice: “Presi dei numeri non primi, la loro somma da un numero dispari”. E’ falsa. Basta pensare a 9+15=24.

Dimostrazione per assurdo
La dimostrazione per assurdo richiede di negare la tesi per contraddire l’ipotesi, per cui dovremmo affermare che:”Un numero pari maggiore di 2 non è somma di due primi”. Allora presi due primi, anche uguali, si scopre che:3+3=6, 3+5=8, 3+7=10, etc. Per cui l’ipotesi è contraddetta e come conseguenza la congettura forte di Goldbach è vera. Ma è “sempre” vera?

Il dubbio
In realtà nella congettura sono gli avverbi sottintesi “almeno” o “sempre” che negli anni sono stati messi in dubbio, cioè che “dato un numero pari maggiore di due si possono sempre trovare due numeri primi la cui somma ridiano il numero pari”. Però per trovare una controprova occorre trovare una coppia $p,q = \{p,q \in N \mid p,q \text{ primi}\}$ tale che non sia vera l’ipotesi della congettura, ma finora non s’è mai provata neanche computazionalmente.

Quanto vale C?

Riuscire a calcolare C nella formula G(N)=DN-C/2 significherebbe calcolare il G(N) reale in modo preciso. Il che potrebbe dare ulteriori elementi di indagine e di riflessione.

Ad esempio nel caso delle somme di Goldbach per N=20 le soluzioni sono G(N)=2, il che significa che nella (6) C deve valere 4. Ma come si fa a vedere sul reticolo delle somme che C=4?

DETERMINAZIONE DI C PER G(N) REALE – ALGORITMO RISOLUTIVO

Se si osserva il reticolo quadrato, in riferimento alle cancellazioni delle soluzioni, ogni numero pari è interessato dai composti precedenti al numero stesso nel reticolo quadrato. Una soluzione algoritmica, da me proposta, per il calcolo della cancellazione dei composti si basa semplicemente sulle seguenti regole:

1. se il numero N-3 non ha composti precedenti, il numero di cancellazioni è zero o con peso 0;
2. ogni composto precedente a N-3 va considerato con peso 2;
3. ogni composto che sommato a sé stesso è uguale al numero N va considerato di peso 1;
4. presi due composti, la cui somma danno il numero N, il più grande composto dei due si conta con peso 0 (per evitare di contare due volte le cancellazioni non si contano le 2 del composto più grande);
5. Quando N-3 e il composto sono uguali, si include anche N-3 come composto e con peso 2;
6. La divisione (DN-C)/2 va arrotondata per eccesso. Ad esempio se il risultato della divisione è 2,5 il valore ottenuto va arrotondato a 3.

Uno schema è presentato nella tabella successiva.

N Numero pari	N-3	Composto successivo a N-3	Numeri composti precedenti a N-3	C cancellazioni	DN=(N-4)/2	DN-C	G(N)= (DN-C)/2
6	3	9	0	0	1	1	1
8	5	9	0	0	2	2	1
10	7	15	0	0	3	3	2
12	9	15	1	2	4	2	1
14	11	15	1	2	5	3	2
16	13	15	1	2	6	4	2
18	15	15	2	1+2 (1)	7	4	2
20	17	21	2	2+2	8	4	2
22	19	21	2	2+2	9	5	3
24	21	21	3	2+0(2)+2	10	6	3
26	23	25	3	2+2+2	11	5	3
28	25	25	4	2+2+2+2	12	4	2
30	27	27	4	2+1+2+2 (3)	13	6	3
32	29	33	5	2+2+2+2+2	14	4	2
34	31	33	5	2+2+2+0+2 (4)	15	7	4
36	33	33	6	2+2+0+2+0+2 (5)	16	8	4
38	35	39	7	7*2=14	17	3	2
40	37	39	7	6*2+0=12 (6)	18	6	3

(1) col composto 9: 1 soluzione perchè 9+9=18
(2) coi composti 15 e 9: Il 15 più grande si conta 0
(3) col composto 15: 1 soluzione perchè 15+15=30
(4) i composti con somma 34 sono 9+25, per cui 25 ha peso 0
(5) i composti con somma 36 sono 9+27 e 15+21, per cui sia 27 che 21 hanno peso 0
(6) i composti con somma 40 sono 15+25, per cui il 25 ha peso 0.

Questo comporta di dover saper calcolare tutti i numeri composti dei numeri dispari che esistono prima del numero N-3 con N-3 incluso. Non è difficile creare un algoritmo che faccia tali calcoli.

Una osservazione circa l'arrotondamento per eccesso: si nota che è sempre di 0,5 e non per tutti i calcoli ovvero in molti casi non è necessario l'arrotondamento; cioè se indichiamo con **ar l'arrotondamento** risulta che esso è sempre contenuto nell'intervallo di valori tale che:

$$\mathbf{0 \leq ar \leq 0{,}5}$$

Se con un excel si verificano i valori reali (DN-C)/2 si nota tale andamento. Il che è quasi sempre dovuto ad un valore dispari di DN rispetto ad un C pari, ma sempre con DN>C. Se entrambi DN e C sono dispari non c'è arrotondamento.

Rappresentazione algebrica del problema di Goldbach

Un'altra osservazione si può fare ripensando al reticolo e all'algoritmo proposto. Soffermiamoci su N=18 della figura sottostante. Si osserva che la diagonale DN ha la stessa quantità di numeri (N-4/ 2) del lato dei numeri che vanno da 6 a 18 orizzontale e anche nel caso verticale, cioè pari a [(N-6)/ 2 +1] = (N-4)/ 2 dove vi sono sia i primi che i composti che danno luogo alle cancellazioni.

A	15	13	11	9	7	5	3
B	3	5	7	9	11	13	15
DN	**18**	**18**	**18**	**18**	**18**	**18**	**18**

In effetti DN è un vettore riga ottenuto dalla somma di due vettori A e B di uguale cardinalità m (m elementi), cioè:

$$DN = A + B = B + A, \text{ con } dni=ai+bi$$

In generale l'operatore somma è una trasformazione o una funzione che mappa nel caso che stiamo esaminando due insiemi di numeri dispari maggiore di 2 fino a N-3, qualunque sia N, in uno solo di numeri N pari:

$$+ : A,B \rightarrow DN$$

In generale si dice "Relazione binaria sugli insiemi A e B è un sottoinsieme $\Re$ del prodotto cartesiano A x B, cioè a $\Re$ appartengono tutte le coppie o n-ple ordinate (a,b) con $a \in A$ e $b \in B$".

Se A=B oppure nel caso di vettori riga $B=A^T$ (dove T=trasposta) allora <u>la relazione $\Re$ è una relazione su A</u>.
Nel nostro caso $A=\{a |\ a>2,\ a \in [3..N-3], a \text{ dispari}\}$ e $B=A^T$ perché $B=\{b |\ b>2,\ b \in [N-3..3],\ b \text{ dispari}\}$ dove a=b.

In particolare la soluzione di Goldbach **non** scaturisce dalla **relazione totale $\Re$=A x B** ma da un suo sottoinsieme $\Re_g$, cioè da una relazione binaria che seleziona solo le coppie di numeri dispari primi di A x B e che sono compresi nell'intervallo [3..N-3], qualunque sia N pari. La relazione $\Re$ come anche $\Re_g$ gode anche di simmetria, perchè $A=A^T$.

In altri termini Goldbach è:
$A=\{a |\ a>2,\ a \in [3..N-3], a \text{ dispari}\}$ e $B=A^T$ o $B=\{b |\ b>2,\ b \in [N-3..3],\ b \text{ dispari}, a=b$
$\forall (a \in A, b \in B)$: a dispari primo, b dispari primo $\exists$ N pari

$$\Re_g : (a,b) \rightarrow a+b=N$$

Se ritorniamo a parlare in termini vettoriali (o anche di n-ple) se m è la cardinalità o l'ordine di A e di B, anche DN ha cardinalità m; ovviamente la somma di vettori gode anche della proprietà commutativa.

Vettore delle soluzioni Goldbach Vsg_N
Possiamo considerare **Vsg_N il "Vettore delle soluzioni Goldbach o n-pla delle soluzioni di Goldbach"**, quel vettore Vsg_N tale che il generico elemento:

- $Vsg_N i = ai+bi$ se ai è primo e bi è primo,
- $Vsg_N i=0$ se ai o bi non sono primi ma almeno uno è un composto
- $Vsg_N i=0$ quando si supera l'elemento centrale di posizione=N/2 (perché le situazioni 3+5 e 5+3 vanno contate una sola volta).

La definizione del vettore o dell'n-pla rispetta funzionalmente il fatto che le soluzioni di Goldbach, cioè le coppie di dispari anche numeri primi che mi danno una soluzione uguale a N pari (ma devo escludere la parte simmetrica), sono date da:

```
goldbach n = [(x,n-x) | x <- [3..n], x <= n-x, isprime x, isprime (n-x)]
```

N	Vsg_N	G(N)
6	(3,0)	1
8	(8,0)	1
10	(10,10,0)	2
12	(0,12,0,0)	1
14	(14,0,14, 0,0)	2
16	(16,16,0,0,0,0)	2

18	(0,18,18,0,0,0,0)	2
20	(20,0,20,0,0,0,0,0)	2
22	(22,22,0,0,22,0,0,0,0)	3

In base a quanto abbiamo finora visto le cose fondamentali per il prosieguo della dimostrazione sono:

- essendo m l'ordine di A e B, il numero di elementi di DN è uguale a quello di A e di B.
- il mapping dai due vettori A,B ad uno DN, o della relazione $\Re$ che è una relazione su A, ci porta alla conclusione che è sufficiente analizzare uno solo dei vettori, ad esempio A. In altri termini possiamo ragionare sull'ordine di A anzicchè su quello di DN.

Dimostrazione (R. Turco)
In base ai due punti di sopra si può scomporre il vettore A di ordine m in due vettori:

- **Vettore dei primi Vap** di ordine m
- **Vettore dei composti Vac** di ordine m

$$A = Vap + Vac$$

I due vettori sono definiti nel seguente modo:

- Vap=ai se ai è primo o Vap=0 se ai è composto
- Vac=ai se ai è composto o Vac=0 se ai è primo

In realtà Vap contiene per ogni N tutti i dispari da 3 a N-3 e da cui eliminiamo poi i composti, per cui rimangono solo primi. Tale vettore, per costruzione, non può avere nulli tutti i dispari dell'intervallo [3..N-3], che rappresentano una "proiezione" di dispari sul DN costituito da N pari in gioco, anche perché qualsiasi N pari riusa sempre tutti i dispari rimasti del mapping appartenente all'intervallo [3..N-3] del pari immediatamente precedente.

Se chiamiamo np il numero di primi e nc il numero di composti allora:

$$m = np + nc$$

cioè la somma dei numeri di primi e dei numeri composti deve corrispondere alla cardinalità m (numero di dispari tra [3..N-3])che corrisponde al numero di elementi di DN.

Per assurdo almeno np=1 e al massimo nc=m-1; cioè per assurdo Vap deve avere almeno un primo mentre il resto degli elementi sono a 0 e Vac per assurdo dovrebbe avere tutti composti tranne uno a zero in corrispondenza del primo di Vap.

La vera dimostrazione sarebbe quella della proposizione diretta: "Nell'ambito della congettura forte di Goldbach, dato un numero N pari maggiore di 2 e due Vettori di numeri primi a partire da 3, con i vettori A e B tali che $B=A^T$, nel vettore B non esistono composti dispari consecutivi nell'intervallo $[(N/2)_d, N-3]$, tali da annullare

contemporaneamente tutti i numeri primi nell'intervallo precedente $[3,(N/2)_d]$ del vettore A, dove $(N/2)_d$ è il valore dispari maggiore o uguale a N/2." .

In pratica ragionando per assurdo, per ottenere che vengano cancellati tutti i primi dell'intervallo $[3,(N/2)_d]$ deve sempre essere che N-3 è composto, N-5 è composto, N-7 è composto etc. almeno fino al valore dispari maggiore o uguale a N/2.

Ovvero che fissato un N qualsiasi pari, nell'intervallo $3..(N/2)_d$ ci sono dei primi ma nell'intervallo tra $(N/2)_d..N$ ci sono solo composti.

Se si dimostrasse che tutto ciò è impossibile questo garantirebbe che:

$$nc < m.$$

Un Teorema interessante è: "*Esiste sempre un primo p nell'intervallo* $n \leq p < 2n$". Esso è **il Postulato di Bertrand**, dimostrato da Chebyshev.

Il teorema è possibile anche interpretarlo che "esiste sempre un primo nell'intervallo N/2 e N". Per cui questo dimostrerebbe che la proposizione precedente che "nell'intervallo N/2 e N ci siano tutti composti" è falsa.

D'altra parte supponiamo per assurdo che N=6 e che abbiamo un insieme finito A=[3] e che tra 3..6 non esistono primi ma solo composti. L'algoritmo successivo dimostra che ciò non è vero:

a. N/2=3
b. p←3
c. q←p+2
d. Se q è primo N/2←N/2+2 e si ritorna a c.

Cioè nel tentativo di cercare quel valore di N/2 da cui esistono solo composti fino a N, noteremo che N/2 si incrementerà all'infinito.

Di conseguenza è vero che:

$$nc < m \text{ (ovvero } G(N)=0 \text{ è impossibile)}$$

Ma i composti veramente influiscono sulle soluzioni di Goldbach oppure no?

Con i concetti emersi dall'algoritmo si possono poi fare ulteriori osservazioni. Se poniamo $C=C_2+C_1$, dove C_2 è la somma dei pesi dei composti che danno luogo a cancellazioni di peso 2 e C_1 l'analoga per quelli di peso 1, si ottiene che:

$$G(N) = DN/2 - C_2/2 - C_1/2, \text{ per cui è:}$$

$$G(N) = G^*(N) - [G_2(N) + G_1(N)] \quad (7)$$

Si deduce, poi, che per N pari e N<10

$$G(N)=G^*(N)=DN/2 \quad (8)$$

E' sempre vero che G*(N) ≥1. G*(N) rappresenta il numero di soluzioni sulla diagonale DN.

Se si traccia su degli assi cartesiani G*(N)=DN/ 2 (arrotondato all'intero per eccesso) sulle ordinate ed N sulle ascisse, si vede un andamento a scalino di G*(N) al crescere di N.

Inoltre per N≥12 vale la (7). Dove si può asserire che $1 \geq G_1(N) \geq 0$, perché $G_1(N)$ è dovuto a quei composti tali che N = N/ 2+N/ 2 con N/ 2 intero; il che è possibile una sola volta per un dato N. In tal caso G1(N) = (1+1)/2=1.

Intanto non può essere che $G^*(N) < G_1(N)=1$. Difatti significherebbe che:

$$DN/2 = (N-4)/4 < 1$$

da cui N < 8; ma per N=6 G(N)=G*(N)=1. Per cui G*(N) ≥1.

$G_2(N)$, per come è definito, corrisponde al numero di composti che danno cancellazioni di peso 2. Per essere G(N) non nullo deve essere $G^*(N) > G_2(N)+G_1(N)$.

Occorrerebbe, quindi, dimostrare che è vera questa espressione per ogni N. In altri termini serve dimostrare, ritornando alla situazione del reticolo, che il numero di complessi C<DN.

Un modo di ragionare è al contrario con la proposizione inversa già vista prima, cioè quello di verificare che dati due primi, se è possibile iterativamente ottenere tutti i pari maggiore di 2, senza utilizzare i composti (cioè che i composti alla fine non influiscono sulle soluzioni di Goldbach).

Una formula generatrice di pari maggiori di 2 con p e q primi maggiori di 2 è la seguente:

p=3
q=p+2k, con k>0

k	**Q**	**N ottenuti**
1	5	6,8,10
2	7	12,14 oltre ai precedenti
3	9	Non lo considero il **composto 9** (cancella 16,18)
4	11	16,18,20,22 oltre ai precedenti
5	13	24,26 oltre ai precedenti
6	15	Non considero il **composto 15** (cancella 28,30)
7	17	28,30,32,34 oltre ai precedenti
8	19	36,38

9	21	Non lo considero il **composto 21** (cancella 40,42)
10	23	40,42,44,46

Con tale formula generatrice di pari maggiore di 2 si dimostra che l'effetto dei composti è nullo sui primi rimanenti, perché il numero primo successivo al composto fornisce le soluzioni dei pari cancellati dal composto e le sue soluzioni pari.

Per cui effettivamente:

$$G^*(N) > G_2(N)+G_1(N)$$

Per cui G(N) non può annullarsi per nessun N, ovvero le cancellazioni dovute ai composti effettivamente sono tali che:

$$C < DN \text{ nella formula } G(N) = (DN - C)/2.$$

ANDAMENTO GRAFICO DI G(N)

E' possibile generare l'andamento grafico di G(N) in funzione di N, ad esempio con una semplice utilità grafica come gnuplot (Vedi APPENDICE). Tramite un programma C è possibile ottenere su un file l'insieme dei punti N, G(N) da visualizzare con l'utilità.

L'andamento a cresta o a zig-zag è stato l'elemento che ha creato il dubbio che G(N) potesse annullarsi per qualche N pari.

INSIEMI ECCEZIONALI DI GOLDBACH

Vaughan e Montgomery hanno dimostrato che esistono degli insiemi: E(x) = {x pari | x non è somma di due numeri primi}.

Questo però non invalida la seguente proposizione: **"Esistono infinite soluzioni di Goldbach tali che degli interi pari e maggiore di 2 sono somma di due numeri primi" (R. Turco).** Tale affermazione deriva dal fatto che, per costruzione, un qualsiasi computer rifacendosi ad esempio alla espressione funzionale in APPENDICE sottoposta a WinHugs (goldbach n) troverà sempre soluzioni escludendo l'insieme E(x).

APPLICAZIONI DI GOLDBACH

Nel seguito vengono indicate alcune delle possibili applicazioni del Teorema della congettura forte di Goldbach.

GENERATORE DI PRIMI

La congettura/ Teorema Goldbach è possibile sfruttarla come generatore di due primi. Per un umano è più semplice pensare casualmente ad un numero pari di k cifre del tipo:

$2x10^7$, $2x7x10^{20}$, etc

Allora con un semplice programma potremmo trovare la i-esima soluzione di Goldbach per tale numero pari e ottenere due numeri primi casuali, dove la casualità è legata solo a quella del numero pari di partenza.

Con la generalizzazione è possibile ottenere anche coppie di numeri primi positivi e negativi.

STUDIO DEI NUMERI GEMELLI
Il gruppo ERATOSTENE ha dimostrato il legame esistente tra i numeri gemelli (primi consecutivi o a distanza 2) e le soluzioni di Goldbach. Per cui è vero il Teorema: "Per N pari e nella forma N=12n (forma padre) la coppia di numeri primi ottenibile dall'ultima soluzione di Goldbach è costituita da due numeri gemelli" (M. Nardelli - F. Di Noto).

La condizione N pari e N=12n è la condizione necessaria ma da sola non sufficiente. La condizione necessaria e sufficiente è che N pari, N=12n e che i primi siano l'ultima coppia delle soluzioni di Goldbach.

IMPLEMENTAZIONE DELL' ALGORITMO DI RICERCA SOLUZIONI DI GOLDBACH
Presentiamo due algoritmi, uno in linguaggio C ed uno funzionale con WinHugs (standard Haskell).

L'algoritmo proposto precedentemente, per gli interi positivi, implementabile in linguaggio C si basa sul concetto di ricercare sul reticolo quadrato i numeri composti dispari minori o uguali a N-3 generati dalla formula con 2i+1, a partire da i=N-3 fino a 3 e verificando per quale valore è divisibile il composto.

Nel cercare i composti, occorre evitare di contarli due volte tra i due cicli for. I numeri dispari, nei due cicli for, è come se fossero su due righe appaiate e con valori dispari al contrario.

Es: Per N=18 -> N-3 = 15 e le due righe sono:

15	13	11	9	7	5	3
3	5	7	9	11	13	15

Da notare che verticalmente la somma è sempre 18. L'algoritmo cerca i "composti con i valori a scendere della prima riga", composti che corrispondono a quelli divisibili per un "numero dispari con valore a salire della seconda riga". Per il composto trovato si verificano le regole discusse precedentemente.

Tuttavia questo metodo ha il "difetto" che per calcolare il G(N) reale di un N elevato bisogna scorrere a "forza bruta" tutti i composti. L'algoritmo fornito è circa $O(N^3)$, cioè al crescere di N i tempi di elaborazione diventano cubici.

In APPENDICE presentiamo tre algoritmi:

- un primo algoritmo in linguaggio C, limitato a numeri interi a 32 bit o 64 bit a seconda della macchina in gioco per determinare le soluzioni di Goldbach.
- Un secondo algoritmo in linguaggio funzionale WinHugs, molto sintetico data la natura del linguaggio e sempre per le soluzioni di Goldbach
- Un terzo algoritmo in linguaggio C per ottenere su file le soluzioni di Goldbach e presentarle con gnuplot graficamente a video.

APPENDICE
Nel seguito sono proposti su Windows due compilatori open source: DevC++ e WinHugs e l'utilità GNUPLOT, tutti liberamente scaricabili da INTERNET.

ALGORITMO LINGUAGGIO C PER LE SOLUZIONI DI GOLDBACH
Sorgente divisibilita.h

```
int divisibile(unsigned long int Num, unsigned long int Div);
unsigned long int quoto(unsigned long int Num, unsigned long int Div);
int GiDiN(unsigned long int N);
int GiDiNWithPlot(unsigned long int N);
```

Sorgente divisibilita.c

```
#include <stdio.h>
#include <stdlib.h>
#include "divisibilita.h"

int divisibile(unsigned long int Num, unsigned long int Div){
  int ret=0;

  if( Num%Div == 0)
    ret = 1;

  return ret;
}

unsigned long int quoto( unsigned long int Num, unsigned long int Div){
   unsigned long int quot=0;
   quot = Num/Div;
   return quot;
}
```

Sorgente giDiN.c

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>

int GiDiN(unsigned long int N){

     unsigned long int i=0, j=0, k=0, t=0, pesoTot=0, peso=0, DN=0, GN=0,
countComposti=0, CompostobyExam=0;

     if( N <= 4 ) return -1;
     if( N%2 != 0 ) return -2;
     printf("\n*******************************************",N);
     printf("\nValore richiesto G(%d) ...",N);
     printf("\nRicerca composti tra 3 e %d ...\n",N-3);


     if( N-3 < 9 ){
       pesoTot = 0;
     }
     else
     {
            peso = 0;

            for(j=N-3; j>=3; j=j-2) {  /* Cerco i composti a scendere */

              for(i=3; i<j; i=i+2){    /* a salire cerco i divisori */

                  if( divisibile(j,i) == 1){   /* Se il composto è divisibile
per un numero dispari */
                      printf("\n\n%d \tdivisibile per %d: -> %d composto", j, i,
j);
                      countComposti++;
                      peso = 2;
```

```
                        for(t=i; t<j; t=t+2){  /* Cerco il composto che sommato al
precedente mi da N */

                          if( (prime(t,0) != 1) && (t + j) == N ){
                             printf("\n\t%d+%d=%d", t,j, N);
                             peso = 0;
                             t=N;        /* Per uscire dal for */
                           }

                        }

                        i = N;  /* per uscire dal for xchè basta trovare un
divisore affinchè sia composto */

                        if( (j+j) == N ){
                           peso = 1;
                           printf("\n%d+%d=%d\n", j, j, N);

                        }

                        printf("\n%d \tpeso %d", j, peso);
                        pesoTot = pesoTot +  peso;


                     }/* if */

                   }/* for */
              }/* for */

     }/* fine else */

     /* Applico le formule */

     DN = (N-4)/2;
     if( (DN - pesoTot)%2 == 0 ) /* Se è divisibile (senza resto) uso la formula
senza approssimazione */
        GN = (DN - pesoTot)/2;
     else
        GN = ((DN - pesoTot)/2) + 1; /* altrimenti approssimo */

     printf("\n\nPeso complessivo per %d composti : %d", countComposti,
pesoTot);
     printf("\n\n#composti : %d", countComposti);
     printf("\nN-3: %d", N-3);
     printf("\nDN : %d", DN);
     printf("\nG(%d) : %d", N, GN);
     printf("\n*********************************************\n",N);

     return;
}
```

Sorgente prime.c

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>

unsigned long int prime(unsigned long int iVal, int iDeb)
{
  int i=0, iCount=0;
  unsigned long int iSq=0, iPri=0;

  /* iCount conta i Divisori */
```

```
  float fVal = iVal;

  if( (iVal == 0) || (iVal ==1) ) return iPri;  /* si esclude lo zero e l'1 */

  iSq = sqrt(fVal);

  if( iDeb > 0 )
    printf("\n sqrt : %d\n", iSq);

  if( iVal%2 == 0){

     iCount++;
  }
  else{
    /* Cerco i divisori con il modulo escludendo l'1 e il 2*/

  for(i=3;i<=iSq;i=i+2){ /* Cerco i divisori dispari */
       if( iVal%i == 0) {
         iCount++; /* Esiste un divisore, allora non è primo */
         break;    /* Interrompo al primo Divisore trovato */
       }
   }
  }
  if (iCount == 0 ) iPri=1;  /* Se iCount = 0 allora è primo */

  return iPri;
}
```

Sorgente main.c

```
#include <stdio.h>
#include <stdlib.h>
#include "divisibilita.h"

int main(int argc, char *argv[])
{
  unsigned long int i=0, Num=0, Val=0;
  int retcode=0;

  do{
       printf("\n\n*** Calcolo di G(N) reale delle soluzioni di Goldbach ***");
       printf("\n\nInserisci il numero pari di cui calcolare G(N) (0 per
uscire): ");
       scanf("%d",&Num);
       if( Num != 0 ){

          retcode=GiDiN(Num);
          if( retcode == -1 ){
            printf("\nWarning il numero deve essere pari e maggiore di 4 per
avere come somma due numeri dispari...\n\n");
          }
          if( retcode == -2 ){
            printf("\nIl numero non risulta pari ...\n\n");
          }
          system("PAUSE");
       }


     }while(Num != 0 );

  return 0;
}
```

ALGORITMO FUNZIONALE (WINHUGS) PER LA RICERCA DELLE SOLUZIONI DI GOLDBACH

Sorgente math.hs

```
divide k n = mod n k == 0
factors n = [k | k <- [1..n], divide k n]
isprime n = factors n == [1,n]
listprime n = [k | k <-[2..n], isprime k]
goldbach n = [(x,n-x) | x <- [3..n], x <= n-x, isprime x, isprime (n-x)]
g n = length (goldbach n)
lastg n = last(goldbach n)
```

ALGORITMO G(N) CON GNUPLOT

GNUPLOT è liberamente scaricabile da INTERNET. L'algoritmo in C proposto chiede fino a che numero pari si vuole generare G(N) e crea un file gn.txt contenente la coppia di valori N, G(N). Poi si lancia gnuplot.exe.

Come suggerisce il programma C si può inizialmente, a scopi di valutazione di come varia G(N), accontentarsi del grafico prodotto col comando:

gnuplot>plot "gn.dat" with lines

Successivamente si può studiare l'help e tutte le possibilità di gnuplot col comando:
gnuplot>help

Sorgenti C e H precedenti necessari:

- divisibilita.h
- divisibilita.c
- prime.c

SORGENTI ULTERIORI

gdiNwithPlot.c

```
include <stdio.h>
#include <stdlib.h>
#include <math.h>

int GiDiNWithPlot(unsigned long int N){

     unsigned long int i=0, j=0, k=0, t=0, pesoTot=0, peso=0, DN=0, GN=0,
countComposti=0;
     FILE *fp;

     if( N <= 4 ) return -1;
     if( N%2 != 0 ) return -2;


     if( N-3 < 9 ){
       pesoTot = 0;
     }
     else
     {
            peso = 0;

            for(j=N-3; j>=3; j=j-2) {  /* Cerco i composti a scendere */

              for(i=3; i<j; i=i+2){    /* a salire cerco i divisori */
```

```
                  if( divisibile(j,i) == 1){   /* Se il composto è divisibile
per un numero dispari */

                      countComposti++;
                      peso = 2;


                      for(t=i; t<j; t=t+2){  /* Cerco il composto che sommato al
precedente mi da N */

                        if( (prime(t,0) != 1) && (t + j) == N ){

                           peso = 0;
                           t=N;        /* Per uscire dal for */
                         }

                      }

                      i = N;  /* per uscire dal for xchè basta trovare un
divisore affinchè sia composto */

                      if( (j+j) == N ){
                         peso = 1;


                      }

                      pesoTot = pesoTot +  peso;

                   }/* if */

                 }/* for */
            }/* for */

     }/* fine else */

     /* Applico le formule */

     DN = (N-4)/2;
     if( (DN - pesoTot)%2 == 0 ) /* Se è divisibile (senza resto) uso la formula
senza approssimazione */
        GN = (DN - pesoTot)/2;
     else
        GN = ((DN - pesoTot)/2) + 1; /* altrimenti approssimo */

     fp=fopen("gn.txt","a");
     if( fp != NULL ){
       fprintf(fp,"%d %d\n", N, GN);
       fclose(fp);
     }
     else{
       return -3;
     }
     return 0;
}
```

main.c

```
#include <stdio.h>
#include <stdlib.h>
#include "divisibilita.h"

int main(int argc, char *argv[])
```

```
{
  unsigned long int i=0, Num=0, Val=0;
  int retcode=0;

        printf("\n\n*** Calcolo di G(N) reale delle soluzioni di Goldbach ***");
        printf("\n\nInserisci fino a che numero pari vuoi il G(N): ");
        scanf("%d",&Num);

        if( Num < 6 ) {
             printf("\nWarning il numero deve essere pari e maggiore di 4 per
avere come somma due numeri dispari...\n\n");
             system("PAUSE");
             exit(0);
        }
          system("DEL gn.txt");
          for( i=6; i<=Num; i=i+2 ){

             retcode=GiDiNWithPlot(i);
             if( retcode == -1 ){
               printf("\nWarning il numero deve essere pari e maggiore di 4 per
avere come somma due numeri dispari...\n\n");
               break;
             }
             if( retcode == -2 ){
               printf("\nIl numero non risulta pari ...\n\n");
               break;
             }
             if( retcode == -3 ){
               printf("\nError file di plot non trovato ...\n\n");
               break;
             }

          }
          if( retcode == 0 ){
            printf("\n\nPredisposto file gn.txt da usare con gplot\n\n");
            printf("\nLancia gnu.bat e otterrai il prompt DOS di gplot.\n");
            printf("\ngnuplot> plot \"gn.txt\" with lines \n\n");
            system("PAUSE");
          }


  return 0;
}
```