Congettura debole di Goldbach già dimostrata.

Ne consegue la congettura forte

(accenni alla fattorizzazione alla Fermat e alla RH1)

Gruppo "B. Riemann"*

Francesco Di Noto, Michele Nardelli

***Gruppo amatoriale per la ricerca matematica sui numeri primi, sulle loro congetture e sulle loro connessioni con le teorie di stringa.**

Abstract

In this paper we show the connections between, strong Goldbach's conjecture and weak Goldbach's conjecture, recently proved.

Riassunto

Dalla recente dimostrazione della congettura debole di Goldbach (N' dispari maggiore di 5, ossia N $\geq$ 7, ne consegue automaticamente la dimostrazione della congettura forte (N pari $\geq$ 4 come somma di due numeri primi)

°°°°°°°°°°°°°°

Prima di mostrare la nostra dimostrazione, riportiamo qualche brano

di Wikipedia

Congettura debole di Goldbach

Da Wikipedia, l'enciclopedia libera.

Nella teoria dei numeri, la **congettura debole di Goldbach**, conosciuta anche come **congettura di Goldbach sui dispari** o **problema dei 3 primi**, afferma che:

- **Ogni numero dispari maggiore di 7 può essere espresso come somma di tre primi dispari.**

o equivalentemente:

- **Ogni numero dispari maggiore di 5 può essere espresso come somma di tre numeri primi.**

(Un numero primo può essere usato più di una volta nella somma.)

…

Nel 1997, Deshouillers, Effinger, Te Riele e Zinoviev dimostrarono[1] che l'ipotesi di Riemann generalizzata implica la congettura di Goldbach debole. Questo risultato combina un'affermazione generale per numeri maggiori di 10^{20} con una ricerca estensiva al computer per casi piccoli. **Inoltre, se la Congettura di Levy fosse vera, la congettura debole di Goldbach sarebbe vera anch'ess**a.

Nel 2012 e 2013 Harald Helfgott ha pubblicato su internet due articoli che dimostrerebbero la congettura incondizionatamente per ogni intero maggiore di 7.[2][3][4]

…"

Osservazioni:

noi abbiamo da tempo mostrato che il numero minimo come somma di tre primi è 7 (Riferimenti finali riguardanti Goldbach), quindi senza bisogno di grandi numeri connessi con l'ipotesi di Riemann generalizzata, e anche la verità della congettura di Levy, dalla quale abbiamo ottenuto un'ipotesi RH - equivalente (vedi Riferimenti finali riguardanti Riemann).

Inoltre, Wikipedia sembra ancora scettica sulle recenti proposte di dimostrazione da parte di Harald Helfgott:

“Nel 2012 e 2013 Harald Helfgott ha pubblicato su internet due articoli che dimostrerebbero la congettura incondizionatamente per ogni intero maggiore di 7.[2][3][4] “

Nostra nuova proposta di dimostrazione della congettura forte di Goldbach basata proprio sulla proposta di Harald Helfgott

senza condizioni e con numero minimo 7

Da N’ dispari $\geq$ 7, somma di tre primi, ne togliamo uno qualsiasi dei tre (che è dispari) , rimane un numero pari N somma dei due numeri primi rimanenti, proprio come dice la congettura forte di Goldbach , che così ne consegue automaticamente, per tutti i numeri dispari $\geq$ 7 e per tutti i numeri pari $\geq$ 4

esempi:

5 +13 + 19 = 37 = N’ dispari somma di tre primi

37 - 5 = 32 = 13 + 19 quindi 37 = 5 + 13 + 19 tre primi

37 -7 = 30 = 17 + 13 37 = 7 + 17 + 13 tre primi

37 - 13 = 24 = 5 + 19 37 = 13 + 5 +19 come sopra

37 – 19 = 18 = 13 + 5 37 = 19 + 13 +5 come sopra

37 - 23 = 14 = 3 + 11 **37 = 23 + 3 + 11 altri tre primi**

37 - 29 = 8 = 3 + 5 **37 = 29 + 3 + 5 altri tre primi**

Cosi' pure anche per tutti gli altri numeri dispari, a cominciare dal 7 = 2 + 2 +3 con 7 numero minimo per la congettura debole di Goldbach; i numeri dispari che generano il numero pari 4 = 2+2 sono di forma N' - p = 4 sono somma dei tre primi p, 2, 2, quindi d = p +2 +2 , i soli casi in cui è presente 2 poiché 2 è il solo numero numero primo pari . Escludendo il 4, che pure soddisfa la congettura debole per N' = p +2 +2, tutti gli altri numeri pari generati sono somma di due numeri primi dispari, per es. 6 = 3 +3, 8 = 3+ 5,

10 = 3 + 7 = 5 +5

12 = 5 +7, ecc.

9 = 3 +3 + 3

9 - 3 = 6 = 3 +3 **9 = 3 + 3 + 3 tre primi con 3 ripetuto**

9 – 5 = 4 = 2 + 2 **9 = 5 + 2 + 2 tre primi, con 2 ripetuto**

Notiamo che, nelle righe evidenziate in giallo, (ma anche nelle altre) vi sono i numeri 3, 5, 8 e 13, tutti numeri di Fibonacci e i due numeri 8 e 24 che sono rispettivamente i numeri connessi ai modi che

corrispondono alle vibrazioni fisiche delle superstringhe e delle stringhe bosoniche attraverso le seguenti equazioni modulari di Ramanujan:

$$8 = \frac{1}{3} \frac{4\left[anti\log \frac{\int_0^\infty \frac{\cos \pi txw'}{\cosh \pi x} e^{-\pi x^2 w'} dx}{e^{-\frac{\pi t^2}{4} w'} \phi_{w'}(itw')} \right] \cdot \frac{\sqrt{142}}{t^2 w'}}{\log\left[\sqrt{\left(\frac{10+11\sqrt{2}}{4} \right)} + \sqrt{\left(\frac{10+7\sqrt{2}}{4} \right)} \right]} . \quad (1)$$

$$24 = \frac{4\left[anti\log \frac{\int_0^\infty \frac{\cos \pi txw'}{\cosh \pi x} e^{-\pi x^2 w'} dx}{e^{-\frac{\pi t^2}{4} w'} \phi_{w'}(itw')} \right] \cdot \frac{\sqrt{142}}{t^2 w'}}{\log\left[\sqrt{\left(\frac{10+11\sqrt{2}}{4} \right)} + \sqrt{\left(\frac{10+7\sqrt{2}}{4} \right)} \right]} . \quad (2)$$

La congettura ammette le ripetizioni di uno dei tre primi

11 = 3 + 5 +3

11 - 3 = 8 = 3 + 5   11 = 3 + 3 + 5   tre primi con 3 ripetuto

11 - 5 = 6 = 3 + 3   11= 5 + 3 + 3   tre primi come sopra

11 – 7 = 4 = 2 +2   11 = 7 + 2 +2   tre primi con 2 ripetuto

13 = 3 + 5 + 5   …

13 - 3 = 10 = 5 + 5   …

13 - 5 = 8 = 3 + 5   …

13 - 7 = 6 = 3 +3 **…**

15 = 3 +7 + 5 = 5 + 5 + 5 **…**

15 - 3 = 12 = 5 + 7 **…**

15 - 5 = 10 = 3 + 7= 5 + 5 **…**

15 – 7 = 8 = 5 +3 **…**

15 - 11 = 6 = 3 +3 **…**

e cosi via: togliendo da ogni numero dispari N’ $\geq$ 7 progressivamente tutti i numeri primi successivi da 3 fino a N’ – 4 (si esclude N’- 2 poiché 2 è minore di 4 , numero minimo per la congettura forte di Goldbach, e quindi non può essere la somma di due numeri primi), si ottengono altrettanti numeri pari, a loro volta somma di due numeri primi, e anche più di una volta. Più grande quindi è N’, maggiori possibilità ci sono affinché sia somma di tre primi, e quindi non esistono contro esempi, e pertanto la congettura debole è vera.

Anche qui nelle due righe evidenziate in giallo, vi sono i numeri 3, 5 e 8 che sono numeri di Fibonacci ed il numero 8 che è connesso ai modi corrispondenti alle vibrazioni fisiche delle superstringhe attraverso la seguente funzione modulare di Ramanujan:

$$8 = \frac{1}{3}\frac{4\left[anti\log\frac{\int_0^{\infty}\frac{\cos\pi t x w'}{\cosh\pi x}e^{-\pi x^2 w'}dx}{e^{-\frac{\pi t^2}{4}w'}\phi_{w'}(itw')}\right]\cdot\frac{\sqrt{142}}{t^2 w'}}{\log\left[\sqrt{\left(\frac{10+11\sqrt{2}}{4}\right)}+\sqrt{\left(\frac{10+7\sqrt{2}}{4}\right)}\right]}.$$

Infine, i numeri pari di forma 6k e quindi multipli di 6, hanno più coppie di Goldbach (circa il doppio) rispetto ai numeri pari vicini di forma 6k – 2 e 6k +2, e tutti i numeri pari sono di forma 6k-2, 6k e 6k +2, come da seguente tabella 1, per k a partire da 1 .

Il numero 2 è di forma 6k +2 per k = 0, poiché 6*0 +2 = 0 +2 = 2

TABELLA 1

6k -2	**6k**	**6k+2**
4	**6**	**8**
10	**12**	**14**
16	**18**	**20**
22	**24**	**26**
…	**…**	**…**

Poiché la formula approssimativa del numero G(N) delle coppie di Goldbach è N / (ln N)^2, e tale formula dà risultati sempre crescenti

per 6k -2 e 6k +2 (circa il doppio per 6k) , la congettura forte di Goldbach è anch'essa vera.

(Negli esempi precedenti tutti i numeri pari più piccoli compaiono sempre, e aumentando N' appaiono anche tutti gli altri numeri pari più grandi in ordine decrescente, e sempre più volte). La suddetta formula dà risultati approssimativi ma molto attendibili, con piccole differenze tra stima e valori reali.

TABELLA 2

N pari	$(\ln N)^2$ crescente	$N/(\ln N)^2$ crescente	Valore reale Crescente irregolare	differenza intera
4	1,92	2,08	1	1
6	3,21	1,86	1	0
8	4,32	1.85	1	0
10	5,30	1,58	2	1
12	6,17	1,94	1	0
14	6,96	2,01	2	0
16	7,68	2,08	2	0
18	8,35	2,15	3	1
20	8,97	2,22	2	0
22	9,55	2,30	3	1
24	10,10	2,37	3	1
26	10,61	2,45	3	1
…	…	…	…	…
118	22,75	5,18	6	1
120	22,92	5,29	12	7
122	23,07	5,28	4	1
…	…	…	…	…

Come si vede, all'inizio , per numeri pari piccoli, il maggior numero di coppie di Goldbach non si nota tanto, ma per numeri più grandi, per esempio 120, tale differenza si nota bene, poiché 12 di 120 è il doppio del 6 precedente di 118 e il triplo di 4 per 122. Il perché è spiegabile con il fatto che per numeri pari N di forma 6k, i multipli di 3 e di altri numeri primi formano molte coppie tra loro , lasciando più spazio ai numeri primi di formare altre coppie di Goldbach; mentre per numeri di forma 6k - 2 e 6k + 2 si formano molte più coppie miste tra numeri primi e numeri composti, diminuendo le possibilità di formazione di coppie di Goldbach (entrambi primi).Vedi riferimento finale sui numeri primoriali e la congettura di Goldbach. Nei numeri primoriali si ha il massimo numero di coppie di Goldbach rispetto ai numeri pari precedenti.

Notiamo che, nelle prime due colonne evidenziati in giallo, vi sono i numeri 8, 16, 24 e 120 (16 = 8 * 2 e 120 = 24 * 5), dove 8 e 24 sono rispettivamente i numeri connessi ai modi che corrispondono alle vibrazioni fisiche delle superstringhe e delle stringhe bosoniche attraverso le seguenti equazioni modulari di Ramanujan:

$$8=\frac{1}{3}\frac{4\left[anti\log\dfrac{\int_0^\infty \dfrac{\cos\pi txw'}{\cosh\pi x}e^{-\pi x^2 w'}dx}{e^{-\frac{\pi^2}{4}w'}\phi_{w'}(itw')}\right]\cdot\dfrac{\sqrt{142}}{t^2 w'}}{\log\left[\sqrt{\left(\dfrac{10+11\sqrt{2}}{4}\right)}+\sqrt{\left(\dfrac{10+7\sqrt{2}}{4}\right)}\right]}. \quad (1)$$

$$24=\frac{4\left[anti\log\dfrac{\int_0^\infty \dfrac{\cos\pi txw'}{\cosh\pi x}e^{-\pi x^2 w'}dx}{e^{-\frac{\pi^2}{4}w'}\phi_{w'}(itw')}\right]\cdot\dfrac{\sqrt{142}}{t^2 w'}}{\log\left[\sqrt{\left(\dfrac{10+11\sqrt{2}}{4}\right)}+\sqrt{\left(\dfrac{10+7\sqrt{2}}{4}\right)}\right]}. \quad (2)$$

Interessanti anche i numeri* 4,32 7,68 10,10 *e* 22,92 *che sono connessi al rapporto aureo* Φ (1,61803398…), *al suo inverso* 1 / Φ (0,61803398…) *ed a* π . *Infatti abbiamo:

Φ^3 = 4,236 ≈ 4,320; Φ^4 + 1 / Φ = 6,8541 + 0,618… = 7,472 ≈ 7,680;

Φ^5 – (1 / Φ) = 11,09016 – 0,61803398… = 10,472 ≈ 10,100;

Φ^7 – Φ^4 = 29,0344 – 6,8541 = 22,18 ≈ 22,92;

π^2 + (1 / Φ) = 10,487 ≈ 10,100; 2π + Φ = 7,9012 ≈ 7,68;

π + 2(1 / Φ) = 4,3770 ≈ 4,32; π^3 – π^2 + Φ = 22,7547 ≈ 22,92.

Le terne di Goldbach della congettura debole dipendono, come numero, T(N’) dal numero G(N) delle coppie di Goldbach dei numeri pari N che si ottengono dalle differenze N = N’ - p. Se N’ - p è un numero pari di forma 6k, e quindi con più coppie di Goldbach, si

hanno quindi anche un maggiore numero di terne T(N').

Ovvio che le Terne di Goldbach per un certo N' dispari sono quindi più numerose delle coppie di Goldbach per i due numeri N pari vicini, e cioè N' - 1 ed N' +1.

Qui abbiamo la congettura forte per due numeri primi (k =2) , e la congettura debole per tre numeri primi (k = 3).

Ma la congettura di Goldbach può essere estesa, e dimostrata, per qualunque numero k >3, e con numero minimo $N_{min} = 2k$ se k è pari , e 2k+1 se k è dispari . Per la congettura forte, infatti N_{min} è, con k=2, 2*2 = 4, mentre per la congettura debole abbiamo N_{min} = 2*3 + 1 = 7, coerentemente con la dimostrazione di Harald Helfgott. (vedere Riferimenti finali per Goldbach, in particolare 5a), sulle estensioni della congettura di Goldbach a k primi)

Conclusioni e conseguenze

Possiamo concludere che dalla dimostrazione della congettura debole di Goldbach ne consegue direttamente e immediatamente, come abbiamo visto, la dimostrazione della congettura forte, e , indirettamente, tutte le altre congetture estese riguardanti qualsiasi

numero k di numeri primi la cui somma sia N pari o dispari, rispettivamente con k pari o dispari , purchè il numero minimo N_{min} sia 2k e 2k+1 affinchè N sia somma di k primi.

Conseguenze della dimostrazione della congettura di Goldbach si potrebbero avere per la fattorizzazione più veloce dei numeri RSA con rapporto r = q/p variabile da 1 a 2 o poco più. Per esempio, per un rapporto r ≈ 2, p è ≈ 70% di n = √N , e la somma *p + q* è di poco superiore a 2n (esattamente 2n per *q* e *p* numeri primi gemelli). Per cui essendo q ≈ 2p, p + q ≈ 3p , e quindi p ≈ 2n/3 e q ≈ 3n / 2, formule interessanti per numeri RSA con rapporto r ≈ 2 .

Il problema è che è difficile trovare il rapporto esatto conoscendo solo N = p*q, tranne che nei casi in cui p e q sono primi gemelli o molto vicini, e quindi con rapporto leggermente superiore ad 1, poiché in tal caso la parte decimale di n è molto alta, tipo 0,9…, mentre per rapporti più alti , da 1 a 2, tale parte decimale diventa caotica è non più utilizzabile per stimare il rapporto r = q/p (vedi Rif. finali sulla Fattorizzazione e i numeri RSA , in particolare 2c) sulla nostra "Ipotesi percentuale", non ancora dimostrata, e 6a) sul nostro teorema fondamentale della fattorizzazione, TFF, da noi

recentemente elaborato e dimostrato).

La congettura di Goldbach è stata già usata per costruire algoritmi con cui tentare la fattorizzazione numeri RSA, ma senza grossi risultati, poiché la crittografia RSA è ancora vigente. Tali algoritmi, spesso basati sulla fattorizzazione alla Fermat, potrebbero essere migliorati in futuro, ma non è questo il nostro scopo principale (che è quello di conoscere bene i numeri primi e le loro connessione, in questo caso Goldbach e fattorizzazione più o meno veloce).

Del resto, per fattorizzare un numero RSA -2048, di 617 cifre, occorrerebbero circa 15 miliardi di anni (l'età dell'Universo), e con la nostra formula p ≈ 2n/3 ci metteremo solo 5 miliardi di anni al massimo, ma non è proprio un gran progresso. Fattorizzare numeri RSA di 200 o 300 cifre non è però più un gran problema con i calcoli a mezzo GRID o supercomputer, e tali numeri saranno sostituiti dall'anno prossimo, 2014, con numeri RSA - 2048 o anche più grandi, per una maggiore sicurezza informatica*. Tuttavia, la congettura di Goldbach, apparentemente inutile, potrebbe essere, se studiata bene a fondo, essere utile per algoritmi di fattorizzazione più veloci.

L'algoritmo di Fermat tiene conto della semisomma *s = (p+q)/2*, ed è

molto efficiente per numeri *p* e *q* gemelli o comunque molto vicini, per cui sarebbe sconsigliabile usarli per formare grossi numeri RSA. Solo in questo caso la congettura di Goldbach, per via della suddetta semisomma *s*, e della semidifferenza *d* se molto piccola , sembrerebbe allora veramente pericolosa per la crittografia RSA.

Riportiamo un breve brano sulla sicurezza informatica:

*** Infine se la vostra richiesta di sicurezza è "assoluta", come ad esempio per applicazioni militari, il suggerimento è di usare chiavi a 2048 o 4096 bit.**

Andrea Pasquinucci

Consulente di Sicurezza Informatica

pasquinucci@ucci.it

Anno	***Personale***	***Aziendale***	***Governativo***
1995	**768**	**1280**	**1536**
2000	**1024**	**1280**	**1536**
2005	**1280**	**1536**	**2048**
2010	**1280**	**1536**	**2048**
2015	**1536**	**2048**	**2048**

Lunghezza minima (in bits) delle chiavi RSA per uso Personale, Aziendale e Governativo consigliata da Bruce Schneier in *Applied Cryptography*, 1995

Dal sito del Prof. Andrea Pasquinucci:

www.ucci.it/docs/ICTSecurity-2002-01.pdf

1. **“ ICT Security n.1 Maggio 2002** p. 1 di 3

La crittografia a chiavi pubbliche è a rischio? “

Ecco perché la congettura di Goldbach, attualmente ritenuta frettolosamente poco utile e in genere trascurata dalla comunità matematica ufficiale (i dilettanti invece sono più interessati e prolifici nei tentativi di dimostrare la congettura, spesso con discreti risultati) invece in futuro potrebbe essere molto importante (per esempio suggerisce di evitare imprudenze tipo l’uso di numeri gemelli o molto vicini per formare numeri RSA facilmente fattorizzabili nella crittografia RSA). I numeri primi per formare numeri RSA sono però scelti con algoritmi random , cioè casuali, e quindi potrebbero generare coppie di numeri primi vicini, e pertanto potrebbero sfuggire ad un eventuale controllo preventivo in tal senso.

Un altro legame molto importante potrebbe esserci con l’ipotesi RH1, ipotesi RH equivalente, poiché, per numeri pari N di forma 6k, il numero di coppie di Goldbach è direttamente proporzionale all’abbondanza (somma di divisori σ(n)/N), molto importante nella RH1 (abbiamo proposte di dimostrazione, vedi Rif, 1 a) e 2 a) finali)

Riferimenti finali

a) Sulle congetture di Goldbach

1a) " I numeri primoriali p# alla base della dimostrazione definitiva della congettura di Goldbach (nuove evidenze numeriche)"

Francesco Di Noto, Michele Nardelli

2a) "CONCETTO MATEMATICO DI "ABBONDANZA" E IL RELATIVO GRAFICO PER LA RH1 "

Francesco Di Noto, Michele Nardelli (Gruppo B. Riemann)

3a) "NOVITA' SULLA CONGETTURA DEBOLE DI GOLDBACH"

Gruppo "B.Riemann"

Francesco Di Noto,Michele Nardelli

4a) "TEORIA COMPUTAZIONALE DEI NUMERI E IL PROBLEMA P = NP: i tempi di calcolo per la fattorizzazione come sottoproblema di P = NP, in particolare per i numeri RSA con la congettura forte " p' primo minimo = $2n/3 \approx 67\%$ di $n = \sqrt{N}$"

Gruppo "B. Riemann"

Francesco Di Noto, Michele Nardelli

5a) ESTENSIONI DELLE CONGETTURE, FORTE E DEBOLE,

DI GOLDBACH (a k = primi , con N e k entrambi pari o dispari)

Gruppo “B. Riemann”*

Francesco Di Noto, Michele Narde

6a) “ IL TEOREMA FONDAMENTALE DELLA FATTORIZZAZIONE”

Gruppo “B.Riemann”*

Francesco Di Noto, Michele Nardelli

7a) “FATTORIZZAZIONE VELOCE COME PROBLEMA NP (NON POLINOMIALE)”

Gruppo “B.Riemann”*

Francesco Di Noto, Michele Nardelli

8a) “ PROBLEMI NP: LE APPROSSIMAZIONI DELLA NATURA E QUELLE DEI MATEMATICI “

Gruppo “B. Riemann”

9a) Alcuni metodi noti di fattorizzazione veloce (crivello quadratico, radici quadrate di 1 mod N, algoritmo di fattorizzazione di Fermat, di Pollard, congettura debole e forte e ipotesi percentuale per i numeri RSA con un attendibile rapporto q/p ≈ 2)

Francesco Di Noto, Michele Nardelli

10a) “Matematica con i numeri primi e le forme 6k $\pm$ 1”

Francesco Di Noto, Michele Nardelli, Pier Francesco Roggero

b) Sulle ipotesi RH equivalenti

1b) "IPOTESI SULLA VERITA' DELLE CONGETTURE SUI NUMERI PRIMI CON GRAFICI COMET E CONTRO-ESEMPI NULLI (Legendre, Goldbach, Riemann...) "

Michele Nardelli ,Francesco Di Noto

2b) "**La funzione di Landau come ipotesi RH equivalente II (La nostra proposta di dimostrazione empirica con tabelle e grafico comet; ulteriori connessioni con le partizioni di numeri)** "

Francesco Di Noto e Michele Nardelli

3b) "Ipotesi sulle funzioni zeta per altre serie numeriche simili alla serie dei numeri primi"

(I "parenti poveri" dei numeri primi : numeri fortunati, numeri di Polignac, numeri di Cramer ecc. Analogie con i numeri primi, relative funzioni zeta con probabile parte reale ½ anche per essi).

Francesco Di Noto, Michele

4b) "Congettura di Levy come ipotesi RH equivalente e relativo grafico comet"

Gruppo "B. Riemann"*

Francesco Di Noto, Michele Nardelli

5b) "Ipotesi RH equivalenti, le funzioni σ(n), φ(n), (n) e le forme

numeriche 6k $\pm$ 1 (Accenno finale alla relazione Fattorizzazione veloce – RH) “

Gruppo “B. Riemann”*

Francesco Di Noto, Michele Nardelli, Pier Francesco Roggero

c) Sulla fattorizzazione e i numeri RSA

1c) “Connessione tra ipotesi RH e crittografia RSA: un mito da sfatare

Francesco Di Noto, Michele Nardelli

2c) “Ipotesi su p < n come possibile percentuale di n = √N per una fattorizzazione più veloce “

Francesco Di Noto, Michele Nardelli

3c) “I numeri semiprimi e i numeri RSA come loro sottoinsieme”

Francesco Di Noto, Michele Nardelli

4c) “I NUMERI RSA : UNA PICCOLA STATISTICA SUI RAPPORTI r = q/p E RELATIVE OSSERVAZIONI “

Gruppo “B. Riemann”

Francesco Di Noto , Michele Nardelli

5c) “INFINITE ESTENSIONI DEI NUMERI PRIMI DI SOPHIE

GERMAIN (connessioni con test di primalità e fattorizzazione veloce)

Gruppo “B. Riemann”

Michele Nardelli, Francesco Di Noto

6c) PROPOSTA DI FATTORIZZARE IL NUMERO RSA- 2048

cercando p tra il 70 % e il 71% della sua radice quadrata,

corrispondente ad un rapporto r = q/p ≈2)

Gruppo “B. Riemann

Nardelli Michele, Francesco Di Noto

FINE