

PERCHE' CERCARE NUMERI PRIMI GRANDI?

Sul sito del prof. Umberto Cerruti:
http://alpha01.dmunito.it/personalpages/cerruti/primi/primi_grandi/motivazioni.html possiamo leggere, tra tante altre cose sui numeri primi, anche l'articolo "Perché cercare numeri primi grandi?", che per i lettori eventualmente interessati riportiamo per esteso (con qualche nostro commento ove occorra), essendo interessati all'argomento. La caccia ai grandi numeri primi è infatti nel nostro programma, già con qualche risultato positivo (vedi "Lavori Prof. Di Maria") e con una nuova ricerca attualmente in corso.

Perché cercare numeri primi grandi?

1. Per passione e tradizione

Certamente passione e tradizione sono due motivazioni fondamentali che spingono l'uomo ad avventurarsi in luoghi inesplorati o – non è così diverso come può sembrare – a difendere e continuare ciò che corre il rischio di di essere perduto per sempre o di inaridire. I numeri interi sono la strada verso l'infinito, una strada bene ordinata dove ad ogni passo cisi accorge di poter proseguire. A molti sono sembrati e sembrano il fondamento dell'universo: per questo i numeri primi, gli indivisibili, che formano ogni intero, hanno affascinato _ almeno dal 300 AC, i tempi di Euclide – ogni matematico e tante altre persone."

Commento: perfettamente d'accordo, questa è una delle nostre motivazioni. Ricordiamo anche Pitagora, il primo pensare che l'intero universo sia regolato dai numeri. Noi

del nostro piccolo gruppo Eratostene, possiamo aggiungere che i numeri scelti dalla natura per governare e regolare l'universo sono in modo particolare sia i numeri primi, sia anche quelli di Fibonacci e le partizioni di numeri, $p(n)$.. Vedi nostro recente lavoro “La serie di Fibonacci e le altre serie numeriche naturali (s_{nn}) – come la natura evita i quadrati” (al quale seguirà tra qualche mese la seconda parte, con sottotitolo “perché la natura evita i quadrati”, ed entrambi dedicati a Pitagora e a Fibonacci.

2. Per le tecniche matematiche e informatiche sviluppate nella ricerca.

Gran parte della teoria dei numeri è nata e cresciuta attorno alla ricerca dei numeri primi. Per più di tre secoli l'ultimo teorema di Fermat è stato un formidabile motore per il progresso dei più diversi settori della matematica. Il problema del millennio, la più importante congettura aperta della matematica, riguarda la distribuzione dei numeri primi, ovvero gli zeri della funzione zeta di Riemann.

Su un problema apparentemente esoterico come la congettura di Goldbach è stato persino scritto un gradevolissimo romanzo!

Eseguire milioni di quadrati con numeri di milioni di cifre non è certo facile! Questo è però necessario per eseguire certi testi di primalità. Come sempre la necessità di superare i limiti posti dall'hardware e dalle tecniche di calcolo ha portato ad importanti innovazioni. Ne citiamo due.

- . utilizzare networks di migliaia di PC messi in rete
- . moltiplicare con la Fast Fourier Transform

Commento: anche questa è una nostra motivazione, per esplorare gli angoli ancora bui della Teoria dei numeri in generale e dei numeri primi in particolare. Circa l'ultimo teorema di Fermat, lo abbiamo collegato sia alla congettura di Goldbach, sia all'ipotesi di Riemann. Su quest'ultima abbiamo già scritto diversi articoli, alcuni anche con l'aiuto

del nostro collaboratore esterno Ing. Rosario Turco, che stà continuando ancora in questa importante direzione.

Circa la congettura di Goldbach, abbiamo già pubblicato sul nostro sito e sui siti collegati diversi lavori sulla sua soluzione e sulle connessioni con altre congetture (primi gemelli, ecc.).

3. Per collezionismo.

Da sempre gli uomini collezionano cose grandi e preziose (sovente preziose in quanto rare)

Che dire dunque dei numeri di Mersenne?

Negli ultimi 2300 anni sono stati trovati soltanto 40 numeri di Mersenne!

4. Per agonismo

A tutti piace essere primi in qualcosa, possedere un record, vedere ciò mai che occhi umani hanno visto prima.

La storia dei numeri primi è anche una storia di records: si veda lo splendido libro di Ribenboim, "The book of prime number records" Superate il record (2002, J.Gallot) dei primi gemelli!

5. Per arricchirsi

. Premio di 100.000 \$ per un primo di 10.000.000 di cifre, etc...

. Premio di 1.000.000 per la congettura di Riemann

Commento: per il primo premio, non sappiamo se è stato già aggiudicato, mentre per il secondo sappiamo che la risposta è negativa, non essendo ancora dimostrata l'ipotesi di Riemann. Comunque ci sono altri premi; peccato però che la RSA abbia eliminato qualche anno fa le sfide per la fattorizzazione di grandi numeri composti (esempi di famosi numeri RSA usati in crittografia), proprio mentre

anche noi ci stavamo provando tramite l'algoritmo di Fermat, basato su semidifferenza e semisomma dei numeri primi p e q tali che $N = p \times q$ (e quindi indirettamente anche sulla congettura di Goldbach, N pari = $p + q$).

Questa non è una delle motivazioni principali della nostra ricerca, ma un premio del genere naturalmente non ci dispiacerebbe affatto!

6. Per beneficenza

John Cosgrave dona ad un centro di ricerche per il cancro i proventi della pubblicazione di un bel libretto dedicato al "primo del millennio", un numero primo di esattamente 2000 cifre da lui scoperto.

7 Per la crittografia moderna

Molti metodi e protocolli crittografici, come l'RSA, si basano sulla relativa facilità di trovare numeri primi grandi, opposta all'enorme difficoltà di fattorizzare interi opportunamente scelti.

Si vedano p.e. il metodo dello scambio delle chiavi di Diffie – Hellmann

Commento: questa è pure una delle nostre motivazioni: metodi per calcolare numeri primi grandi (vedi per esempio il lavoro del nostro collaboratore esterno Ing. Cristiano Teodoro, "Come generare numeri primi grandi – (How generating large Prime Numbers, nella sezione "Lavori Ing. Cristiano Teodoro") , e non certo per violare il sistema RSA, come invece vorrebbero fare gli hackers, con gravi danni per l'e-commerce, i sistemi bancari, le comunicazioni Internet, i codici militari, ecc. ecc..

8. Per la generazione di numeri pseudocasuali **Gruppo ERATOSTENE**