CONGETTURA DELLA INVIOLABILITA'

DELLE CRITTOGRAFIE RSA ED ECC

Brevi riflessioni sull'ipotesi di

Riemann e la fattorizzazione veloce, ecc.

Francesco Di Noto, Michele Nardelli

Abstract

In this paper we show that does not exists a connection between Riemann hypothesis and fast factoring

Riassunto

In questo breve lavoro divulgativo osserviamo che non esiste una connessione diretta tra Ipotesi di Riemann e la fattorizzazione veloce in grado di violare la crittografia RSA idem per la crittografia ECC e l'ipotesi di Birch e Swinneron – Dyer.

La nostra congettura dice che :

"nessuna dimostrazione dell'ipotesi di Riemann e di Birch e Swinnerton –Dyer sarà di alcuna utilità nella violazione delle rispettive crittografie RSA ed ECC"

Nei riferimenti finali alcuni nostri link e osservazioni per approfondire l'argomento.

°°°°°

Stando a casa a scanso di coronavirus, abbiamo fatto qualche riflessione sull'ipotesi di Riemann e della sua presunta relazione con la fattorizzazione dei numeri semi primi N = p*q; ecco brevemente le nostre conclusioni: tale connessione non esiste (o se esistesse sarebbe molto debole e quindi inefficace a questo scopo) , poichè gli zeri coniugati di zeta sono simmetrici rispetto alla parte reale 1/2 (le loro parti immaginarie si

elidono calcolando la loro media aritmetica e rimane la sola parte reale),

cosi come anche le coppie di Goldbach (due numeri primi a somma N sono simmetrici rispetto alla loro semisomma s = N/2 e loro media aritmetica); ma i numeri primi p e q sono asimmetrici (tranne i numeri gemelli o vicinissimi tra loro) rispetto alla radice quadrata n d N, che è invece una media geometrica. Per esempio 127 e 229 sono simmetrici alla loro semisomma 178 (poichè 127=178-51 e 229 =178 +51, con 51 = d = semi

differenza), ma non alla radice quadrata 170 (intera) di 127*229 = 29083 loro prodotto, infatti 127 = 170 - 43 e 229 =170 + 59; la loro differenza 229 - 127= 102 viene divisa in due parti asimmetriche 43 + 59, e non 51 e 51 come per l'ex congettura di Goldbach. Proprio per questa asimmetria la fattorizzazione veloce è impossibile, come ben sappiamo,e tale difficoltà è alla base della nota crittografia RSA. Inoltre i numeri primi sono disposti su una linea numerica mono-dimensionale, mentre i numeri semi primi sono disposti su un piano bidimensionale come rettangoli N = p*q .

Quindi niente, almeno per ora, connessioni evidenti e utili tra fattorizzazione veloce ed eventuali future dimostrazioni dell'ipotesi di Riemann, in altre parole tra RH ed RSA . Esse potranno essere utili in matematica (conferma di moltissimi teoremi che si basano sulla presunta verità della RH), o in fisica (possibile connessione con i livelli di energia degli atomi), ma non con la fattorizzazione veloce, problema di tipo NP (altro problema del millennio, come la RH).

La cosa è importante, per esempio, perchè

una qualsiasi dimostrazione della RH non influirebbe sulla crittografia RSA che protegge i nostri conti correnti bancari, anche se molti di questi sono. protetti dalla crittografia ECC, ancora più difficile da violare, neanche in caso di dimostrazione della congettura collegata di Birch e Swinnerton - Dyer, ancora più difficile della RH. Solo i futuri computer quantistici potrebbero violare la crittografia RSA con l'algoritmo di Shor, ma già si stanno sviluppando nuove crittografie basate su reticoli resistenti, si pensa, anche a tali computer (un miliardo più potenti dei

computer attuali, il primo già in costruzione, costerà un miliardo di dollari...) . Tempi duri quindi per gli hacker, bravi informatici ma meno in teoria dei numeri. Non rimane loro che usare la nota tecnica fraudolenta del phishing, inducendo correntisti ingenui nonostante la prudenza consigliata da polizia postale e giornali ecc.) a comunicare a false e-mail i propri dati bancari. Occhio quindi cari amici, non cascateci! Inoltre, sul web circolano algoritmi di fattorizzazione basati per lo più sull'algoritmo di Fermat. ma ancora, per

fortuna, non in grado di violare la RSA.

I più importanti sono :

il crivello del campo numerico di Pomerance, (dal libro di Marcus du Sautoy "L' enigma dei numeri primi", pag 442Brano da Sautoy pag. 442- 443:

"Il crivello del campo numerico di Pomerance funziona in base al metodo di fattorizzazione di Fermat, ma cambiando continuamente il calcolatore a orologio usato per tentare di scomporre il numero. Il metodo è simile al crivello di Eratostene, la tecnica inventata dal bibliotecario alessandrino che

individua i numeri primi prendendo in considerazione un primo alla volta per poi depennare tutti i numeri che sono suoi multipli. Così, facendo passare i numeri attraverso setacci con maglie di diverse dimensioni, i numeri che non sono primi vengono eliminati senza che ci sia bisogno di esaminarli uno per uno. Nell'attacco portato da Pomerance, invece di usare setacci con maglie di diverse dimensioni si varia il numero di ore sul quadrante dei calcolatori a orologio. I calcoli eseguiti su ogni singolo calcolatore a orologio

fornivano a Pomerance informazioni sempre più precise sui possibili fattori primi di un numero: tanto maggiore era il numero di orologi che fosse riuscito a usare, quanto più avrebbe potuto avvicinarsi alla scomposizione di un numero nei suoi costituenti primi...”

Nonostante ciò, nemmeno con questo metodo riusci a violare la crittografia RSA .

Ma il nostro scopo non è quello di violare le crittografie note, tutt’ altro.

Conclusione

Possiamo concludere dicendo che la connessione RH - RSA non esiste, anche

perchè una fattorizzazione veloce è del tutto indipendente dalla RH, come pure la crittografia ECC e i metodi per la sua decrittazione non dipendono dalla verità della congettura di Birch e Swinnerton –Dyer , peraltro già dimostrata per i ranghi 0 e 1 ma non ancora per quelli superiori.

Riferimenti

2

La fattorizzazione e il crivello del campo numerico - mat ...

http://www.mat.uniroma3.it/scuola_orientamento/alumni/laureati/tiberio/SINTESI.pdf

3. Marcus du Sautoy, " L'equazione da un milione di dollari" (Rizzoli)

" La domanda da un milione di dollari, che prende il nome di congettura di Birch e Swinnerton – Dyer, è la seguente: esiste un modo per stabilire quali curve ellittiche possiedono infiniti punti le cui coordinate sono numeri interi o frazioni?
E a chi importa, direte voi?: In realtà dovrebbe importare a tutti noi,, dato che e oggi la matematica delle curve ellittiche viene usata nei cellulari e nelle smart card per proteggere i nostri segreti, così come si nei sistemi di controllo del traffico aereo per garantire la nostra sicurezza. Con questo nuovo metodo di cifratura il numero della vostra carta di credito o un vostro messaggio vengono convertiti per mezzo di ingegnose operazioni matematiche in un punto di una curva ellittica. Per cifrare il messaggio, quel punto viene spostato utilizzando la procedura geometrica che abbiamo spiegato, così da generare nuovi punti. Ricostruire a ritroso questa procedura richiede conoscenze matematiche di cui al momento non disponiamo. Ma se riusciste a risolvere questo

problema da un milione di dollari, probabilmente non vi importerebbe nulla del premio, dato che finireste per diventare gli hacker più potenti del pianeta"

4 . Marcus du Sautoy, " L'equazione da un milione di dollari" (Rizzoli)

"... Gli antichi greci escogitarono un metodo geometrico per individuare, una volta che sene sia trovato uno, altri punti (*x*,*y*) in cui *x* e *y* sono entrambi frazioni. Tracciamo una linea retta che tocchi appena la curva nel primo punto da noi individuato; non deve intersecare la curva in quel punto, deve avere l'angolo esatto per sfiorarla... Tale retta si chiama tangente alla curva nel punto (*x*,*y*) .

Prolungandola , scopriamo che la retta intersecherà la curva in un nuovo punto. L'entusiasmante scoperta fatta dagli antichi greci è che entrambe le coordinate di questo nuovo punto saranno anch'esse frazioni...

Per esempio, se tracciamo la tangente alla curva ellittica $y^2 = x^3 - 2$ nel punto $(x,y) = (3, 5)$ scopriamo che essa interseca la curva in un nuovo punto $(x,y) = (129/100 , 383/1000)$, in cui entrambe le coordinate sono frazioni .

....

Nel caso della nostra curva $y^2 = x^3 – 2$,

questo procedimento genera infiniti punti le cui coordinate sono frazioni, ma ci sono curve ellittiche per le quali è impossibile ottenere un numero infinito di tali punti. Prendiamo per esempio la curva definita dall'equazione :

$$y^2 = x^3 - 43x + 166$$

In questo caso esiste soltanto un numero finito di punti per i quali sia *x* sia *y* sono numeri interi o frazioni :

(*x*,*y*) = (0, 0), (3, 8), (3, -8), (-5, 16), (-5,-16), (11, 32), (11, -32). In effetti, tutti questi punti hanno coordinate intere. Il tentativo di

utilizzare il trucco geometrico che abbiamo appreso oppure l'algebra per ottenere altri punti con coordinate frazionarie non fa che dare di nuovo uno di questi sette punti.

La domanda da un milione di dollari, che ende il nome di congettura di Birch e Swinnerton – Dyer, è la seguente: esiste un modo per stabilire quali curve ellittiche possiedono infiniti punti le cui coordinate sono numeri interi o frazioni? E a chi importa, direte voi?: In realtà dovrebbe importare a tutti noi,, dato che e oggi la matematica delle curve ellittiche viene usata nei cellulari e nelle smart card per

proteggere i nostri segreti, così come si nei sistemi di controllo del traffico aereo per garantire la nostra sicurezza.

Con questo nuovo metodo di cifratura il numero della vostra carta di credito o un vostro messaggio vengono convertiti per mezzo di ingegnose operazioni matematiche in un punto di una curva ellittica. Per cifrare il messaggio, quel punto viene spostato utilizzando la procedura geometrica che abbiamo spiegato, così da generare nuovi punti. Ricostruire a ritroso questa procedura

richiede conoscenze matematiche di cui al momento non disponiamo. Ma se riusciste a risolvere questo problema da un milione di dollari, probabilmente non vi importerebbe lla del premio, dato che finireste per diventare li hacker più potenti del pianeta”

Osservazione:

non potrebbe essere necessario dimostrare l’ipotesi di Birch e Swinnerton – Dyer, poiché basterebbe migliorare gli algoritmi per il calcolo del logaritmo discreto necessari alla violazione della crittografia ECC , cosi come

per la crittografia RSA, non è necessaria una sua dimostrazione, ma solo un ottimo perfezionamento degli algoritmi di fattorizzazione, soprattutto quello di Fermat

5 Nostra osservazione

Algoritmo di Shor

per i futuri computer quantistici (se ne costruendo uno in America che costerà un miliardo di dollari), con lo scopo, più o meno velato, di violare la crittografia RSA. Ma farebbe solo la prima parte, la più facile, del lavoro, ma occorreranno 15 anni con l computer di cui sopra, ancora troppi.. I legittimi segreti (militari, industriali, finanziari, ecc.) protetti dalla RSA sono poi anche protetti dai numeri casuali (128 cifre binarie o più, 196 o 248) per decifrare i quali occorrono 10^36 anni. Con i prossimi computer quantistici (anche se un miliardo di volte più potenti dei normali computer, ma siamo ancora a 10 000 volte...) ce ne vorranno 10^27, di anni.

Un ‘eventuale dimostrazione dell’ipotesi di Riemann (limitata ai soli numeri primi ma non anche ai semiprimi tra i quali i numeri -RSA)) non sarebbe di nessun aiuto, come invece sperano invano alcuni matematici (forse occorrerebbe una specifica ipotesi di Riemann e relativa funzione zeta, possibilmente ancora più rognosa da dimostrare). Quindi , tali matematici possibilisti e hacker vari possono, per il momento, mettersi il cuore in pace e rinunciare all’idea di violare la crittografia RSA, almeno per qualche secolo...o forse per sempre.
(P.S. Esistono già metodi di fattorizzazione presumendo che la RH sia vera, ma non sono all’altezza del compito e la RSA è ancora lì, inviolabile!)

6

Di Noto Settembre 2008 - CNR Solar

eprints.bice.rm.cnr.it/611/1/Dinar1.pdf

http://eprints.bice.rm.cnr.it/611/1/Dinar1.pdf

Ma anche la Fisica quantistica e le Matrici sono collegabili ai numeri primi e alla funzione zeta, come nello schema precedente. A supporto di quanto sopra, riportiamo qualche brano dal libro di

Marcus du Sautoy “L’enigma dei numeri primi” pag. 519: “… La nuova svolta impressa da Berry potrebbe portare ad un’unificazione di tre grandi temi scientifici: la fisica quantistica (la fisica dell’estremamente piccolo), il caos (la matematica dell’impredicibilità) e i numeri primi (gli atomi dell’aritmetica). Forse, tutto considerato, l’ordine che Riemann aveva sperato di scoprire nei numeri primi è descritto dal caos quantistico. Ancora una volta i numeri primi ribadiscono il loro carattere enigmatico. L’apparente legame fra la distribuzione statistica degli zeri e quella dei livelli energetici ha convinto molti fisici a prendere parte alla ricerca di una dimostrazione dell’ipotesi di Riemann. All’origine degli zeri potrebbero esserci proprio le frequenze di un tamburo matematico; se così fosse, i fisici quantistici risulterebbero essere i meglio equipaggiati per individuare quei tamburi. Le loro stesse esistenze vibrano al suono di quei tamburi. Anche se abbiamo tutte queste prove del fatto che gli zeri di Riemann sono vibrazioni, tuttavia non sappiamo che cosa sia a vibrare (le stringhe? N.d.A.A.) Può darsi che la fonte della vibrazione sia puramente matematica, senza alcun modello fisico. E’ vero che la matematica che spiega gli zeri potrebbe essere la stessa matematica del caos quantistico, ma questo non significa che una soluzione avrà necessariamente una manifestazione fisica. Berry non la pensa così. Secondo lui, una volta che la matematica sarà stata definita completamente, emergerà un corrispondente modello fisico i cui livelli energetici rispecchieranno gli zeri di Riemann. << Non ho alcun dubbio che quando qualcuno avrà trovato l’origine degli zeri, quel qualcuno realizzerà il modello fisico. >> Non è possibile che quel modello esista già, nascosto da qualche parte dell’universo, in attesa di essere scoperto?” E anche un brano dal libro di J. Derbyshire “L’ossessione dei numeri primi” (Bollati Boringhieri), pag. 335: “ … Questo è il genere di spazio che Alain Connes ha costruito per il suo operatore di Riemann, uno spazio adelico. Poiché è adelico, incorpora in se i numeri primi, per così dire. Gli operatori che agiscono su questo spazio sono necessariamente basati sui numeri primi. Ora potete, spero, vedere come si può costruire un operatore di Riemann i cui autovalori sono proprio gli zeri non banali della funzione zeta, e il cui spazio (lo spazio sul quale opera) abbia incorporati i numeri primi (vedi connessioni con i Gruppi simmetrici di Lie e i numeri primi N.d.A.A.)”. E ancora: “ In un certo senso è vero, e la costruzione di Connes è brillante e davvero molto elegante, con i livelli di energia che sono proprio gli zeri di zeta sulla retta critica. Purtroppo, finora non ha fornito alcun indizio circa il perché non potrebbero esistere zeri di zeta fuori dalla retta critica!” Forse la spiegazione risiede nel fatto che: a) Tutti gli autovalori di una matrice hermitiana sono numeri reali, e non numeri immaginari; b) Tutti i livelli energetici debbono essere espressi da numeri reali (e non da numeri immaginari, cosa che le leggi della fisica quantistica vietano), inoltre, b) potrebbe essere benissimo una conseguenza di a) c) Poiché le stringhe, alla base della fisica quantistica (stringhe –quark- bosoni (forze) – fermioni – atomi (materia)), vibrano con frequenze esprimibili con numeri primi, a) e b) sarebbero dirette conseguenze di c). Ecco quindi come i numeri primi, normali o naturali (connessi ai numeri di Fibonacci f - tramite la loro forma 6f+1, come già accennato all’inizio) che fossero, si ritrovano poi a cascata su tutti i fenomeni fisici (e non) sottostanti: quantistici, nucleari (stabilità di alcuni elementi chimici), astronomici (orbite dei pianeti), persino biologici (degenerazione del DNA legata ai numeri p-adici e quindi anche ai numeri primi) ecc. ecc. Vedi il nostro lavoro (Rif. 1): “ I numeri primi in natura : fisica quantistica, fisica nucleare, biochimica, genomica , psicologia” nel quale sono citati, tra gli altri, i lavori di B. Dragovich and A. Dragovich “p-Adic Modelling of the Genome and the Genetic Code” e “p-Adic Degeneracy of the Genetic Code”, il primo dei quali reperibile sul sito indicato dell’Università inglese di Exeter (Rif. 2)

...

Rif.2 http://www.secamlocal.ex.ac.uk/people/staff/mrwatkin/zeta/physics.htm

Caltanissetta 2.4. 2020