SICSI VIII ciclo
Classe A042 - Storia dell'Informatica e del Calcolo Automatico

Storia dei Numeri Primi

I Precursori della Crittografia Moderna

Prof. Aniello Murano

Spec.: Vinicio Barbieri

Indice

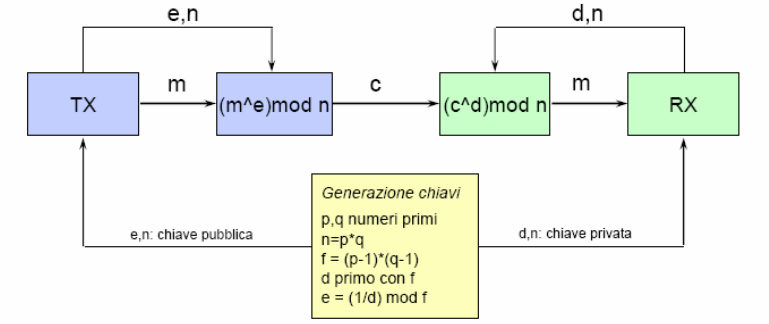
- Introduzione
- Esempio di Utilizzo nella Crittografia (RSA)
- Cenni Storici Sui Numeri Primi
- Generalizzazione del Piccolo Teorema di Fermat: Il Teorema di Eulero-Fermat
- Ipotesi di Riemann

Introduzione

- Ho scelto questo argomento in primo luogo perché costituisce un'interessante combinazione di matematica a prima vista molto astratta e di applicazioni assai concrete
- A partire dalla definizione dei numeri primi (Sono numeri interi e positivi che hanno come divisori solo l'unità e sè stessi) sarebbe possibile tenere una lunga trattazione ..., ma, per ovvi motivi, cercherò di essere sintetico!

RSA: Rivest, Shamir, Adleman

- Algoritmo che sfrutta l'esponenziale modulare e la complessità computazionale della fattorizzazione

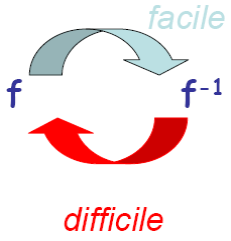


RSA: Robustezza

- La robustezza di RSA si basa sulla difficoltà di scomporre in fattori primi n, qualora n sia generato dal prodotto di due grandi numeri primi.
- f(n)=(p-1)*(q-1) è la funzione di Eulero (numero di interi inferiore a n e primi con esso) Con RSA la cifratura è a blocchi di m. La lunghezza in binario di m deve essere minore di n.

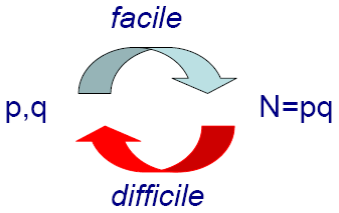
RSA: Sicurezza

- La sicurezza di RSA consiste nell'essere una funzione "one way", nel senso che risulta facile da calcolare (esiste un algoritmo veloce) , ma difficile da invertire (non esiste, o si crede che non esista, un algoritmo veloce).

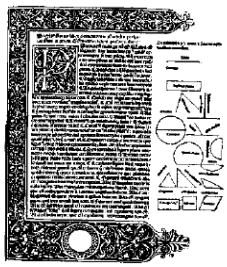


RSA: Conclusioni

- La ragione di tutto ciò risiede proprio nel fatto che effettuare una moltiplicazione tra i due numeri p e q risulta semplice e veloce (operazione di codifica N = pq), viceversa la divisione in fattori primi è difficile se non si conosce la chiave (operazione di decodifica molto lunga).



Cenni Storici



- Tra le più antiche testimonianze troviamo sicuramente quella degli Antichi Greci, i quali, per primi, dimostrarono che: “Ogni intero è esprimibile come prodotto di primi.”
- In particolare, Euclide (350-300 a.C.) è stato il primo a dimostrare che: “I numeri primi non sono un numero finito”. Dimostrazione presentata da Euclide nel IX libro degli Elementi.

Crivello di Eratostene

- Eratostene (275-195 a.C.) inventò un metodo per determinare i numeri primi, di cui segue un semplice esempio.
- Determiniamo i numeri primi tra 2 e 20, per farlo cancelliamo prima tutti i multipli di 2 e poi di 3

  2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

  Il procedimento termina con l'eliminazione dal setaccio dei multipli di 3 perchè 3 è il massimo intero primo il cui quadrato non supera 20.

  2 3 5 7 11 13 17 19

Fermat

- Fermat (1601-1665) pensa di aver trovato una formula che produce solo numeri primi ennesimo numero di Fermat $2^{2^n}+1$
- Purtroppo per n maggiore o uguale a 5 la formula perde valenza, e pertanto i numeri di Fermat non hanno prodotto che 4 numeri primi

Beffa di Fermat

- Ogni numero primo avente la forma di 4n+1 può essere scritto in modo unico come la somma di due quadrati (per n=7, $29=2^2+5^2$).Sebbene sostenga di possedere la dimostrazione, tralascia di mettere per iscritto la maggior parte dei dettagli.
- Però egli dimostra quello che è conosciuto come il piccolo teorema di Fermat: Sia p un numero primo ed n relativamente primo con p. Allora $n^{p-1} \equiv 1 \, mod \; p$

Mersenne

- Mersenne (1588-1648) riprende la formula di Fermat, la modifica, e ne elabora una molto più efficace non per scoprire tutti i numeri primi, ma un elenco maggiore: 2^n-1 i numeri primi dati dalla formula precedente, per particolari valori di n sono noti come primi di Mersenne.
- Mersenne afferma che per valori di n non superiori a 257, 2^n-1 è primo se e solo se n=2,3,5,7,13,19,31,67,127,257
- I matematici ritengono i numeri di Mersenne infiniti, tuttavia manca ancora la dimostrazione della veridicità di questa affermazione

Eulero

- Eulero (1707-1783) dimostra come abbiamo già visto che la formula di Fermat ($2^{2n}+1$) perde di validità per n>4
- Inoltre scopre un algoritmo attraverso cui è possibile ricavare alcuni numeri primi: x^2+x+41 sostituendo, infatti, ad x i numeri compresi tra 0 e 39, si ottengono alcuni numeri primi.
- Considerando poi la formula x^2+x+q ci si accorge che, scegliendo q=2,3,5,11,17 si trovano numeri primi per ogni valore di x compreso tra 0 e q-2

Goldbach

- Goldbach (1690-1764), in una lettera ad Eulero, propone due congetture
- La prima afferma che ogni numero dispari maggiore di 5 può essere scritto come somma di 3 numeri primi: $n=q_1+q_2+q_3$ dove n è un numero dispari maggiore di 5 e q_1, q_2, q_3 sono numeri primi
- La seconda che ogni numero pari maggiore di 2 può essere scritto come somma di 2 numeri primi: $n=q_1+q_2$ un numero pari maggiore di 2, e q_1, q_2 sono numeri primi.
- Queste due congetture sono ancora oggi prive di dimostrazione

Problema Aperto

- Successivamente Gauss, Legendre, Dirichlet, ma soprattutto Riemann cercarono una formula per determinare quanti fossero i numeri primi compresi tra 1 ed N
- Anche se la disposizione dei primi sembrava caotica, Riemann scoprì che era comunque possibile determinare una funzione che ne prevedesse l'ordine
- Tuttavia non poteva dimostrare che questo ordine sarebbe sempre stato rispettato, anche se pensava di sì...

Generalizzazione del Piccolo Teorema di Fermat

- Il Teorema di Eulero-Fermat dice che se n è un intero positivo ed a è coprimo rispetto ad n , allora: $a^{\varphi(n)} \equiv 1 \pmod{n}$ dove f(n) indica la funzione phi di Eulero. Questo teorema è una generalizzazione del Piccolo Teorema di Fermat.
- Eulero generalizzò questa serie nella seguente funzione $\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \ldots$ e ne calcolò alcuni valori

Ipotesi di Riemann

- Un secolo dopo Riemann considerò il caso in cui s sia un numero complesso, in tal caso la funzione può anche annullarsi per alcuni valori di s. Alcuni zeri sono considerati banali, mentre di particolare interesse sono gli zeri con parte reale compresa tra 0 e 1. Riemann riuscì a calcolare diversi zeri in questa striscia e notò che avevano tutti parte reale = 1/2; formulò allora la congettura che tutti gli zeri della funzione zeta avessero parte reale = 1/2.
- L'andamento della funzione zeta (e la distribuzione dei suoi zeri) risulta quindi, attraverso complessi passaggi, legato alla distribuzione dei numeri primi immersi nell'insieme dei numeri naturali.

Soluzione del Problema

- Pare che Riemann avesse risolto la congettura che porta il suo nome, ma purtroppo parte delle sue carte furono distrutte dopo la sua morte da una domestica

Conclusioni

- A 150 anni di distanza la congettura di Riemann attende ancora una dimostrazione (o una confutazione) e costituisce uno dei più famosi problemi irrisolti della matematica. Essendo la congettura di Riemann collegata alla serie dei numeri primi dalla formula di Eulero, e alle formule per il calcolo del numero di numeri primi, alcuni pensano che un'eventuale dimostrazione di questa congettura potrebbe aprire la strada alla scoperta di nuovi più efficienti metodi per fattorizzare un numero nei suoi fattori primi, e quindi minare le fondamenta del cifrario RSA.

Bibliografia

- J.H. Conway, R.K. Guy: Il Libro dei Numeri, Hoepli, Milano 1999
- H. Davenport: Aritmetica Superiore, Zanichelli, Bologna 1994
- G.H. Hardy, E.M. Wright: An Introduction to the Theory of Numbers, quinta edizione, Oxford University Press, Oxford 1979
- J.J. O'Connor, E.F. Robertson: Prime numbers http://www.gap.dcs.stand.ac.uk/history/HistTopics/Prime_numbers.html
- N. Koblitz, A Course in Number Theory and Cryptography, Graduate Texts in Mathematics 114, Springer, New York 1987.
- S. Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, Anchor Books, Londra 1999. Traduzione italiana: Codici & Segreti, Rizzoli, Milano 1999.

This document was created with Win2PDF available at http://www.win2pdf.com.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.