STATISTICA, anno LXIV, n. 2, 2004

TEST DI PRIMALITÀ DETERMINISTICI E PROBABILISTICI

Alfredo Rizzi

1. PREMESSA

Le questioni riguardanti i numeri primi hanno interessato molti studiosi sin dagli albori della matematica. Basti ricordare nell'antichità Euclide e negli ultimi quattrocento anni Fermat, Eulero, Legendre, Gauss, Hilbert.

Gauss, nel 1801, nelle *Disquisitiones Arithmeticae*, affermava che il problema di distinguere i numeri primi da quelli composti e della fattorizzazione di questi ultimi è uno dei più importanti ed utili in aritmetica; inoltre, Egli aggiungeva, la stessa dignità della scienza sembra richiedere che si debba esplorare ogni via che consenta di meglio chiarire un problema così elegante.

Giovanni Prodi, ad una domanda postagli sui risultati che più lo avevano colpito, tra quelli conseguiti in matematica negli ultimi decenni ha risposto: "I teoremi probabilistici di primalità. In queste teorie la probabilità interviene nel cuore del ragionamento; mi sembra molto interessante che si possa ottenere un abbassamento della complessità pagandolo con l'introduzione di un margine di incertezza". (Cohen, 2000).

Le grandi risorse di calcolo a disposizione degli studiosi di tutto il mondo hanno spinto molti a trattare questioni relative ai numeri primi e a cercare di *falsificare* specifiche congetture. Sulla rete *web* esistono numerosi siti che riguardano questi numeri. Forse è il caso più noto di informazione scientifica che avviene in tempo reale non su carta stampata; per quanta riguarda la matematica questi siti sono tra i più frequentati. Ciò induce anche molti ricercatori a cimentarsi su questioni relative ai numeri primi non sempre di grande importanza. Vengono così stimolate forme di emulazione che vedono protagoniste molte università di tutto il mondo ed in particolare statunitensi, nella speranza di battere qualche primato anche per brevi periodi, come avviene per i record sportivi. Ciò è avvenuto – ed avviene! –, ad esempio, per quello che riguarda l'individuazione del più grande numero primo conosciuto, che impegna in maniera massiccia le risorse di calcolo di alcune università. Per molti anni – fino a che non fu dimostrato il famoso *teorema dei quattro colori* – nel *numeratore postale* dell'università dell'Illinois compariva una dizione che affermava che il ventitreesimo numero di Mersenne è primo (par. 2.3).

Quando si parla di ricerche sui numeri primi si fa spesso riferimento alle possi-

bili applicazioni in crittografia ed in particolare al sistema di crittografia a chiave pubblica RSA (Rivest e altri, 1978).

La crittografia aveva avuto il suo sviluppo in millenni di storia per esigenze di carattere militare. E' diventata disciplina di insegnamento universitario negli Stati Uniti all'incirca negli ultimi venticinque anni, in Italia da poco tempo.

Il grande sviluppo delle comunicazioni digitali, delle informazioni trasmesse da satelliti, della posta elettronica, e dell'invio di *file* tramite *reti* tra privati, Enti, Pubbliche amministrazioni ecc. impone sistemi di cifratura che abbiano un adeguato grado di sicurezza.

Il sistema RSA si basa sulla scelta di due primi sufficientemente grandi e su relazioni introdotte da Eulero nel 1700 (par. 2.1). Da qui l'interesse per le ricerche di base sui numeri primi che, in qualche modo, potrebbero avere ricadute operative sui diversi sistemi di cifratura.

In Italia, come negli altri Paesi più industrializzati, gli aspetti giuridici della firma digitale sono stati affrontati ormai da molti anni ed hanno trovato la loro formalizzazione in disposizioni legislative degli ultimi anni[1]. Le comunicazione tra Enti, ed in particolare con e tra le Pubbliche amministrazioni, stanno diventando sempre più veloci e sicure.

Ma io ritengo che questo rinnovato interesse per le ricerche sui primi prescinda anche da queste applicazioni e sia dettato più che altro da *curiosità scientifica* per problemi facilmente comprensibili ed apparentemente non complessi.

Naturalmente RSA è il sistema di cifratura più noto al grande pubblico, per sua natura limitato in quanto non consente di cifrare *messaggi* di grandi dimensioni. Esso rappresenta solo una piccolissima parte dei sistemi crittografici oggi in uso che consentono di *mascherare* grandi quantità di informazioni; questi si basano sui principi dell'algebra modulare ed in generale sulla *teoria dei codici*. La crittografia moderna si avvale di tecniche essenziali per la sicurezza delle informazioni e la protezione dei dati. La letteratura scientifica è copiosa; alcuni grandi editori dedicano a questa disciplina interi cataloghi. Citiamo per tutti il libro di Hunter del 2001.

In questa Nota ricorderemo alcuni dei principali risultati classici su cui si basano le attuali ricerche sui numeri primi (par. 2) e ci soffermeremo sui test di primalità deterministici (par. 3) e probabilistici (par. 4).

---

[1] D.P.R 28 dicembre 2000 n. 405 pubblicato sulla Gazzetta ufficiale del 20 febbraio 2001.
Il D.P.R. definisce come firma digitale il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica ed una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

2. ALCUNI RICHIAMI DI RISULTATI NOTI

2.1 *Le basi teoriche su cui si basano i test di primalità sia deterministici sia probabilistici affondano nelle ricerche del matematico svizzero Leonardo Eulero (1707-1783) e del francese Pierre de Fermat (1601-1665)*

Sia Z_n l'insieme degli interi $Z_n = [1,2,...,n]$.

Sia P l'insieme dei numeri primi $P = [1,2,3,5,7,11,13,...,n,....]$ ove n ha solo i divisori banali *1* ed *n*.

Sono di fondamentale importanza i due teoremi:

Teorema 1. I numeri primi sono infiniti.

L'elegante e coincisa dimostrazione di questo teorema, riportata in molti testi di aritmetica elementare, viene attribuita ad Euclide attorno al 300 avanti Cristo. Essa si basa su un rigoroso ragionamento ed è comprensibile anche da coloro che hanno conoscenze matematiche veramente elementari[2].

Teorema 2. Ogni numero intero n può essere scomposto in un unico modo nel prodotto dei suoi fattori primi: $n = p_1^a p_2^a ... p_r^a$ *ove* p_i *sono numeri primi* $p_1 < p_2 < ... < p_r$ *e gli* a_r *sono tutti positivi.*

La semplice dimostrazione è lasciata come esercizio ai lettori in molti testi di aritmetica elementare.

Sia Z_n^* l'insieme degli interi primi con *n*. Ad esempio $Z_3^* = [1,2]$, $Z_5^* = [1,2,3,4]$, $Z_{15}^* = [1,2,4,7,8,11,13,14]$.

La cardinalità di Z_n^* è indicata con $\Phi(n)$. Questa funzione è nota come funzione di Eulero.

Teorema 3. Il numero degli interi primi con n è pari a: $\Phi(n) = n \Pi(1-1/p)$ *ove p varia su tutti i primi che dividono n (compreso n se esso è primo).*

La dimostrazione è riportata nei testi di teoria dei numeri, in particolare nel libro di Cormen *et al.* del 1995.

Ad esempio, il numero degli interi primi con *15* è pari a: $\Phi(15) = 15\ (1-1/3)\ (1-1/5)) = 8$ in quanto i numeri primi che dividono *15* sono proprio *3* e *5*. Z_{15}^* ha cardinalità pari ad *8*.

---

[2] Non si può non pensare alla lunga e complessa dimostrazione del cosiddetto ultimo teorema di Fermat (il quale, come è ben noto, afferma la irrisolubilità in numeri interi dell'equazione: $x^n+y^n=z^n$, $n>2$). questa importante dimostrazione è stata pubblicata da Andrew Wiles negli "*Annals of Mathematics*" nel maggio 1995. Lo studioso era stato lungamente impegnato nell'affinamento del lavoro, dopo aver ricevute critiche su parti non trascurabili del medesimo. La dimostrazione di Wiles è stata lungamente applaudita dagli studiosi riuniti a Berlino per il periodico congresso mondiale dei matematici del 1998. Essa, però, sembra comprensibile solo a pochi ricercatori. La dimostrazione occupa due manoscritti di più di 130 pagine! Si può definire antidemocratica? Data per scontata la correttezza del lavoro dell'insigne matematico, sarà possibile trovare dimostrazioni più semplici e comprensibili?
L'importante lavoro di Wiles ha posto fine al sogno di molti volenterosi dilettanti della matematica che si erano cimentati con la famosa congettura ed avevano creduto di averla risolta.

Se n è primo la funzione $\Phi(n)$ di Eulero si riduce a: $\Phi(n) = n(1-1/n) = n-1$. Se n è composto, $\Phi(n) < n-1$.

Teorema di Eulero. Per qualsiasi intero $n>1$, $a^{\Phi(n)} = 1 \pmod n \ \forall a \in Z_n$

Per la dimostrazione, ad esempio (Cormen *et al.*, 1995). Il teorema di Fermat – cosiddetto piccolo teorema di Fermat – si può considerare un caso particolare di quello di Eulero, qualora n sia primo. Fermat, in sostanza, aveva formulato una congettura la quale trova completa dimostrazione come caso particolare del teorema precedente. Essa era stata anche dimostrata in diversi modi da alcuni matematici del '700.

Teorema di Fermat: Se n è primo si ha: $a^{n-1} = 1 \pmod n \ \forall a \in Z\, n^*$

Eulero aveva notato alcune connessioni tra la teoria dei numeri primi e la serie:

$\varsigma(s) = 1 + 1/2^s + 1/3^s + ... + 1/n^s + ...$ dove s è un numero intero.

Questa serie è un caso particolare della serie di Dirichlet. La somma di tale serie è una funzione che da allora è nota come $\varsigma(s)$ di Bernhard Riemann (1826-1866). Eulero aveva scoperto la formula che lega tale funzione ai numeri di Bernoulli determinando le due relazioni: $\varsigma(2) = \pi^2/6$ *e* $\varsigma(4) = \pi^4/90$.

Eulero aveva anche determinata la relazione della funzione di Riemann con i numeri primi: $\varsigma(s) = \Pi 1/[1/(1-p^s)]$ ove p sono primi.

Riemann ha studiato la medesima serie per il caso in cui s sia una variabile complessa.

La congettura di Riemann, ad oggi non dimostrata, afferma che tutti gli zeri immaginari della funzione $\varsigma(s)$ abbiano una parte reale pari ad ½. Come è noto, questa congettura è stata indicata da Hilbert nel 1900 come una delle 10 questioni a quell'epoca non risolte.

Nel 1986 è stato dimostrato che i primi 1.500.000.000 *zeri non banali* della funzione zeta di Riemann hanno parte reale pari ad ½ (Van de Lune *et al.*, 1986).

Nel 1901 von Koch ha dimostrato che la congettura di Riemann è equivalente alla seguente ipotesi:

$$\pi(n) = Li(n) + O(n^{1/2} \log n)$$

ove $\pi(n)$ rappresenta il numero dei primi inferiori ad n e $Li(n)$ è il *valore principale* dell'integrale di $1/\log n$ limitato tra 0 ed n.

2.2 *Il numero dei numeri primi inferiori ad un prefissato n*

Una importante questione relativa ai numeri primi è la seguente.

Quanti sono i numeri primi inferiori od uguali ad n? Tale numero viene spesso indicato con $\pi(n)$.

Nel 1798 Legendre ha pubblicato nel libro *Essai sur la teorie des Nombres* la congettura: $\pi(n)$ è approssimato da $n/(\log n - 1{,}08366)$.

Gauss fornisce, nel 1849, la seguente stima: $\pi(n)$ è approssimato dal valore principale dell'integrale, limitato tra *0* ed *n*: $Li(n) = \int 1/\log x \, dx$.

Nel 1896 Hadamard e de la Vallée Poussin hanno dimostrato il:

Teorema dei numeri primi: $\pi(n)$ è asintotico ad $n/\log n$.

Più in generale vale l'approssimazione:

$\pi(n) = Li(n) + O(ne^{-a\sqrt{\log n}})$ per qualche costante *a.*

L'errore dipende dalla dimensione da quella che è nota come *regione senza zero* della funzione di Riemann. Esso cresce al decrescere della dimensione di questa regione.

I moderni elaboratori elettronici hanno consentito di confrontare i livelli di approssimazione delle formule menzionate anche per valori di *n* molto elevati.

La tabella seguente si riferisce alle potenze di 10 che vanno da 1000 a 10 miliardi.

TAVOLA 1

Potenze di 10 che vanno da 1000 a 10 miliardi

n	$\pi(n)$	Gauss	Legendre	$n/(\log n-1)$
10^3	168	178	172	169
10^4	1.229	1.246	1.231	1.218
10^5	9.592	9.630	9.588	9.512
10^6	78.498	78.628	78.534	78.030
10^7	664.579	664.918	665.138	661.459
10^8	5.761.455	5.762.209	5.769.341	5.740.304
10^9	50.847.534	50.849.235	50.917.519	50.701.542
10^{10}	455.052.511	455.055.614	455.743.004	454.011.971

Per i grandi valori di *n* considerati, l'approssimazione di Gauss è decisamente la migliore. Ad esempio per *n=10* miliardi l'approssimazione di Gauss è superiore al valore esatto espresso da $\pi(n)$ di *3.103* unità, quella di Legendre di circa *690.000* unità. Anche se questa tavola sembra suggerire regolarità di comportamento delle differenze tra $\pi(n)$ e le diverse approssimazioni, si può verificare empiricamente che queste differenze, all'aumentare di *n,* assumono segni sia positivi sia negativi.

Benedetti (1967, 1977) ha approfondito, da un punto di vista statistico alcune questioni relative alla distribuzione dei numeri primi ed alla *congettura di Goldbach.*

2.3 *Particolari insiemi di numeri primi*

Esistono molte espressioni che forniscono insiemi di infiniti numeri primi. Ad esempio la relazione $p=2n+1$ al variare di n nell'insieme Z_n dei numeri naturali fornisce tutti i primi ma, naturalmente, anche tutti dispari non primi.

I *numeri di Mersenne* sono quelli che si ottengono dalla espressione 2^n-1 al variare di *n* nell'insieme degli interi. I primi numeri dell'abate francese Marin Mersenne

(1588-1648) sono *3*, *7*, *31*, *127*. La congettura iniziale era che l'espressione indicata fornisse numeri primi solo per *n* uguale *2*, *3*, *5*, *7*, *13*, *17*, *19*, *31*, *67*, *127*, e *257*. Eulero, 100 anni più tardi, la verificò per *n=31*. Alla fine del 1800 è stata verificata per *n* uguale ad altri valori. Ad oggi sono noti soltanto 39 *primi di Mersenne* individuati in gran parte negli ultimi dieci anni. Non è noto se *i primi di Mersenne* siano infiniti.

I primi di Mersenne soddisfano al teorema di Lucas-Lehmer:

Teorema 7: Per p dispari un numero di Mersenne è primo ***se e solo se*** $2^p - 1$ *divide* $S(p-1)$ *ove* $S(n+1) = [S(n)]^2 - 2$ *e* $S(1)=4$ *(Lehmer,1930).*

Ad esempio, si ha: $S(2)=14$; $S(3)=194$; $S(4)=194^2-2$. Per $p=3$ $S(2)=14$ che divide 2^3-1. Per $p=4$ $S(3)=194$ non divide *15*.

Il test che deriva dalla applicazione di questo teorema è particolarmente veloce per i *calcolatori binari* perché non richiede operazioni di divisione.

Il più grande numero primo conosciuto al dicembre 2002, è un *primo di Mersenne*. Esso è $2^{13.466.917}-1$. Questo numero è stato individuato da Michael Cameron, uno studente canadese di 20 anni che partecipava ad un progetto di ricerca per individuare numeri di Mersenne, noto come *Gimps*, acronimo di Great Internet Mersenne Prime Research. Il tempo di elaborazione per individuare quello che, ad oggi, è il più grande numero primo conosciuto, è stato di 13.000 anni!

Gauss aveva dimostrato che ogni numero primo della forma $4n+1$ può decomporsi nella somma di due quadrati.

I numeri *perfetti,* sono uguali alla somma dei loro divisori con l'esclusione del numero stesso. I primi quattro sono *6*, *28*, *496*, *8128*. Ad essi sono stati attribuiti nel passato particolari significati mistici. Per essi vale il:

Teorema 8: Un numero è perfetto se e solo se è uguale a $2^{n-1}(2^n-1)$ *e* 2^n-1 *è primo.*

La dimostrazione è riportata, ad esempio, nel sito *web*: http://www.utm.edu/research.html

I *numeri di Fermat* sono della forma 2^k+1 con k potenza di *2*. Per k uguale rispettivamente a *1*, *2*, *4*, *8*, *16* si hanno i numeri primi: *3*, *5*, *17*, *257*, *65537*. Fermat aveva congetturato che tutti i numeri forniti dall'espressione precedente siano primi. La congettura cade per i valori di k pari a *32* e *64*. Non è stata ancora dimostrata la congettura in base alla quale i *numeri di Fermat* sono infiniti.

I *primi di Sophie Germain* sono i primi p per i quali $2p+1$ sono ancora numeri primi. Ad esempio, *2*, *3*, *5*, *11*, *23* sono di questa natura. Non lo sono *7*, *13*, *17*, *19*. I *primi di Sophie Germain*[3] sono stati così chiamati dopo che questa autrice ave-

[3] Sophie Germain (1776-1831) aveva scritto a Gauss presentandosi come Antoine-August Leblanc, per timore che anche il grande matematico avesse qualche prevenzione contro le donne che si dedicavano alla matematica. Quando Gauss apprese la verità non dimostrò alcuna forma di misogenia. In seguito, conosciuti i risultati delle sue ricerche, si adoperò affinché l'università di Gottinga le conferisse una laurea ad honorem. Purtroppo la Germain morì poco prima della cerimonia di conferimento del riconoscimento accademico.

va provato la congettura di Fermat per gli esponenti divisibili per questo tipo di primi.

Per tali numeri vale la seguente congettura (Agraval, 2002) che fornisce la loro densità:

Congettura: Il numero dei primi di Sophie Germani è asintotico a $D_x/log^2 x$ ove D_x è una costante stimata in circa *0,661*.

I *numeri di Carmichael* sono quei numeri non primi che soddisfano alle condizioni del cosiddetto piccolo teorema di Fermat (2.1) per ogni $a \in Z_n^*$. I primi tre numeri di Carmichael sono *561*, *1105* e *1729*. Essi sono estremamente rari. Ad esempio per *n=100.000.000* essi sono solo *255*. Si dimostra (Cormen, 1995) sia che essi non devono essere divisibili per il quadrato di qualsiasi primo sia che devono essere il prodotto di almeno 3 primi. Così, ad esempio *561* è il prodotto di *3*, *11* e *17*.

2.4 *Alcune congetture sui numeri primi*

Ricordiamo alcune famose congetture sui numeri primi che non hanno ancora trovata dimostrazione. Supponiamo che *n* sia un numero intero.

- *Congettura di Goldbach* in base alla quale ogni numero pari maggiore di *2* si può scrivere come somma di due primi.
- *Congettura dei "primi gemelli"* in base alla quale è infinito il numero dei primi che differiscono di due unità, quali, ad esempio, *5* e *3*; *7* e *5*; *13* ed *11*.
- *Esistono infiniti primi della forma n^2+1?*
- *La sequenza di Fibonacci contiene infiniti numeri primi?*
- *I primi di Fermat sono infiniti?*
- *I primi di Mersenne sono infiniti?*
- *Tra n^2 ed $(n+1)^2$ esiste sempre almeno un numero primo?*
- *Ogni numero primo dispari si può scrivere come somma di tre primi.*

3. TEST DETERMINISTICI DI PRIMALITÀ

3.1 *Chiameremo "test deterministici di primalità" quelle procedure che consentono di determinare se un numero è primo applicando uno specifico algoritmo*

La *teoria della complessità,* importante ramo della *Computer Science*, permette di quantificare le difficoltà computazionali di una specifica procedura. In generale la *complessità* è misurata dalle risorse di elaborazione necessarie alla implementazione degli algoritmi in, termini di capacità di memoria, tempi di esecuzione, ecc. Per il problema della determinazione della primalità di un intero è sufficiente riferirsi al tempo di esecuzione dell'algoritmo.

Il più semplice *test deterministico di primalità* per un numero *n* è quello che si basa sulle successive divisioni di *n* per tutti i primi inferiori alla radice quadrata di *n.* Naturalmente questo test non è applicabile per interi sufficientemente grandi.

Esistono molti test deterministici di primalità validi in casi per numeri inferiori ad un particolare *n*. Ad esempio (Pomerance *et al.*, 1980):

- se $n<1.373.653$ e soddisfa la relazione di Fermat (par. 2.1) per entrambe le *basi 2* e *3*, allora *n* è primo;
- se $n<25.326.001$ e soddisfa la relazione di Fermat (par. 2.1) per tutte le *basi 2* e *3*, *5* allora *n* è primo;
- se $n<2.152.3002.898.747$ e soddisfa la relazione di Fermat (par. 2.1) per tutte le *basi 2* e *3*, *5*, *7*, *11* allora *n* è primo;
- se $n<341.550.071.728.321$ e soddisfa la relazione di Fermat (par. 2.1) per tutte le *basi 2* e *3*, *5*, *7*, *11* allora *n* è primo;

Per i numeri di Mersenne vale il teorema di Lucas-Lehmer (par. 2.3.1)

3.1 *Il test di Lucas*

Nel 1876 Edouard Lucas aveva dimostrato il seguente

Teorema 9: Se a ed n sono primi, n>1, e se $a^{n-1}=1 \pmod n$, $a^{n-1/q} \neq 1 \pmod n$, *per tutti i primi che dividono q, allora n è primo.*

Per la dimostrazione Crandall e Pomerance, 2001. Nelle applicazioni di questo importante teorema ci si scontra con il problema di sia di individuare il valore *a* sia in quello di trovare tutti i primi che dividono *n–1*.

3.2 *Gli importanti risultati di M.Agrawal, N.Kayal e N. Saxena*

I tre autori in una Nota apparsa nel sito *web* http://www.cse.iitk.ac.in/news.primality.html hanno proposto un test deterministico che si basa sul seguente:

Teorema 10: p è primo se e solo se :$(x-a)^p = (x^p-a) \pmod p$ *ove a è un intero primo con p.*

La semplice dimostrazione si basa sul fatto che, se *i* è compreso tra *0* e *p* i coefficienti $\binom{n}{p}$, calcolati modulo *p*, nello sviluppo del binomio a primo membro della relazione precedente sono nulli ed inoltre $a^p=a. \pmod p$

Viceversa se *p* non è primo un suo fattore non divide $\binom{n}{p}$ (*mod p*), e quindi la relazione indicata non è valida.

L'algoritmo fornito dagli autori – implementato in sole 13 righe – consente di stabilire se un numero è primo o composto. Esso fornisce la risposta *primo* se il numero è primo, *composto* se il numero è composto.

Il risultato di maggior interesse teorico, dimostrato dagli Autori nel lavoro citato, è il seguente:

Teorema 11. La complessità asintotica dell'algoritmo è: $O^{\log n}$

In pratica però, in molti casi, come ricordano gli Autori, esso è più veloce di quanto indicato. Ad esempio per i primi di Sophie Germain (par. 2.3.3) nella espressione della complessità asintotica dell'algoritmo l'esponente di logaritmo si riduce da *12* a *6*.

Si tratta, quindi, di un algoritmo *P*, ovvero di un algoritmo il cui tempo di esecuzione è funzione di un polinomio che dipende da *n*.

Gli altri algoritmi per l'analisi della primalità noti in letteratura sono *NP*, ossia la loro esecuzione in un tempo *polinomiale* dipende da procedure non deterministiche.

Il risultato di M. Agrawal, N. Kayal e N. Safena, come si è detto ha grande importanza teorica; non sembra avere grande interesse operativo in quanto i tempi di applicazione, anche con le possibili riduzioni dovute ad analisi particolari, sono notevoli.

Ad esempio nel 1983 Adlemane, Pomerance e Rumely hanno fornito un algoritmo deterministico di primalità che opera in tempi $(\log n)^{O(\log\log\log n)}$. Tutti gli altri algoritmi conosciuti a quei tempi operavano in tempi esponenziali.

Nel 1986, Goldwasser e Kilian avevano proposto un algoritmo randomizzato, basato sulle curve ellittiche, che opera in ipotesi molto larghe, in tempo polinomiale per *quasi* tutti gli input. L'algoritmo fornisce un certificato di *primalità*.

Confrontiamo gli ordini di grandezza dei tempi di implementazione dei primi due algoritmi ricordati:

TAVOLA 2

Tempi di implementazione

N	Agraval e altri	Adleman e altri
10^{20}	20^{12}	$20^{0,11}$
10^{50}	50^{12}	$50^{0,23}$
10^{100}	100^{12}	$100^{0,30}$
10^{1000}	1000^{12}	$1000^{0,48}$

Come si vede chiaramente l'algoritmo di Adleman ed altri è sempre preferibile a quello di Agraval nei casi considerati.

L'algoritmo di Agraval ed altri è preferibile a quello di Adleman ed altri qualora: $12 < \log\log\log n$ e quindi n – cioè il numero che si vuole stabilire se è primo o meno – è maggiore di *10* elevato a *10* elevato a *10* elevato a *12*; un tale numero è uguale ad uno seguito da *12.000* zeri.

4. TEST PROBABILISTICI DI PRIMALITÀ

I *test probabilistici di primalità* consentono di verificare l'ipotesi nulla o di base: H_0 : n è un numero primo. Se l'ipotesi viene rifiutata il numero è sicuramente composto. Se il test fa rifiutare l'ipotesi di base vi è probabilità pari a uno che il numero sia composto. Si tratta di un test statistico in cui la probabilità *dell'errore di seconda specie*, ossia di *accettare* una ipotesi falsa, è un numero diverso da zero. Si tratta di test statistici del tutto particolari, su cui la letteratura scientifica non si è molto soffermata.

Il più noto tra i test statistici di primalità è quello di Miller e Rabin proposto nel 1976.

Definiamo *testimone* un numero *a* per cui vale il cosiddetto piccolo teorema di Fermat (par. 2.1) pur essendo il numero composto.

Il test in questione si basa sul seguente:

Teorema 12: Se n è un numero dispari composto, allora il numero dei testimoni che n è composto è almeno (n-1)/2.

La dimostrazione è riportata in Cormen (1975).

Il test di Miller e Rabin si applica più volte sullo stesso *n*. Poiché le *s* prove sono indipendenti vale il:

Teorema 13: Considerato un n intero dispari ed un intero s , la probabilità che un numero composto sia considerato primo è inferiore a 2^{-s}.

Prove empiriche hanno mostrato che la probabilità che un numero composto risulti primo risulta di gran lunga inferiore a quella indicata.

Definito *pseudo primo* un numero composto che soddisfa al piccolo teorema di Fermat (par. 2.1), è stato verificato che esistono solo *21.253* di tali numeri di base *2* inferiori a *25* miliardi. Vi è, quindi, una probabilità di circa $8\ 10^{-6}$ che un numero composto *n* soddisfi alla relazione $2^{n-1}=1$ (*mod n*).

Di seguito sono riportati i numeri *pseudo primi* inferiori a *500* rispetto alle basi indicate.

base	numeri pseudo primi <500
2	341
3	91; 121
4	15; 85; 91; 341; 435; 451
5	217
6	35; 185; 217; 301; 481
7	25; 325
8	9; 21; 45; 63; 65; 105; 117; 133; 153; 231; 273; 341; 481
9	91; 121; 205
10	9; 33; 91; 99; 259; 451; 481
11	15; 133; 259; 305; 481
12	65; 91; 133; 143; 145; 247; 377; 385
13	21; 85; 105; 231; 357; 427
14	15; 39; 65; 195; 481
15	341
16	15; 51; 85; 91; 255; 341; 435; 451
17	9; 45; 91; 145; 261
18	25; 49; 65; 85; 133; 221; 323; 325; 343; 425; 451
19	9; 15; 45; 49; 153; 169; 343
20	21; 57; 133; 231; 399

Ciò significa, ad esempio, che il numero composto *9* è uno *pseudo primo* di base *8* in quanto $8^8-1=1$ (*mod 9*).

5. CONCLUSIONI

Oggi esistono siti web che consentono di verificare se un numero è primo o composto in *tempo reale*, nel senso che forniscono risposte che, in molti casi, sem-

brano immediate a chi ha posto la domanda al sistema. Naturalmente i tempi di risposta dipendono dalla grandezza del numero.

Ad esempio il sito http://www.alpetron.com.ar, approntato da Alejandro Alpern, consente di determinare se un numero è primo o composto. La procedura di fattorizzazione si basa il metodo delle curve ellittiche. Il numero può avere un numero massimo di *1000* cifre binarie. Poiché le fattorizzazioni sono effettuate utilizzando le risorse di calcolo dell'utente, la procedura può svolgersi in più sedute di elaborazione. E' possibile, inoltre, far ricorso ad espressioni numeriche in cui sono presenti alcuni operatori algebrici per le quattro operazioni tradizionali, per l'esponenziale, per il fattoriale, per ottenere il più grande primo inferiore – $B(n)$- e superiore – $N(n)$- al numero dato, i numeri di Fibonacci e di Lucas, ecc.

Le funzioni $B(n)$ e $N(n)$ si basano sul test di Miller-Rabin (par. 4) applicato per *20* iterazioni dopo aver effettuato le usuali divisioni per i primi *100* numeri primi.

Peraltro, in molti degli algoritmi implementati negli elaboratori elettronici esistono delle semplici *routine* che provano la divisibilità del numero per particolari sottoinsiemi e riducono notevolmente le ulteriori prove da effettuare.

Ad esempio, applicando semplici criteri di divisibilità per i numeri *3*, *5*, 7 il numero delle prove di primalità si riduce del *54* per cento. Tale percentuale sale al *76* per cento se le prove si riferiscono ai primi inferiori a *100* – essi sono *25* – e al *80* per cento se ci si riferisce ai primi inferiori a *256*, che sono in numero di *54*.

Il ben noto *crivello* di Eratostene non è poi così fuori moda!

I problemi di fattorizzazione di un numero e quelli della determinazione se un numero è primo sono per loro natura diversi; in molte procedure di elaborazione, però, essi vengono trattati contemporaneamente. In ogni caso è *più facile,* stabilire se un numero è primo piuttosto che trovarne tutti i suoi fattori. Ad oggi, con i supercalcolatori a disposizione e con i migliori algoritmi conosciuti, non è possibile fattorizzare numeri aventi più di alcune centinaia di cifre.

Inoltre i metodi deterministici e non deterministici coesistono, alle volte, nelle stesse procedure. Si individuano algoritmi sempre più efficienti e di facile implementazione.

Ma è indubbio che i test probabilistici di primalità sono gli unici applicabili qualora *n* sia *particolarmente* elevato e non si abbia la *fortuna* di incorrere in situazioni del tutto particolari. Ad esempio che il numero sia composto e divisibile per uno dei primi iniziali.

Come abbiamo cercato di mostrare in questo lavoro i test deterministici di primalità sono applicabili a numeri aventi un numero di cifre sempre più grande, in tempi relativamente brevi. Tale numero di cifre è comunque limitato, come insegna la *teoria della complessità.* I test probabilistici di primalità forniscono risultati assolutamente accettabili per le applicazioni in situazioni molto generali; richiedono tempi di elaborazione trascurabili. Nelle situazioni reali di ricerca sono quelli applicabili.

Dipartimento di Statistica Probabilità e Statistiche applicate ALFREDO RIZZI
Università di Roma "La Sapienza"

RIFERIMENTI BIBLIOGRAFICI

L.M. ADLEMAN, C. POMERANCE, R.S. RUMELY, (1983), *On distinguishing prime numbers from composite numbers*, Ann.Math., 117, pp. 173-206.

M. AGRAWAL., N. KAYAL, N. SAFENA, (2002), *primes in P*, sito web http://www.utm.edu/ research.html, August 6.

M. AGRAWAL, S. BISWAS, (1999), *Primality and identity testing via Chinese remaindening*, Proc.Ann.IEEE Symp. On Foundations of Computer Sciences, pp. 202-209.

C. BENEDETTI, (1967), *Ricerche statistiche sui numeri primi*, Metron, vol. XXVI, n. 3-4.

C. BENEDETTI, (1977), *La congettura di Golbach come un problema di correlazione*, Metron, vol. XXXV, n. 3-4.

L. BIGGERI, (1999), *Diritto alla 'privacy' e diritto all'informazione statistica*, in Sistan-Istat, "Atti della Quarta Conferenza Nazionale di Statistica", Roma, 11-13 novembre 1998, Roma, Istat, Tomo 1, pp. 259-279.

S. COHEN, (2000), *Ascoltando Giovanni Prodi*, Bollettino dell'Unione Matematica Italiana, Serie VIII, vol. III-a.

T.H. CORMEN, C.E. LEISERSON, R.L. RIVEST, (1995), *Introduzione agli algoritmi*, vol. III, Jackson Libri, Milano.

R. CRANDALL, C. POMERANCE, (2001), *Prime numbers: a computational perspective*, Springer Verlag, New York.

D.E. KNUTH, (1998), *The Art of Computer Programming*, vol. II, Addison: Wesley.

S. GOLDWASSER, J. KILIAN, (1986), *Almost all primes can be quickly certified*, Proceedings of Annual IEEE Symposium on Foundations of Computer Science, pp. 316-329.

J.M.D. HUNTER, (2001), *An information Security handbook*, Springer.

D.N. LEHMER, (1931), *An extended theorie of Luca's function*, Ann.Math., pp. 419-448.

G. MILLER, (1975), *Riemann's hypothesis and test for primality's*, Proc. Of the seventh Annual ACM Symposium on the Theorie of Computing, pp. 234-239.

C. POMERANCE, (1984), *Lectures notes on primality testing and factoring,* Notes volume 4, Mathematical Association of America, pp. 34.

C. POMERANCE, J.L. SELFRIDGE, S.S. WAGSTAFFJR, (1980),*The pseudoprimes to 25 10^9*, Math. Comp., 35, pp. 1003-1086.

M.O. RABIN, (1980), *Probabilistic algorithm for primality testing*, J. Number Theory, 12, pp. 128-138.

N. RENZONI, (2002), Test probabilistici di primalità, Archimede, 3, pp. 146-149.

P. RIBENBOIM, (1995), *The new book of prime number records*, 3rd edition, Springer-Verlag, New York.

A. RIVEST, A. SHAMIR, L. ADLEMAN, (1978), *A method for obtaining digital signature and public-key cryptosystems*, Comm. ACM N.21, 2, pp. 120-126.

A. RIZZI, (1989), *Verifiche di pseudo casualità in crttografia*, in Secondo Simposio su: Stato e Prospettive della Ricerca Crittografica in Italia, Fondazione Bordoni, pp. 1-24.

S.J. SHEATER, M.C. JONES, (1991), *A reliable data-based bandwidth selection method for kernel density estimation*, Journal of the Royal Statistical Society, Serie B, 53, pp. 683-690.

J. VAN DE LUNE, H.J.J. RIELE, D.T. WINTER, (1986), *On the zeros of the Riemann zeta function in the critical strip*, Math. Comp.

M.P. WAND, M.C. JONES, (1995), *Kernel smoothing*, Chapman and Hall, London.

ALCUNI SITI WEB SUI NUMERI PRIMI (attivi a gennaio 2003)

http://www.cse.iitk.ac.in/news.primality.html

http://www.anujsrh.com/crypto/prime.html

http://www.security_labs.org

http://www.bbc.co.uk/hi/sci/tech/1693364
http://www.csm,astate.edu
http://www.itcvolta.it/testPrim
http://www.mersenne.org/prime.html
http://www.utm.edu/research.html
http://www.crypto.cs.mcgill.ca
http://www.alpetron.com.ar

RIASSUNTO

Test di primalità deterministici e probabilistici

In questo lavoro l'A. dopo aver ricordato l'importanza che rivestono i numeri primi in molti settori della matematica ed in particolare in crittografia, richiama alcuni risultati noti di teoria di teoria dei numeri con riferimento alle ricerche di Eulero, Fermat, Legendre, Rieman e di altri studiosi. Esistono molte espressioni che forniscono insiemi di infiniti numeri primi; tra di essi i primi di Mersenne godono di interessanti proprietà. È ben noto, inoltre che esistono diverse congetture sui numeri primi che attendono una dimostrazione o il rigetto di esse.

I test deterministici di primalità sono quelle procedure che consentono di determinare se un numero è primo o meno. Esse non sono applicabili in molte situazioni di interesse pratico, ad esempio nella crittografia a chiave pubblica, perché implicherebbero tempi di esecuzione non sopportabili.

I test probabilistici di primalità consentono di verificare l'ipotesi nulla o di base: il numero è primo. Nel lavoro si commentano i più noti di questi test che forniscono risultati accettabili nelle applicazioni. In sostanza solo l'approccio probabilistico consente di determinare se un numero è primo o meno.

SUMMARY

Primality deterministic and primality probabilistic tests

In this paper the A. comments the importance of prime numbers in mathematics and in cryptography. He remembers the very important researches of Eulero, Fermat, Legendre, Rieman and others scholarships. There are many expressions that give prime numbers. Between them Mersenne's primes have interesting properties. There are also many conjectures that still have to be demonstrated or rejected.

The primality deterministic tests are the algorithms that permit to establish if a number is prime or not. There are not applicable in many practical situations, for instance in public key cryptography, because the computer time would be very long. The primality probabilistic tests consent to verify the null hypothesis: the number is prime. In the paper there are comments about the most important statistical tests.