Alla ricerca dei numeri primi

Fino a poco tempo fa anche un calcolatore di grandi dimensioni avrebbe impiegato almeno un secolo per stabilire se un numero di cento cifre fosse primo o composto; oggi basta un minuto

di Carl Pomerance

I numeri primi formano la base moltiplicativa del sistema dei numeri. Un numero si dice primo se non è il prodotto di numeri naturali minori di esso. Il numero primo 11, per esempio, non può essere scomposto in fattori minori: solo 1×11 è uguale a 11. Viceversa, un numero si dice composto se può essere espresso come prodotto di due o più fattori. Il numero composto 12 è uguale a $2 \times 2 \times 3$. Ogni intero maggiore di 1 o è primo, o è il prodotto di un unico insieme di numeri primi. Questo fatto, noto già ai greci antichi, ha un ruolo tanto importante, nel sistema dei numeri naturali, da meritare il nome di teorema fondamentale dell'aritmetica.

Com'è possibile determinare se un numero è primo o composto? Il metodo più semplice consiste nel dividere il numero in esame per gli interi della successione 2, 3, 4... Se una qualsiasi delle divisioni non dà resto, il numero è composto e divisore e quoziente sono suoi fattori. Se si sono controllati tutti gli interi fino al numero in questione e nessuna divisione è senza resto, il numero è primo. In effetti, non è necessario arrivare fino al numero in esame; la procedura può essere interrotta non appena il divisore ecceda la sua radice quadrata. La ragione è semplice: i fattori, se esistono, devono essere almeno due e quindi, se un numero ha un fattore maggiore della sua radice quadrata, deve anche averne uno minore.

Limitando le divisioni per tentativi alla radice quadrata, si rende molto più rapido il test di primalità. È possibile mettere in atto anche altre scorciatoie, eliminando per esempio tutti i possibili divisori pari maggiori di 2. Ciononostante, l'algoritmo della serie di divisioni per tentativi è assolutamente inapplicabile al controllo dei più grandi numeri primi conosciuti. Consideriamo il numero $2^{44\,497} - 1$, che Harry L. Nelson e David Slowinski del Lawrence Livermore Laboratory hanno dimostrato essere primo; esso è formato da 13 395 cifre. Se un calcolatore fosse in grado di controllare un milione di divisioni al secondo e si fermasse alla radice quadrata del numero, gli occorrerebbero 10^{6684} anni per espletare il suo compito.

L'inconveniente deriva dal fatto che il metodo delle divisioni fa molto più del necessario: non solo ci dice se un numero è primo o composto, ma ci fornisce anche i fattori di ogni numero composto. Sebbene esistano metodi di fattorizzazione indipendenti da quello delle divisioni per tentativi, nessuno di essi è in grado di fattorizzare in un tempo ragionevole un numero arbitrario di «sole» 100 cifre, anche ricorrendo a un grande calcolatore. Del resto, è possibile stabilire se un numero è primo o no senza essere costretti a trovarne i fattori qualora sia composto. Se il numero non possiede fattori piccoli, questi metodi risultano quasi sempre più efficienti di quelli che usano la fattorizzazione. Negli ultimi anni è stato sviluppato un metodo che consente al calcolatore di determinare la primalità di un qualsiasi numero di 100 cifre in 40 secondi di tempo macchina.

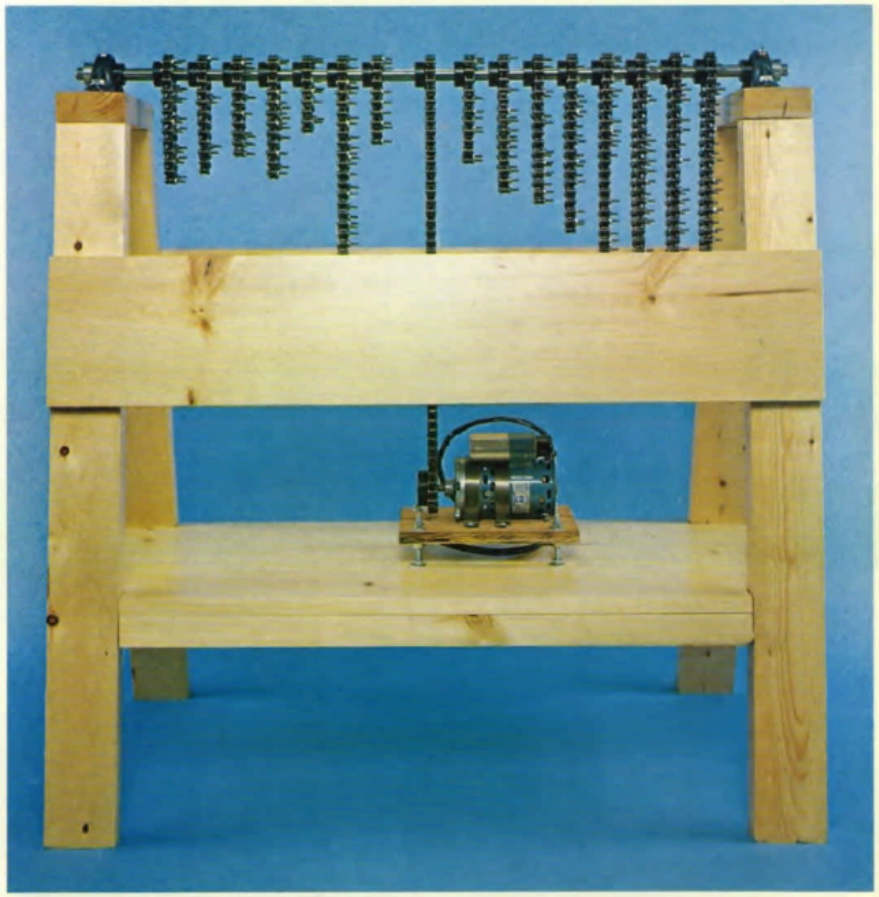
Il problema della primalità e quello a esso superficialmente collegato della fattorizzazione appartengono alla teoria dei numeri, quella branca della matematica che tratta delle proprietà dei numeri interi; essa è ricca di problemi straordinariamente semplici nella loro formulazione, ma notoriamente difficile da risolvere. I problemi di teoria dei numeri che hanno a che fare con la primalità hanno affascinato i matematici fin dai tempi di Euclide.

Così pare che esista un'infinità di numeri primi gemelli, ossia coppie di primi che, al pari di 17 e 19, differiscono di 2. Ma si tratta di una congettura non dimostrata. È quasi certamente vero che esiste sempre almeno un numero primo fra i quadrati di due numeri successivi, ma anche questa è un'asserzione non dimostrata. Christian Goldbach nel 1742 ipotizzò che ogni numero pari maggiore di 2 sia la somma di due primi; 32, per esempio, è la somma di 13 e 19. La congettura di Goldbach ha resistito a tutti i tentativi di dimostrazione, anche se nel 1937 il matematico russo I. M. Vinogradov ha dimostrato che tutti i numeri dispari «abbastanza grandi» possono essere espressi come somma di tre primi. Vinogradov non è stato tuttavia in grado di esplicitare chiaramente cosa si debba intendere per «abbastanza grandi».

Un corollario del teorema di Vinogradov asserisce che tutti i numeri pari abbastanza grandi possono essere espressi come somma di quattro primi. In base al teorema, poi, se a è un numero pari abbastanza grande e b è un numero dispari tale che $b = a - 3$, è sempre possibile rappresentare b come somma di tre primi. Il numero pari a in questione è quindi la somma di quei tre primi e di 3 (numero primo). Nel 1966 il matematico cinese Chen Jing-run mostrò che tutti i numeri pari abbastanza grandi possono essere espressi come somma di un numero primo e di un numero che o è primo, o è la somma di due primi. Queste approssimazioni alla congettura di Goldbach costituiscono risultati profondi, nel senso che la loro dimostrazione richiede un'analisi matematica avanzata ed è piuttosto difficile.

Molti enunciati sui numeri primi, però, possono essere dimostrati con metodi elementari, e molte di queste dimostrazioni sono deliziosamente ingegnose. Così, era noto già a Euclide che il numero dei primi è infinito. L'argomentazione è di tipo indiretto; si assume che il numero dei primi sia finito, dal che scende l'esistenza di un massimo numero primo, e successivamente si ricava una contraddizione. Supponiamo allora che p sia il massimo numero primo e consideriamo il numero N definito come il prodotto di tutti i primi fra 2 e p. Il numero $N + 1$ sarà primo o composto. Dato che $N + 1$ è maggiore di p, in base all'ipotesi di partenza dovrà essere composto (altrimenti sarebbe un primo maggiore di p); ma allora per il teorema fondamentale dell'aritmetica dovrà avere dei fattori primi. Peraltro $N + 1$ era stato costruito in modo che la sua divisione per un numero primo qualunque, compreso fra 2 e p, desse sempre resto 1. I suoi fattori primi (se esistono) devono quindi essere maggiori di p. L'ipotesi che esista un massimo numero primo conduce allora a una contraddizione, sicché l'insieme dei primi non ha un limite superiore.

In modo analogo è facile dimostrare che esistono dei primi consecutivi la cui differenza può essere grande quanto si vuole. Consideriamo la successione di numeri $n! + 2, n! + 3, n! + 4, \ldots, n! + n$, dove $n!$ (da leggersi n fattoriale) è il prodotto di tutti gli interi da 1 a n. Si noti che $n! + 2$ è divisibile esattamente per 2, $n! + 3$ per 3, $n! + n$ per n. Tutti gli $n - 1$ numeri della successione sono composti e la suc-

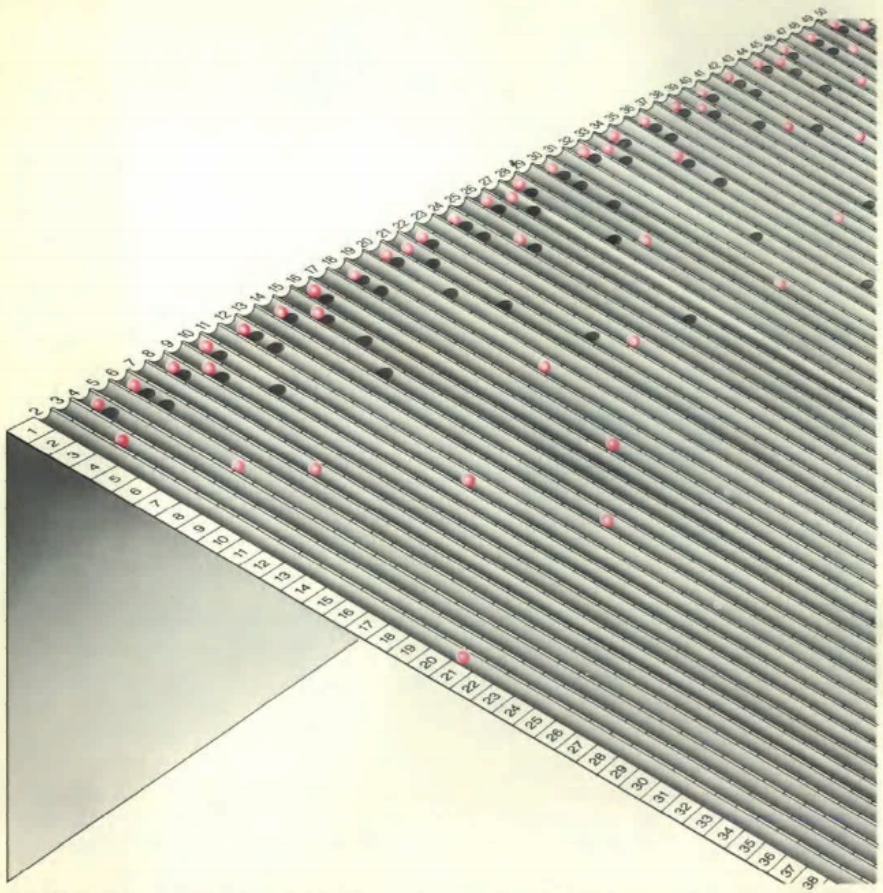


La prima macchina approntata per lo studio del sistema numerico fu costruita nel 1926 da D. H. Lehmer, dell'Università della California a Berkeley. Costruita con un cavalletto di legno, catene di bicicletta e altro materiale facilmente reperibile, questa macchina era una sorta di calcolatore specializzato, che poteva essere programmato per la ricerca rapida di numeri di forma particolare, necessari per la risoluzione di determinati problemi di teoria dei numeri. Il test di primalità, ovvero la classificazione di un numero come primo o composto è uno fra i più importanti di questi problemi. (Un numero primo è un numero divisibile esattamente solo per se stesso e per 1; se un numero possiede altri divisori, è composto.) Le condizioni che devono essere soddisfatte da una soluzione numerica del problema devono essere programmate sulla macchina di Lehmer inserendo dei bulloni in certi anelli delle catene di bicicletta. Quando queste vengono fatte girare da un motore, la macchina rimane in movimento finché tutti i bulloni non sono allineati in alto; quindi si spegne automaticamente. Il numero corrispondente alla configurazione delle catene al momento dell'arresto soddisferà le condizioni imposte. Lehmer costruì diverse versioni della macchina, ma la versione del 1926 è andata distrutta. La macchina mostrata nella fotografia è una ricostruzione dovuta a Roberto Canepa della Carnegie-Mellon University, conservata al Computer Museum di Marlboro, nel Massachusetts.

cessione stessa può essere prolungata a piacere scegliendo n abbastanza grande.

Molti matematici hanno considerato la teoria dei numeri come la «regina della matematica», sia per l'intricata bellezza delle sue dimostrazioni, sia perché il suo studio ha sempre avuto il fascino di una forma di pura contemplazione, senza il peso di possibili conseguenze pratiche. Dal 1977, tuttavia, lo sviluppo della teoria dei numeri è stato stimolato anche dalla scoperta che essa avrebbe potuto avere importanti applicazioni nella crittografia, lo studio delle condizioni di riservatezza nelle comunicazioni. In quell'anno, Ronald L. Rivest del Massachusetts Institute of Technology, Adi Shamir del Weizmann Institute of Science e Leonard M. Adleman dell'Università della Southern California notarono che era possibile fondare un sistema crittografico a chiave pubblica sulla difficoltà di fattorizzazione di un numero composto molto grande, che sia per esempio il prodotto di due numeri primi di 100 cifre.

In un sistema crittografico a chiave pubblica lo strumento di codifica del messaggio può essere reso di ragione pubblica senza pregiudicare la sicurezza del codice. Il codice Rivest-Shamir-Adleman si basa sulla relativa facilità della determinazione della primalità di due grandi numeri e del valore del loro prodotto da un lato, e dalla



Il crivello per la ricerca dei numeri primi, attribuito all'antico studioso greco Eratostene, è stata una delle prime tecniche escogitate per distinguere i numeri primi, compresi entro un certo limite, da quelli composti. Qui il crivello è un piano inclinato in cui sono stati praticati dei fori. I numeri da controllare rispetto alla primalità sono rappresentati da biglie che rotolano lungo scanalature sul piano. Dapprima si fanno dei fori nella seconda riga, una scanalatura sì e una no, all'infuori di quella contrassegnata con 2. Quindi si cerca la prima scanalatura senza fori, in pratica la terza. Si eseguono dei fori nella terza riga, ogni tre scanalature, all'infuori della scanalatura contrassegnata con 3. Il procedimento continua con l'approntamento di fori nella quinta riga ogni cinque scanalature, ogni sette scanalature nella settima riga, e via dicendo, fermandosi alla riga contrassegnata da un numero minore o uguale alla radice quadrata del massimo dei numeri da controllare. Le biglie che non cadono nei fori corrispondono ai numeri primi. Per esempio, tutti i 25 primi minori di 100 possono essere determinati considerando tutte le biglie da 2 a 100 che superano la settima riga di fori. (Non esistono primi maggiori di sette minori o uguali alla radice quadrata di 100.)

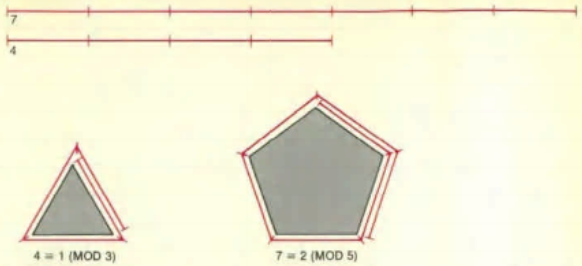
elevata difficoltà pratica di fattorizzare tale valore se non si sa come è stato costruito. Rendendo pubblico il prodotto di 200 cifre di due primi di 100 cifre, chiunque potrebbe codificare un messaggio utilizzando tale numero, ma solo la conoscenza dei due fattori primi renderebbe possibile la decodifica. Esistono sistemi crittografici a chiave pubblica che non dipendono dalla fattorizzazione, ma il sistema Rivest-Shamir-Adleman basa la sua sicurezza sulla intrattabilità del problema della fattorizzazione e la sua operatività sul fatto che i due numeri di 100 cifre siano effettivamente primi. Un test di primalità che non dipenda dalla fattorizzazione sarebbe quindi di grande interesse per i sistemi crittografici (si veda l'articolo *Crittografia a chiave pubblica* di Martin E. Hellman, in «Le Scienze», n. 136, dicembre 1979).

Tutti i metodi di controllo della primalità che non dipendono dalla fattorizzazione traggono la loro importanza da un teorema formulato per la prima volta in una lettera inviata da Pierre de Fermat all'amico Bernard Frénicle de Bessy, datata 18 ottobre 1640. Il teorema, noto come piccolo teorema di Fermat, stabilisce che se n è un numero primo e b un intero, $b^n - b$ è un multiplo di n. Per esempio, se n è uguale a 7 e b è uguale a 2, il teorema asserisce correttamente che $2^7 - 2$, ovvero 126, è un multiplo di 7.

Rispetto alla primalità, l'importanza del teorema sta nella sua equivalenza logica con l'asserzione che se $b^n - b$ non è un multiplo di n, allora n è un numero composto. Quando n è uguale a 4 e b è uguale a 3, $3^4 - 3$ è uguale a 78, che dà resto diverso da zero (per la precisione, 2) quando viene diviso per 4. Il piccolo teorema consente di concludere in modo indiretto che 4 non è primo.

Per quanto il piccolo teorema costituisca un risultato fondamentale e potente, possiede diverse dimostrazioni elementari, una delle quali verrà riportata più sotto. Il teorema consente di stabilire proprietà di numeri così grandi da non poter essere scritti in forma decimale. Dal fatto che $2^{44\,497} - 1$ è primo, per esempio, il teorema fa scendere che il numero ottenuto elevando 3 alla $(2^{44\,497} - 1)$-esima potenza e togliendo dal risultato 3, è ancora divisibile per $2^{44\,497} - 1$. Il risultato dell'elevazione a potenza è tanto grande da non poter essere scritto sotto forma decimale. Inoltre, il processo di divisione che dovrebbe fornire esplicitamente il quoziente non potrebbe essere eseguito da alcun calcolatore fisicamente concepibile.

Per arrivare ad avamposti così lontani del sistema dei numeri, si può usare la ruota aritmetica ideata da Carl Friedrich Gauss. A lui si deve la formulazione dell'aritmetica modulare, in cui la grandezza assoluta di un numero è irrilevante e ciò che conta è la dimensione dell'ultimo giro compiuto dalla ruota aritmetica per raggiungerlo. Il numero n viene espresso come resto dopo essere stato diviso per un qualche altro numero m, detto modulo. Il resto viene scritto nella forma n modulo



L'aritmetica modulare costituisce un sistema di calcolo con importanti applicazioni ai test di primalità. Nell'aritmetica modulare l'unica cosa che conta in un numero n è il resto che si ottiene dividendo n per un qualche modulo m. La grandezza assoluta di un numero viene completamente ignorata. Il più familiare dei sistemi di aritmetica modulare è quello utilizzato per il calcolo del tempo, in cui le ore vengono indicate specificandone il valore modulo 12. Il simbolo ≡ va letto «è congruo a»; i numeri ai suoi lati danno lo stesso resto quando vengono divisi per il modulo. Per esempio, $4 \equiv 1$ (mod 3) significa che 4 e 1 danno lo stesso resto (1) quando vengono divisi per 3.

m, oppure n (mod m). Il numero m indica la grandezza della ruota, n la grandezza assoluta del numero e n (mod m) la grandezza dell'ultimo giro parziale della ruota necessario per raggiungere n.

Nell'aritmetica modulare esistono analoghi stretti di molte leggi dell'aritmetica ordinaria. In particolare è possibile sommare e moltiplicare, a condizione di esprimere i risultati come congruenze; tutti i numeri che danno uno stesso resto rispetto a un dato modulo sono detti congrui rispetto a quel modulo.

Nell'aritmetica ordinaria, 6 più 7 è uguale a 13, un risultato riproducibile in aritmetica con un modulo, per esempio, 5. Si ha infatti che 6 (mod 5) + 7 (mod 5) è congruo a 1 + 2 ovvero a 3, e che 13 (mod 5) è anch'esso congruo a 3. Analogamente, 4×5 è uguale a 20, mentre nell'aritmetica modulo 3 il prodotto ha la forma 4 (mod 3) × 5 (mod 3), e il risultato è congruo a 1×2. Tale prodotto è quindi 2, ma anche 20 (mod 3) è congruo a 2.

Nella notazione di Gauss il piccolo teorema di Fermat stabilisce che, se n è primo, $b^n - b$ è congruo a 0 (mod n) o, in altri termini, $b^n - b$ è un multiplo di n. Il vantaggio di questa notazione sta nel fatto che le regole dell'aritmetica modulare rendono possibile calcolare il valore di $b^n - b$ modulo n senza dover dividere $b^n - b$ per n. Per numeri come $2^7 - 2$ il vantaggio offerto dal sistema di Gauss non sembra molto significativo, in quanto la divisione diretta è semplice. Tuttavia per trovare il resto, quando si divide un numero come $3^{1037} - 3$ per 1037, l'aritmetica modulare diventa pressoché indispensabile.

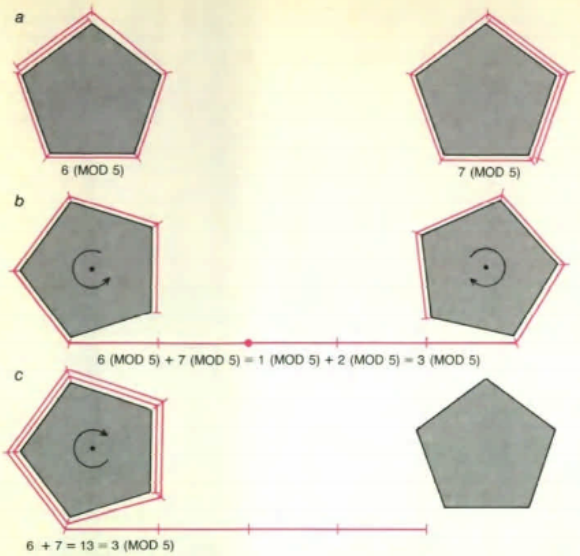
L'essenza del problema sta nel trovare 3^{1037} (mod 1037); nell'aritmetica modulare non è necessario calcolare il valore dell'enorme numero 3^{1037}. Tutto ciò che serve è la ripetuta applicazione del fatto che il resto del quadrato di un numero è congruo al quadrato del resto del numero.

Così, una volta calcolato 3^8 (mod 1037), si può ottenere 3^{16} (mod 1037) elevando al quadrato il resto di 3^8 e trovando il resto di questo numero modulo 1037. In questo modo si possono trovare i resti modulo 1037 di 3, 3^2, 3^4... fino a 3^{1024}. Il numero 3^{1037} è uguale a $3^{(1024+8+4+1)}$, che a sua volta è uguale a $3^{1024} \times 3^8 \times 3^4 \times 3$ per la legge del prodotto di potenze della stessa base; quindi 3^{1037} (mod 1037) è congruo a 3^{1024} (mod 1037) × 3^8 (mod 1037) × 3^4 (mod 1037) × 3 (mod 1037). Quando si sono eseguiti tutti i calcoli, si trova che 3^{1037} è congruo a 845 (mod 1037), per cui $3^{1037} - 3$ è congruo a 842 (mod. 1037) *(si veda l'illustrazione a pagina 91)*. Sulla base del piccolo teorema di Fermat, 1037 deve quindi essere composto, dato che il resto della divisione di $3^{1037} - 3$ per 1037 non è uguale a zero. Questo procedimento non dà praticamente alcun suggerimento per l'identificazione dei fattori di 1037.

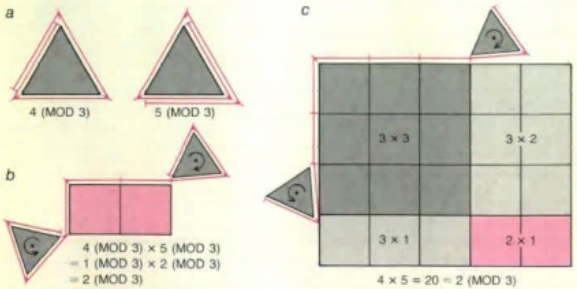
Può essere divertente seguire il procedimento con un calcolatore programmabile. Per evitare errori di arrotondamento, i valori di n dovrebbero essere limitati a numeri le cui cifre siano al più la metà di quelle visualizzabili sul calcolatore. Con un calcolatore di grandi dimensioni, i calcoli possono essere eseguiti rapidamente anche quando i numeri in ingresso hanno migliaia di cifre, quindi con il test di Fermat si possono individuare numeri composti enormemente grandi.

La dimostrazione del piccolo teorema di Fermat deriva da una semplice conseguenza del teorema fondamentale dell'aritmetica. Se un numero primo divide esattamente il prodotto di più numeri, divide esattamente almeno uno dei fattori. 4×9, ossia 36, per esempio, è divisibile esattamente per il primo 3 e ovviamente anche uno dei suoi fattori, 9, è divisibile per 3. L'enunciato non vale per numeri composti: 4×9 è divisibile per 6, ma né 4, né 9 sono divisibili per 6.

Per dimostrare il risultato di Fermat secondo cui $b^n - b$ è un multiplo di n quando è primo, notiamo che $b^n - b$ è uguale a $b\,(b^{n-1} - 1)$. Quindi, se b stesso è un multiplo di n lo è anche $b^n - b$. Il



Nell'aritmetica modulare l'addizione viene eseguita come nell'aritmetica ordinaria. Si determinano i resti di ciascun numero rispetto al modulo assegnato e successivamente li si somma. Se il valore ottenuto è maggiore del modulo, si trova il resto della somma. Nell'esempio viene calcolata la lunghezza totale di due corde, rispettivamente pari a 6 e 7, modulo 5. Nell'aritmetica modulo 5 si ignora il numero degli avvolgimenti completi attorno a un pentagono, e si considera unicamente quella parte della corda che resta dopo l'ultimo giro completo. Quindi, modulo 5, 6 è congruo a 1 e modulo 7 a 2 *(a)*. Quando si considerino unite le due corde, la lunghezza totale dei due resti è 3 *(b)*. Avvolgendo la corda attorno al pentagono, la sua lunghezza eccedente i giri completi è 3, di modo che la somma ordinaria di 6 e 7 è congrua a 3 modulo 5 *(c)*. Come regola generale, la somma dei resti di due numeri è congrua al resto dell'ordinaria somma degli stessi.



Nell'aritmetica modulare anche la moltiplicazione viene data in modo analogo a quella ordinaria. Nell'esempio, 4 e 5 sono moltiplicati modulo 3 e vengono rappresentati come corde avvolte intorno a un triangolo. Il resto di ogni numero è la lunghezza della corda che resta dopo l'ultimo giro completo attorno al triangolo *(a)*. Il resto di 4 modulo 3 è 1 e il resto di 5 modulo 3 è 2. Il prodotto dei due resti è l'area del rettangolo che ha lati uguali alla lunghezza di ciascun resto. In altri termini, 1 per 2 è uguale a 2 *(b)*. Il prodotto di 4 e 5, d'altra parte, è l'area del rettangolo di lati di lunghezza 4 e 5. Il resto del prodotto *(c)* viene ottenuto ignorando l'area di ciascun rettangolo piccolo i cui lati abbiano lunghezza pari a quella di una corda che compia un numero intero di avvolgimenti completi attorno al triangolo *(aree in grigio)*. L'area del rettangolo restante *(in colore)* è il resto del prodotto di 4 per 5 modulo 3. La regola generale asserisce pertanto che il prodotto dei resti di due numeri è congruo al resto del loro prodotto.

teorema resta da dimostrare solo per il caso in cui b non sia un multiplo di n: la dimostrazione parte da questa ipotesi.

L'idea di base è che se i numeri b, $2b$, $3b$... fino a $(n-1)b$ vengono moltiplicati fra loro, il loro prodotto può essere espresso nella forma $b^{n-1}(n-1)!$. D'altra parte, dal teorema fondamentale dell'aritmetica segue che i resti modulo n di b, $2b$, $3b$... $(n-1)b$ sono i numeri 1, 2, 3... $(n-1)$ eventualmente in ordine differente. Un po' di algebra elementare ci consente di concludere che $(b^{n-1}-1)(n-1)!$ è un multiplo di n. Dato che il numero primo n non è un divisore di nessuno dei numeri fra 1 e $n-1$, mentre è un divisore di $(b^{n-1}-1)(n-1)!$, un'altra applicazione del teorema fondamentale dell'aritmetica comporta che n è un divisore di $b^{n-1}-1$. Poiché $b^{n-1}-1$ è un fattore di (b^n-b), il teorema è dimostrato.

Potrebbe sembrare che il piccolo teorema di Fermat risolva completamente il problema della primalità, poiché sembra fornire un metodo semplice per distinguere un numero primo da uno composto; sfortunatamente si tratta di una conclusione affetta da un vizio logico. Se per qualche numero b, b^n-b dà resto differente da zero quando viene diviso per n, allora n è certamente composto. Supponiamo tuttavia che b^n-b sia un multiplo di n. Ne segue che n deve essere primo?

Svariati esempi suggeriscono una risposta affermativa: 2^2-2 è un multiplo di 2, 2^3-2 è multiplo di 3, 2^5-2 è multiplo di 5 e 2, 3, 5 sono tutti primi. Circa 2500 anni fa i matematici cinesi scoprirono tale campione e ipotizzarono che se 2^n-2 è multiplo di n, n deve essere primo. Gottfried Wilhelm Leibniz, che svolse uno studio sulle figure binarie dello *I Ching*, prestò fede a questo risultato. Nel 1919, tuttavia, il matematico francese Pierre Frèdéric Sarrus notò che $2^{341}-2$ è un multiplo di 341 anche se 341 è un numero composto, il prodotto di 11 e 31. Dal lavoro di Sarrus sono stati scoperti molti altri controesempi riguardanti diversi valori della base b: $3^{91}-3$ è un multiplo del numero composto 91, $4^{15}-4$ è un multiplo del numero composto 15. Tutti questi enunciati possono essere controllati con un piccolo calcolatore sfruttando l'aritmetica modulare già descritta.

Un numero che, secondo il test di Fermat per un valore assegnato di b, non risulta composto, prende il nome di pseudoprimo in base b. Il numero 341 è pseudoprimo in base 2, mentre 91 è pseudoprimo in base 3 e 15 in base 4. Di fatto esiste un'infinità di pseudoprimi in ogni base b. Alcuni numeri composti, come 561 (il prodotto di 3, 11, 17) e 1729 (il prodotto di 7, 13, 19) sono pseudoprimi in ogni base b. Numeri siffatti sono detti numeri di Carmichael dal nome del matematico americano R. D. Carmichael, che scoprì le loro proprietà nel 1909.

L'esistenza di numeri di Carmichael pone fine alla speranza che il test di Fermat, almeno nella sua formulazione originaria, possa separare tutti i primi dai composti. Peraltro, i numeri di Carmichael sono molto rari, e rari sono anche gli pseudoprimi in una singola base, se confrontati con i numeri primi. Jan Bohman dell'Università di Lund ha dimostrato che esistono esattamente 882 206 716 primi minori di 20 miliardi. John L. Selfridge della rivista «Mathematical Reviews» e Samuel S. Wagstaff, Jr. dell'Università della Georgia hanno calcolato che esistono solo 19 865 pseudoprimi in base 2 minori di 20 miliardi. Se si eseguisse il test di Fermat in base 2 per tutti i numeri inferiori a 20 miliardi, la percentuale di errore sarebbe di circa uno su un milione.

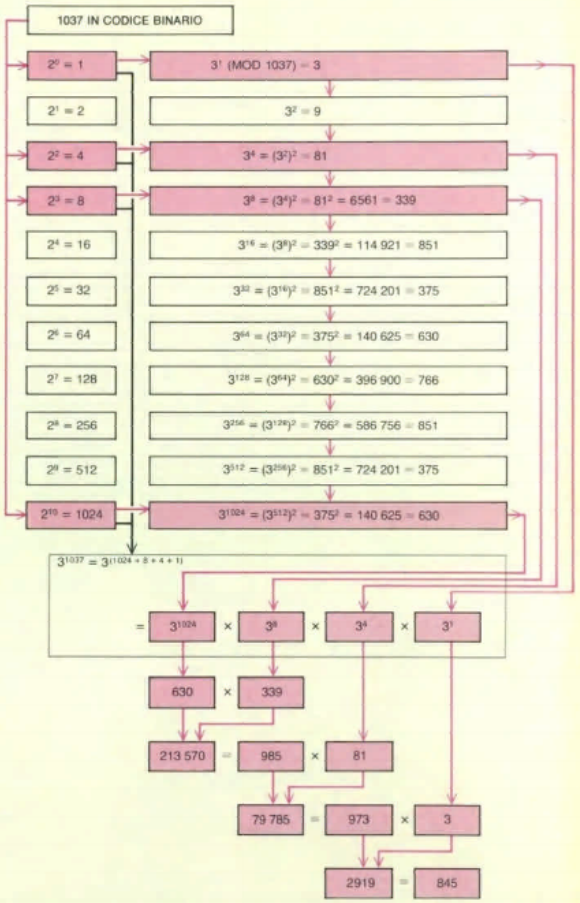
La scarsità di pseudoprimi in base 2, fra tutti i numeri inferiori a 20 miliardi, fa pensare che, se un numero supera il test di Fermat in base 2, è molto probabile che sia primo. Inoltre, se il numero è un numero composto che supera il test di Fermat in base 2, potrebbe non passarlo in base 3. Sarebbe piacevole poter asserire che, applicando il test di Fermat alla base 3, si riduce significativamente la probabilità che un numero composto continui a comportarsi come se fosse un numero primo. Poiché tuttavia i test possono non essere indipendenti, è possibile che quello in base 3 non elimini ancora molti composti che non siano già stati eliminati dal test in base 2.

Recentemente D. H. Lehmer dell'Università della California a Berkeley e, indipendentemente, Robert M. Solovay del California Institute of Technology e Volker Strassen del Politecnico federale svizzero hanno sviluppato una variante del test di Fermat che soddisfa al requisito dell'indipendenza in differenti basi. Il test ha la caratteristica che se il numero n in esame è composto, risulta tale per almeno la metà dei valori della base b compresi fra 1 e n. Sicché scegliendo a caso 100 basi differenti e applicando il test di Lehmer-Solovay-Strassen, la probabilità che qualche numero composto n superi tutti e 100 i test è minore o uguale a una su 2^{100} ovvero a una su 10^{30}.

Solovay e Strassen dicono che il loro è un «test di primalità Monte Carlo» (numerosi metodi probabilistici matematici e fisici prendono il nome da quella città, nota per i suoi giochi d'azzardo). Dal punto di vista pratico la denominazione sembra precisa; parrebbe infatti che nella applicazione crittografica il funzionamento di un codice non venga inficiato dalla piccolissima probabilità che i numeri su cui si basa non siano in realtà primi. È stato anche osservato, su basi che ritengo filosoficamente fragili, che dal momento che ogni ordinaria dimostrazione è soggetta a correzioni ed errori umani, si potrebbe accettare una forte conferma probabilistica della primalità come una sua dimostrazione matematica.

In effetti abbiamo buone ragioni per credere che la probabilità di errore di una dimostrazione matematica sia molto superiore a 1 su 10^{30}. La storia della matematica offre numerosi esempi di «dimostrazioni» che si sono poi rivelate erronee o fuorvianti. Esiste però una differenza qualitativa, di grande rilievo per i matematici, fra una conferma probabilistica e una dimostrazione matematica. Una dimostrazione è un argomento deduttivo, in cui ogni passo segue dai precedenti. La forza della dimostrazione non deriva solo dal fatto che è possibile controllare la validità delle conclusioni, ma anche dal fatto che la validità segue in forza dell'argomento. Ritengo che il test di primalità Monte Carlo induca piuttosto a pensare che fra i concetti di dimostrazione e di certezza corre una notevole differenza.

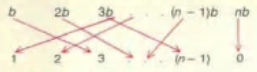
Nel 1876 il matematico francese Edouard A. Lucas espose un solido test di primalità per un qualsiasi numero n. Supponiamo che esista un numero b per il quale b^{n-1} sia congruo a 1 modulo n, mentre $b^{(n-1)/p}$ non sia congruo a 1 modulo n per ogni fattore primo p di $n-1$. Lucas dimostrò che in tal caso n deve essere primo.



Con l'aritmetica modulare si evitano calcoli che nell'aritmetica ordinaria richiederebbero molto tempo e sarebbero esposti a errori. Il diagramma di flusso mostra come si possa trovare il resto quando si divide il numero 3^{1037} per 1037, senza dover calcolare il valore effettivo di 3^{1037}. Il metodo si fonda sul fatto che il resto del quadrato di un numero per un dato modulo è uguale al quadrato del resto di quel numero per lo stesso modulo. Elevando ripetutamente al quadrato il resto di una potenza di 3 e prendendo il resto del risultato, si può trovare una successione di resti modulo 1037, di 3, 3^2, 3^4, 3^8, 3^{16}, fino a 3^{1024}. Dato che 3^{1037} è uguale a $3^{1024} \times 3^8 \times 3^4 \times 3$, il resto di 3^{1037} diviso per 1037 è uguale al resto del prodotto dei resti 3^{1024} (mod 1037) $\times$ 3^8 (mod 1037) $\times$ 3^4 (mod 1037) $\times$ 3 (mod 1037). Il procedimento può essere svolto da un calcolatore programmabile.

SI CONSIDERINO I NUMERI $b, 2b, 3b, \ldots, (n-1)b, nb$

TROVANDO I RESTI MODULO n DI QUESTI NUMERI SI DETERMINA UNA CORRISPONDENZA IN CUI I RESTI SONO UNA PERMUTAZIONE DEI COEFFICIENTI DI b.



QUINDI $b \times 2b \times \ldots \times (n-1)\,b \pmod{n} = 1 \times 2 \times \ldots \times (n-1) \pmod{n}$.

PERCIÒ $|b \times 2b \times \ldots \times (n-1)b| - |1 \times 2 \times \ldots \times (n-1)| = 0 \pmod{n}$.

MA $b \times 2b \times \ldots \times (n-1)b = b^{n-1}(n-1)!$ E $1 \times 2 \times \ldots \times (n-1) = (n-1)!$

QUINDI $|b \times 2b \times \ldots \times (n-1)b| - |1 \times 2 \times \ldots \times (n-1)| =$

$|b^{n-1}(n-1)!| - |(n-1)!| = (b^{n-1}-1)(n-1)! = 0 \pmod{n}$.

PERTANTO $(b^{n-1}-1)(n-1)!$ È UN MULTIPLO DI n, IL CHE È SUFFICIENTE PER DIMOSTRARE IL TEOREMA DI FERMAT.

La dimostrazione del «piccolo teorema» di Fermat discende dall'applicazione del teorema fondamentale dell'aritmetica e dalle regole di moltiplicazione nell'aritmetica modulare. Il piccolo teorema di Fermat asserisce che se n è un numero primo e b un intero, $b^n - b$ è un multiplo di n. Se b è un multiplo di n, la conclusione è pressoché immediata: dato che $b^n - b$ è uguale a $b(b^{n-1} - 1)$, b è un fattore di $b^n - b$ e $b^n - b$ è un multiplo di n. Se b non è multiplo di n, basta dimostrare che $b^{n-1} - 1$ è multiplo di n. Un corollario del teorema fondamentale dell'aritmetica ci dice che se un primo divide esattamente il prodotto di più numeri, divide anche uno dei numeri. Quindi, poiché n non divide esattamente nessuno dei numeri fra 1 e $n - 1$, non dividerà esattamente neppure $(n-1)!$. Ne segue che se si riesce a dimostrare che n divide esattamente $(b^{n-1} - 1)\,(n-1)!$, allora anche $b^{n-1} - 1$ e $b^n - b$ sono divisibili esattamente per n; ne consegue che $(b^{n-1} - 1)$ e $(b^n - b)$ sono anch'essi divisibili per n. Consideriamo i numeri b, $2b$, $3b$, fino a nb. Nessuna coppia di numeri ib e jb può dare lo stesso resto quando siano divisi per n. Altrimenti $ib - jb$, che è uguale a $(i - j)\,b$, sarebbe un multiplo di n, dato che la sottrazione cancellerebbe i resti. Poiché b non è multiplo di n, il teorema fondamentale dell'aritmetica implica che $i - j$ è un multiplo di n. Il numero n, tuttavia, non può essere diviso senza resto da un qualsiasi numero $i - j$, dove i e j siano stati scelti nella successione di numeri da 1 a n. La supposizione che ib e jb diano lo stesso resto, una volta divisi per n, conduce a una contraddizione. Poiché il resto della divisione di nb per n è 0 e la divisione per n dà resti solo fra 1 e $n - 1$, i numeri $b, 2b, \ldots, (n-1)b$, se divisi per n danno resti compresi fra 1 e $n - 1$, in un ordine opportuno. Il diagramma mostra che dividendo per n i numeri b, $2b, \ldots (n-1)b$ e prendendo i resti, si può stabilire una corrispondenza fra b, $2b, \ldots (n-1)b$ e $1, 2, \ldots (n-1)$. Dato che i resti dei numeri di ciascun insieme sono gli stessi, a meno dell'ordine, il resto del prodotto $b \times 2b \times \ldots \times (n-1)b$ è uguale al resto del prodotto $1 \times 2 \times \ldots \times (n-1)$. Sottraendo un prodotto dall'altro si cancellano i resti e la differenza dei due prodotti è un multiplo di n. Con pochi passaggi algebrici è possibile dimostrare che la differenza dei due prodotti è uguale a $(b^{n-1} - 1)(n-1)!$, per cui l'espressione è divisibile esattamente per n. È stato in questo modo dimostrato il piccolo teorema di Fermat per tutti i numeri interi b.

341 PSEUDOPRIMO IN BASE 2

$$2^{341} = 2^{256} \times 2^{64} \times 2^{16} \times 2^{4} \times 2$$
$$= 64 \times 16 \times 64 \times 16 \times 2 \pmod{341}$$
$$= 2 \pmod{341}$$

QUINDI $2^{341} - 2 = 0 \pmod{341}$

PERTANTO 341 SUPERA IL TEST DI FERMAT IN BASE 2

MA $341 = 11 \times 31$

561 PSEUDOPRIMO IN OGNI BASE

$$2^{561} = 2^{512} \times 2^{32} \times 2^{16} \times 2$$
$$= 103 \times 103 \times 460 \times 2 \pmod{561}$$
$$= 2 \pmod{561}$$

QUINDI $2^{561} - 2 = 0 \pmod{561}$

PERTANTO 561 SUPERA IL TEST DI FERMAT IN BASE 2

MA $561 = 3 \times 11 \times 17$

$$3^{561} = 3^{512} \times 3^{32} \times 3^{16} \times 3$$
$$= 273 \times 273 \times 69 \times 3 \pmod{561}$$
$$= 3 \pmod{561}$$

QUINDI $3^{561} \times 3 = 0 \pmod{561}$

PERTANTO 561 SUPERA IL TEOREMA DI FERMAT IN BASE 3

Gli pseudoprimi sono numeri che superano il test di primalità derivato dal piccolo teorema di Fermat per qualche base b, ma che tuttavia sono numeri composti. Quindi, uno pseudoprimo in base b è un numero composto n che divide senza resto $b^n - b$. Il matematico francese Pierre Frédéric Sarrus osservò per primo nel 1919 che 341, il prodotto di 11 per 31, è uno pseudoprimo in base 2. Nel nostro caso viene mostrato che $2^{341} - 2$ è divisibile per 341, sfruttando l'aritmetica modulare in modo analogo a quello dell'illustrazione della pagina precedente. Alcuni numeri, detti numeri di Carmichael, in onore del matematico americano R. D. Carmichael che scoprì le loro proprietà, sono pseudoprimi in ogni base b. Il numero 561, prodotto di 3,11 e 17, è il più piccolo dei numeri di Carmichael; qui viene mostrato che è pseudoprimo nelle basi 2 e 3.

Supponiamo, per esempio, che n sia 257; allora $n - 1$ è 256, ossia 2^8, quindi tutti i fattori primi p di $n - 1$ sono uguali a 2. Per provare che n è primo, bisogna trovare un b tale che b^{256} sia congruo a 1 modulo 257, ma non è così per $b^{256/2}$. Sebbene il test non dia indicazioni su come trovare il particolare numero b, molti di tali numeri soddisfano le condizioni del teorema per qualsiasi primo n. Una ricerca casuale condurrà quasi sempre al successo. Quando b è uguale a 3, per esempio, 3^{256} è congruo a 1 modulo 257, mentre $3^{256/2}$ non è congruo a 256 modulo 257. Quindi 257 è primo. Sebbene sia anch'esso di tipo Monte Carlo, nel senso che b deve essere scelto a caso, una volta trovato il numero, il test di Lucas fornisce una rigorosa dimostrazione di primalità.

C'è un aspetto del test di Lucas che ne limita l'applicabilità a numeri di una certa forma: se non si possono trovare tutti i fattori primi p di $n - 1$, non può essere utilizzato. Ovviamente, se si pensa che sia primo, n è dispari e $n - 1$ è divisibile per 2. Ma questa buona partenza non basta; il test di Lucas non è generalmente applicabile agli altri $n - 1$ fattori, in modo semplice come nel mio esempio.

Se tutti i fattori primi di $n + 1$ possono essere trovati più facilmente di quelli di $n - 1$, esiste un altro test (anch'esso proposto per la prima volta da Lucas) per stabilire la primalità di n. Lehmer lo ha migliorato nel 1930 e per i numeri a cui può essere applicato in questa forma fornisce un procedimento che gira molto velocemente su un grande calcolatore. Grazie a esso è stata dimostrata la primalità dei più grandi numeri primi conosciuti, numeri della forma $2^p - 1$, dove p stesso è un numero primo. Tali numeri sono detti numeri di Mersenne, dal nome del matematico francese del XVII secolo che compilò per primo un elenco di numeri primi p per i quali riteneva che fosse primo anche $2^p - 1$. È evidente che se n è un numero di Mersenne, si conoscono tutti i fattori primi di $n + 1$: sono tutti uguali a 2.

Nel 1975 John Brillhart dell'Università dell'Arizona, Lehmer e Selfridge hanno mostrato come costruire un test di primalità per un numero n se si conoscono solo alcuni dei fattori primi di $n - 1$ o $n + 1$. Hugh C. Williams dell'Università di Manitoba ha portato questo tipo di test a una grande raffinatezza: per controllare la primalità di n sono sufficienti fattorizzazioni parziali di $n^2 + 1$, $n^2 - n + 1$ e $n^2 + n + 1$. Se però nessuno di questi si fattorizza con facilità, il test si arena. Per quanto questi metodi consentano di controllare molti numeri primi di 100 cifre, si è stimato che per condurre a termine l'esame di certi primi riottosi occorrerebbe un secolo di tempo macchina. Sarebbe quindi necessario un test di primalità che non dipendesse dalla particolare forma del numero in esame.

Nel 1980 Adleman e Robert S. Rumely dell'Università della Georgia hanno sviluppato un test che ha radicalmente modificato l'efficienza del controllo della primalità di grandi numeri che non abbiano una particolare forma. Nella formulazione originaria il test era in grado di saggiare la primalità di qualsiasi numero di 50-100 cifre in 4 - 12 ore di tempo macchina su un grande calcolatore. Henri Cohen dell'Università di Bordeaux e Hendrik W. Lenstra, Jr. dell'Università di Amsterdam hanno significativamente migliorato il test, tanto che attualmente gira 1000 volte più velocemente: un numero di 100 cifre può essere controllato in circa 40 secondi sul calcolatore Cyber 170-750 della Control Data Corporation.

Da dove proviene tanta efficienza del test di Adleman-Rumely? I suoi dettagli richiedono la conoscenza tecnica della teoria dei numeri algebrici, ma in sostanza è simile a quello di Fermat. Vengono costruiti due numeri ausiliari, detti il numero iniziale I e il numero euclideo E. Il numero I è il prodotto di svariati primi come $2 \times 5 \times 5 \times 7 = 210$. Il numero euclideo E deve invece questo nome al fatto che la sua definizione ricorda la dimostrazione di Euclide dell'esistenza di un'infinità di primi. E è il prodotto di tutti i primi $p, q, r, \ldots$ tali che i numeri $p - 1$, $q - 1$, $r - 1, \ldots$ sono tutti fattori di I. Il numero 70, per esempio, è un fattore di 210 e dato che 70 è minore di uno rispetto al primo 71, questo (71) è definito come un fattore di E. I fattori di 210 che sono predecessori di un primo sono 1, 2, 6, 10, 30, 42, 70 e 210 stesso. Quindi E è il prodotto dei primi 2, 3, 7, 11, 31, 43, 71, 211, ovvero è il numero 9 225 988 926. Il numero E deve essere costruito in modo da essere maggiore della radice quadrata del numero n di cui si controlla la primalità. Nel mio esempio con il numero iniziale 210 il metodo di Adleman-Rumely potrebbe lavorare con un n non maggiore di 10^{19}. Il tempo di calcolo è proporzionale a una potenza del numero I, pertanto questo andrebbe scelto il più piccolo possibile. Vi è una sorta di tensione dinamica fra I ed E. Perché il test sia valido, E deve essere grande; perché il test sia rapido, I deve essere piccolo. Inoltre, poiché E dipende da I, i numeri ausiliari non possono essere scelti indipendentemente uno dall'altro. Il numero 210 è un buon esempio di scelta di I, poiché si tratta di un numero relativamente piccolo con numerosi fattori che sono predecessori di un primo. Per dimostrare che il test di Adleman-Rumely è sempre veloce, era necessario verificare che fosse sempre possibile trovare dei numeri E e I opportuni e valutarne la grandezza.

Per un caso, si trattava di un lavoro già svolto. Nel 1955, Karl Prachar della Facoltà di agraria dell'Università di Vienna mostrò che esiste un'infinità di interi tra i cui fattori molti sono predecessori di un primo. Per applicare il risultato di Prachar al test di Adleman-Rumely nella sua forma originale, era necessario mostrare che il numero I può essere costruito in modo da essere «libero da quadrati», ossia non divisibile per alcun quadrato di un intero maggiore di 1. Cohen e Lenstra hanno recentemente dimostrato che, nella loro variante del test, la condizione della libertà da quadrati può essere eliminata. È stato possibile anche rafforzare il risultato di Prachar impiegando le scoperte di Patrick X. Gallagher della Columbia University e di Enrico Bombieri dell'Institute for Advanced Study e dell'Università di Pisa. Andrew M. Odlyzko dei Bell Laboratories e io abbiamo analizzato la costruzione dei numeri che possono recitare la parte di I nel nuovo test.

Dopo la costruzione di I ed E, sono stati sviluppati alcuni test analoghi a quello di Fermat per ogni coppia di primi p e q in cui p, il primo membro della coppia, è un fattore di E e q, secondo membro della coppia, è un fattore di $p - 1$. Il test non viene eseguito sui numeri interi, ma in rapporto ai cosiddetti interi algebrici che corrispondono a p e q. Un intero algebrico è un numero complesso che è radice di

I NUMERI PRIMI DI MERSENNE FINO A $2^{62\,982}$

VALORE DI p PER CUI $2^p - 1$ È PRIMO	$2^p - 1$	DATA DELLA DIMOSTRAZIONE	AUTORE DELLA DIMOSTRAZIONE	CALCOLATORE UTILIZZATO
2	3	ANTICHITÀ	CITATO NEGLI *ELEMENTI* DI EUCLIDE	
3	7			
5	31			
7	127			
13	8191	1461	CITATO NEL CODICE LAT. MONAC. 14 908	
17	131 071	1588	PIETRO ANTONIO CATALDI	
19	524 287			
31	2 147 483 647	1772	LEONHARD EULER	
61	19 CIFRE	1883	I. M. PERVOUCHINE	
89	27 CIFRE	1911	R. E. POWERS	
107	33 CIFRE	1914	R. E. POWERS, E. FAUQUEMBERGE	
127	39 CIFRE	1876 – 1914	ÉDOUARD LUCAS, E. FAUQUEMBERGE	
521	157 CIFRE	1952	RAPHAEL M. ROBINSON	SWAC
607	183 CIFRE			
1279	386 CIFRE			
2203	664 CIFRE			
2281	687 CIFRE			
3217	969 CIFRE	1957	HANS RIESEL	BESK
4253	1281 CIFRE	1961	ALEXANDER HURWITZ	IBM-7090
4423	1332 CIFRE			
9689	2917 CIFRE	1963	DONALD B. GILLIES	ILLIAC-II
9941	2993 CIFRE			
11 213	3376 CIFRE			
19 937	6002 CIFRE	1971	BRYANT TUCKERMAN	IBM 360/91
21 701	6533 CIFRE	1978	LAURA NICKEL, CURT NOLL	CDC-CYBER-174
23 209	6987 CIFRE	1979	CURT NOLL	CDC-CYBER-174
44 497	13 395 CIFRE	1979	HARRY L. NELSON, DAVID SLOWINSKI	CRAY-1

I numeri primi di Mersenne sono numeri primi predecessori di una potenza di 2. Il loro nome deriva da quello del matematico francese Marin Mersenne. Si tratta di numeri primi studiati fin dall'antichità, poiché, come mostrò già Euclide, se $2^p - 1$ è primo, $2^{p-1}(2^p - 1)$ è perfetto, ossia è uguale alla somma di tutti i suoi fattori, escluso se stesso. Se $2^p - 1$ è primo, anche p è primo, mentre l'inverso non è sempre valido. Non si sa se esista un'infinità di primi di Mersenne, né se esista un'infinità di composti di Mersenne, ma entrambe le asserzioni appaiono verosimili. Recentemente l'aumento dei numeri primi di Mersenne è andato di pari passo con la crescita delle capacità di calcolo. Secondo i dati di David Slowinski del Lawrence Livermore Laboratory, per dimostrare che $2^{8191} - 1$ non è primo, occorrono 100 ore macchina con un calcolatore ILLIAC-I, 5,2, ore con un IBM Sistema 7090, 49 minuti circa con un ILLIAC-II, 3,1 minuti con un IBM 360/91 e 10 secondi con il CRAY-1. Slowinski e Harry L. Nelson, anch'egli del Lawrence Livermore, hanno preso in esame tutti i numeri di Mersenne per valori di p fino a 50 000, senza trovare alcun primo maggiore di $2^{44\,497} - 1$. Recentemente Guy M. Haworth, Steven M. Holmes, David J. Hunt, Thomas W. Lake e Stewart F. Reddaway della International Computing Limited hanno proseguito la ricerca con un ICL-DAP, un supercalcolatore con 4096 elaboratori che lavorano in parallelo. Pur avendo portato il valore di p fino a 62 982, non hanno trovato alcun nuovo primo di Mersenne.

ARTE

LE SCIENZE *edizione italiana di* **SCIENTIFIC AMERICAN**

ha dedicato all'argomento diversi articoli:

L'olografia nel campo del restauro
di F. Gori e G. Urbani (n. 74)

L'origine dell'ambiguità nelle opere di Maurits C. Escher
di M. L. Teuber (n. 75)

Pieter Bruegel il Vecchio e la tecnica del Cinquecento
di H. A. Klein (n. 117)

La conservazione della pietra
di K. L. Gauri (n. 120)

I disegni preistorici tracciati sul terreno in Perù
di W. H. Isbell (n. 124)

L'«infrarosso colore» nell'indagine dei dipinti
di M. Matteini, A. Moles e P. Tiano (n. 142)

La statica dall'arte alla scienza
di S. Clara Roero (n. 150)

Norme architettoniche nella Cina del XII secolo
di E. Glahn (n. 155)

L'architettura di Christopher Wren
di H. Dorn e R. Marck (n. 157)

L'acustica dei piani armonici di violino
di C. Maley Hutchins (n. 160)

Conservazione e restauro
di P. Parrini (n. 161)

Intarsi rinascimentali: l'arte della geometria
di A. Tormey e Y. Farr Tormey (n. 169)

DIMENSIONE DEL NUMERO

TEST DI PRIMALITÀ	20 CIFRE	50 CIFRE	100 CIFRE	200 CIFRE	1000 CIFRE
DIVISIONE PER TENTATIVI	2 ORE	10^{11} ANNI	10^{36} ANNI	10^{86} ANNI	10^{486} ANNI
LUCAS, BRILLHART-LEHMER-SELFRIDGE, WILLIAMS	5 SECONDI	10 ORE	100 ANNI	10^{8} ANNI	10^{44} ANNI
ADLEMAN-RUMELY, COHEN-LENSTRA	10 SECONDI	15 SECONDI	40 SECONDI	10 MINUTI	1 SETTIMANA

Il tempo richiesto per il controllo della primalità di un numero varia notevolmente in base al tipo di test adottato. Nella tabella si assume l'uso di un calcolatore veloce. In particolare, per il metodo di divisione si assume l'uso di un calcolatore che esegua un milione di divisioni al secondo, indipendentemente dalla grandezza dei numeri esaminati. Il tempo di calcolo per una famiglia di test del tipo di quello ideato dal matematico francese Édouard A. Lucas è a volte poco confortante; alcuni numeri primi di forma particolare possono essere controllati molto più velocemente. La maggior parte dei tempi indicati sono risultati di stime, ma le caselle in colore riportano valori effettivamente ottenuti su calcolatori. Combinando i tre tipi di test, è possibile ottenerne uno ancora più veloce.

un'equazione algebrica a coefficienti interi, in cui il coefficiente della potenza di grado massimo dell'incognita è 1. Per esempio, $\sqrt{2}$, i (la radice quadrata immaginaria di -1) e $(-1+i\sqrt{3})/2$ sono tutti interi algebrici in quanto radici delle equazioni algebriche $x^2-2=0$, $x^2+1=0$, $x^3-1=0$.

Se il numero n, di cui si controlla la primalità, non supera il test corrispondente a una delle coppie di primi p e q, allora viene classificato come composto, ma se li supera tutti non è certo che sia primo, anche se il numero di possibili fattori che resta da esaminare è piccolo. Adleman e Rumely hanno mostrato che ogni numero composto n che superi tutti i test del tipo Fermat deve avere i fattori primi in un insieme con esattamente I elementi. Lenstra ha mostrato che i numeri nell'insieme sono i residui delle potenze n, n^2, n^3... fino a n^I, modulo E. Provando con le divisioni se oltre a 1 e a n ciascuno dei numeri dell'insieme divide esattamente n, n è composto, altrimenti deve essere primo. Per quanto l'ultimo passo del procedimento di Adleman-Rumely assomigli a un processo di fattorizzazione, devo sottolineare che la sua conclusione risulta valida solo se n ha superato tutti i precedenti test di tipo Fermat. La maggior parte e forse tutti i numeri composti cadono per almeno uno dei test di Fermat, sicché non è necessario disporre di un fattore che debba essere trovato per divisione all'ultimo passo.

La velocità e l'applicabilità generale dei nuovi test hanno aperto la strada all'esame teorico di numeri precedentemente inaccessibili anche ai calcolatori più veloci. Supponiamo ora di sottoporre al test un numero con molto più di 100 cifre. In quanto tempo ci si può aspettare che il test emetta il suo responso? Questa e altre domande analoghe sono di grande importanza teorica per una branca della scienza dei calcolatori che prende il nome di teoria della complessità. Secondo una definizione correntemente accettata nella teoria della complessità, un test di primalità sarà «lento» dal punto di vista computazionale se non può essere eseguito in quello che è detto tempo polinomiale. Vale a dire, un test è lento a meno che il tempo impiegato per esaminare un numero n non sia minore di una potenza fissata k del numero di cifre di n. Indicherò il numero di cifre di n con $d(n)$. Si noti che $d(n)$ stesso è un numero, il cui numero di cifre sarà $d(d(n))$.

In base alla definizione fornita dalla teoria della complessità, i test di Adleman-Rumely e Cohen-Lenstra sono lenti. Il tempo di calcolo ha come limite $d(n)$ elevato alla $d(d(d(n)))$ moltiplicato per qualche costante c. L'espressione $d(d(d(d(n))))$ è il numero di cifre del numero di cifre del numero di cifre di n. Quale che sia la costante c per tale espressione, alla fine il prodotto di c per tale espressione eccederà la costante k, crescendo indefinitamente all'aumentare di n. Il limite del tempo di calcolo non è quindi polinomiale.

Tuttavia, per numeri relativamente «piccoli» il criterio proposto può essere fuorviante, in quanto $d(d(d(n)))$ in tal caso cresce all'infinito a una velocità decisamente ragionevole. Così, anche per un numero come 10^{1000}, $d(d(d(n)))$ è ancora uguale a 1. Il primo numero n per il quale l'espressione è uguale a 2 è $10^{999999999}$; in altre parole, per tutti i numeri inferiori il tempo di esecuzione dei nuovi test è limitato dalla potenza c di $d(n)$. Quindi i nuovi test non possono girare in tempo polinomiale, ma «quasi».

Ora che il test di primalità può essere eseguito rapidamente anche per numeri relativamente grandi, la nostra attenzione può rivolgersi al problema correlato della fattorizzazione. Dei progressi in questo campo avrebbero riflessi immediati sui sistemi crittografici basati sulla fattorizzazione. Gli sviluppi dei test di primalità non hanno direttamente a che fare con la fattorizzazione; d'altra parte, nessuno ha ancora dimostrato che questa sia intrattabile: nulla ci garantisce che domani qualcuno non possa inventare un metodo di fattorizzazione rivoluzionario. Una decisione circa la sicurezza a lunga scadenza dei sistemi crittografici a chiave pubblica basati sulla fattorizzazione coinvolge un giudizio soggettivo sui possibili progressi in materia. I recenti sviluppi nel campo dei test di primalità sottolineano la potenziale vulnerabilità di questi tipi di codice di fronte a nuovi risultati teorici.