BOLLETTINO

UNIONE MATEMATICA ITALIANA

Sezione A – La Matematica nella Società e nella Cultura

LUISELLA CAIRE, UMBERTO CERRUTI

Questo numero è primo? Sì, forse, dipende ...

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. 9-A—La Matematica nella Società e nella Cultura (2006), n.3-1, p. 449–481.

Unione Matematica Italiana

http://www.bdim.eu/item?id=BUMI_2006_8_9A_3-1_449_0

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)
SIMAI & UMI*

<http://www.bdim.eu/>

Questo numero è primo? Sì, forse, dipende ...

LUISELLA CAIRE - UMBERTO CERRUTI

*I think prime numbers are like life:
they are very logical, but you can never work out the rules,
even if you spend all your time thinking about them.*

Mark Haddon, The curious incident of the dog in the night-time

1. – Introduzione.

Un numero primo è un intero divisibile solo per uno e per se stesso.

Ci immaginiamo questi numeri come oggetti «infrangibili». Se cade per terra 256 si sbriciola in otto pezzi. Al contrario 257 rimane tal quale, e non c'è modo di romperlo. Si tratta di un concetto così semplice!

Eppure pochi concetti altrettanto semplici sono stati oggetto di tanti studi, da tanti diversi punti di vista, nel corso dei secoli, e hanno trascinato con sé tanti progressi fondamentali in matematica.

Per iniziare, con il suo Teorema Fondamentale dell'Aritmetica, Euclide ci ha assicurato che i primi sono gli irriducibili costituenti della materia numerica, gli atomi dell'universo degli interi.

Questa materia (i numeri interi) potrebbe essere infinita anche se esistesse un numero finito di primi. Ma essi sono infiniti, e nel corso dei secoli i ricercatori hanno speso sempre nuove energie, e percorso sempre nuove strade, per provarlo.

Inoltre i matematici hanno cercato di svelare i misteri della distribuzione dei numeri primi. Essi appaiono in modo apparentemente imprevedibile. Al tempo stesso la sequenza dei numeri primi obbedisce a leggi precise: per esempio tra n e $2n$ c'è sempre almeno un numero primo, mentre tra $n! + 2$ ed $n! + n$ non se ne trova neppure uno. È perfettamente comprensibile che molte tra le migliori menti matematiche si siano dedicate allo studio di questa meravigliosa successione.

Può sembrare strano, invece, che negli ultimi decenni siano stati fatti notevoli investimenti per riuscire a rispondere a questa domanda: *dato un numero N , esso è primo?*

In fondo che interesse ha sapere con certezza che *questo particolare intero N è primo?*

Le motivazioni che sostengono lo sviluppo impetuoso di questo recente campo di ricerca sono essenzialmente due:

- il problema si rivela immediatamente assai interessante per le idee matematiche che genera e le tecniche che utilizza
- i numeri primi grandi sono diventati indispensabili per gran parte degli attuali metodi di crittografia a chiave pubblica (si veda [10]).

Nel corso di questi nuovi studi, l'occhio degli esperti ha iniziato a guardare ai numeri primi ancora sotto un altro punto di vista. Nonostante la definizione di numero primo sia un concetto così semplice, e sembri non ammettere sfumature, i matematici (incalzati dal mondo 'pratico') hanno cominciato a indagare se potessero esserci 'imitazioni' di un numero primo, a chiedersi:

Ci possono essere primi di dubbia autenticità, come quadri o gioielli, che dividono gli esperti?

Avrebbe senso *scommettere* sulla primalità di un numero?

Fino ad una trentina di anni fa queste domande sarebbero sembrate ridicole.

Oggi chiunque si occupi professionalmente di crittografia sa che molti sistemi utilizzati (per esempio il famoso RSA) hanno una piccola (ma in genere non nulla) probabilità di malfunzionamento: può accadere infatti che alcuni interi che vengono usati, e sono di essenziale importanza per la sicurezza, *non siano* primi, anche se *sembrano* tali.

Esistono dei *criteri di primalità* che dicono con certezza se N è primo o meno. Essi però sono polinomiali (cioè terminano in un tempo che è $O(\log^k N)$, dove k non dipende da N) solo per interi che hanno una forma particolare.

In questo articolo ci occupiamo di diversi tipi di criteri di primalità.

Nei paragrafi 2 e 3 parliamo di criteri di primalità *certi* (o *deterministici*). In genere essi hanno il grande handicap di non essere polinomiali, e quindi non efficienti, ma si rivelano utili se applicati a

interi di forma particolare, per esempio ai numeri di Mersenne e a quelli di Fermat.

Nel paragrafo 4 trattiamo dei test *probabilistici* di primalità. Se essi rispondono no, siamo sicuri che il numero è composto, mentre quando rispondono sì esiste una probabilità (che si può rendere piccola a piacere) che non siano primi. Il grande vantaggio sta nel fatto che essi sono polinomiali.

Infine, nell'ultimo paragrafo ci occupiamo di criteri di primalità *condizionati*, cioè vediamo come, se l'ipotesi estesa di Riemann è vera, alcuni test probabilistici diano origine a criteri certi e polinomiali.

2. – Criteri di primalità.

2.1. – *Crivello di Eratostene.*

Euclide (Elementi, Libro IX) provò che i numeri primi sono infiniti: potremmo portare più di 50 dimostrazioni di questo fatto, che utilizzano quasi tutti i metodi della matematica, dall'analisi, all'aritmetica, all'algebra, alla topologia, alla combinatorica ...[2], [19]

Eratostene, con il suo famoso crivello, che risale al 250 a.C. circa, fornì il primo metodo per selezionare i numeri primi nell'insieme dei numeri naturali.

Scriviamo tutti gli interi tra 2 ed N :

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, ..., N

Cancelliamo tutti i multipli di 2 (escluso 2):

2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, ..., N

Consideriamo il più piccolo numero rimasto diverso da 2, cioè 3, e cancelliamo tutti i suoi multipli (escluso lui stesso):

2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29, ..., N

Continuiamo con 5:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots, N$$

ecc

L'algoritmo, anche se non polinomale, è abbastanza efficace (nel nostro piccolo esempio, dopo solo tre passi abbiamo già trovato tutti i primi fino a 29); si può renderlo ancora più efficace, osservando che, se N non è primo, ha almeno un fattore primo minore o uguale a $\sqrt{N}$.

2.2. – Criterio di Wilson.

Questo è un criterio 'a molte mani': fu ideato da John Wilson e pubblicato da Waring nel 1770; pare che fosse già noto in precedenza a Leibniz, e fu provato da Lagrange nel 1773.

TEOREMA 2.1. – Criterio di Wilson

Un numero n è primo se e solo se

$$(n - 1)! \equiv -1 \pmod{n}$$

DIMOSTRAZIONE. – Se $(n - 1)! \equiv -1 \pmod{n}$, allora $(n - 1)! + hn = -1$; dunque l'unico intero positivo che può dividere sia n che $(n - 1)!$ è 1; pertanto n non ha fattori in comune con tutti gli interi che lo precedono ed è primo.

Viceversa, se n è primo, $\mathbb{Z}_n$ è un campo e quindi l'equazione $x^2 = 1$ in $\mathbb{Z}_n$ ha solo le soluzioni $x = \pm 1$. Dunque gli unici elementi che sono inversi di se stessi sono ± 1 . Pertanto gli elementi di $\mathbb{Z}_n^*$ si possono elencare mettendo a fianco ad ognuno il suo inverso (con le sole eccezioni di ± 1). È evidente allora che il loro prodotto è uguale a -1 . $\square$

ESEMPIO 2.2

Sia $n = 13$. Scriviamo i prodotti dei numeri da 1 a 12 accoppiandoli come detto sopra.

$$1 \cdot (2 \cdot 7) \cdot (3 \cdot 9) \cdot (4 \cdot 10) \cdot (5 \cdot 8) \cdot (6 \cdot 11) \cdot 12 = 12 = -1 \pmod{13}.$$

Si tratta di una formula elegante ma inefficace. Si legge su molti testi che la sua inefficacia è dovuta alla necessità di calcolare $n!$, che è subito troppo grande: ad esempio, $1000!$ ha 2568 cifre. Ma il motivo reale non è questo, perché i calcoli vengono effettuati modulo n e quindi il prodotto $1 \cdot 2 \cdot \dots \cdot (n-1)$ si esegue dividendo sempre i prodotti di due numeri per n e prendendo i resti, e quindi il calcolo modulo n di $(n-1)!$ non supera mai $n-1$.

Il problema vero è che non esiste alcun modo per calcolare il fattoriale velocemente, se non fare tutti i prodotti, e ci sono troppi passi da fare.

È interessante notare che, partendo da criteri che non sono efficaci per la generalità degli interi, si può arrivare con spostamenti progressivi a criteri che lavorano molto bene in casi particolari.

Un esempio di questa ‘tecnica degli spostamenti progressivi’ è fornita dai criteri di Lucas e di Pépin.

2.3. – Criteri di Lucas e Pocklington.

Esistono diverse versioni del Criterio di Lucas. Diamo direttamente quella più efficace.

CRITERIO 2.3. – Criterio di Lucas [12] (1876)

Un numero $n \in \mathbb{N}$ è primo se e solo se per ogni divisore primo q di $n-1$ esiste un $a \in \mathbb{N}$ tale che

1. $a^{n-1} \equiv 1 \pmod{n}$
2. $a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$

DIMOSTRAZIONE. – Se n è primo, il gruppo $G = \mathbb{Z}_{n-1}^*$ è ciclico e ha ordine $n-1$. Pertanto se a è un generatore di G le condizioni di 2.3 sono banalmente verificate. Dall’altro lato, se n soddisfa le due condizioni di 2.3, si prova che $n-1$ divide l’ordine del gruppo $\mathbb{Z}_{n-1}^*$, cioè $\varphi(n)$. Pertanto $n-1$ deve essere uguale a $\varphi(n)$. Allora n è coprimo con tutti gli interi che lo precedono, e ne segue la tesi. $\square$

Questo criterio si può usare solo se si conoscono tutti i divisori primi

di $n - 1$. È stato 'migliorato' da Pocklington, il quale ha provato che è sufficiente conoscere una fattorizzazione parziale di $n - 1$. Vale infatti il seguente

TEOREMA 2.4. – Teorema di Pocklington

Sia $n - 1 = rs$, dove $(r, s) = 1$, $r = \prod_{i=1}^m q_i^{v_i}$ e $r > \sqrt{n}$.

Se, per ogni fattore primo q di r esiste un a tale che

- (i) $a^{n-1} \equiv 1 \pmod{n}$
- (ii) $(a^{\frac{n-1}{q}} - 1, n) = 1$

allora n è primo.

DIMOSTRAZIONE. – Sia p un primo che divide n e sia e il periodo di a in $\mathbb{Z}_p^*$. Sia q un fattore primo di r di molteplicità v . Allora, per l'ipotesi (i), $e | n - 1$ e per la (ii), $e \nmid \frac{n-1}{q}$.

Dunque $q^v | e$.

Poiché $e | p - 1$, anche $q^v | p - 1$. Ripetendo il ragionamento per tutti i fattori q_j di r , si avrà che $r | p - 1$.

Pertanto $\sqrt{n} < r < p$ e dunque $n = p$. □

Il criterio di Lucas risulta straordinariamente efficace per i numeri della forma $2^s + 1$. Infatti da 2.3 e dal Criterio di Eulero 2.11 (che si vedrà tra poco) si ottiene immediatamente il seguente

COROLLARIO 2.5. – Sia $n = 2^s + 1$; n è primo se e solo se esiste un a tale che $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$. □

2.4. – I numeri di Fermat e il Criterio di Pépin.

DEFINIZIONE 2.6. – Si dice **k-esimo numero di Fermat** il numero

$$F_k = 2^{2^k} + 1$$

Osserviamo che se $n = 2^s + 1$ è primo, allora s deve essere della forma $s = 2^k$.

Infatti se fosse $s = ab$, con b fattore dispari, si avrebbe $2^s + 1 = (2^a)^b + 1 \equiv (-1)^b + 1 \pmod{2^a + 1} \equiv 0 \pmod{2^a + 1}$, e quindi $2^a + 1$ dividerebbe n .

Pertanto i numeri della forma $2^s + 1$ che sono primi (dei quali tratta il Corollario 2.5), sono numeri di Fermat.

I primi cinque numeri di Fermat sono:

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537.$$

Essi sono primi.

È estremamente interessante sapere quali numeri di Fermat sono primi (in questo caso vengono detti **Primi di Fermat**).

Fermat congetturò che fossero tutti primi: è stata la sua peggiore congettura. Infatti $F_5 = 2^{2^5} + 1 = 641 \times 6700417$.

Fu Eulero nel 1732 a dimostrare che F_5 è divisibile per 641. Provò infatti che ogni divisore primo di F_n deve essere della forma $k \cdot 2^{n+2} + 1$. Nel caso di F_5 , per $k = 1, 2, 3, 4, 5$, si trovano i numeri 129, 257, 385, 513, 641. Di questi solo 257 e 641 sono primi, e F_5 è divisibile per 641.

Con i mezzi di calcolo attuali Fermat non avrebbe fatto questo errore; un tempo i calcoli con i numeri ‘grandi’ erano appannaggio di poche persone. Esistevano nel 1700 e nel 1800 utilissimi ‘mostri computazionali’; ad esempio Zerah Colburn nei primi anni dell’800, a soli 8 anni, fattorizzò F_5 a mente in meno di un minuto; un altro esempio fu Zacharias Dahse che, a metà ‘800, calcolò le tavole dei logaritmi naturali, 200 cifre decimali di π e poi, incoraggiato da Gauss, i numeri primi fino a 8 milioni.

Sappiamo pochissimo sugli F_n , perché sono subito enormi.

F_{36} ha circa $2 \cdot 10^{10}$ cifre: un nastro su cui fosse scritto (supponendo di scrivere 5 cifre in un centimetro) circonderebbe la terra (la circonferenza dell’equatore è di circa 40 000 km.)

Nessuno sa se vi siano altri primi di Fermat (oltre F_0, F_1, F_2, F_3, F_4). È un vero peccato.

Si sa che da F_5 a F_{32} sono tutti composti (da F_5 a F_{11} sono stati completamente fattorizzati, ma non si conosce nessun fattore primo di F_{14} , di F_{20} , di F_{22} né di F_{24}).

Di molti numeri di Fermat non si sa neppure se sono composti (ad

esempio, per F_{33}). Viceversa, di alcuni ‘mostri’ si conosce almeno un fattore (al novembre 2005 $F_{2478782}$ era il più grande numero di Fermat di cui si conosceva un fattore, cioè $3 \cdot 2^{2478785} + 1$).

I numeri primi di Fermat sono indissolubilmente legati al problema della divisione del cerchio in parti uguali, utilizzando solo riga e compasso. Questo problema venne affrontato per la prima volta da Euclide, che fornì le costruzioni del triangolo equilatero e del pentagono regolare. Fu Gauss a fare il passo avanti successivo, mostrando (a 19 anni) nelle sue *Disquisitiones* la costruzione del poligono regolare con 17 lati. Rimase tanto colpito da questa scoperta da chiedere di incidere sulla sua pietra tombale un poligono regolare di 17 lati (cosa che non fu eseguita...)

Dimostrò poi che è possibile costruire con riga e compasso un poligono regolare con un numero primo p di lati, se p è un primo di Fermat. La parte ‘solo se’ venne provata da Wantzel nel 1836. Questo è il risultato finale:

TEOREMA 2.7. – *È possibile costruire un poligono regolare con n lati se e solo se*

$$n = 2^k q_1 q_2 \dots q_s,$$

dove i q_j sono primi di Fermat non ripetuti. □

Il Criterio di Pépin permette di constatare la primalità di F_k in modo incredibilmente diretto:

CRITERIO 2.8. – **Criterio di Pépin** per i numeri di Fermat

$$F_k \text{ è primo se e solo se } 3^{\frac{F_k-1}{2}} \equiv -1 \pmod{F_k}$$

Da dove viene quel 3?

Se $3^{\frac{F_k-1}{2}} \equiv -1 \pmod{F_k}$ allora F_k è primo per 2.5.

Però, se F_k è primo, perché $3^{\frac{F_k-1}{2}}$ deve valere -1 modulo F_k ?

La risposta viene dal Criterio di Eulero e dalla Legge di Reciprocità Quadratica.

2.5. – Il Simbolo di Legendre e il Criterio di Solovay - Strassen.

Introduciamo i simboli di Legendre e di Jacobi, che ci saranno utili più volte nel seguito.

DEFINIZIONE 2.9. – Il **simbolo di Legendre** $\left(\frac{a}{p}\right)$ è definito solo se p è un numero primo dispari (a può essere un intero qualsiasi).

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ è un quadrato modulo } p \\ 0 & \text{se } p \text{ divide } a \\ -1 & \text{se } a \text{ non è un quadrato modulo } p \end{cases}$$

DEFINIZIONE 2.10. – Il **simbolo di Jacobi** $\left(\frac{a}{b}\right)$ è definito solo se b è un numero dispari (a può essere un intero qualsiasi).

Sia $b = p_1 p_2 \dots p_h$, dove i primi p_j possono essere ripetuti. Allora:

$$\left(\frac{a}{b}\right) := \prod_{j=1}^h \left(\frac{a}{p_j}\right)$$

Il Teorema seguente contiene le regole più utili per il calcolo del simbolo di Legendre.

TEOREMA 2.11

1. Criterio di Eulero

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \quad \text{se } p \text{ non divide } a$$

$$2. \quad \left(\frac{-1}{p}\right) = 1 \quad \text{se } p \equiv 1 \pmod{4}$$

$$\left(\frac{-1}{p}\right) = -1 \quad \text{se } p \equiv 3 \pmod{4}$$

$$3. \quad \left(\frac{2}{p}\right) = 1 \quad \text{se } p \equiv \pm 1 \pmod{8}$$

$$\left(\frac{2}{p}\right) = -1 \quad \text{se } p \equiv \pm 3 \pmod{8}$$

4. Legge di Reciprocità Quadratica

$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ se p e q sono due primi dispari entrambi congrui a 3 modulo 4

$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ in tutti gli altri casi. □

La famosa *Legge di Reciprocità Quadratica* fu dimostrata da Gauss nel 1796. Gauss considerava questo teorema uno dei più bei risultati della sua intera produzione, e ne diede otto dimostrazioni diverse. Ne esistono attualmente decine: in [11] ne sono riportate ben 196!

Il Criterio di Eulero non si estende al simbolo di Jacobi. Invece i punti 2, 3, 4 di 2.11 valgono anche per il simbolo di Jacobi, ove si sostituiscano a p e a q due interi dispari a e b . Non è difficile vedere che utilizzando successive ‘inversioni’ e riduzioni del ‘numeratore’ modulo il ‘denominatore’, si ottiene un algoritmo polinomiale per il calcolo del simbolo di Jacobi (e quindi del simbolo di Legendre).

Per dimostrare il Criterio di Pépin, il 2.8, ci serve questa proprietà immediata dei numeri di Fermat:

PROPRIETÀ 2.12. – Per $k > 0$, si ha

$F_k \equiv 5 \pmod{12}$, e quindi, in particolare, $F_k \equiv 1 \pmod{4}$ e $F_k \equiv 2 \pmod{3}$. □

Possiamo ora finalmente provare il Criterio di Pépin:

F_k è primo se e solo se $3^{\frac{F_k-1}{2}} \equiv -1 \pmod{F_k}$

DIMOSTRAZIONE DEL CRITERIO DI PÉPIN. – Ci manca solo una implicazione.

Supponiamo che F_k sia primo.

Per il Criterio di Eulero 2.11.1, $3^{\frac{F_k-1}{2}} \equiv \left(\frac{3}{F_k}\right)$. Da 2.12 e 2.11.4, $3^{\frac{F_k-1}{2}} \equiv \left(\frac{F_k}{3}\right)$.

Infine, poiché 2 non è un quadrato modulo 3, ovvero $\left(\frac{2}{3}\right) = -1$, da 2.12 si ottiene $3^{\frac{F_k-1}{2}} \equiv -1 \pmod{F_k}$. □

Abbiamo osservato che il Criterio di Eulero non si estende al simbolo di Jacobi.

Se n non è primo, possono esistere interi a , coprimi con n , tali che $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$.

Se n non è primo, esistono *sempre* questi interi *sinceri*, che dicono ‘ n non è primo’? La risposta è nel teorema seguente, che rivelerà tutta la sua importanza quando si parlerà dei *test* di primalità.

CRITERIO 2.13. – Criterio di Solovay-Strassen

n è primo se e solo se per ogni a coprimo con n si ha $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$. □

Nel paragrafo seguente vedremo due criteri di primalità analoghi a quello di Lucas 2.3 e di Pocklington 2.4. Essi si basano sulle successioni ricorrenti lineari.

3. – Numeri primi e successioni ricorrenti lineari.

Chiunque si sia accostato, anche solo per curiosità, alla teoria dei numeri, avrà incontrato, almeno una volta, la successione

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \dots$$

dei **numeri di Fibonacci**.

Leonardo Pisano, detto Fibonacci (1170-1250), introdusse questa successione come modello di crescita di una popolazione di conigli, soggetta a queste regole:

1. Ogni coppia è o matura o immatura.
2. Dopo un mese una coppia immatura diventa matura.
3. Ogni coppia matura produce ogni mese una coppia immatura.
4. Per tutta la durata della simulazione, nessuna coppia muore.

Diciamo F_n il numero di coppie presenti al mese n -esimo dall’inizio della simulazione. (Utilizziamo, come è consuetudine, la stessa nota-

zione per l' n -esimo numero di Fibonacci e di Fermat: il contesto chiarisce a quale classe di numeri stiamo riferendoci).

Diamo le condizioni iniziali, supponendo che al primo mese ci sia una coppia immatura:

$$\begin{cases} F_0 = 0 \\ F_1 = 1 \end{cases}$$

La generazione $\mathcal{G}_n$ all' n -esimo mese (di cardinalità F_n) è formata da due parti: la generazione precedente $\mathcal{G}_{n-1}$ più una parte $\mathcal{N}$ di coppie nuove; queste ultime vengono dalla parte matura di $\mathcal{G}_{n-1}$, che ha cardinalità F_{n-2} . Dunque:

$$F_n = F_{n-1} + F_{n-2}.$$

Osserviamo che questo modello dà luogo ad una **crescita esponenziale**; si prova infatti che

$$F_n = \left[\frac{a^n}{\sqrt{5}} \right]$$

dove a è la **sezione aurea**

$$a = \frac{1 + \sqrt{5}}{2}.$$

I numeri di Fibonacci appaiono in moltissime applicazioni della matematica, dalla fillotassi alle oscillazioni dei mercati finanziari.

Molto importante per le sue proprietà di divisibilità è anche la sequenza (che utilizzeremo tra breve)

$$2, 1, 3, 4, 7, 11, 18, \dots$$

detta successione dei **numeri di Lucas**:

$$\begin{cases} L_0 = 2 \\ L_1 = 1 \\ L_n = L_{n-1} + L_{n-2} \end{cases}$$

Consideriamo ora, più in generale le *successioni ricorrenti lineari di ordine 2* (che abbrevieremo con *srl*).

DEFINIZIONE 3.1. – Una successione $A = (a_n)$ di elementi di un anello commutativo R si dice **successione ricorrente lineare di ordine 2** se esistono $h, k \in R$ tali che, per ogni $n \geq 2$ si abbia

$$a_n = ha_{n-1} - ka_{n-2}.$$

Si dice **polinomio caratteristico** di A il polinomio $f(x) = x^2 - hx + k \in R[x]$.

Fissati $h, k \in R$, vi sono infinite srl con lo stesso polinomio caratteristico $f(x) = x^2 - hx + k$, al variare dei valori iniziali a_0 e a_1 .

Denotiamo la srl (a_n) di polinomio caratteristico $f(x) = x^2 - hx + k$ e valori iniziali a_0, a_1 , con

$$a_n = W_n(a_0, a_1, h, k).$$

Nel seguito supporremo che R sia un dominio di integrità e che $\mathbb{K} \supseteq R$ sia un campo contenente le radici di $f(x)$.

DEFINIZIONE 3.2. – Diciamo **successioni di Fibonacci generalizzate** le sequenze del tipo

$$U_n(h, k) = W_n(0, 1, h, k), \quad h, k \in R.$$

Diciamo **successioni di Lucas generalizzate** le sequenze del tipo

$$V_n(h, k) = W_n(2, h, h, k), \quad h, k \in R.$$

Riscrivendo con questa notazione i numeri di Fibonacci e di Lucas, abbiamo:

$$F_n = U_n(1, -1)$$

$$L_n = V_n(1, -1).$$

Fissati $h, k \in \mathbb{K}$, consideriamo l'insieme di tutte le srl di polinomio caratteristico $f(x) = x^2 - hx + k$:

$$\mathcal{S}(f(x)) := \{(W_n(a, b, h, k)) : a, b \in \mathbb{K}\}.$$

$\mathcal{S}(f(x))$ è un $\mathbb{K}$ -spazio vettoriale di dimensione 2. Una sua base è data dalla coppia di successioni

$$\{(T_n(h, k)), (U_n(h, k))\}$$

dove $T_n(h, k) = W_n(1, 0, h, k)$ e $U_n(h, k) = W_n(0, 1, h, k)$ (U_n è la successione di Fibonacci generalizzata).

Infatti T_n e U_n sono linearmente indipendenti e, qualunque sia $W_n(a, b, h, k) \in \mathcal{S}(f(x))$, si ha $W_n = aT_n + bU_n$.

C'è un'altra base molto importante di $\mathcal{S}(f(x))$.

Poniamo $\Delta = h^2 - 4k$, e supponiamo $\Delta \neq 0$ e $k \neq 0$, in modo che $f(x)$ abbia radici α, β in $\mathbb{K}$ distinte e non nulle. Allora:

PROPRIETÀ 3.3. – Se α, β , sono le radici di $f(x)$, allora:

- (i) $\alpha^n = W_n(1, \alpha, h, k)$ e $\beta^n = W_n(1, \beta, h, k)$
- (ii) le successioni (α^n) e (β^n) formano una base di $\mathcal{S}(f(x))$.

DIMOSTRAZIONE. – Poiché α è radice di $f(x)$, si ha $\alpha^2 = h\alpha - k$ e dunque $\alpha^n = h\alpha^{n-1} - k\alpha^{n-2}$, che è la relazione di ricorrenza. Inoltre $\alpha^0 = 1$ e $\alpha^1 = \alpha$ sono le condizioni iniziali. Dunque $\alpha^n = W_n(1, \alpha, h, k)$ e $(\alpha^n) \in \mathcal{S}(f(x))$.

Analogamente per (β^n) .

Le successioni (α^n) e (β^n) sono linearmente indipendenti perché

$$\begin{vmatrix} 1 & 1 \\ \alpha & \beta \end{vmatrix} = \beta - \alpha \neq 0. \quad \square$$

COROLLARIO 3.4

(i) Per ogni successione $W_n(a_0, a_1, h, k) \in \mathcal{S}(f(x))$, esistono e sono unici $A, B \in \mathbb{K}$ tali che $W_n(a, b, h, k) = A\alpha^n + B\beta^n$.

(ii) Per le successioni di Fibonacci e di Lucas generalizzate, si ha:

$$U_n(h, k) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad \forall n \in \mathbb{N}$$

$$V_n(h, k) = \alpha^n + \beta^n, \quad \forall n \in \mathbb{N}.$$

DIMOSTRAZIONE. – (i) Poiché (α^n) e (β^n) formano una base di $\mathcal{S}(f(x))$, esistono e sono unici $A, B \in \mathbb{K}$ tali che $W_n(a, b, h, k) = A\alpha^n + B\beta^n$ e

dunque in particolare:

$$\begin{cases} a_0 = A + B \\ a_1 = Aa + B\beta \end{cases}$$

da cui si ricavano

$$\begin{cases} A = \frac{a_1 - a_0\beta}{a - \beta} \\ B = \frac{a_0a - a_1}{a - \beta} \end{cases}$$

(ii) Seguono subito ponendo $(a_0, a_1) = (0, 1)$ e $(a_0, a_1) = (2, h)$ e tenendo presente che $h = a + \beta$. $\square$

Per capire il legame tra le *srl* e i numeri primi, occorrono ancora alcune considerazioni algebriche.

Siano p un primo tale che $p \nmid 2k\Delta$ e sia $R = \mathbb{Z}_p$. Sia $\mathbb{K}$ il campo di spezzamento di $f(x)$ su $\mathbb{Z}_p$, cioè la più piccola estensione di $\mathbb{Z}_p$ contenente le radici di $f(x)$.

Si devono distinguere due casi:

(I) $\left(\frac{\Delta}{p}\right) = 1$: dunque $a, \beta \in \mathbb{Z}_p$ e $\mathbb{K} = \mathbb{Z}_p$.

(II) $\left(\frac{\Delta}{p}\right) = -1$: in questo caso $a, \beta \notin \mathbb{Z}_p$ e $\mathbb{K} = \mathbb{Z}_p(a) = GF(p^2)$, il campo finito che contiene p^2 elementi.

In entrambi i casi $\mathbb{K}$ ha caratteristica p ed è definito il **morfismo di Frobenius**:

$$\begin{cases} \Phi : \mathbb{K} \rightarrow \mathbb{K} \\ \Phi : a \mapsto a^p \end{cases}$$

Si osservi che Φ è un morfismo additivo perché vale una interessante proprietà che collega i numeri primi con i coefficienti binomiali, e precisamente

3.5

$$n \text{ è primo} \Leftrightarrow n \text{ divide } \binom{n}{h}, \quad \forall h, 1 \leq h \leq p-1.$$

Stabiliamo ora due lemmi per trarre una utile proprietà del morfismo di Frobenius.

LEMMA 3.6

$$\forall a \in \mathbb{K}, \quad \Phi(a) = a \Leftrightarrow a \in \mathbb{Z}_p$$

DIMOSTRAZIONE. – Segue dal Piccolo Teorema di Fermat 4.3 e dalla proprietà che in un campo l'equazione $x^p = x$ ha al più p soluzioni. $\square$

LEMMA 3.7

$$\forall a \in \mathbb{K}, \forall g(x) \in \mathbb{Z}_p[x], \quad g(a) = 0 \Rightarrow g(\Phi(a)) = 0. \quad \square$$

Dai due lemmi segue che

PROPRIETÀ 3.8. – *Il morfismo di Frobenius permuta gli zeri di ogni polinomio a coefficienti in $\mathbb{Z}_p$, lasciando fissi solo quelli che stanno in $\mathbb{Z}_p$.* $\square$

Pertanto

$$\begin{array}{ll} \text{nel caso (I):} & \Phi(a) = a, \quad \Phi(\beta) = \beta \\ \text{nel caso (II):} & \Phi(a) = \beta, \quad \Phi(\beta) = a. \end{array}$$

Torniamo ora alle successioni di Fibonacci e Lucas generalizzate, per stabilirne i legami con la primalità. Fissati $h, k \in \mathbb{K}$, scriveremo U_n e V_n in luogo di $U_n(h, k)$ e $V_n(h, k)$.

TEOREMA 3.9. – **Proprietà di divisibilità**

Sia p un primo tale che $p \nmid 2k\Delta$. Allora:

- (a) $p \mid U_{p - \left(\frac{\Delta}{p}\right)}$
- (b) $p \mid U_p - \left(\frac{\Delta}{p}\right)$

(c) $p|V_p - h$

(d) $p|F_{p-\left(\frac{p}{5}\right)}$

(e) $p|F_p - \left(\frac{p}{5}\right)$

DIMOSTRAZIONE. – Facendo i calcoli modulo p :

(a) nel caso (I): $U_{p-\left(\frac{\Delta}{p}\right)} = U_{p-1} = \frac{\alpha^{p-1} - \beta^{p-1}}{\alpha - \beta} = \frac{1 - 1}{\alpha - \beta} = 0.$

nel caso (II): $U_{p-\left(\frac{\Delta}{p}\right)} = U_{p+1} = \frac{\alpha^{p+1} - \beta^{p+1}}{\alpha - \beta} = \frac{\beta\alpha - \alpha\beta}{\alpha - \beta} = 0$

(b) nel caso (I): $U_p = \frac{\alpha^p - \beta^p}{\alpha - \beta} = \frac{\alpha - \beta}{\alpha - \beta} = 1 = \left(\frac{\Delta}{p}\right)$

nel caso (II): $U_p = \frac{\alpha^p - \beta^p}{\alpha - \beta} = \frac{\beta - \alpha}{\alpha - \beta} = -1 = \left(\frac{\Delta}{p}\right).$

(c) nel caso (I): $V_p = \alpha^p + \beta^p = \alpha + \beta = h$

nel caso (II): $V_p = \alpha^p + \beta^p = \beta + \alpha = h.$

(d) Se $p = 5$ il risultato segue dal fatto che $\left(\frac{5}{5}\right) = 0$ e $F_5 = 5$. Se $p \neq 5$, si deve provare che $p|F_{p-1}$ se $p \equiv \pm 1 \pmod{5}$, e che $p|F_{p+1}$ se $p \equiv \pm 2 \pmod{5}$. Ciò segue immediatamente da (a), tenendo presente che $\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right).$

(e) Segue immediatamente da (b), allo stesso modo che (d). $\square$

Osserviamo che esistono algoritmi polinomiali molto efficaci per il calcolo dei termini $W_n(a, b, h, k)$ con indici n elevati.

Dalle proprietà di divisibilità delle successioni generalizzate di Fibonacci si ricava un notevole criterio di primalità (si veda [7]):

TEOREMA 3.10. – Criterio $n + 1$

Un numero $n \in \mathbb{N}$ è primo se e solo se per ogni divisore primo q di $n + 1$ esiste una srl $U_n = U_n(h, k)$ tale che

1. $\left(\frac{\Delta}{n}\right) = -1$
2. $U_{n+1} \equiv 0 \pmod{n}$
3. $U_{\frac{n+1}{q}} \not\equiv 0 \pmod{n}$ □

Il teorema 3.10 è l'analogo del Criterio di Lucas 2.3, nel quale si richiede invece la fattorizzazione di $n - 1$.

Sussiste inoltre un criterio analogo a quello di Pocklington, dove si suppone questa volta di conoscere una fattorizzazione parziale di $n + 1$.

TEOREMA 3.11. – Criterio di Morrison

Sia dato $n \in \mathbb{N}$ tale che $n + 1 = rs$, dove $(r, s) = 1$, $r = \prod_{i=1}^m q_i^{v_i}$ e $r > \sqrt{n} + 1$.

Se per ogni primo q che divide r esiste una srl $U_n = U_n(h, k)$ tale che

1. $\left(\frac{\Delta}{n}\right) = -1$
2. $n | U_{n+1}$
3. $(U_{\frac{n+1}{q}}, n) = 1$

allora n è primo.

Il teorema 3.10 è particolarmente efficace per provare la primalità di numeri della forma $2^n - 1$, i famosi *numeri di Mersenne*.

3.1. – I numeri di Mersenne e il Criterio di Lucas-Lehmer.

L'abate Mersenne (1588-1648) era affascinato da questi numeri, tra i quali si trovano i più grandi primi noti.

DEFINIZIONE 3.12. – Si dice **numero di Mersenne** un intero del tipo

$$M_n = 2^n - 1$$

dove $n \in \mathbb{N}$.

Se M_n è primo, si dice **primo di Mersenne**.

Scriviamo i primi sette numeri di Mersenne

$$M_1 = 1, M_2 = 3, M_3 = 7, M_4 = 15, M_5 = 31, M_6 = 63, M_7 = 127.$$

M_2, M_3, M_5, M_7 sono primi, M_1, M_4, M_6 non lo sono. Si osservi che gli indici che corrispondono a numeri primi sono anch'essi primi. In effetti si può facilmente dimostrare il seguente

TEOREMA 3.13. – Teorema di Cataldi-Fermat

Se M_n è primo, allora n è primo. □

Purtroppo, l'inverso del teorema precedente non vale: ad esempio 11 è primo, ma $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$.

I numeri di Mersenne sono collegati con uno straordinario fenomeno dei numeri naturali:

DEFINIZIONE 3.14. – *Si dice che il numero naturale P_n è un **numero perfetto** se è uguale alla somma dei suoi divisori (compreso 1 ed escluso P_n).*

Dunque essi sono l'anello di congiunzione tra la struttura moltiplicativa e quella additiva di $\mathbb{N}$.

Elenchiamone alcuni:

$$P_1 = 6, P_2 = 28, P_3 = 496, P_4 = 8.128, \dots$$

La storia dei numeri perfetti è molto interessante.

I greci ne conoscevano solo quattro, P_1, P_2, P_3, P_4 , e davano un'enorme importanza a questi numeri, dal punto di vista matematico, ma anche filosofico e metafisico.

Nel Medio Evo, sei erano i numeri perfetti noti, ed erano messi in relazione con la creazione del mondo, che anch'essa aveva richiesto sei giorni.

Più tardi fu congetturato che:

1. tra due potenze di dieci, ci doveva essere sempre un numero perfetto (e dunque, l' n -esimo numero perfetto doveva avere n cifre).
2. i numeri perfetti dovevano alternarsi con cifre finali 6 e 8.

Entrambe le congetture sono false. Non c'è nessun numero perfetto di 5 cifre: il quinto è

$$P_5 = 2^{12}(2^{13} - 1) = 33550336$$

e termina con 6, ma P_6 termina di nuovo con 6 (e non con 8).

Mersenne conosceva solo 8 numeri perfetti ($P_1, \dots, P_8$) e scriveva, nel 1644:

‘Dal fatto che i numeri perfetti siano così rari, vediamo chiaramente come sia giusto paragonare i numeri perfetti con gli uomini perfetti’.

Riscriviamo i primi quattro numeri perfetti, mettendoli in relazione con i numeri di Mersenne:

$$P_1 = 6 = 1 + 2 + 3 = 2 \cdot 3 = 2^1 \cdot M_2$$

$$P_2 = 28 = 1 + 2 + 4 + 7 + 14 = 2^2 \cdot 7 = 2^2 \cdot M_3$$

$$P_3 = 496 = \dots = 2^4 \cdot 31 = 2^4 \cdot M_5$$

$$P_4 = 8.128 = \dots = 2^6 \cdot 127 = 2^6 \cdot M_7.$$

Sembra che siano tutti del tipo $2^{p-1} \cdot M_p$ (con p primo). Ma non tutti i numeri $2^{p-1} \cdot M_p$ sono perfetti: ad esempio $2^{10} \cdot M_{11}$ non è perfetto.

Questo succede perché M_{11} non è primo.

Infatti vale il seguente teorema (già noto ad Euclide):

TEOREMA 3.15. – *Se M_p è primo, allora $2^{p-1} \cdot M_p$ è perfetto.* □

Dunque, ogni primo di Mersenne dà origine ad un numero perfetto (pari).

Ma vale anche il viceversa, infatti:

TEOREMA 3.16 (di Eulero)

Se N è un numero perfetto pari, allora esiste un primo $p \in \mathcal{P}$ tale che $N = 2^{p-1} \cdot M_p$, dove M_p è un primo di Mersenne. □

Concludendo:

Esiste una corrispondenza biunivoca tra i numeri perfetti pari e i primi di Mersenne.

Sui numeri perfetti ci sono molte questioni aperte. Ne citiamo alcune, e alcuni risultati parziali ottenuti.

1. Non si sa se esistano infiniti numeri perfetti pari.
2. Non si sa se ci siano numeri perfetti dispari. Si sa che, se esiste un perfetto dispari, allora:

- deve essere della forma $p^{4m+1} \cdot q^2$, dove p è un primo del tipo $4k + 1$ (Eulero)
- deve essere maggiore di 10^{300} (Brent et al., 1991)
- deve avere almeno 75 diversi fattori primi (Hare, 2005)
- deve avere un fattore primo maggiore di 10^8 (Goto e Ohno, 2006)

Data la corrispondenza biunivoca scritta sopra, la conoscenza dei numeri perfetti pari dipende da quella dei primi di Mersenne.

Sono noti attualmente 43 primi di Mersenne, ai quali corrispondono 43 numeri perfetti. In quasi 2500 anni, dai tempi di Euclide, questi sono i soli numeri perfetti trovati!

L'ultimo primo di Mersenne è stato scoperto il 15 Dicembre 2005 da Curtis Cooper e Steven Boone: $2^{30.402.457} - 1$ è il più grande numero primo noto, con ben 9.152.052 cifre! Siamo a un passo dalla soglia dei 10 milioni di cifre, per la quale la Electronic Frontier Foundation offre 100.000 dollari. Il premio precedente — di 50.000 dollari — è stato assegnato nel 2000 a Nayan Hajratwala il quale trovò nel 1999 il 38-esimo primo di Mersenne (2.098.960 cifre).

Ad $M_{30.402.457}$ corrisponde il numero perfetto $P_{43} = 2^{30.402.456} (2^{30.402.457} - 1)$.

Curtis Cooper e Steven Boone sono docenti presso la Central Missouri State University (CMSU) e partecipano da anni alla **GIMPS** (Great Internet Mersenne Prime Search).

I due professori (e la CMSU) si sono ben meritato il record mondiale che hanno conquistato: coordinano il lavoro di ben 700 computers. Si tratta però di una impresa collettiva, che da soli non avrebbero potuto realizzare. In base a questa considerazione, la scoperta sarà attribuita a 'Cooper, Boone, Woltman, Kurowski, et al'. Gli altri sono le decine di migliaia di volontari che partecipano alla GIMPS.

GIMPS è un progetto gestito da PrimeNet, un sistema di calcolo

parallelo distribuito in rete a livello mondiale, creato nel 1997 da Scott Kurowski, basato sulla medesima tecnologia di Entropia, impresa fondata da Kurowski stesso.

Nel momento in cui scriviamo il server di PrimeNet connette 71218 computers, che eseguono qualcosa come 19162 gigaflops al secondo, con una potenza di calcolo pari a quella di 342 supercomputer Cray T932.

Chiunque può unirsi alla ricerca, è sufficiente scaricare il software necessario, ovviamente gratuito. Il bello è che l'utente non si accorge nemmeno di averlo, perché funziona solo quando la CPU non è impegnata a fare altro.

La parte più interessante del software è di George Woltman, che ha implementato in linguaggio macchina un sofisticato algoritmo di Richard Crandall, che consente di eseguire velocemente i quadrati necessari per dimostrare la primalità dei numeri di Mersenne. Si tratta di moltiplicare numeri di milioni di cifre. L'algoritmo è descritto — tra mille altri affascinanti risultati — nel bellissimo libro [8] che Crandall ha scritto con Carl Pomerance.

Per stabilire la primalità dei numeri di Mersenne si utilizza una variante di 3.10, il Criterio di Lucas-Lehmer:

CRITERIO 3.17. – Criterio di Lucas-Lehmer

M_n è primo se e solo se divide $V_m(4, 1)$, con $m = 2^{n-2}$. □

Questi sono i V_k iniziali, $0 \leq k \leq 10$:

2, 4, 14, 52, 194, 724, 2702, 10084, 37634, 140452, 524174.

I calcoli possono essere sveltiti utilizzando la successione S_k , così definita:

$$\begin{cases} S_1 = 4 \\ S_k = S_{k-1}^2 - 2, \quad \forall k > 1. \end{cases}$$

Questi sono i primi quattro S_k :

4, 14, 194, 37634.

È facile dimostrare che, per ogni k maggiore di 0 si ha:

$$S_k = V_{2^{k-1}}(4, 1)$$

Pertanto da 3.17 si ottiene come corollario:

TEOREMA 3.18. – Criterio di Lucas-Lehmer (*seconda forma*)
 M_n è primo se e solo se divide S_{n-1} . □

È in questa forma che il Criterio viene effettivamente utilizzato.

Naturalmente, ogni volta che si esegue un quadrato lo si riduce modulo M_n . In questo modo si lavora sempre con interi minori di M_n .

Vediamo i casi di $M_{19} = 524287$ e di $M_{23} = 8388607$.

Quella che segue è la sequenza $S_1, S_2, \dots, S_{22}$ modulo M_{19} :

{4, 14, 194, 37634, 218767, 510066, 386344, 323156, 218526, 504140, 103469, 417706, 307417, 382989, 275842, 85226, 523263, 0, 524285, 2, 2, 2}.

C'è 0 al posto 18, pertanto M_{19} è primo.

Questa è la stessa sequenza modulo M_{23} :

{4, 14, 194, 37634, 7031978, 7033660, 1176429, 7643358, 3179743, 2694768, 763525, 4182158, 7004001, 1531454, 5888805, 1140622, 4321431, 7041324, 2756392, 1280050, 6563009, 6107895}.

L'elemento di posto 22 non è 0, quindi M_{23} non è primo.

4. – Test di primalità.

Ogni condizione *necessaria ma non sufficiente* può servire per definire un *test di primalità*. Questa condizione deve essere verificabile in tempo polinomiale, altrimenti meglio sarebbe ricorrere ai *criteri di primalità*, dei quali si è parlato nei paragrafi precedenti.

Per mettere su un test di primalità sono necessari due ingredienti:

4.1

1. Una proprietà P , definita su $\mathbb{N}$, che è vera se n è primo.
2. Un algoritmo polinomiale A , il quale, ricevuto n in input, in tempo $O(\log^k n)$ (con k indipendente da n), risponde alla domanda: 'P(n) è vera?'

Ecco come viene usato un test di primalità:

DEFINIZIONE 4.2. – Funzionamento di un Test di Primalità

*Dati P e A come in 4.1, e assegnato n in input, se $A(n)$ è 'no' allora n è dichiarato **certamente composto**.*

*Se invece $A(n)$ è 'sì', allora n è dichiarato **probabilmente primo**.*

*Un intero composto che risulti probabilmente primo si dice **pseudoprimo**.*

Naturalmente un test di primalità risulterà tanto più interessante quanto più rari sono gli pseudoprimi. Inoltre appare evidente l'importanza di saper valutare, per un dato test, la probabilità che ha un numero composto di fingere di essere primo, di passare cioè dalla parte dei primi.

Il prototipo di tutti i test è il Test di Fermat, che si basa sul Piccolo Teorema di Fermat (PTF):

TEOREMA 4.3. – Piccolo Teorema di Fermat

Se n è primo e $(n, a) = 1$, allora $a^{n-1} \equiv 1 \pmod{n}$. □

DEFINIZIONE 4.4. – Un intero n composto si dice pseudoprimo di Fermat sulla base a se

$$a^{n-1} \equiv 1 \pmod{n}.$$

Possiamo pensare al test di Fermat come ad una grande festa cui tutti ambiscono partecipare. Solo alcuni però, i primi, hanno il diritto di entrare. A guardia del palazzo sono posti tutti i numeri positivi. Quando arriva il signor n viene circondato dagli a che sono minori di lui e non hanno con lui divisori in comune. Si tratta di $\varphi(n)$ individui mascherati, detti testimoni. n si rivolge a uno di loro (a caso) e chiede: «Riconosci che io sono primo?». Se n è davvero primo, chiunque sia l'interpellato risponderà sempre, sinceramente, 'sì', e n passerà. Se invece n non è primo la cosa si complica, perché alcuni testimoni (forse prezzolati..) *mentono*. Allora n ha una probabilità di partecipare alla festa dei primi, senza esserlo,

pari a:

$$\frac{\text{numero dei falsi testimoni}}{\varphi(n)}$$

Il più piccolo pseudoprimo di Fermat sulla base 2 è $341 = 11 \times 31$. Questo significa che 2 è disposto a testimoniare falsamente che 341 è primo. In realtà 341 è un tipo molto abile, ci sono ben 100 basi bugiarde sul totale di $\varphi(341) = 300$ basi! 341 ha probabilità $\frac{1}{3}$ di passare indisturbato.

Invece $111 = 3 \times 37$ ha solo 4 basi favorevoli: 1, 38, 73, 110 (si noti che 1 e $n - 1$ sono screditati: 1 è disposto a testimoniare per qualsiasi numero, mentre $n - 1$ farebbe passare tutti i dispari...). Pertanto la probabilità di 111 di passare è appena $\frac{1}{18}$, in quanto $\varphi(111) = 72$.

Sembra incredibile ma esistono individui che — al pari dei primi — affrontano tranquilli le schiere dei testimoni, perché sanno che sono tutti dalla loro parte. Mentre per i primi *tutti* i testimoni affermano il vero, in questo caso tutti mentono.

Questi numeri, che sono pseudoprimi su *ogni* base, devono soddisfare la seguente condizione:

4.5 C1

Per ogni a coprimo con n , $a^{n-1} \equiv 1 \pmod{n}$

L'esistenza di numeri soddisfacenti **C1** fu congetturata nel 1899 da Korselt, il quale li caratterizzò mediante questa proprietà:

4.6 C2

*Un intero n verifica **C1** se e solo se*

1. *n è prodotto di primi distinti: $n = p_1 p_2 \dots p_k$*
2. *Per ogni primo p_i che divide n si ha che $p_i - 1$ divide $n - 1$*

Dunque **C1** è equivalente a **C2**. Questo non ci rende probabilmente più fiduciosi riguardo alla esistenza di siffatte creature. Appare molto strano che se capita che n sia divisibile, diciamo, per 31, allora $n - 1$ debba per forza essere divisibile per 30, e così via per tutti i primi che dividono n .

Korselt non trovò alcun esempio e lasciò impregiudicata la questione della loro esistenza. Probabilmente, visto che il primo esemplare è veramente piccolo, non si impegnò molto nella ricerca. Nel 1910 Robert D. Carmichael scoprì che 561 appartiene alla privilegiata schiera dei numeri che, da allora, vengono chiamati **numeri di Carmichael**. Infatti:

1. $561 = 3 \times 11 \times 17$
- 2 2, 10 e 16 dividono 560.

Carmichael trovò i primi 15 numeri che portano il suo nome:

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973.

Preso da irrefrenabile entusiasmo congetturò che:

4.7. – Congettura di Carmichael.

Esistono infiniti numeri di Carmichael.

Questa congettura rimase aperta per più di ottanta anni, e venne finalmente provata vera da Alford, Granville e Pomerance nel 1994 [4].

Un test di primalità è essenzialmente un filtro. Esistono test più forti, ovvero filtri più fini, del test di Fermat? Come si è detto all'inizio del paragrafo ogni condizione necessaria alla primalità può servire come test. E se provassimo con il criterio di Eulero (2.11.1)?

DEFINIZIONE 4.8

*Un intero n composto si dice **pseudoprimo di Eulero sulla base a** se:*

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

È immediato constatare, elevando al quadrato entrambi i membri della precedente espressione, che

TEOREMA 4.9. – *Se n è pseudoprimo di Eulero sulla base a allora n è pseudoprimo di Fermat sulla stessa base.* □

Il Criterio di Solovay-Strassen 2.13 assicura che per gli pseudoprimi di Eulero non esiste un analogo dei numeri di Carmichael. Gli unici che passano con certezza lo sbarramento dei testimoni sono i primi. Per ogni altro intero esistono basi che possono smascherarlo.

Il numero 341 ha, come abbiamo visto, 100 testimoni di Fermat favorevoli, ma solo 50 di Eulero. L'imprendibile, per Fermat, 561 ora ha soltanto 160 testimoni dalla sua parte nel test di Eulero. È la metà esatta della totalità dei testimoni, in quanto $320 = \varphi(561)$.

A questo punto c'è una osservazione estremamente interessante da fare: se n è composto non potrà mai avere più della metà dei testimoni di Eulero a favore! Vediamo da vicino questo risultato affascinante, la cui dimostrazione — puramente algebrica — è semplice ed elegante al tempo stesso.

TEOREMA 4.10. – Teorema di Solovay-Strassen

Se n è composto, $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ per al più $\frac{\varphi(n)}{2}$ basi a .

DIMOSTRAZIONE. – Poniamo $H = \left\{ a : a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n} \right\}$. Il simbolo di Jacobi $\left(\frac{a}{n}\right)$ è moltiplicativo, cioè $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right)$. Pertanto H è chiuso rispetto al prodotto ed è un sottogruppo di $\mathbb{Z}_n^*$. Poiché n è composto, per 2.13, H è contenuto strettamente in $\mathbb{Z}_n^*$. Poiché H è un sottogruppo il suo ordine deve dividere l'ordine di $\mathbb{Z}_n^*$, che è $\varphi(n)$.

Pertanto il massimo ordine possibile di H è $\frac{\varphi(n)}{2}$. □

Otteniamo da questo un interessante *test probabilistico* ([20]):

4.11. – Montecarlo test di Solovay-Strassen.

Siano $a_1, a_2, \dots, a_k$ k basi scelte a caso in modo indipendente.

Il numero n viene testato su tutte le basi a_j .

Se per una di queste si ha $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ allora n è certamente composto.

Altrimenti n è primo con probabilità non minore di $1 - \frac{1}{2^k}$.

Introduciamo ora un test molto efficace, proposto da Miller [13] e successivamente modificato da Rabin [17], [18]. Esso si basa sulla seguente condizione necessaria di primalità:

PROPRIETÀ 4.12. – Raffinamento del PTF

Se n è primo e $n - 1 = 2^s t$, con t dispari, allora $a^t \equiv 1 \pmod{n}$ oppure $a^{2^j t} \equiv -1 \pmod{n}$ per almeno un j , $0 \leq j \leq s - 1$.

DIMOSTRAZIONE. – Riscriviamo il piccolo teorema di Fermat 4.3 in una forma equivalente:

se n è un primo che non divide a , allora n divide $a^{n-1} - 1$.

Sia dato un intero n tale che $n - 1 = 2^s t$, con t dispari. Usando ripetutamente la identità $(a - b)(a + b) = a^2 - b^2$, si ottiene subito:

$$a^{n-1} - 1 = (a^t - 1)(a^t + 1)(a^{2t} + 1) \dots (a^{2^j t} + 1) \dots (a^{2^{s-1} t} + 1)$$

Segue che, se n è un primo che non divide a , allora n divide almeno uno dei fattori del prodotto a destra della uguaglianza. $\square$

DEFINIZIONE 4.13. – *Un intero n tale che $n - 1 = 2^s t$, con t dispari, si dice **pseudoprimo forte** sulla base a (coprime con n) se $a^t \equiv 1 \pmod{n}$ oppure $a^{2^j t} \equiv -1 \pmod{n}$ per almeno un j , $0 \leq j \leq s - 1$.*

*Equivalentemente diciamo che **n ha superato il test di Miller sulla base a .***

L'aggettivo *forte* si riferisce al seguente fatto:

TEOREMA 4.14. – *Se n è pseudoprimo forte sulla base a allora n è pseudoprimo di Eulero sulla stessa base.* $\square$

Ricordiamo che 341, lo pseudoprimo di Fermat sulla base 2, disponeva di 100 testimoni falsi di Fermat e 50 di Eulero. 341 risulta essere uno pseudoprimo forte ancora su 50 basi, quindi in questo caso non si è ottenuto un miglioramento.

Se consideriamo il numero di Carmichael 561, esso aveva 320 basi a

favore nel test di Fermat e 160 nel test di Eulero. Invece 561 è uno pseudoprimo forte per appena 10 basi!

Rabin ha dimostrato che il numero delle basi rispetto alle quali un intero composto n è uno pseudoprimo forte non supera mai un quarto del totale. Pertanto si ha un nuovo test probabilistico, più forte:

4.15. – Montecarlo test di Rabin-Miller

Siano $a_1 a_2, \dots, a_k$ k basi scelte a caso in modo indipendente.

Il numero n viene testato su tutte le basi a_j .

Se per una di queste n non supera il test di Miller allora n è certamente composto. Altrimenti n è primo con probabilità non minore di $1 - \frac{1}{4^k}$.

Le condizioni del teorema 3.9, verificate da ogni primo p , danno luogo ad altri test di primalità. Enunceremo tra questi il **test di Lucas** e il **test di Fibonacci**.

DEFINIZIONE 4.16. – *Si dice **pseudoprimo di Lucas** un intero composto n tale che $n | U_{n - \left(\frac{\Delta}{n}\right)}$. Si dice **pseudoprimo forte di Fibonacci** un intero composto n tale che $n | F_{n - \left(\frac{5}{n}\right)}$ e $n | F_n - \left(\frac{n}{5}\right)$.*

L'interesse dei test di primalità fondati sulle *srl* risiede nel fatto che essi risultano, sperimentalmente, complementari al test di Miller 4.13.

Si tratta di una questione molto concreta: su Maple, Mathematica e altri sistemi di calcolo algebrico-simbolico è implementato un test veloce di primalità ([21]). Esso è basato su varianti di un famoso test dovuto a Baillie e Wagstaff [5], e cioè:

4.17. – Test di Baillie e Wagstaff

Sia n il numero da testare. Si scelgano Δ , h , k in modo che

- Δ sia il minimo intero della forma $5 + 4k$ tale che $\left(\frac{\Delta}{n}\right) = -1$
- h sia il minimo dispari maggiore di $\sqrt{\Delta}$
- $k = \frac{h^2 - \Delta}{4}$.

Se $n|U_{n+1}(h, k)$ e passa il test di Miller sulla base 2, allora n è dichiarato primo.

Alcuni congetturano che questo sia un effettivo criterio di primalità: non si conoscono controesempi.

Per ulteriori approfondimenti, si veda [14].

5. – Criteri che dipendono dalla Congettura Estesa di Riemann.

La Congettura Estesa di Riemann (ERH) consiste in realtà di infinite ipotesi distinte.

Per formulare la ERH ci servono i concetti di *carattere modulare* e di *L-funzione di Dirichlet*.

DEFINIZIONE 5.1. – Diciamo che una funzione χ di dominio $\mathbb{N}$ e codominio $\mathbb{C}$ è un carattere modulo n se:

1. χ ha periodo n , ovvero $\chi(x) = \chi(x + n)$
2. $\chi(x) = 0$ per ogni x non coprimo con n
3. $\chi(xy) = \chi(x)\chi(y)$ se x e y sono coprimi con n .

DEFINIZIONE 5.2. – Diciamo **funzioni L di Dirichlet** le funzioni:

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

dove χ è un carattere modulo n .

Possiamo ora enunciare la ERH:

Congettura Estesa di Riemann (ERH)

Per ogni carattere χ modulo n , gli zeri complessi della funzione $L(\chi, s)$ hanno parte reale $\frac{1}{2}$.

La ERH implica la classica Congettura di Riemann, considerata uno dei problemi aperti più importanti della intera matematica.

Congettura di Riemann (RH)

Gli zeri complessi della funzione zeta di Riemann $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ hanno parte reale $\frac{1}{2}$.

La ERH ha conseguenze del tutto inaspettate, come il Teorema di Ankeny e Bach.

Ricordiamo che Z_n^* è il gruppo moltiplicativo formato dalle classi coprime con n .

TEOREMA 5.3. – (di Ankeny-Bach)

Supponiamo valida la ERH. Se H è un sottogruppo proprio di Z_n^* , esiste un intero positivo minore di $2 \log^2 n$ che non appartiene ad H .

□

Ad esempio, questo teorema assicura che (sempre supponendo valida la ERH) esiste in Z_n^* un non quadrato minore di $2 \log^2 n$.

Concludiamo presentando due criteri di primalità *deterministici e polinomiali*. Essi però non sono *incondizionati*, poiché dipendono dalla ERH.

5.4. – Criterio deterministico e polinomiale di Solovay-Strassen

Assumiamo la ERH. n è primo se e solo se $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ per ogni intero positivo $a < 2 \log^2 n$.

DIMOSTRAZIONE. – Una parte è banale. Supponiamo n composto. Sappiamo da 2.13 che $H = \left\{ a : a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n} \right\}$, è un sottogruppo proprio di Z_n^* . Per il Teorema di Ankeny-Bach 5.3 esiste un a non appartenente ad H minore di $2 \log^2 n$. Pertanto n sarà certamente smascherato, testandolo su tutte le basi, prima di arrivare a $2 \log^2 n$.

□

Infine, ricordando 4.14, da 5.4 si ottiene subito:

5.5. – Criterio deterministico e polinomiale di Miller

Assumiamo la ERH. n è primo se e solo se n passa il Test di Miller su tutte le basi $a < 2 \log^2 n$.

□

6. – Conclusioni.

In questo articolo abbiamo trattato solo di alcuni algoritmi tra quelli esistenti che decidono se un numero è primo (deterministici o probabilistici, condizionati o incondizionati, polinomiali o non polinomiali).

Non ci è stato possibile anche solo accennare a tutti i metodi effettivamente utilizzati per provare la primalità di un intero.

Forse tra le lacune più grandi ci sono il famoso APR (acronimo dei nomi degli autori Adleman, Pomerance, Rumely [1]), il primo metodo deterministico che termina in tempo ‘quasi’ polinomiale $(\log n)^{c \log \log \log n}$, ECPP (Elliptic Curves Primality Proving) [9], un metodo Las Vegas che, se termina, dà la risposta giusta in tempo polinomiale, e soprattutto il rivoluzionario AKS [3], da Agrawal, Kayal e Saxena, i tre indiani che nel 2002 hanno aperto un passaggio storico, trovando il primo metodo deterministico polinomiale incondizionato. A ECPP e AKS dedicheremo un prossimo articolo sul Bollettino.

Vi sono poi altri recenti concetti di pseudoprimality (con relativi test).

Per avere un’idea più ampia della varietà delle tecniche utilizzate si veda ‘lo stato dell’arte’ nel 2004 in [6]: in esso vengono descritti 14 metodi incondizionati e 3 condizionati per provare che un numero è primo e 4 metodi per provare che è composto, insieme con i tempi per trovare e per verificare i certificati.

RIFERIMENTI BIBLIOGRAFICI

- [1] L. M. ADLEMAN - C. POMERANCE - R. S. RUMELY, *On distinguishing prime numbers from composite numbers*, *Annals of Mathematics*, **117** (1983), 173-206.
- [2] A. N. AGADZHANOV, *Unusual infinity of prime numbers*, URL: <http://citeseer.ifi.unizh.ch/agadzhanov01unusual.html>, 2001
- [3] M. AGRAWAL - N. KAYAL - N. SAXENA, *PRIMES is in P*, *Annals of Mathematics*, **160** (2004), 781-793.
- [4] W. R. ALFORD - A. GRANVILLE - C. POMERANCE, *There are infinitely many Carmichael numbers*, *Annals of Mathematics*, **139** (1994), 703-722.

- [5] R. BAILLIE - S. S. WAGSTAFF, Jr., *Lucas pseudoprimes*, Mathematics of Computation, **35** (1980), 1391-1417.
- [6] D. J. BERNSTEIN, *Distinguishing prime numbers from composite numbers: the state of the art in 2004*, URL: <http://cr.yp.to/papers.html#prime2004> (2004).
- [7] J. BRILLHART - D. H. LEHMER - J. L. SELFRIDGE, *New Primality Criteria and Factorizations for $2^m \pm 1$* , Mathematics of Computations, **29** (1975), 620-647.
- [8] R. CRANDALL - C. POMERANCE, *Prime Numbers: a computational perspective*, Springer-Verlag, 2002.
- [9] S. GOLDWASSER - J. KILIAN, *Primality Testing using Elliptic Curves*, Journal of the ACM, **46** (1999), 450-472.
- [10] A. LANGUASCO - A. ZACCAGNINI, *Introduzione alla Crittografia*, Hoepli Editore, Milano, 2004.
- [11] F. LEMMERMEYER, *Reciprocity Laws: From Euler to Eisenstein*, Springer, 2000.
- [12] E. LUCAS, *Sur la recherche des grands nombres premiers*, Association Française pour l'Avancement des Sciences, Comptes Rendus, **5** (1876), 61-68.
- [13] G. L. MILLER, *Riemann's Hypothesis and tests for Primality*, J. of Comp. Sys. Sci. **13** (1976), 300-317.
- [14] S. MÜLLER, *On the combined Fermat/Lucas probable prime test*, in Crypto & Coding '99, Lecture Notes in Computer Science 1746, Springer-Verlag 1999, 222-235.
- [15] H. C. POCKLINGTON, *Determination of the prime or composite nature of large numbers by Fermat's theorem*, Proceedings of the Cambridge Philosophical Society, **18** (1914), 29-30.
- [16] C. POMERANCE, *Primality testing: variations on a theme of Lucas*, in corso di pubblicazione su Proceedings of MSRI Workshop, J. Buhler and P. Stevenhagen, eds. 2005, URL: <http://cm.bell-labs.com/cm/ms/who/carlp/primalitytalk5.ps>
- [17] M. O. RABIN, *Probabilistic Algorithms*, in 'Algorithms and Complexity: new directions and recent results', J. F. Traub Edt., Academic Press, 1976, 21-39.
- [18] M. O. RABIN, *Probabilistic Algorithms for Testing Primality*, Journal of Number Theory, **12** (1980), 128-138.
- [19] P. RIBENBOIM, *The Book of Prime Numbers Records*, Springer-Verlag, 1988.
- [20] R. M. SOLOWAY - V. STRASSEN, *A fast Montecarlo test for primality*, SIAM Journal on Computing, **6** (1977), 84-85.
- [21] S. Y. YAN, *Primality testing of large numbers in Maple*, Computers & Mathematics with Applications, **12** (1995), 1-8.

Luisella Caire: Dipartimento di Matematica, Politecnico di Torino,
Corso Duca degli Abruzzi 24, 10129 Torino, Italy,
e-mail: luisella.caire@polito.it

Umberto Cerruti: Dipartimento di Matematica, Università di Torino,
Via Carlo Alberto 10, 10121 Torino, Italy,
e-mail: umberto.cerruti@unito.it