UNIVERSITÀ DEGLI STUDI DI TRENTO

DIPARTIMENTO DI MATEMATICA

Laurea Triennale in Matematica

Una retrospettiva su variazioni del test di Lucas

Candidato:
Leonardo Errati

Relatore:
Willem Adriaan de Graaf

Indice

Contenuti

Discuteremo su variazioni del test di primalità di Lucas partendo dall'indistricabile contesto storico in cui sono inevitabilmente immerse.

Nel primo capitolo introdurremo i concetti necessari: teoria dei numeri, teoria dei gruppi e cenni sulle sequenze di Lucas. Nel secondo capitolo studieremo il test di Lucas-Lehmer per i numeri di Mersenne. Nel terzo capitolo costruiremo il test di Bailie-PSW partendo dal test di Fermat e da quello di Lucas.

Nomenclature

Algebra

$\gcd(a, b)$	*greatest common divisor*, massimo comune divisore tra a e b
$\mathrm{mod}(n)$	congruenza in modulo n, i calcoli che precedono la dicitura sono da intendersi come svolti nelle classi di resto modulari
$a \mid b$	a divide b per a e b in $\mathbb{Z}$, ovvero b è un multiplo intero di a, ed analogamente $a \nmid b$ indica che è falso

Insiemi numerici

$\mathbb{N}$	l'insieme dei numeri naturali; come spiegheremo, includiamo lo zero
$\mathbb{Z}$	l'anello dei numeri interi

Altri simboli

F_n	$2^{2^n} - 1$, l'n-esimo numero di Fermat
M_n	$2^n - 1$, l'n-esimo numero di Mersenne; indica un esponente n qualunque, primo o composto
M_p	$2^p - 1$, il p-esimo numero di Mersenne con p primo; lo useremo per sottolineare la richiesta di primalità per p rispetto al caso generale
W_p	$\frac{2^p+1}{3}$, il p-esimo numero di Wagstaff ove p primo

Test di primalità

$\mathrm{fpsp}(a)$	Insieme dei primi probabili di Fermat sotto il parametro a, in letteratura "pseudoprimi"
$\mathrm{lpsp}(P, Q)$	Insieme dei primi probabili di Lucas sotto i parametri (P, Q), in letteratura a volte confusi con gli "pseudoprimi"
$\mathrm{sfpsp}(a)$	Insieme dei primi probabili del test forte di Fermat (vedasi Miller-Rabin) sotto il parametro a, in letteratura "pseudoprimi"
$\mathrm{slpsp}(P, Q)$	Insieme dei primi probabili del test forte di Lucas sotto i parametri (P, Q), in letteratura a volte "pseudoprimi"

Introduzione

L'algebra non è come un gelato

Capita spesso in matematica di avere un problema dalla formulazione estremamente facile ma dalla difficile risoluzione; anzi, a volte alcuni problemi possono sembrare irrisolvibili, o addirittura si dimostra che non sia possibile risolverli! Questa peculiarità rende la matematica estremamente diversa da un gelato, che prima o poi si scioglie; lei resta spesso salda, seppure non sempre.
La stessa idea si applica all'algebra, ed in particolare ai criteri di primalità: nulla è più semplice del chiedersi "*is p prime?*", tutt'altra cosa è rispondere. Ancora oggi, questo problema non si è "sciolto".

Il contenuto: Introdurremo molto brevemente il concetto di *numeri primi* per sottolineare l'importanza storica che hanno ricoperto e l'evoluzione nella loro ricerca. Subito dopo parleremo di aritmetica modulare e teoria dei gruppi, ma prima di entrare nel pieno dell'azione faremo bene a presentare le sequenze di Lucas - protagoniste della vicenda.
Finalmente potremo ricavare quanto possibile dal criptico articolo di Edouard Lucas "*Théorie des Fonctions Numériques SimplementPériodiques*", con il quale nel 1878 introduce le omonime sequenze applicandole in vari aspetti della matematica; ci concentreremo in particolare sulla loro applicazione nei test di primalità.

Non esiste un vero e proprio *test di Lucas*: il corpus del suo articolo è estremamente confuso e non esente da errori. Di fatto tutti i test presentati derivano dal lavoro di catalogazione e ricostruzione di altri matematici. Proprio per questo abbiamo preferito dare centralità nel secondo capitolo all'estremamente interessante contesto storico che avvolge i numeri di Mersenne, e da lì risaliremo gradualmente le pagine della storia verso il **test di Lucas-Lehmer**.
Data la natura del secondo test che presenteremo, il **test di Baillie-PSW**, abbiamo prediletto un approccio più teorico e meno storico nel presentarlo: partiremo quindi dai test di Lucas e di Fermat. Potremo poi dedicarci ad alcuni aspetti interessanti delle sue applicazioni.

Vale la pena sottolineare che non presenteremo l'interezza dei test derivanti dall'articolo di Lucas; molti purtroppo richiedono di conoscere la parziale fattorizzazione di un numero collegato al nostro, esempio è il test di Pocklington. Nonostante quest'ultimo sia deterministico, la richiesta di una fattorizzazione completa lo rende meno interessante dei due che presenteremo.

Gli algoritmi: Useremo alcuni algoritmi in Python3 per implementare i test che studieremo; a scopo didattico lo faremo in modo non ottimizzato e senza usare funzioni di libreria, risulterà un programma sicuramente più lento ma simile alla teoria svolta. Faremo eccezione per la generazione casuale di numeri, l'unico punto dove sappiamo sia bene avere un buono *pseudo-random number generator* e quindi un programma di libreria ottimizzato.

Capitolo 1

Fondamenti di algebra

"Dio creò i primi dieci numeri, tutto il resto è opera dell'uomo."

LEOPOLD KRONECKER

In questo capitolo introdurremo i concetti fondamentali per la costruzione dei risultati futuri. Inizieremo con un breve cenno alla *teoria elementare dei numeri*, dove parleremo di numeri primi, alcuni metodi di ricerca dei primi, aritmetica modulare e residui quadratici. In seguito ci occuperemo della *teoria elementare dei gruppi*, con la costruzione di un gruppo partendo da un monoide e la caratterizzazione di alcuni gruppi utili. Concluderemo studiando le *sequenze di Lucas* ed alcuni loro rimarcabili utilizzi in teoria dei numeri.

1.1 Teoria dei numeri: la ricerca dei primi

Fin dall'antichità i nostri antenati hanno provato a quantificare numericamente ciò che vedevano: si pensi ad alcuni graffiti, pitture rupestri ed a molte delle prime incisioni, secondo una delle possibili interpretazioni si trattava proprio di numeri - ed a volte addirittura in sistema decimale.
Nel corso del tempo si è andata ad associare la definizione di **numero naturale** a tutti quei numeri che è possibile trovare in natura.

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, \dots\} \tag{1.1}$$

Potremmo addentrarci nella controversa questione dell'elemento zero nei naturali, ma basti sapere che la definizione di Giuseppe Peano (19esimo secolo) è quasi universalmente accettata in quanto concorde con le strutture assiomatiche della logica matematica. Gli **assiomi di Peano** sono:

(i) esiste un naturale, lo zero (0)

(ii) ogni numero naturale ha un numero naturale successore

(iii) numeri naturali diversi hanno numeri naturali successori diversi

(iv) non esiste un naturale n che abbia lo zero come suo successore

(v) ogni sottoinsieme di naturali che contenga lo zero e il successore di ogni proprio elemento coincide con l'intero insieme dei numeri naturali

In parallelo si affronta la questione della definizione formale di *numero intero*; fin dall'antichità Euclide riteneva intuitivo spingersi all'indietro nella linea dei

numeri, ma per una buona definizione formale dovremo aspettare la logica matematica del diciannovesimo secolo. Possiamo considerare su $\mathbb{N} \times \mathbb{N}$ la relazione $\mathcal{Z}$ definita come

$$(a, b)\ \mathcal{Z}\ (c, d) \iff a + d = b + c \tag{1.2}$$

dove intuitivamente (a, b) è costruito per rappresentare $b - a$; si verifica che $\mathcal{Z}$ è una relazione di equivalenza, ed una volta definite su $\mathbb{N} \times \mathbb{N}/\mathcal{Z}$ le operazioni

$$[(a, b)] + [(c, d)] \coloneqq [(a + c, b + d)]$$
$$[(a, b)] \cdot [(c, d)] \coloneqq [(ac + bd, ad + bc)]$$

abbiamo costruito l'**insieme dei numeri interi**.

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, +1, +2, +3, \dots\} \tag{1.3}$$

Questo insieme è il campo di indagine della teoria dei numeri: già Euclide aveva espresso interesse nello studio dei numeri interi, seppur ancora non possedesse una loro formalizzazione rigorosa; in particolare si interessa della natura dei *numeri primi*.

Definizione 1.1 (Numeri primi ed irriducibili)**.** *Notiamo innanzitutto che in $\mathbb{Z}$ si definiscono **unità**, o anche **elementi invertibili**, gli elementi ± 1. Sia ora $p \in \mathbb{Z}$, lo diciamo **elemento primo** se ogni volta che $p \mid ab$ allora $p \mid a$ oppure $p \mid b$, ed **elemento irriducibile** se ogni volta che $p = ab$ abbiamo a o b unità.*

Spesso ci si riferisce ingenuamente alla definizione di irriducibile quando si definisce un primo come un "numero con divisori solo 1 e sé stesso", ma non è del tutto sbagliato; è possibile dimostrare che in $\mathbb{Z}$ le due definizioni sono equivalenti. Chiaramente la definizione più "ingenua" caratterizza solo i primi positivi, ma è comune restringervisi in quanto lo studio di un primo p è un lavoro identico allo studio di $-p$. Come propone Richard K. Guy in *unsolved problems in number theory*, possiamo elegantemente partizionare gli interi positivi (ovvero non-nulli) in tre classi:

(i) unità: 1

(ii) primi: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \dots$

(iii) composti: $4, 6, 8, 9, 10, 12, 14, 15, 16, \dots$

Ma a cosa serve tutto questo? Per quale motivo è interessante sapere se un numero è primo?

Teorema 1.2 (Teorema fondamentale dell'Algebra)**.** *Ogni intero diverso da 0 ed 1 presenta una scrittura come prodotto di primi; questa inoltre è unica a meno di ordinamento e della presenza di elementi invertibili.*

Corollario 1.3. *Vi sono infiniti numeri primi (in $\mathbb{Z}$).*

Dimostrazione di Euclide. Appare per la prima volta in [31, proposizione 20]. Suppongo per assurdo che siano finiti, e considero N il prodotto di tutti i primi $p_1, \dots, p_n$. Allora $M = N + 1$ per Teorema 1.2 ha una fattorizzazione in primi

$$M = q_1 \dots q_k = p_1 \dots p_n + 1$$

Per non cadere in contraddizione dovrei avere $n \geq k > 1$ e $q_i = p_j$ per ogni q_i ed un certo p_j, ma se fosse vera questa ultima condizione avrei $p_j \mid N$ e $p_j \mid M$, che implica $p_j \mid (N + 1) - N = 1$, cosa impossibile per un primo. □

Il Corollario 1.3 rappresenta la chiave di volta del nostro lavoro, ovvero capire *come possiamo determinare se un dato intero n sia primo*. Se avessimo solo finiti primi questo non sarebbe nemmeno un compito troppo interessante. Anzi, potrebbe essere persino già concluso. Inoltre lo stesso corollario ci fa capire in parte perché la ricerca di primi sia interessante: il teorema fondamentale dell'algebra, di fatto, è la base della crittografia come la intendiamo oggi.

Un metodo semplice ed intuitivo per rispondere alla nostra domanda segue la **trial division**, ovvero un insieme di tentativi di divisione per tutti gli m minori di n (e maggiori di 1). In Python: [1]

Codice 1.1: trial division

```
def trialDivision(n):                                    1
    for m in range(2,n):                                 2
        if n % m == 0:                                   3
            return "composite, divisor: " + str(m)       4
        return "prime"                                   5
```

Ma l'idea più semplice non sempre è la migliore: questo algoritmo sarebbe estremamente lento per grandi valori di n, e richiederebbe la conoscenza dei primi minori di n. Al primo problema si potrebbe parzialmente rimediare dividendo fino a $\sqrt{n}$ e non oltre, ed al secondo - per esempio - costruendo una tabella di primi fino ad n con il **crivello di Eratostene**. Queste due osservazioni sono giustificate, infatti:

(i) Se un intero n non-nullo può essere fattorizzato in $n = ab$ almeno uno dei due deve essere minore di $\sqrt{n}$; infatti se entrambi fossero maggiori avrei

$$n = ab > (\sqrt{n})(\sqrt{n}) = n$$

(ii) Il *crivello di Eratostene* permette di costruire una tabella di tutti i primi fino ad un certo n intero positivo fissato eliminando i multipli dei primi che incontro.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

Tre rapidi passaggi bastano per trovare tutti i primi tra 1 e 25, ma non dobbiamo lasciarci ingannare: l'algoritmo può rivelarsi estremamente dispendioso in termini di risorse.

[1] In realtà il codice proposto è una via di mezzo tra un *test di primalità* ed un *algoritmo di fattorizzazione*, questo perché fornisce un divisore di n.

Nonostante tutte le possibili accortezze, l'ostacolo della complessità computazionale resta ancora insormontabile; ma non è necessariamente un male, in quanto la quasi inattaccabilità del problema è ciò che lo rende rilevante in ambiti quale la crittografia. Ora introdurremo alcuni concetti fondamentali per distinguere in classi i test di probabilità: ad esempio, come possiamo valutarne l'efficienza?

Definizione 1.4 (Test deterministici e probabilistici)**.** *Un algoritmo per determinare se un dato n è primo viene detto **test di primalità**. Questo può essere*

(i) ***probabilistico**: se afferma che n è primo (in altre parole, se n passa il test) allora associa una certa probabilità $\mathcal{P}(n)$ che lo sia effettivamente*

(ii) ***deterministico**: se afferma che n è primo allora abbiamo un risultato certo; possiamo vederlo come un test probabilistico di probabilità $\mathcal{P}(n) = 1$*

Leggendo questa definizione sembrerebbe siano valori maggiori di $\mathcal{P}(n)$ a generare test "più buoni"; questo è solo marginalmente vero, ed in effetti un test T - considerato come un insieme di criteri da verificare - viene detto **più forte** di un test V se $\mathcal{P}_T(n) > \mathcal{P}_V(n)$. In generale non esiste un metodo per confrontare due test sotto ogni aspetto, potrei averne uno molto forte e molto ostico da implementare o addirittura dispendioso a livello computazionale: un esempio è la trial division, un test di primalità deterministico quindi molto forte, che però ha un costo pesante in termini di risorse. Come vedremo, spesso la via preferibile è il giusto mezzo.
Siccome in letteratura sono spesso utilizzati in modo confuso o contrastante, definiamo formalmente i seguenti termini:

Definizione 1.5 (Pseudoprimi, primi probabili)**.** *Sia dato un test di primalità probabilistico, un qualunque numero che lo passa viene detto **primo probabile** (probable prime); se sappiamo che è composto lo definiamo invece **pseudoprimo** (pseudoprime).*

Infatti molti autori definiscono "pseudoprimo" un qualunque n che passi il test - primo o composto che sia - ma in questo modo si perde una certa capacità espressiva del linguaggio che noi preferiamo mantenere.
Possiamo associare ad un primo probabile la probabilità che sia effettivamente primo, e questa ovviamente dipenderà dal test che stiamo utilizzando. Nel caso di test deterministico tali definizioni non sono necessarie, sappiamo che se un intero lo passa è necessariamente primo.

1.2 Teoria dei numeri: aritmetica modulare

Abbiamo osservato come $\mathbb{Z}$ sia il campo di interesse della teoria dei numeri, ma non è del tutto esatto; sarebbe ingiusto non parlare delle *classi di resto modulari*. Non entreremo troppo in dettaglio, ma ogni buon libro di teoria dei numeri può sufficere, si veda ad esempio [26].
Per ogni n intero definiamo su $\mathbb{Z}$ la relazione

$$a \mathcal{R}_n b \iff a - b = kn \text{ per } k \text{ intero} \tag{1.4}$$

Si verifica che è di equivalenza, e viene detta **relazione di congruenza**. Allora definiamo il quoziente $\mathbb{Z}/\mathcal{R}_n$ come $\mathbb{Z}_n$, la **classe di resto in modulo** n. Potremmo dimostrare che è un insieme finito.

Lemma 1.6 (Elementi di $\mathbb{Z}_n$)**.** *Nell'insieme $\mathbb{Z}_n$ ogni elemento è un divisore dello zero oppure un elemento invertibile.*[2]

Ora consideriamo $\mathbb{Z}_n^*$ **insieme degli elementi invertibili in modulo** n, ovvero gli $a \in \mathbb{Z}_n$ tali che esiste un $b \in \mathbb{Z}_n$ per cui $ab = [1]_n$ classe di resto di 1 in modulo n. Si noti che se a ed n sono coprimi allora è sicuramente invertibile - quindi un elemento di $\mathbb{Z}_n^*$; basta usare il lemma di Bezout.

Definizione 1.7 (Funzione di Eulero)**.** *Detta k la somma degli m interi coprimi con N, per $0 \leq m \leq N$, definisco la* ***funzione "toziente" di Eulero*** *come*

$$\begin{aligned} \varphi : \mathbb{N} &\longrightarrow \mathbb{N} \\ N &\longmapsto k \end{aligned}$$

Si dimostra, tra le altre cose, che se N è primo $\varphi(N) = N - 1$ e se $N = p^n$ potenza di primo allora $\varphi(N) = p^{n-1}(p-1)$. La funzione φ gode di molte altre proprietà interessanti che non tratteremo perché non di nostro interesse; si veda sempre [26].

Teorema 1.8 (Teorema di Eulero)**.** *Se n ed a sono interi coprimi, ovvero se a appartiene a $\mathbb{Z}_n^*$, allora vale*

$$a^{\varphi(n)} \equiv 1 \mod n \tag{1.5}$$

Corollario 1.9 (Piccolo teorema di Fermat)**.** *Sia p primo, a intero qualunque,*

$$a^{p-1} \equiv 1 \mod p \tag{1.6}$$

Notiamo che una volta invertito logicamente il Corollario 1.9 può essere usato come test di primalità probabilistico: se esiste un intero a per cui non valga l'Equazione 1.6, allora p non può essere primo. Devo quindi scegliere vari a_i tra 1 e $p-1$, e più ne scelgo più ho sicurezza nel risultato del test. Purtroppo non avrò mai certezza assoluta per la forma stessa dell'inversione.

Definizione 1.10 (Residuo quadratico)**.** *un intero m viene detto* ***residuo quadratico in modulo*** *n se esiste un intero k per cui*

$$k^2 \equiv m \mod n \tag{1.7}$$

Intuitivamente si tratta di interi m che in aritmetica modulare ammettono una "radice quadrata".

Definizione 1.11 (Simbolo di Legendre-Jacobi)**.** *Sia p un primo dispari, n un intero; definisco il* ***simbolo di Legendre*** *come*

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{se } p \mid a \\ +1 & \text{se } a \text{ è residuo} \mod p \\ -1 & \text{se } a \text{ non è residuo} \mod p \end{cases} \tag{1.8}$$

Possiamo generalizzarlo per p non primo: sia infatti N un intero dispari non necessariamente primo con decomposizione da Teorema 1.2 in primi $p_1^{e_1}, \ldots, p_k^{e_k}$, allora

$$\left(\frac{n}{N}\right) = \left(\frac{n}{p_1}\right)^{e_1} \cdots \left(\frac{n}{p_k}\right)^{e_k} \tag{1.9}$$

[2]Notiamo che $\alpha = [k]_{\mathcal{R}_n}$ si dice **divisore dello zero** se $\alpha^x \equiv 0$ per un certo x.

Teorema 1.12 (Criterio di Eulero)**.** *Sia p un primo dispari ed a in $\mathbb{Z}_p^*$, allora*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p \tag{1.10}$$

Questo criterio mi permette di trovare i primi p per cui un dato a è residuo quadratico; può essere sfruttato per costruire dei test di primalità, ma non approfondiremo.

Teorema 1.13 (Legge di reciprocità quadratica)**.** *Siano p e q due primi distinti e maggiori di 2, notiamo come questo implica che siano congrui ad 1 oppure 3 in $\mod 4$. Allora*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \tag{1.11}$$

Segue che l'esponente è pari se almeno uno tra p e q è congruo ad $1 \mod 4$ e dispari solo quando entrambi sono congrui a $3 \mod 4$.

Questo risultato permette di calcolare agevolmente ogni simbolo di Legendre. Gauss resterà così colpito dalla legge di reciprocità quadratica da fornirne svariate dimostrazioni ed invaghirsi della teoria dei numeri, arrivando a definirla "la regina della matematica".

1.3 Teoria elementare dei gruppi

Definiamo alcune strutture algebriche:

Definizione 1.14 (Gruppo)**.** *Sia G un insieme non vuoto, $*$ un'operazione binaria*

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (h, g) &\longmapsto h * g =: (hg) \end{aligned} \tag{1.12}$$

che soddisfi le proprietà di:

(i) ***associatività**: $a(bc) = (ab)c$ per ogni a, b, c in G*

(ii) ***esistenza dell'elemento neutro**: un e in G tale che $ge = eg = g$ per ogni g in G*

(iii) ***esistenza dell'inverso**: un $\overline{g}$ in G tale che $g\overline{g} = \overline{g}g = e$ per ogni g in G*

*Allora la coppia $(G, *)$ viene detta **gruppo**.*
*Se l'operazione è commutativa lo diciamo **gruppo abeliano**.*

Definizione 1.15 (Monoide)**.** *Sia M un insieme non vuoto, $*$ un'operazione binaria*

$$\begin{aligned} * : M \times M &\longrightarrow M \\ (m, n) &\longmapsto m * n \end{aligned} \tag{1.13}$$

*che soddisfi le proprietà di associatività ed esistenza dell'elemento neutro. Allora la coppia $(M, *)$ viene detta **monoide**.*

Dalla Definizione 1.15, è chiaro che prendendo tutti e soli gli elementi invertibili di un monoide $(M, *)$ - ovvero gli m in M tali che $nm = e$ per un certo n in M - ottengo un gruppo che soddisfa la Definizione 1.14. Infatti tale insieme è sicuramente non vuoto perché contiene e, e rispetta la definizione di gruppo in ogni altro punto. Si noti che stiamo usando la *notazione moltiplicativa* per i gruppi, ovvero scriviamo $g * h$ come gh; tutto questo può facilmente essere rivisto in notazione additiva. Indicheremo con 1 l'unità del gruppo.

Se ripensiamo alla sezione precedente, possiamo senza dubbio arricchire i risultati visti sfruttando questo nuovo formalismo. Innanzitutto per n intero si ha che $\mathbb{Z}_n$ è un monoide, basta scegliere una delle due operazioni, solitamente il prodotto; questo perché così facendo abbiamo popolato $\mathbb{Z}_n^*$ dei suoi elementi moltiplicativamente invertibili. Possiamo anche dimostrarlo formalmente, infatti la classe di 1 vi appartiene ed è l'unità, l'associatività deriva da quella di $\mathbb{Z}$ e l'inverso si ottiene dall'*identità di Bezout*: degli interi m ed n sono coprimi se e solo se esistono degli x ed y interi con

$$mx + ny = 1 \tag{1.14}$$

quindi per trovare l'inverso moltiplicativo di $M = [m]_{\mathcal{R}_n}$ classe di equivalenza in $\mathbb{Z}_n^*$ basta sfruttare 1.14 ed applicarvi l'aritmetica modulare. La chiusura per moltiplicazione sfrutta le proprietà del minimo comune multiplo, infatti se a ed n sono coprimi, b ed n sono coprimi, allora lo sono anche ab ed n; questo si verifica facilmente.

Definizione 1.16 (Gruppo ciclico)**.** *Un gruppo G si dice **ciclico** se esiste un suo elemento g tale che*

$$G = \{g^n \mid n \in \mathbb{Z}\} \tag{1.15}$$

dove ricordiamo che stiamo usando la notazione moltiplicativa.

Si può verificare che gli $\mathbb{Z}_n^*$ sono ciclici se e solo se $n = 1, 2, 4, pk, 2pk$ per p un primo dispari e k un intero positivo.

L'ultimo punto su cui ci soffermeremo è l'**ordine di un gruppo** ("moltiplicativo" nel nostro caso), ovvero il numero di elementi che contiene. Siccome stiamo lavorando su gruppi moltiplicativi l'ordine $\mathrm{ord}(G)$ equivale al minimo intero positivo x tale che $g^x = 1$ per ogni g in G. Bisogna sottolineare che in generale tale $\mathrm{ord}(G)$ non necessariamente esiste, ma se il gruppo è ciclico l'ordine moltiplicativo esiste ed equivale alla sua cardinalità.
Ad esempio prendiamo $\mathbb{Z}_7^*$, la cui struttura è semplice da descrivere essendo 7 un primo; proprio perché è primo, tutti gli m minori di 7 coprimi con esso sono $1, 2, 3, 4, 5, 6$. Si verifica che la cardinalità di uno $\mathbb{Z}_n^*$ è $\varphi(n)$, quindi nel nostro caso $\varphi(7) = 7 - 1 = 6$. Il gruppo è chiaramente ciclico di ordine 6, ed ogni elemento ha ordine che divide 6. Possiamo facilmente verificare che la classe di 2 ha ordine 3, infatti $2^2 \equiv 4$ e $2^3 \equiv 8 \equiv 1$ in modulo 7.

Lemma 1.17 (Ordine di un elemento)**.** *Sia G un gruppo moltiplicativo ciclico di ordine finito n, allora ogni elemento ha ordine che divide n.*

Riportiamo il risultato per completezza, avendolo usato sopra: può essere dimostrato come corollario del teorema di Lagrange, che non tratteremo. Rimandiamo ad un qualunque testo sulla teoria dei gruppi per una trattazione più completa.

1.4 Sequenze di Lucas e di Fibonacci

Nel 1202 il matematico italiano Leonardo Fibonacci pubblica il *Liber Abbaci* (o *Liber Abaci*), un trattato di straordinaria rilevanza storica; basti pensare che è questo ad introdurre i numeri indo-arabi in Europa. Tra le altre cose, Fibonacci studia un modello idealizzato di crescita in una popolazione di conigli.[3]

"Un uomo ha una coppia di conigli in un certo luogo interamente circondato da un muro. Vorremmo sapere quante coppie ne verranno allevate in un anno…"

(Leonardo Pisano "Fibonacci", *Liber Abbaci*)

Non entreremo troppo nel dettaglio del quesito logico proposto e risolto da Fibonacci, ma restringendosi alle condizioni

(i) nel mese iniziale ho solo una coppia di conigli appena nati

(ii) ogni coppia diventa fertile al primo mese dalla nascita

(iii) ogni coppia necessita di un mese per dare alla luce un nuovo coniglio

riesce a ricostruire il modello matematico della popolazione; detto m il numero di coppie di conigli in un mese ed n quella del precedente, nel successivo avrò $n+m$ conigli. Come si può notare il numero di coppie presenti ogni mese segue la successione dei **numeri di Fibonacci**[4] F_n, seppur opportunamente troncata:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

Tuttavia il nome "successione di Fibonacci" non verrà utilizzato fino al diciannovesimo secolo da Édouard Anatole Lucas, teorico dei numeri francese che nel 1878 pubblica uno studio in cui illustra le proprietà generali delle **sequenze di Lucas**, una generalizzazione dei numeri di Fibonacci.

Definizione 1.18 (Sequenze di Lucas)**.** *Siano dati due interi P e Q, definiamo ricorsivamente le due sequenze*

$$\begin{aligned} U_0(P,Q) &= 0 \\ U_1(P,Q) &= 1 \\ U_k(P,Q) &= P \cdot U_{k-1}(P,Q) - Q \cdot U_{k-2}(P,Q) \end{aligned} \tag{1.16}$$

$$\begin{aligned} V_0(P,Q) &= 2 \\ V_1(P,Q) &= P \\ V_k(P,Q) &= P \cdot V_{k-1}(P,Q) - Q \cdot V_{k-2}(P,Q) \end{aligned} \tag{1.17}$$

*per $k > 1$ naturale. Queste sono sequenze lineari di secondo ordine, e vengono dette rispettivamente **sequenza primaria** e **secondaria** di Lucas a parametri P e Q, oppure "sequenze gemelle", o ancora "sequenze compagne". Si noti che entrambe possono essere definite in modo ricorsivo dall'equazione caratteristica*

$$x^2 - Px + Q = 0 \tag{1.18}$$

Denotiamo inoltre con D il discriminante dell'equazione caratteristica, ovvero

$$D = P^2 - 4Q \tag{1.19}$$

[3] Si veda ad esempio [2] per un'edizione commentata del testo originale di Fibonacci.
[4] sequenza OEIS numero A000045.

Possiamo subito notare che ponendo $P = 1$ e $Q = -1$ otteniamo come $U(P,Q)$ la sequenza dei numeri di Fibonacci F_n e come $V(P,Q)$ la sequenza dei *numeri di Lucas*[5] L_n:

$$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, \ldots$$

Per quanto abbiamo visto F_n ed L_n sono ben più che legate, sono *gemelle*. Potremmo anche estendere le sequenze di Fibonacci e Lucas ad indici in tutto $\mathbb{Z}$: infatti per $k \in \mathbb{Z}^-$ basta scrivere $L_{-k} = (-1)^k L_k$ e $F_{-k} = (-1)^{k+1} F_k$. Queste due estensioni vengono dette **negafibonacci** e **negalucas**.

Il formalismo delle sequenze di Lucas permette di ottenere molte serie note, ad esempio la sequenza dei *numeri di Pell*:

$$U_n(2,-1) : 0, 1, 2, 5, 12, 29, 70, 169, 408, \ldots$$

e la sequenza gemella dei *numeri di Pell-Lucas*:

$$V_n(2,-1) : 2, 2, 6, 14, 34, 82, 198, 478, \ldots$$

Non ci addentreremo troppo nell'argomento in quanto questo esula dalla nostra trattazione, ma è interessante notare che $U_n(2,-1)/U_{n-1}(2,-1)$ converge al *rapporto argenteo* $1 + \sqrt{2}$, e di conseguenza

$$\frac{U_n(2,-1) - U_{n-1}(2,-1)}{U_{n-1}(2,-1)}$$

è una sequenza di razionali che approssimano $\sqrt{2}$. Altre sequenze possono essere ottenute partendo dalla teoria delle sequenze di Lucas, che a tutti gli effetti sono considerabili come la generalizzazione di molte sequenze note.

Osservazione 1.19. *Alcune osservazioni preliminari:*

(i) *Si noti che se $D \neq 0$ possiamo usare le due soluzioni dell'equazione caratteristica per descrivere gli elementi delle due sequenze 1.16 e 1.17. Infatti una volta dette $\alpha = (P + \sqrt{D})/2$ e $\beta = (P - \sqrt{D})/2$ le due radici possiamo scrivere*

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\sqrt{D}}$$

$$V_n = \alpha^n + \beta^n$$

(ii) *Cosa rende particolare il caso $D = 0$? Possiamo subito verificare che $D = 0$ se e solo se $P = 2\lambda$ e $Q = \lambda^2$ per un certo λ intero. Infatti se $P = 2\lambda$ e $Q = \lambda^2$ ottengo subito $D = 0$, l'altra implicazione è altrettanto banale - basta porre $\lambda = \alpha = \beta$. L'equazione caratteristica si rivela essere un importante strumento per lo studio delle sequenze di Lucas.*

(iii) *Anche α^n e β^n rispettano l'equazione 1.18, ma non otteniamo necessariamente una sequenza di interi. Difatti è banale dimostrare che*

$$\alpha^n = \frac{V_n + U_n\sqrt{D}}{2}$$

[5] sequenza OEIS numero A000032.

$$\beta^n = \frac{V_n - U_n\sqrt{D}}{2}$$

e già nel caso $(P, Q) = (1, -1)$ *otteniamo* $\alpha^n = (18 + 8\sqrt{5})/2$, $\beta^n = (18 - 8\sqrt{5})/2$.

(iv) *Per i punti precedenti possiamo affermare che le sequenze gemelle sono caratterizzate dagli interi* P *e* Q*; è interessante notare che fissati* P *e* Q *(e di conseguenza il loro discriminante) si ottiene lo stesso valore di* D *una volta scelti*

$$\tilde{P} = P + 2$$
$$\tilde{Q} = P + Q + 1$$

La verifica è immediata, infatti la nuova equazione caratteristica ha come discriminante $\tilde{D}$ *il valore*

$$\begin{aligned}\tilde{D} &= (P+2)^2 - 4(P+Q+1)\\ &= P^2 + 4 + 4P - 4(P+Q+1)\\ &= P^2 - 4Q = D\end{aligned}$$

Nel 1913 Carmichael pubblica l'articolo *On the Numerical Factors of the Arithmetic Forms* $\alpha_n \pm \beta_n$ [8], in cui studia il lavoro di Lucas e corregge alcuni errori, oltre ad ampliarne la portata. Il suo contributo sarà fondamentale per generalizzare i risultati di Lucas e rendere meno complesse ma più eleganti le loro applicazioni, già lo stesso Lucas infatti proponeva varie applicazioni nel campo della teoria dei numeri: frazioni continue, equazioni trigonometriche, criteri di primalità... Tuttavia le sue idee erano esposte in modo contorto e non sempre lineare.
Esploreremo a tempo debito il ruolo delle sequenze di Lucas nei criteri di primalità. Per questo compito risulterà cruciale calcolare termini di U e V ad indice molto elevato; riportiamo alcuni risultati che permettono di ottenere questi risultati in modo veloce ed efficiente.

Teorema 1.20. *Siano* n *ed* m *dei naturali, allora*

$$U_{n+m} = U_m V_n - Q^n U_{m-n}$$
$$V_{m+n} = V_m V_n - Q^n V_{m-n}$$

Dimostrazione. Per l'osservazione 1.19 vale

$$\begin{aligned}U_{n+m} &= \frac{\alpha^{n+m} - \beta^{n+m}}{\alpha - \beta}\\ &= \frac{(\alpha^m - \beta^m)(\alpha^n + \beta^n)}{\alpha - \beta} - \frac{\alpha^n\beta^n(\alpha^{m-n} - \beta^{m-n})}{\alpha - \beta}\\ &= U_m V_n - \alpha^n\beta^n U_{m-n} = U_m V_n - Q^n U_{m-n}\end{aligned}$$

Procediamo quindi in modo analogo, scrivendo

$$\begin{aligned}V_{m+n} &= \alpha^{m+n} + \beta^{m+n}\\ &= (\alpha^m + \beta^m)(\alpha^n + \beta^n) - \alpha^n\beta^n(\alpha^{m-n} + \beta^{m-n})\\ &= V_m V_n - \alpha^n\beta^n V_{m-n} = V_m V_n - Q^n V_{m-n}\end{aligned}$$

□

Corollario 1.21.

$$U_{2n} = U_n V_n$$
$$V_{2n} = V_n^2 - 2Q^n$$

Dimostrazione. Basta porre $m = n$ in 1.20. □

Corollario 1.22.

$$U_{n+1} = PU_n - QU_{n-1}$$
$$V_{n+1} = PV_n - QV_{n-1}$$

Dimostrazione. Anche qui basta usare 1.20 con $m = 1$. □

I corollari 1.21 e 1.22 permettono di computare $U_k(P, Q)$ e $V_k(P, Q)$ per valori di k molto alti in un numero di passi relativamente basso, proporzionale a $\log_2(k)$. Sia dato ad esempio $k = 100$, procedendo all'inverso da 100 sappiamo che necessiteremo di calcolare $k = 50, 25, 13, 12, 7, 6, 4, 3, 2, 1$ e questo vale per ogni valore arbitrario di P, Q. La procedura può essere migliorata: infatti se volessi calcolare U_k non necessiterei di nessun V_j, e specularmente per V_k di nessun U_j. Si può anche dimostrare che il calcolo degli U_j è più lento, ma solo di un fattore numerico relativamente piccolo. Concludiamo in bellezza con il seguente teorema, che ci permette di calcolare in modo ancora più efficiente le due sequenze associate; le operazioni tra matrici infatti possono essere rimarcabilmente ottimizzate.

Teorema 1.23.

$$\begin{bmatrix} U_{n+1} \\ U_n \end{bmatrix} = \begin{bmatrix} P & -Q \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{1.20}$$

$$\begin{bmatrix} V_{n+1} \\ V_n \end{bmatrix} = \begin{bmatrix} P & -Q \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} P \\ 2 \end{bmatrix} \tag{1.21}$$

Dimostrazione. Possiamo dimostrarlo facilmente procedendo per induzione con le equazioni del Teorema 1.22. □

Vale la pena sottolineare che non abbiamo neanche scalfito la superficie dei criteri di costruzione dei termini delle serie gemelle. Solitamente alcuni casi vengono classificati in letteratura nelle categorie:

(i) *Binary-U*, *Binary-V* quando si ricava U_k in termini di altri U_i oppure V_k in termini di altri V_i

(ii) *V-from-U*, *U-from-V* in casi autoesplicativi

Un'ottima fonte per approfondire è il capitolo ottavo di [23].

1.5 Applicazioni alla teoria dei numeri

Da questo punto utilizzeremo U_n e V_n per indicare rispettivamente le sequenze $U_n(P,Q)$ e $V_n(P,Q)$ senza appesantire la notazione. Le seguenti proprietà torneranno utili soprattutto costruendo test di primalità:

Teorema 1.24 (Congruenze modulari)**.** *Sia n un primo intero dispari, siano P e Q interi tali che n sia coprimo con Q. Allora*

(i) $U_{n-\left(\frac{D}{n}\right)} \equiv 0 \mod n$

(ii) $V_{n-\left(\frac{D}{n}\right)} \equiv 2Q^{\frac{[1-(D/n)]}{2}} \mod n$

(iii) $U_n \equiv \left(\frac{D}{n}\right) \mod n$

(iv) $V_n \equiv P \mod n$

Si veda [25] per approfondire questo teorema; notiamo che in letteratura il primo criterio è il più utilizzato nella costruzione di test di primalità, mentre molto poco è noto sugli altri. La dimostrazione di questo criterio richiede una lunga catena di risultati sulle sequenze di Lucas simili a quelli della sezione precedente, che però sarebbe dispersivo riportare qui: è possibile trovarla nell'eccellente [24]. Per i restanti criteri sono buone fonti [11] e [8, 9], che ne elencano molti altri.

Teorema 1.25. *Valgono i seguenti risultati:*

(i) *se Q e P sono pari, allora U è pari (per $n \geq 2$) e V_n è pari (per $n \geq 1$)*

(ii) *se Q è pari e P è dispari, allora U e V sono dispari (per $n \geq 1$)*

(iii) *se Q è dispari e P è pari, allora $U \equiv n \pmod 2$ e V è pari*

(iv) *se Q e P sono dispari, allora U e V sono pari se 3 divide n, altrimenti sono dispari*

Dimostrazione. La dimostrazione richiede una lunga catena di lemmi intermedi che il poco spazio non ci permette di inserire, è possibile trovarla in [24]. □

Teorema 1.26 (Potenze di α e β in campo quadratico)**.** *Siano P e Q interi dati, D il discriminante associato all'Equazione 1.18 determinata dai parametri P e Q, supposto non nullo. Siano $\alpha = P + \sqrt{D}/2$ e $\beta = P - \sqrt{D}/2$ le radici dell'equazione caratteristica. Sia infine q un primo dispari. Allora valgono*

$$\alpha^q \equiv \begin{cases} \alpha & \mod q \quad \text{se } \varepsilon(q) = 1 \\ \beta & \mod q \quad \text{se } \varepsilon(q) = -1 \\ P/2 & \mod q \quad \text{se } \varepsilon(q) = 0 \end{cases} \tag{1.22}$$

$$\beta^q \equiv \begin{cases} \beta & \mod q \quad \text{se } \varepsilon(q) = 1 \\ \alpha & \mod q \quad \text{se } \varepsilon(q) = -1 \\ P/2 & \mod q \quad \text{se } \varepsilon(q) = 0 \end{cases} \tag{1.23}$$

Dimostrazione. Dimostriamo intanto la prima formula: la otteniamo usando rispettivamente la scrittura esplicita di $(a+b)^q$ in modulo q, il piccolo teorema di Fermat (Teorema 1.9) ed il criterio di Eulero (Teorema 1.12).

$$\begin{aligned}\alpha^q &= \left(\frac{P+\sqrt{D}}{2}\right)^q \equiv \frac{P^q + (\sqrt{D})^q}{2^q} \mod q \\ &\equiv \frac{P + D^{(q-1)/2}(\sqrt{D})}{2} \equiv \frac{P + \varepsilon(p)\sqrt{D}}{2} \mod q\end{aligned}$$

La seconda formula si ricava in modo identico. □

La teoria delle sequenze di Lucas in effetti è piena di interessanti applicazioni alla teoria dei numeri; concludiamo il capitolo con qualche curiosità a riguardo. Ad esempio scrivendo le sequenze per $P = 3$ e $Q = 2$ si ottiene la sequenza $U_n(P,Q)$ dei *numeri di Mersenne*, oggetto di interesse nel prossimo capitolo.

$$U_n(3,2) = 2^n - 1 \tag{1.24}$$

$$\begin{aligned} U_0 &= 0 = 2^0 - 1 & U_4 &= 15 = 2^4 - 1 \\ U_1 &= 1 = 2^1 - 1 & U_5 &= 31 = 2^5 - 1 \\ U_2 &= 3 = 2^2 - 1 & U_6 &= 63 = 2^6 - 1 \\ U_3 &= 7 = 2^3 - 1 & U_7 &= 127 = 2^7 - 1 \end{aligned}$$

La proprietà descritta dall'Equazione 1.24 si verifica facilmente per induzione; infatti la tabella può essere utilizzata come verifica del caso base, e per il passo induttivo

$$\begin{aligned} U_n &= 3 \cdot U_{n-1} - 2 \cdot U_{n-2} \\ &= 3\left(2^{n-1} - 1\right) - 2\left(2^{n-2} - 1\right) \\ &= 3 \cdot 2^{n-1} - 3 - 2^{n-1} + 2 = 2^n - 1 \end{aligned}$$

Altrettanto interessante è la sequenza gemella V_n,

$$V_n(3,2) = 2^n + 1$$

che ha come sottosequenza quella dei *numeri di Fermat* $2^{2^k} + 1$. Non tratteremo tali numeri, ma possiamo già notare il parallelo con i numeri di Mersenne; anche questi sono interessanti dal punto di vista storico per la ricerca di primi nella loro serie.

Chiaramente sfruttando i criteri di costruzione degli U_n e dei V_n potremmo già abbozzare qualche risultato sulla primalità dei numeri di Mersenne; compiendo uno sforzo per trattenerci dal farlo già ora, proseguiamo parlando proprio di loro.

Capitolo 2

Il test di Lucas-Lehmer

"Chiaramente questa è una delle più grandi difficoltà della matematica [...], riconoscere se un dato numero di quindici o venti cifre sia primo; un intero secolo non sarebbe sufficiente per indagare il problema con gli strumenti a noi noti."

MARIN MERSENNE

Lo scopo di questo capitolo sarà costruire e studiare il test di Lucas-Lehmer partendo dall'articolo originale di Lucas (1878).
Inizieremo con una non facile ricostruzione del contesto storico: le fonti sembrano essere contrastanti, ad esempio su alcune date delle corrispondenze. In quei casi, per i risultati abbiamo deciso di utilizzare la data della prima pubblicazione in cui appaiono dimostrati interamente, mentre per le congetture abbiamo fatto bastare un enunciato sufficientemente chiaro.
In seguito illustreremo il contorto articolo di Lucas e ne estrarremo alcune informazioni interessanti, per poi entrare nel vivo dell'argomento e prima enunciare e poi dimostrare il test di Lucas-Lehmer.

Concluderemo con uno sguardo finale sul suo enorme impatto nella ricerca dei primi di Mersenne.

2.1 La ricerca dei primi di Mersenne

I numeri nella forma $2^n - 1$ sono sempre stati dei "sospetti primi"; se ci pensiamo, non pochi dei primi che conosciamo hanno questa forma:

$2^2 - 1 = 3$	**primo**	$2^5 - 1 = 31$	**primo**
$2^3 - 1 = 7$	**primo**	$2^6 - 1 = 63$	**non primo**
$2^4 - 1 = 15$	**non primo**	$2^7 - 1 = 127$	**primo**

Possiamo notare uno schema, infatti i numeri nella forma $2^n - 1$ sembrano essere primi solo per un esponente n primo. Questa caratteristica era stata notata anche in antichità; intorno all'anno 100 Nicomaco di Gerasa (ca. 60 - 120) costruisce il primo elenco noto di primi in questa forma, usando come esponenti $n = 2, 3, 5, 7$. Non è ben chiaro quanti e quali di questi siano stati effettivamente verificati da Nicomaco stesso, probabilmente si trattava solo di un elenco di proprietà già note dal passato. Anche Euclide era estremamente interessato a questa classe di primi, incontrati durante lo studio dei numeri perfetti [27].

L'idea che la costruzione possa funzionare per ogni n primo cade solo nel 1536, quando Hudalricus Regius (pseudonimo del monaco Ulrich Rieger) dimostra che $2^{11} - 1$ non è primo fattorizzandolo in

$$2^{11} - 1 = 2047 = 23 \times 89$$

In realtà il risultato sembra essere addirittura antecedente, infatti già un manoscritto del 1456 contiene una lista dei primi cinque primi di tale forma e non include 2047; era forse un fatto noto non ancora formalizzato.

numero	cifre	anno	stato	dimostrato da	metodo
$2^2 - 1$	1	antichità	primo	-	*trial division*
$2^3 - 1$	1	antichità	primo	-	*trial division*
$2^5 - 1$	2	antichità	primo	-	*trial division*
$2^7 - 1$	3	antichità	primo	-	*trial division*
$2^{11} - 1$	4	1456	composto	Huldaricus	*divisori*

Tabella 2.1: storia dei primi di Mersenne - I

Definizione 2.1 (Numero di Mersenne)**.** *Sia n un intero positivo, $M_n = 2^n - 1$ è detto **numero di Mersenne**. Se è primo viene detto **numero primo di Mersenne**, ed analogamente **numero composto di Mersenne** se è composto.*

Alla luce di questo, possiamo riformulare la scoperta di Huldaricus in termini più rigorosi:

Controesempio 2.2. *Non tutti i numeri di Mersenne con n primo sono primi; infatti per $n = 11$ ottengo un numero composto di Mersenne.*

Stiamo assistendo all'inizio di un nuovo campo di interesse per i teorici dei numeri: se essere primi non basta, allora per quali n ottengo un numero di Mersenne primo? come posso caratterizzarli? e, soprattutto, quanti ne esistono con questa proprietà? Sempre sulla stessa strada, il matematico bolognese Pietro Antonio Cataldi (1548 - 1626) dimostra che M_n è primo solo se n lo è, ma il contrario non vale - e vi sono molti controesempi, come il Controesempio 2.2.

Teorema 2.3. *(Teorema di Cataldi) Condizione necessaria perché M_n sia primo è che n sia primo; equivalentemente, se n non è primo M_n non può esserlo.*

Dimostrazione. Se $n = ab$ ottengo immediatamente

$$2^{ab} - 1 = (2^a - 1)\left(1 + 2^a + 2^{2a} + \cdots + 2^{(b-1)a}\right)$$

e quindi una fattorizzazione di M_{ab}. La stessa fattorizzazione vale ovviamente anche se invertiamo i ruoli a e b per commutatività del prodotto. □

Si noti che in alcuni testi si richiede che n sia primo per poter dire M_n *numero di Mersenne*; noi non richiediamo n primo. D'altro canto, il Teorema 2.3 garantisce l'equivalenza delle due possibili definizioni di *primi di Mersenne* - e sono questi gli interi di nostro interesse. Lucas stesso nei suoi lavori sembra utilizzare la nostra stessa definizione.
Da adesso scriveremo M_p quando sarà opportuno sottolineare che il numero di

Mersenne ha esponente p primo, ed M_n invece indicherà un numero di Mersenne del cui esponente nulla è noto: potrebbe essere primo o composto, ma non riteniamo utile soffermarci a riflettere sulla sua natura.

Cataldi ha anche lo straordinario merito di aver dimostrato formalmente nel 1588 la primalità di M_{19}, che resterà per due secoli il più grande primo conosciuto; sfrutta la tecnica della *trial division*, che abbiamo avuto già modo di conoscere. In realtà Cataldi era andato oltre, ipotizzando la primalità di M_n per $n = 23, 29, 31, 37$ - affermazione smentita nei secoli successivi.

numero	cifre	anno	stato	dimostrato da	metodo
$2^{17} - 1$	6	1588	primo	Cataldi	*trial division*
$2^{19} - 1$	6	1588	primo	Cataldi	*trial division*
$2^{23} - 1$	7	1588	?	Cataldi	*congettura*
$2^{29} - 1$	9	1588	?	Cataldi	*congettura*
$2^{31} - 1$	10	1588	?	Cataldi	*congettura*
$2^{37} - 1$	12	1588	?	Cataldi	*congettura*

Tabella 2.2: storia dei primi di Mersenne - II

Nel 1644 il monaco e matematico francese Marin Mersenne (1588 - 1648) pubblica il *Cogitata Physica-Mathematica* [1] , in cui formula la **congettura di Mersenne**, di critica importanza nella nostra storia:

Congettura 2.4 (di Mersenne)**.** *Tra tutti i numeri di Mersenne M_n con n minore di 258, sono primi di Mersenne solo gli M_n per*

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 \tag{2.1}$$

numero	cifre	anno	stato	dimostrato da	metodo
$2^{31} - 1$	10	1644	?	Mersenne	*congettura*
$2^{67} - 1$	21	1644	?	Mersenne	*congettura*
$2^{127} - 1$	39	1644	?	Mersenne	*congettura*
$2^{257} - 1$	78	1644	?	Mersenne	*congettura*

Tabella 2.3: storia dei primi di Mersenne - III

La congettura si rivelerà essere parzialmente errata, infatti oggi è noto che anche per $n = 61, 89, 107$ abbiamo dei primi (omessi nella congettura), mentre per $n = 67, 257$ si ottengono numeri composti (erroneamente presenti nella congettura). Ma Mersenne stesso aveva scritto

> "*Un intero secolo non sarebbe sufficiente per determinare se sono primi con gli strumenti a noi noti.*"
>
> (Mersenne, *Cogitata Physica-Mathematica*, cap. XIX introduzione)

e nemmeno i suoi contemporanei, pur sapendo che Mersenne non li aveva testati, erano in grado di farlo; erano limitati dai mezzi della propria epoca. Si ipotizza che Mersenne ritenesse M_p primo per i p primi di forma $2^{2k+1} - 1, 2^{2k} + 1$,

$2^{2k} + 3$ o $2^{2k} - 3$; ma anche questa, dal canto suo, è solo una congettura. Altra possibilità è che considerasse M_p primo se e solo se $p = 2^k \pm 1$ o $p = 4^k \pm 1$, ma se questo fosse vero avrebbe incluso anche 61. La realtà è che Mersenne non rivelerà mai come sia giunto a tale conclusione. Nonostante tutto la sua congettura provocherà molto interesse, infatti nessuno aveva ancora dimostrato nulla per n maggiore a 19.

Il numero M_{19} di Cataldi perderà il suo primato solo due secoli dopo, quando nel 1772 Leonhard Euler dimostra la primalità di M_{31} sfruttando la *enhanced trial division* di Fermat, basata sul seguente risultato:

Lemma 2.5 (Trial division di Fermat, 1640)**.** *Se p è un primo dispari, allora tutti i divisori primi di $2^p - 1$ sono nella forma $2kp + 1$ per un certo k intero.*

Dimostrazione. La dimostrazione sfrutta il piccolo teorema di Fermat (Teorema 1.9); sia q un fattore primo di M_p, essendo primo sappiamo dal teorema che q è un fattore di $2^{q-1} - 1$. Per ipotesi q divide $M_p = 2^p - 1$, quindi dalla stessa fattorizzazione del Teorema 2.3 di Cataldi

$$2^{kp} - 1 = (2^p - 1)\left(1 + 2^p + 2^{2p} + \cdots + 2^{(k-1)p}\right)$$

ottengo che q divide anche $2^{kp} - 1$ per ogni k intero positivo; grazie a questo posso verificare che p è il più piccolo intero positivo a per cui q divide $2^a - 1$. Ancora di più, posso affermare che per ogni m intero positivo q divide $2^m - 1$ se e solo se p divide m. Infatti se p divide m posso utilizzare lo stesso trucco della scomposizione, e per l'altro lato ho appena svolto la dimostrazione. Ma poiché sappiamo che q divide $2^{q-1} - 1$, questo implica che p divide $q - 1$.

$$q \equiv 1 \mod (p)$$

Inoltre per ipotesi q divide $2^p - 1$, un numero dispari; q deve essere necessariamente dispari, e quindi posso finalmente scrivere

$$q \equiv 1 \mod (2p) \qquad \square$$

Nel tempo Eulero e Fermat si sono basati sullo stesso risultato per testare alcune affermazioni di Cataldi; Fermat ha ottenuto un fattore per M_{23} (47, con $k = 1$) e per M_{37} (223, con $k = 3$), Eulero invece uno per M_{29} (233, con $k = 3$). In effetti non è del tutto corretto affermare che Eulero abbia sfruttato solamente la enhanced division di Fermat; i risultati su cui lui si basa per individuare i valori critici di cui abbiamo parlato sono i seguenti (che raccoglieremo sotto il nome unico di "enhanced trial division+").

Lemma 2.6 (Teorema del divisore speciale, Eulero)**.** *Se $p = 4m - 1$ (per un certo m intero) e $2p + 1 = 8m - 1$ sono primi, allora M_p è divisibile per $2p + 1$.*

Lemma 2.7 (Teorema migliorato del divisore, Eulero)**.** *Se d è un divisore di M_p, allora è nella forma $2kp + 1$ per un intero k ed un intero positivo d tale che*

$$d \equiv \pm 1 \mod 8 \tag{2.2}$$

In una lettera a Bernoulli, Eulero dichiara di aver sfruttato in passato i suoi teoremi del divisore per dimostrare M_{31} primo. La data che si trova in letteratura varia tra il 1750 circa, quando inserisce il numero in alcuni elenchi, il 1752, anno in cui scrive a Goldbach dichiarando di essere incerto su questo risultato, ed il 1772, anno della lettera a Bernoulli. In particolare risulta che Eulero abbia provato a svolgere ben 84 fattorizzazioni prima di concludere che fosse primo.

numero	cifre	anno	stato	dimostrato da	metodo
$2^{23}-1$	7	1640	composto	Fermat	*enhanced division*
$2^{29}-1$	9	1732	composto	Eulero	*enhanced division +*
$2^{31}-1$	10	1772	primo	Eulero	*enhanced division +*
$2^{37}-1$	12	1640	composto	Fermat	*enhanced division*

Tabella 2.4: storia dei primi di Mersenne - IV

Infine, nel 1867, il matematico francese Fortuné Landry (1799 - 1895) sfrutta ingegnosamente il fallimento del test di primalità per M_{59} e crea quello che sarà e resta ancora *il primo non di Mersenne con il record più longevo*:

$$\frac{2^{59}-1}{179\,951} = 32\,034\,317\,801\,337$$

Questo rappresenta la pietra miliare che chiude l'era della ricerca dei primi di Mersenne "pre-Lucas", ovvero prima della formulazione del test di Lucas. Concludiamo con una tabella riassuntiva, stavolta in ordine cronologico:

numero	cifre	anno	stato	dimostrato da	metodo
$2^{2}-1$	1	antichità	primo	-	*trial division*
$2^{3}-1$	1	antichità	primo	-	*trial division*
$2^{5}-1$	2	antichità	primo	-	*trial division*
$2^{7}-1$	3	antichità	primo	-	*trial division*
~~$2^{11}-1$~~	4	1456	composto	Huldaricus	*divisori*
$2^{13}-1$	4	medioevo	primo	(conteso)	*trial division*
$2^{17}-1$	6	1588	primo	Cataldi	*trial division*
$2^{19}-1$	6	1588	primo	Cataldi	*trial division*
$2^{23}-1$	7	1588	?	Cataldi	*congettura*
$2^{29}-1$	9	1588	?	Cataldi	*congettura*
$2^{31}-1$	10	1588	?	Cataldi	*congettura*
$2^{37}-1$	12	1588	?	Cataldi	*congettura*
~~$2^{23}-1$~~	7	1640	composto	Fermat	*enhanced division*
~~$2^{37}-1$~~	12	1640	composto	Fermat	*enhanced division*
$2^{67}-1$	21	1644	?	Mersenne	*congettura*
$2^{127}-1$	39	1644	?	Mersenne	*congettura*
$2^{257}-1$	78	1644	?	Mersenne	*congettura*
~~$2^{29}-1$~~	9	1732	composto	Eulero	*enhanced division +*
$2^{31}-1$	10	1772	primo	Eulero	*enhanced division +*
~~$2^{53}-1$~~	16	1867	composto	Landry	*enhanced division +*

Tabella 2.5: storia dei primi di Mersenne, ordine cronologico

Vale la pena sottolineare che non abbiamo affrontato la totalità della storia dei numeri di Mersenne, anzi abbiamo appena scalfito la superficie; ad esempio non abbiamo trattato la storia di M_{13}, dimostrato primo in epoca medioevale, a causa della lunga ed intricata disputa sulla sua attribuzione. Sarebbe un compito contorto, forse impossibile, risalire al vero autore. Non abbiamo nemmeno studiato tutte le vicende intorno ai numeri composti di Mersenne, ma in fondo sono i primi l'oggetto del nostro interesse. Per una trattazione completa consigliamo [13], che presenta molti altri degli ingegnosi metodi sviluppati per studiare gli sfuggenti numeri di Mersenne.

2.2 L'articolo di Lucas

Pochi anni dopo, nel 1878, il matematico francese E. Lucas pubblica l'articolo *Théorie des Fonctions Numériques Simplement Périodiques* (Teoria delle Funzioni Numeriche Semplicemente Periodiche) diviso in due parti, [5] e [6]. L'originale in francese, ma è possibile trovare una revisione della prima parte in inglese molto vicina al suo significato in [14].
Qui Lucas raccoglie ampliandoli i suoi precedenti lavori, partendo da [3] del 1876; è riconosciuto come un articolo contorto, una raccolta di risultati sparsi e dimostrati in modo incompleto, insomma non facile da indagare. Più volte si è cercato di revisionarlo, degno di nota è il lavoro anticipato in precedenza di R. D. Carmichael in [8] e [9].

Nel corso dell'articolo Lucas usa spesso la teoria delle sue sequenze, ed inizia riportando interi N di cui vuole studiare la primalità al caso di un termine di sequenze U_n o V_n per opportuni P e Q, in modo da poterli dividere sfruttando i "criteri di divisione" e "di moltiplicazione" delle sequenze. Ad esempio sappiamo dall'Equazione 1.5 che è possibile ottenere i numeri di Mersenne come sequenza di U_n per $P = 3$ e $Q = 2$, quindi sfruttando il Corollario 1.21

$$\begin{aligned} U_{64} &= 2^{64} - 1 \\ &= U_1 V_1 V_2 V_4 V_8 V_{16} V_{32} \end{aligned}$$

Prosegue formulando, sempre partendo dalla teoria delle sequenze, due test iterativi per i numeri di Mersenne: gli enunciati cambiano da una pubblicazione all'altra, e Lucas non li dimostra mai completamente. Il primo è stato in seguito riformulato da P. Pepin in [4], il secondo da D. H. Lehmer in [11]; partendo da entrambi, A. E. Western cercherà di ricomporre il lavoro originale di Lucas in [12], formulando i due teoremi che seguono.

Teorema 2.8 (Lucas I, 1878)**.** *Sia p primo nella forma $2k + 3$, $N = 2^p - 1$ è primo se una volta definita la sequenza $r_0 = 3$, $r_i = r_{i-1}^2 - 2$ ho che*

$$r_{p-2} \equiv 0 \mod N \tag{2.3}$$

Teorema 2.9 (Lucas II, 1878)**.** *Sia p un primo dispari, $N = 2^p - 1$ è primo se*

$$r_{p-2} \equiv 0 \mod N \tag{2.4}$$

ed altrimenti è composto. Qui usiamo la stessa sequenza ma con $r_0 = 4$.

Dimostrazione. Non è nel nostro interesse dimostrare il primo, e del secondo studieremo la versione enunciata da Lehmer in [11], con le dimostrazioni di Bruce e Rosen ([20, 19]). Rimandiamo alla revisione [12] di Western per delle dimostrazioni complete vicine all'originale. □

"*Dal punto di vista di un computer c'è poco da scegliere tra i due test, ma il primo funziona solo per* $p \equiv 3 \mod 4$*, mentre il secondo per ogni* p*. [...] La formulazione successiva di Pepin richiede molto più lavoro computazionale di ciascuno dei due test di Lucas, [...] e non sembra sia mai stata usata.*"

(A. E. Western, *sui test di Lucas e Pepin*, 1932)

Western nota come non sia difficile partire dai due test di Lucas per formularne uno completamente nuovo, ma questo lavoro sarebbe inutile alla luce della efficiente formulazione di Lehmer. Infatti la formulazione del Teorema 2.9 non è quella originale di Lucas, oscura e non ben giustificata, ma quella di Lehmer.

Molti dei criteri di primalità che Lucas utilizza si basano su enunciati sulla falsa riga del Teorema 2.8, o ancora sulla scomposizione dei numeri di Mersenne visti come sequenza di Lucas; è interessante notare come il suo scopo fosse *costruire test per classi di interi*, ed è stato raggiunto passo dopo passo tramite casi particolari dell'esponente in M_n. Esempi interessanti sono i seguenti lemmi.

Lemma 2.10. *Se* $p = 4q + 3$ *è un primo, allora* $2p - 1$ *è primo se e solo se*

$$\frac{1}{\sqrt{2}}\left[(1+\sqrt{2})^p - (1-\sqrt{2})^p\right] \equiv 0 \mod 2p-1$$

Lemma 2.11. *Sia* $p = 2^{4q+1} - 1$ *un primo, allora uso la sequenza con equazione caratteristica associata* $x^2 - 4x + 1$ *e radici* $2 \pm \sqrt{3}$*. p divide* U_{p+1}*.*

In particolare il Lemma 2.11 è spaventosamente simile a quanto osserveremo nella Sezione 3.2 per costruire il test di Baillie-PSW; Lucas era sicuramente vicino al suo traguardo. Per altri esempi di questo tipo si veda [10].

Alcune osservazioni dell'articolo di Lucas sono estremamente interessanti, ad esempio nota dal seguente lemma che Mersenne avrebbe potuto possedere un risultato non distante dal piccolo teorema di Fermat.

Lemma 2.12. *Se* $4q + 3$ *e* $8q + 7$ *sono primi, allora* $2^{4q+3} - 1$ *ha come divisore* $8q + 7$*.*

Dimostrazione. Dal piccolo teorema di Fermat so che

$$2^{8q+6} - 1 \equiv 0 \mod 8q+7$$

e posso scomporre il primo membro in $\left(2^{4q+3}+1\right)\left(2^{4q+3}-1\right)$; ma 2 è residuo quadratico per i primi nella forma $8x + 7$ o $8x + 1$, quindi deve valere

$$2^{4q+3} - 1 \equiv 0 \mod 8q+7$$ □

Il lemma ci permette di costruire la seguente tabella:

q	$n = 4q + 3$ primo	$8q + 7$ divisore
2	11	23
5	23	47
20	83	167
32	131	263
44	179	359
47	191	383
59	239	479
62	251	503

Non abbiamo scelto questi n a caso, ed i nostri occhi non ci ingannano; si tratta di tutti e soli gli n nella forma $4q + 3$ minori di 258, esattamente la soglia della congettura di Mersenne.
Strumenti meno potenti sono necessari per lo studio di M_n con n relativamente piccolo: come detto, già Fermat aveva discusso su molti di loro, e così Eulero. A titolo di esempio, se volessimo cercare p divisore primo di $M_{11} = 2^{11} - 1$, avremmo che $2^{11} - 1 \equiv 1 \mod p$, ovvero che l'ordine di 2 in $\mathbb{Z}_p$ è 11. Questo implica, per fatti noti di teoria dei gruppi, $p - 1 \mid 11$. Abbiamo ottenuto che se tale divisore p esiste ha forma $p = k \cdot 11 + 1$, dove k è un intero pari - infatti se fosse dispari otterremmo p pari. Dopo pochi passaggi abbiamo ottenuto la fattorizzazione completa di M_{11}.

k	p	primo	fattore di M_{11}
2	p=23	sì	sì
4	p=45	no	no
6	p=67	sì	no
8	p=89	sì	sì

Fermat stesso aveva usato una procedura simile per M_{37}, dimostrandolo composto. Ma da dove deriva il grande interesse verso i numeri di Mersenne? Gli sforzi dei matematici nella storia possono essere in parte giustificati da motivi storici, ma derivano soprattutto dal seguente lemma.

Lemma 2.13. *Se un numero nella forma $a^n - 1$ è primo, allora $a = 2$ ed n è primo.*

Dimostrazione. Similmente a quanto visto nella dimostrazione del teorema di Cataldi (Teorema 2.3),

$$a^n - 1 = (a - 1)\left(a^{n-1}a^{n-2} + \cdots + a + 1\right) \tag{2.5}$$

quindi $a - 1 \mid a^n - 1$, e se $a^n - 1$ è primo questo implica $a - 1 = a^n - 1$ oppure $a - 1 = 1$. Il caso $a^n = a$ non ha senso per $n > 1$ ed $a \neq 1$, l'unica possibilità è $a = 2$. Il resto deriva dal teorema di Cataldi. □

Concludiamo ribadendo che Lucas ha svolto anche un importante opera di raccolta e studio dei risultati passati, ed il suo articolo, seppur con qualche errore ed un po' vago, porrà le basi per le ricerche successive.

2.3 Il test di Lucas-Lehmer

Verso il 1930, il teorico dei numeri americano D. H. Lehmer (1905 - 1991) costruisce per la sua tesi di dottorato una nuova formulazione del test di Lucas. Il test di Lucas-Lehmer, noto per essere estremamente veloce ed affidabile, non fornisce purtroppo alcuna informazione sui fattori di M_n se composto.

Teorema 2.14 (Test di Lucas-Lehmer, ca. 1930)**.** *Sia M_p il numero di Mersenne da testare per p primo. Definiamo la sequenza $\{s_i\}_{i\in\mathbb{N}}$ come*

$$s_i = \begin{cases} 4 & \text{per } i = 0 \\ s_{i-1}^2 - 2 & \text{altrimenti} \end{cases} \tag{2.6}$$

Allora M_p è primo se e solo se

$$s_{n-2} \equiv 0 \mod M_p \tag{2.7}$$

Non approfondiremo i motivi della scelta degli s_i in quanto estremamente dispersivi, basti notare che sono estremamente legati alle sequenze di Lucas della Sezione 1.4; infatti $s_k = {}^{V_{2^k}}\!/_{2^{(2^{k-1})}}$ dove V_k è il k-esimo elemento di una sequenza di Lucas con parametri $P = 2$, $Q = -2$. Un'ottima fonte a riguardo è la Sezione 8.2 di [23].

La sequenza 2.6 è detta **sequenza dei residui di Lucas-Lehmer**.[1] Possiamo sfruttare la seguente funzione in Python per calcolare $s_1, \ldots, s_k$:

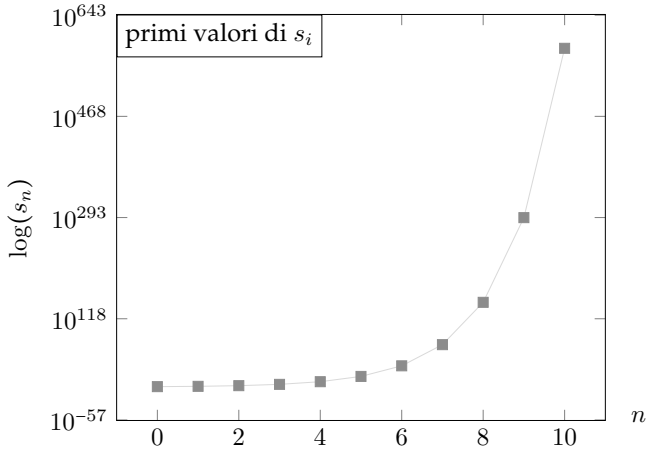
Codice 2.1: residui di Lucas-Lehmer

```
def LLresidual(k):                    1
    s = 4;                            2
    for i in range(1,k+1):            3
        s = (s*s-2)                   4
    return s                          5
```

ed eseguendola per i primi elementi otteniamo

4
14
194
37634
1416317954
2005956546822746114
4023861667741036022825635656102100994
16191462721115671781777559070120513664958590125499158514329308740975788034

[1] sequenza OEIS numero A003010



Notiamo un punto importante: la sequenza dei residui è *troppo* proibitiva da calcolare. Ma siccome l'equazione 2.7 richiede calcoli in aritmetica modulare, possiamo cogliere al volo l'opportunità e calcolare al posto di 2.6 la sequenza modulo M_p, ovvero

$$s_i = \begin{cases} 4 & \text{per } i = 0 \\ s_{i-1}^2 - 2 \mod M_p & \text{altrimenti} \end{cases} \tag{2.8}$$

dove M_p è il numero di Mersenne da testare. Ai nostri scopi la diremo **sequenza dei residui modulari**; si noti che per ben definirla modulo M_n basta restringersi ad un p dispari maggiore di 2, caso nel quale M_p è almeno 7.
Allora basta adattare un po' il codice:

Codice 2.2: residui modulari di Lucas-Lehmer

```
def LLmodresidual(k,n):                                    1
    # n needed to compute M_n = 2^n-1                      2
    s = 4                                                  3
    Mn = 2**n-1                                            4
    for i in range(1,k+1):                                 5
        s = (s*s-2) % Mn                                   6
    return s                                               7
```

Stavolta però dobbiamo contestualizzare la sequenza per un dato M_p. Proviamo ad esempio a calcolare le prime nove entrate per il famoso M_{19} di Cataldi.

$$4, 14, 194, 37634, 218767, 510066, 386344, 323156, 218526, \ldots$$

che sono numeri considerevolmente più maneggevoli di prima! Possiamo spingerci oltre e calcolare s_{17} per M_{19}:

```
In [20]: LLmodresidual(17,19)
Out[20]: 0
```

e questo ci dimostra che M_{19} è *sicuramente primo*; infatti il test di Lucas-Lehmer è **deterministico**. Non è difficile implementare addirittura una versione completa del test in Python:

Codice 2.3: test di Lucas-Lehmer

```
def LucasLehmer(n):                                    1
    # n exponent for M_n num. to test                  2
    s = 4                                              3
    Mn = 2**n-1                                        4
                                                       5
    for i in range(3,n+1):                             6
        s = (s*s-2) % Mn                               7
    text = "2^" + str(n) + " - 1 = " + str(Mn)         8
    if s == 0: return text + " is prime"               9
    else: return text + " is composite"                10
```

ed ora la possiamo sfruttare per verificare agevolmente alcuni risultati che hanno richiesto secoli di sforzi.

```
In [23]: LucasLehmer(31)
Out[23]: '2^31 - 1 = 2147483647 is prime'

In [24]: LucasLehmer(2221)
Out[24]: '2^2221 - 1 = [...] is composite'

In [25]: LucasLehmer(2281)
Out[25]: '2^2281 - 1 = [...] is prime'
```

Tuttavia si incorre molto presto in un problema di natura computazionale; già con $n = 86243$ il calcolatore impiega diversi minuti per riportare il risultato - e come se non bastasse M_{86243} ha "solo" ventiseimila cifre, una inezia in confronto alle decine di milioni di cifre attualmente in studio.

2.4 Dimostrazione del teorema di Lucas-Lehmer

In questa sezione dimostreremo il Teorema 2.14. Non è sempre facile trovare una dimostrazione del risultato, molte pubblicazioni lo riportano senza dimostrarlo o facendolo solo parzialmente. Sono degne di nota le dimostrazioni di

(i) Lehmer (1930), basata sulla teoria delle sequenze di Lehmer, in [11]

(ii) Rosen (1988), basata sui numeri algebrici, in [19]

(iii) Bruce (1993), semplifica la dimostrazione di Rosen sfruttando solo la teoria elementare dei gruppi, in [20]

Per la sufficienza ripercorreremo l'elegante dimostrazione di Bruce, mentre per la necessità seguiremo il ragionamento proposto da Rosen. Si tratta forse delle dimostrazioni più semplici del risultato, ma sorprendenti nella loro eleganza.

Teorema (Test di Lucas-Lehmer, ca. 1930)**.** *Sia M_p il numero di Mersenne da testare per p primo. Definiamo la sequenza $\{s_i\}_{i\in\mathbb{N}}$ come*

$$s_i = \begin{cases} 4 & \text{per } i = 0 \\ s_{i-1}^2 - 2 & \text{altrimenti} \end{cases} \tag{2.9}$$

Allora M_p è primo se e solo se $s_{n-2} \equiv 0 \mod M_p$.

Dimostrazione della necessità. Vale la pena iniziare ragionando sulla sequenza che utilizziamo: si tratta di una sequenza definita per ricorrenza ed in forma chiusa, che usando la stessa notazione di Bruce può essere definita tramite i due valori $\omega = 2 + \sqrt{3}$ e $\overline{\omega} = 2 - \sqrt{3}$. Infatti non è difficile dimostrare che

$$s_k = \omega^{2^k} + \overline{\omega}^{-2^k} \tag{2.10}$$

Procediamo per induzione: se $k = 0$ il risultato è ovvio, $\omega^1 + \overline{\omega}^1 = 2 + 2 = 4$. Per il passo induttivo invece

$$\begin{aligned} s_k = s_{k-1}^2 - 2 &= \left(\omega^{2^{k-1}} + \overline{\omega}^{-2^{k-1}}\right)^2 - 2 \\ &= \omega^{2^k} + \overline{\omega}^{2^k} + 2\left(\omega\overline{\omega}\right)^{2^{k-1}} - 2 = \omega^{2^k} + \overline{\omega}^{2^k} \end{aligned}$$

una volta verificato $\omega\overline{\omega} = 1$. Allora dall'Equazione 2.10 segue che 2.7 equivale a

$$\omega^{2^n} + \overline{\omega}^{-2^n} \equiv 0 \mod M_p \tag{2.11}$$

Ora possiamo procedere: dimostreremo che se la sequenza dell'Equazione 2.8 è tale che $s_{n-2} \equiv 0$ modulo M_p allora M_p è primo. Dall'equazione 2.11, riscrivendo,

$$\omega^{2^{n-2}} + \overline{\omega}^{-2^{n-2}} \equiv 0 \mod M_p$$

$$\omega^{2^{n-2}} + \overline{\omega}^{-2^{n-2}} = k \cdot M_p \quad (k \in \mathbb{Z})$$

e con semplici manipolazioni algebriche arriviamo ad ottenere

$$\omega^{2^{n-2}} = k \cdot M_p - \overline{\omega}^{-2^{n-2}}$$

$$\left(\omega^{2^{n-2}}\right)^2 = \omega^{2^{n-1}} = k \cdot M_p \cdot \omega^{2^{n-2}} - 1 \tag{2.12}$$

Notiamo inoltre che se M_p fosse composto non potrebbe avere un fattore pari, perché i numeri di Mersenne sono dispari - la verifica è elementare. Allora supponiamo per assurdo che M_p sia composto e scegliamo q suo più piccolo fattore primo; necessariamente $q > 2$. Definiamo inoltre l'insieme

$$X = \left\{ a + b\sqrt{3} \mid a, b \in \mathbb{Z}_q \right\} \tag{2.13}$$

su cui possiamo definire in modo evidente le operazioni di addizione e moltiplicazione. Verifichiamo subito che X è chiuso per moltiplicazione, basta scegliere dei rappresentanti come fossimo in $\mathbb{Z}[\sqrt{3}]$ e scrivere

$$(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd \mod q) + \sqrt{3}(ad + bc \mod 1)$$

Di questo insieme potremmo notare che

(i) rispetto all'addizione è un gruppo abeliano

(ii) rispetto alla moltiplicazione è un insieme commutativo ed associativo

(iii) essendo $q > 2$, X contiene sia ω che $\overline{\omega}$

Allora definiamo X^* come l'insieme degli elementi invertibili di X rispetto alla moltiplicazione, per quanto visto nella Sezione 1.3 sappiamo che è un gruppo e l'ordine dei suoi elementi è al più $q^2 - 1$; questo perché $0 \in X$ è (almeno) un elemento non invertibile.

$$|X^*| \leq |X| - 1 = q^2 - 1 \tag{2.14}$$

In parallelo, consideriamo ω come elemento di X. Allora prima di tutto

$$k \cdot n \cdot \omega^{2^{n-2}} \equiv 0 \quad (\text{in } X) \tag{2.15}$$

ed in secondo luogo, per ipotesi assunta, sappiamo che M_p è congruo a zero modulo p. Da 2.14 e 2.15 finalmente otteniamo che $\omega^{2^{n-1}} = -1$; questo implica che $\omega^{2^n} = 1$, quindi ω appartiene agli elementi invertibili di X e si vede facilmente che ha inverso $\omega^{2^{n-1}}$. Allora l'ordine di ω $\mathrm{ord}(\omega)$ divide 2^p, ma abbiamo appena visto che $\omega^{2^{n-1}} = -1$, quindi $\mathrm{ord}(\omega)$ non divide 2^{n-1}; $\mathrm{ord}(\omega)$ è esattamente 2^n. Siccome ω appartiene ad X^*, uniamo quanto osservato in

$$2^n \leq |X^*| \leq q^2 - 1 < q^2 \tag{2.16}$$

Sappiamo inoltre che q è un divisore di M_p ed è il suo minimo fattore primo, e quindi $q^2 \leq 2^n - 1$. Unendo questo a 2.16 arriviamo a notare che

$$2^n \leq q^2 - 1 < q^2 \leq 2^{n-1}$$

ed essendo giunti ad un assurdo possiamo rifiutare l'ipotesi che M_p abbia un minimo fattore primo; non avendone nessuno, è primo. □

Dimostrazione della sufficienza. Supponiamo M_p primo. Consideriamo di nuovo l'insieme dell'Equazione 2.13, ma stavolta modulo M_p. Svolgendo le operazioni modulo M_p, scrivendo $M_p = M$ per semplicità, si ottiene

$$\begin{aligned}(1+\sqrt{3})^M &\equiv 1^M + (\sqrt{3})^M \mod M \\ &\equiv 1 + (\sqrt{3})3^{\frac{M-1}{2}} \mod M\end{aligned}$$

Per legge di reciprocità quadratica (Teorema 1.13) sappiamo che $3^{\frac{M-1}{2}}$ è congruo a ± 1 modulo M. Inoltre sia M che 3 sono congrui ad 1 modulo 4, quindi sempre per reciprocità quadratica ho due casi: M è residuo modulo 3 oppure 3 è residuo modulo M, non entrambi. Però si verifica facilmente che $M \equiv 1$ modulo 3, quindi è residuo quadratico modulo 3. La seconda condizione non può avverarsi, perciò per proprietà del simbolo di Legendre $3^{\frac{M-1}{2}}$ è congruo a -1 modulo M. Sfruttando ω e $\overline{\omega}$ definiti nella dimostrazione precedente, ovvero $\omega = 2 + \sqrt{3}$ e $\overline{\omega} = 2 - \sqrt{3}$, otteniamo $(1+\sqrt{3})^2 = 2\omega$, che ci permette di riscrivere il precedente risultato:

$$(1+\sqrt{3})^{M-1} \equiv -2 \mod M$$

$$\begin{aligned}(2\omega)^{\frac{M-1}{2}} &\equiv -2 \mod M \\ &\equiv 2^{\frac{M+1}{2}} \omega^{\frac{M+1}{2}} \mod M \\ &\equiv 2 \cdot 2^{\frac{M-1}{2}} \omega^{\frac{M+1}{2}} \mod M\end{aligned}$$

Ora invece osserviamo che 2 è residuo quadratico per tutti i primi nella forma $\pm 1 \mod 8$, che è esattamente la forma di M, quindi $2^{\frac{M-1}{2}} \equiv 1 \mod M$ e

$$2\omega^{\frac{M+1}{2}} \equiv -2 \mod M$$

Sappiamo infine che 2 ammette un inverso modulo M, e questo inverso è esattamente $\frac{M+1}{2}$; ricordando anche che $M = 2^n - 1$ ricaviamo

$$\omega^{\frac{M+1}{2}} \equiv -1 \mod M$$

$$\omega^{2^{n-1}} \equiv \omega^{2^{n-2}}\omega^{2^{n-2}} \equiv -1 \mod M$$

e moltiplicando per $\overline{\omega}^{2^{n-2}}$ si ottiene $\omega^{2^{n-2}} + \overline{\omega}^{2^{n-2}} \equiv 0 \mod M$, che per l'Equazione 2.14 è esattamente la tesi. □

2.5 Deus ex machina: confutare Mersenne

Nel 1878 Lucas usa una formulazione iniziale di quello che diventerà il test di Lucas-Lehmer per verificare la primalità di M_{127}. Come abbiamo già ampiamente discusso, si tratta dell'inizio di una rivoluzione nella ricerca dei primi di Mersenne; per tre secoli nessuno si era mai nemmeno avvicinato a completare lo studio degli M_n per n minore di 258, ma in pochi decenni dalla pubblicazione dell'articolo di Lucas si arriverà a completare l'indagine fino al traguardo di Mersenne - e ben oltre.
Grazie al nuovo algoritmo di Lehmer ed all'alba dell'era informatica il problema si sposta: non si tratta più della ricerca del migliore strumento matematico per attaccare il problema, bensì della ricerca del programma più efficiente e del calcolatore più veloce.

Sappiamo che Lehmer stesso prova a testare gli M_n per $n = 139, 149, 257$ intorno al 1930, dimostrandoli composti dopo diverse centinaia di iterazioni del suo test. Vale la pena notare che a questo punto i calcoli sono ancora svolti con un calcolatore manuale, ed hanno richiesto rispettivamente 137, 147, 255 iterazioni.

Il test di Lucas-Lehmer è stato utilizzato nel 1934 dal matematico amatoriale statunitense Ralph Ernest Powers per dimostrare che M_{241} è composto; lo stesso Powers aveva sfruttato in precedenza alcune variazioni dell'algoritmo di Lucas per verificare la primalità di M_{105} ed M_{87} e dimostrare composti M_{103} ed M_{107}, anche se questi ultimi calcoli non sono mai stati verificati.

numero	anno	stato	dimostrato da	metodo	calcoli
M_{89}	1911	primo	R. E. Powers	*test di Lucas*	*manuali*
M_{103}	1914	composto	R. E. Powers	*test di Lucas*	*manuali*
M_{107}	1914	composto	R. E. Powers	*test di Lucas*	*manuali*
M_{109}	1914	primo	R. E. Powers	*test di Lucas*	*manuali*
M_{139}	1926	composto	D. H. Lehmer	*Lucas-Lehmer*	*manuali*
M_{149}	1932	composto	D. H. Lehmer	*Lucas-Lehmer*	*manuali*
M_{257}	1932	composto	D. H. Lehmer	*Lucas-Lehmer*	*manuali*
M_{241}	1934	composto	R. E. Powers	*Lucas-Lehmer*	*manuali*

Tabella 2.6: storia dei primi di Mersenne - V

Nonostante i calcoli fossero ancora svolti manualmente, la rivoluzione nella ricerca dei primi di Mersenne è dietro l'angolo.
Nelle tabelle smetteremo di elencare il numero di cifre di M_n a favore del metodo di calcolo - il motivo sarà chiaro quando introdurremo i calcolatori automatici - e scriveremo gli M_n in notazione compatta; un lettore attento avrà già notato che queste accortezze sembrano preannunciare una crescita esponenziale nel numero di cifre, ed in effetti è quanto ci stiamo preparando ad affrontare.

Nel 1949 il topologo inglese Maxwell Herman Alexander Newman sfrutta il prototipo di computer della Manchester Electronic per tentare di dare inizio alla ricerca automatizzata di primi di Mersenne; su quello stesso prototipo stava lavorando Alan Turing, che migliora l'algoritmo di Newman. Si tratta del *primo tentativo di ricerca di numeri primi tramite calcolatori elettronici*.

Un anno dopo, nel 1950, il *National Bureau of Standards* statunitense commissiona lo **Standards Western Automatic Computer** (SWAC) in attesa della costruzione del più potente Raytheon Digital Automatic Computer (RAYDAC), iniziata nel 1949 e conclusa nel 1953. Nonostante lo SWAC fosse un calcolatore di piccola scala, resterà il più potente computer al mondo fino all'anno successivo. Ci troviamo finalmente ad una svolta: il matematico statunitense Raphael Mitchel Robinson nel 1951 inizia a programmare SWAC per la ricerca di primi di Mersenne, e rimarcabilmente il programma ha funzionato al primo tentativo: il 30 gennaio 1952 Robinson scopre due nuovi primi di Mersenne, M_{521} ed M_{607}. In particolare dimostrerà false alcune affermazioni del matematico francese E. Fauquembergue, che riteneva di aver dimostrato primi M_{101} ed M_{107}. Dopo quasi trecento anni dalla sua formulazione, il range di valori della congettura di Mersenne è stato completamente verificato.

numero	anno	stato	dimostrato da	metodo	calcoli
M_{101}	1914	primo	E. Fauquembergue	*(incerto)*	-
M_{107}	1920	primo	E. Fauquembergue	*(incerto)*	-
M_{521}	1952	primo	R. M. Robinson	*Lucas-Lehmer*	*SWAC*
M_{607}	1952	primo	R. M. Robinson	*Lucas-Lehmer*	*SWAC*
~~M_{101}~~	1952	composto	R. M. Robinson	*Lucas-Lehmer*	*SWAC*
~~M_{107}~~	1952	composto	R. M. Robinson	*Lucas-Lehmer*	*SWAC*

Tabella 2.7: storia dei primi di Mersenne - VI

Lo SWAC verifica anche i risultati precedenti, e quando viene messo all'opera su M_{127} Lehmer - dopo aver speso giorni a svolgere calcoli per lo stesso risultato - vede una macchina completarli in 48 secondi.[2]
In seguito Lehmer afferma che sono necessari circa $(n/100)^3$ secondi di calcoli tramite SWAC per verificare se M_n sia primo, e stima che un minuto di lavoro di SWAC equivalga ad un anno di calcoli manuali. In soli tredici minuti il calcolatore verifica M_{1279} come primo, completando lo studio dei numeri di Mersenne per esponente minore di 2304.[3]

[2]In realtà è marginalmente incorretto affermare che prima di ora si usassero solo calcoli manuali in senso stretto, all'epoca infatti erano disponibili calcolatori da scrivania.
[3]I dati presentati in questo paragrafo derivano da [13].

I primi di Mersenne cresceranno con lo sviluppo dei calcolatori elettronici.
Il matematico Hans Ival Riesel usa il calcolatore svedese *Binär Elektronisk SekvensKalkylator* per studiare gli M_n per n compreso tra 2300 e 3300, trovando nel 1957 il primo M_{3217}.
Nei primi anni '60 Alexander Hurwitz, Sidney Kravitz e Murray Berg usano l'*IBM 7090* per n compreso tra 3000 e 7000. Hurwitz diventa lo scopritore dei primi due **numeri primi titanici**, ovvero con almeno diecimila cifre decimali.

numero	anno	stato	dimostrato da	metodo	calcoli
M_{1279}	1952	primo	R. M. Robinson	*Lucas-Lehmer*	SWAC
M_{3217}	1957	primo	H. I. Riesel	*Lucas-Lehmer*	BESK
M_{4253}	1961	primo	A. Hurwitz	*Lucas-Lehmer*	IBM 7090
M_{4423}	1961	primo	A. Hurwitz	*Lucas-Lehmer*	IBM 7090

Tabella 2.8: storia dei primi di Mersenne - VII

Dovrebbe ormai essere chiaro che la ricerca dei primi di Mersenne ha suscitato grande interesse; da questo punto, grazie all'esponenziale crescita della capacità computazionale dei computer, il problema - inizialmente di natura matematica - è andato gradualmente a rappresentare una sfida all'algoritmo ed al calcolatore migliore. I risultati ottenuti nel corso del tempo sono davvero troppi per essere affrontati singolarmente e con dovizia di dettagli, basti sapere che fino ad ora sono stati trovati oltre cinquanta numeri primi di Mersenne. Raccoglieremo i risultati in una tabella conclusiva a fine capitolo.

Di notevole interesse è la **Great Internet Mersenne Prime Search** (GIMPS), un progetto che si basa sul calcolo distribuito fondato nel 1996 dall'informatico statunitense George Woltman. Volontari in tutto il mondo possono iscriversi al progetto e sfruttare parte della capacità di calcolo del proprio computer per contribuire alla ricerca di primi di Mersenne incredibilmente grandi; attualmente (maggio 2021) GIMPS ha avuto 17 successi. Da luglio 2020 ad ora, il cinquantunesimo e più grande primo di Mersenne (e non) trovato è $M_{82\,589\,933}$ con lo straordinario numero di ventiquattro milioni di cifre decimali.

GIMPS sfrutta l'algoritmo di Lucas-Lehmer unito a diversi trucchi, quali una fase di trial division ed un crivello di Eratostene costruito gradualmente, per eliminare rapidamente potenziali composti e risparmiare capacità computazionale; questa combinazione è ideale nei calcolatori ad architettura binaria per la natura delle operazioni richieste da Lucas-Lehmer, ovvero per i calcoli dell'Equazione 2.8. Dal 2017 GIMP ha iniziato ad implementare anche alcune iterazioni del test di Fermat (si veda la Sezione 3.1), ed è rimarcabile notare come per rendere i calcoli estremamente efficienti le operazioni necessarie siano scritte in linguaggio assembly ed operino tramite una *fast fourier transform*.
Fino al 2020 è stato però necessario verificarli più volte - almeno due per ogni numero di Mersenne testato - a causa di possibili errori di hardware, ma dal 2020 GIMP implementa un algoritmo di Krzysztof Pietrzak ([28]) che fornisce certificati di primalità.
Per altre informazioni di natura matematica è possibile visitare il sito [33], che spiega dettagliatamente il processo utilizzato.

Con tutto ciò che abbiamo visto in questo capitolo, viene naturale tornare indietro e riflettere su ciò che ha dato origine all'interesse verso i primi di Mersenne; si tratta discutibilmente della fantomatica **congettura di Mersenne**.

Congettura (di Mersenne)**.** *Tra tutti i numeri di Mersenne M_n con n minore di* 258*, sono primi di Mersenne solo gli M_n per*

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

Questa ha suscitato molto scalpore all'epoca, quando nessuno era ancora riuscito ad affermare nulla per n maggiore di 19. Possiamo dire di aver compiuto passi da gigante da allora, ed in retrospettiva è possibile correggere l'affermazione di Mersenne.

Congettura (corretta di Mersenne)**.** *Tra tutti i numeri di Mersenne M_n con n minore di* 258*, sono primi di Mersenne solo gli M_n per*

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$$

Un certo senso di superiorità verso l'affermazione di Mersenne è giustificato, ma non dobbiamo dimenticare l'enorme aiuto ricevuto dall'avvento dell'era informatica, e non possiamo nemmeno ignorare il grande debito che nutriamo verso Mersenne e chi nella sua epoca ha usato quanto aveva a disposizione per arrivare a dei risultati tanto sorprendenti.
Concludiamo il capitolo introducendo la "nuova congettura di Mersenne", che cerca di estendere lo spirito dell'originale a tutti gli esponenti interi positivi.

Congettura 2.15 (di Bateman-Selfridge-Wagstaff, 1989)**.** *Sia p un intero positivo dispari; se due delle seguenti condizioni valgono, allora vale anche la terza:*

(i) $p = 2^k \pm 1$ *oppure* $p = 4^k \pm 1$ *per k intero positivo*

(ii) $M_p = 2^p - 1$ *è un primo (**primo di Mersenne**)*

(iii) $W_p = \frac{2^p+1}{3}$ *è un primo (**primo di Wagstaff**)*

Possiamo già azzardare qualche osservazione. Innanzitutto sembra vero affermare che questa congettura corregga gli errori noti dell'originale, difatti 67 e 257 - erroneamente elencati in Mersenne - hanno forma

$$67 = 2^6 + 3$$
$$257 = 2^8 + 1$$

e soddisfano il punto (i), ma è noto da calcoli che non soddisfano (ii) e (iii). Altrettanto interessante è che, come la congettura originale, questa non consideri 89 e 107; soddisfano (ii) ma nessuna delle altre due proprietà. Notiamo infine che se p è composto sicuramente (ii) non vale per Teorema 2.3, e similmente è possibile dimostrare che (iii) non vale. La nuova congettura di Mersenne deve essere solo testata sui p primi dispari positivi. La sequenza di tali p che soddisfano almeno una condizione è archiviata come sequenza OEIS A120334:

$$3, 5, 7, 11, 13, 17, 19, 23, 31, 43, 61, 67, 79, 89, 101,$$
$$107, 127, 167, 191, 199, 257, 313, 347, 521, 607, \ldots$$

Analogamente, la sequenza OEIS A107360 contiene i p individuati che soddisfano tutte le tre condizioni:

$$3, 5, 7, 13, 17, 19, 31, 61, 127$$

Fino alla stesura di questo testo non sono stati trovati controesempi, ovvero casi in cui due proprietà della congettura valgano ma la terza no; si ipotizza che non ne esistano, in quanto le proprietà sono costruite ad hoc per evitare controesempi tramite uno studio dei dati noti. Il prossimo termine della serie - se esiste - non può essere nessun esponente noto di un primo M_p di Mersenne o di un primo W_p di Wagstaff.

"Ero presente quando John Selfridge ha enunciato per la prima volta questa congettura. Le sue osservazioni includevano l'affermazione relativamente banale che la congettura fosse ovviamente vera, che conoscessimo tutti i casi veri e che fosse impossibile dimostrarla; è chiaro anche in termini probabilistici molto vaghi che M_p e W_p sono contemporaneamente primi solo un numero finito di volte. [...] John stesso afferma che la congettura è solo una curiosa e minore coincidenza."

(R. D. Silverman, [32])

Il sito [30] contiene una lista dei valori fino ad ora studiati.

numero	numero cifre	anno	dimostrato da	calcoli
M_{521}	157	1952	R. M. Robinson	SWAC
M_{607}	183	1952	R. M. Robinson	SWAC
$M_{1\,279}$	386	1952	R. M. Robinson	SWAC
$M_{2\,203}$	664	1952	R. M. Robinson	SWAC
$M_{2\,281}$	687	1952	R. M. Robinson	SWAC
$M_{3\,217}$	969	1957	H. I. Riesel	BESK
M_{4423}	1332	1 961	A. Hurwitz	IBM 7090
$M_{1\,398\,269}$	420 921	1996	Armengaud, Woltman	GIMPS
$M_{2\,976\,221}$	895 932	1997	Spence, Woltman	GIMPS
$M_{6\,972\,593}$	2 098 960	1999	Harjatwala, Woltman	GIMPS
$M_{13\,466\,917}$	4 053 946	2001	Cameron, Woltman	GIMPS
$M_{30\,402\,457}$	9 152 052	2005	Cooper, Boone, Woltman	GIMPS
$M_{57\,885\,161}$	17 425 170	2013	Cooper, Woltman	GIMPS
$M_{82\,589\,933}$	24 862 048	2018	Laroche, Woltman	GIMPS

Tabella 2.9: alcuni dei più grandi primi di Mersenne dall'avvento dell'era informatica in poi, divisi per anno

Siccome tutti gli algoritmi utilizzati sono variazioni di Lucas-Lehmer, torniamo piuttosto a sfruttare lo spazio per elencare il numero di cifre di ogni primo e sottolineare lo straordinario progresso nella ricerca. Ad onor del vero, avremmo dovuto inserire *et al.* affianco a tutti i primi associati a GIMPS, sottolineando il contributo di ben più di un paio di personaggi, ma siamo limitati dallo spazio a disposizione. Per un elenco più completo si veda [29], da cui abbiamo preso parte dei dati.
Chiaramente non sono sempre stati scoperti in ordine crescente, e di per sé anche solo definire quando sia avvenuta la scoperta è una questione complessa; alcuni autori preferiscono inserire la data in cui una macchina ha effettuato il calcolo, altri quella in cui un umano ha preso nota del risultato.

Capitolo 3

Il test di Baillie-PSW

"Per interi positivi con forme particolari, tra cui i più famosi sono i numeri di Mersenne $2^p - 1$ con p primo, esistono test di primalità abbastanza rapidi. Ma interi arbitrariamente grandi sfidano anche i più potenti computer quando testati con metodi convenzionali"

MICHAEL OSER RABIN

Lucas non ha solo presentato al mondo lo spettro del test di Lucas-Lehmer, ma anche l'ombra di quello che diventerà uno dei test di primalità più importanti in assoluto. Presenteremo il **test di Baillie-PSW**, ma necessiteremo prima dei test di Fermat e Lucas fortificati; capiremo cosa sia un test "fortificato" e come questi due algoritmi possano essere usati per costruire il mastodontico test Baillie-PSW. Concluderemo con alcune osservazioni ed applicazioni.

Siccome tratteremo di test probabilistici non parleremo più di *teoremi* ma di *algoritmi*. Modificando l'enunciato sarebbe sicuramente possibile rendere l'algoritmo un teorema vero e proprio, ma riteniamo importante sottolineare la differenza tra la costruzione teorica di un teorema e quella di un algoritmo.

3.1 Le basi: il test probabilistico di Fermat

Tra i due test "meno forti" che utilizzeremo per costruire Baillie-PSW, il test di Fermat è il più semplice da formulare. Abbiamo gà visto il teorema 1.9:

Teorema (Piccolo teorema di Fermat)**.** *Sia p primo, a intero qualunque,*

$$a^{p-1} \equiv 1 \mod p \tag{3.1}$$

L'inverso di questo teorema è falso, ad esempio $561 = 3 \cdot 11 \cdot 17$ è composto ma si verifica facilmente con un calcolatore che

$$13^{560} \equiv 1 \mod 561$$

Tuttavia invertendolo logicamente possiamo costruire un test di primalità: se esiste un intero a in $\mathbb{Z}_p^*$ per cui non valga l'Equazione 3.1, allora p non può essere primo. Possiamo formulare questa idea in termini algoritmici.

Algoritmo 3.1 (Test di Fermat)**.** *Sia n un intero positivo, scelgo un a in $\mathbb{Z}_n^*$; se $a^{n-1} \equiv 1 \mod n$ allora n è probabilmente primo (**Fermat probable prime**).*

Chiaramente è un test probabilistico, ovvero se un numero passa il test non siamo certi che sia primo, ma possiamo associarvi una probabilità. L'insieme degli pseudoprimi del test di Fermat sotto una data base a, per ragioni storiche,

viene detto $\mathrm{fpsp}(a)$. Esistono $882\,206\,716$ primi minori di $2 \cdot 10^{10}$, e nello stesso range vi sono $882\,226\,401$ elementi di $\mathrm{fpsp}(2)$: il test di Fermat in base 2 ha solo $19\,685$ falsi positivi (pseudoprimi). Il matematico Henri Cohen lo ha definito un *"industrial grade primality test"* proprio per questa ragione.
Ma è possibile affinarlo?

Un'idea per migliorare il test potrebbe essere iterarlo k volte, ovvero scegliere k basi a_i diverse e ripeterlo per ciascuna di esse. Purtroppo esistono degli pseudoprimi del test di Fermat che restano tali per ogni possibile scelta della base a: questi sono detti **numeri di Carmichael** a causa del lavoro dello statunitense Robert Carmichael in [7], che nel 1910 fornisce il primo esempio di tale numero: 561. Il matematico tedesco Alwin Korselt aveva in precedenza formulato un criterio per individuarli, ma non ha mai fornito un esempio.

Teorema 3.2 (Criterio di Korselt)**.** *Un intero positivo N è numero di Carmichael se e solo se è libero da quadrati*[1] *e per ogni primo p che appare nella sua fattorizzazione*

$$p - 1 \mid N - 1 \tag{3.2}$$

Dimostrazione. Si veda la dimostrazione originale in [7]. □

I numeri di Carmichael costituiscono un duro ostacolo per il test di Fermat, e non uno che è possibile ignorare: infatti sono infiniti. Tra i primi a congetturare questo risultato vi è Paul Erdös, e verrà dimostrato nel 1994 da C. Pomerance, A. Granville e W. R. Alford in "*There are Infinitely Many Carmichael Numbers*".

Teorema 3.3 (Pomerance, Granville, Alford, 1994)**.** *Esistono infiniti numeri di Carmichael, inoltre per n abbastanza grande ve ne sono circa $n^{2/7}$ compresi tra 1 ed n.*

Il loro articolo originale è reperibile in [21]: dopo una breve introduzione storica sfruttano risultati di teoria dei gruppi e di analisi matematica per arrivare a dimostrare il teorema.
Ora che possiamo caratterizzarli e sappiamo che sono infiniti possiamo scrivere la sequenza dei numeri di Carmichael, registrata in OEIS come A002997:

$$561, 1105, 1729, 2465, 2821, 6601, 8911, \ldots$$

Ormai è chiaro che il test di Fermat non sia sufficientemente forte, necessitiamo di un risultato più potente se vogliamo un margine accettabile di sicurezza.
Si hanno nuovi sviluppi solo nel 1975, quando il matematico statunitense Gary Lee Miller scrive la sua tesi di dottorato "*Riemann's Hypothesis and Tests for Primality*" [34], nella quale formula un test di primalità che è deterministico sulla condizione che l'ipotesi di Riemann sia valida. Questa condizione nel momento in cui stiamo scrivendo - e forse per molto tempo a venire - non potrà essere soddisfatta, ma solo accettata sotto osservazioni empiriche.

L'informatico israeliano Michael Oser Rabin nel 1980 si basa sul lavoro di Miller per costruire un test probabilistico, il famoso **test di Miller-Rabin**, che non richiede tale ipotesi ed è notevolmente più veloce; si veda "*Probabilistic algorithm*

[1] Un intero libero da quadrati (*squarefree*) non contiene due volte lo stesso primo nella sua fattorizzazione; ad esempio $75 = 5 \cdot 5 \cdot 3$ non è libero da quadrati.

for testing primality" in [18]. [2] Nonostante non sia più deterministico, l'algoritmo è comunque straordinariamente affidabile e può essere interpretato come una sorta di "estensione" del test di Fermat, che nonostante la sua affascinante semplicità presentava i problemi di cui abbiamo discusso. Di fatto ci si riferisce spesso al test di Miller-Rabin come "*test di Fermat fortificato*".

Algoritmo 3.4 (Test di Miller-Rabin, 1980)**.** *Sia n un intero positivo dispari di cui vogliamo testare la primalità, prendiamo s la valutazione p-adica di 2 in $n-1$, ovvero dobbiamo riuscire a scrivere*

$$n = 2^s m + 1 \tag{3.3}$$

con m dispari. Un'iterazione del test è composta dalle seguenti fasi:

(i) *scelta di una base a intera positiva minore di n*

(ii) *se vale una delle seguenti proprietà, allora n è un primo probabile*

(a) $a^m \equiv 1 \mod n$

(b) $a^{2^r m} \equiv -1 \mod n$ *per un certo r naturale minore di s*

Notiamo che il calcolo della valutazione 2-adica richiede semplicemente di provare a dividere il numero pari $n-1$, un calcolo non eccessivamente dispendioso. Non entreremo nei dettagli della dimostrazione - reperibile in [18] - in quanto non costruttiva, ma possiamo comunque apprezzare le due proprietà utilizzate: Rabin spiega che la prima è un semplice test di Fermat, mentre la seconda equivale a richiedere che le uniche soluzioni di $x^2 \equiv 1 \mod n$ siano ± 1. Per ogni iterazione, se n passa almeno una delle due proprietà il valore a associato viene detto *testimone forte di primalità*.

Come preannunciato, possiamo quantificare la probabilità che un numero composto passi il test fortificato; in quel caso parleremo di **pseudoprimo forte** - ed analogamente, in caso di successo del test, di **primo probabile forte**. Esattamente come prima, diremo uno pseudoprimo del test di Fermat fortificato sotto una data base a è detto $\mathrm{sfpsp}(a)$, dove con "Fermat fortificato" possiamo intendere una singola iterazione di Miller-Rabin.

Teorema 3.5. *Il numero di basi a per cui un intero n composto passa l'iterazione associata ad a del test Miller-Rabin è al massimo $1/4$. Allora se n passa k iterazioni*

$$\mathcal{P}\,(n \text{ primo probabile forte} \mid n \text{ composto}) \leq \frac{1}{4^k} \tag{3.4}$$

Questo teorema è stato studiato da Monier in [16] nel 1980, dove confronta il test di Miller-Rabin con il test di Solway-Strassen:

"*Il nostro lavoro mostra che il primo algoritmo è sempre più efficiente del secondo, sia a livello probabilistico che computazionale.*"

(Monier, *Evaluation and Comparison of Two Efficients Probabilistic Primality Testing Algorithms*, sommario)

[2] In letteratura viene detto anche "*di Rabin-Miller*" per sottolineare come sia stato Rabin a renderlo il test che vediamo oggi; abbiamo scelto di attribuire paternità al risultato in ordine temporale, esattamente come fatto per in precedenza per il test "*di Lucas-Lehmer*".

Di fatto il test Miller-Rabin ha una complessità computazionale estremamente bassa - addirittura polonomiale! - ed una affidabilità notevole; merita a tutti gli effetti l'importanza che gli viene attribuita.

Alla fine del suo articolo Rabin suggerisce come implementare il test, con alcuni accorgimenti come una fase iniziale di trial division per interi minori di un certo N, ad esempio $N = 1000$. Possiamo, come ormai è abitudine, pensare di implementare il test in Python.

Codice 3.1: valutazione 2-adica

```
def two_adic(n):
    s = 0
    if n % 2 == 1:
        return n,0
    while True:
        n,s = n/2, s + 1
        if (n == 1) or (n%2 != 0):
            break
    return int(n),s
```

L'algoritmo per la valutazione 2-adica restituisce una lista di valori: il primo è m dell'Equazione 3.3, il secondo è s. Abbiamo tutto il necessario per svolgere k iterazioni del test sul numero intero n.

Codice 3.2: test di Miller-Rabin

```
from random import randint

def MillerRabin(n,k):
    m,s = two_adic(n−1)
    for i in range(1,k):
        a = randint(1,n−1)
        pass_testone = (pow(a,m,n) == 1)
        pass_testtwo = False
        for r in range(0,s):
            if(pow(a,(2**r)*m,n) == n−1):
                pass_testtwo = True
                break
        if(not (pass_testone or pass_testtwo)):
            return "composto"
    return "probabilmente primo, certezza: (1/4)^" + str(k)
```

3.2 Le basi: il test probabilistico di Lucas

Esistono moltissime formulazioni del test probabilistico di Lucas, che differiscono per peso delle richieste e potenza; spesso si basano sul Teorema 1.24.
Baillie e Wagstaff nel 1980 pubblicano l'articolo "*Lucas Pseudoprimes*" ([15]), in cui cercano di migliorare una famosa formulazione del test di Lucas; ci concentreremo particolarmente su questa e seguiremo in parte i loro passi.
Da qui in poi saranno fondamentali gli strumenti della Sezione 1.4, in particolare l'Osservazione 1.19

Definizione 3.6. *Dati dei parametri interi $P > 0$ e Q qualsiasi, detto D il discriminante dell'equazione caratteristica associata ad $U(P,Q)$ e $V(P,Q)$, diciamo*

$$\delta(n) = n - \left(\frac{D}{n}\right) \tag{3.5}$$

dove $\left(\frac{D}{n}\right)$ è il simbolo di Legendre-Jacobi, d'ora in poi scritto come $\varepsilon(n)$ per mantenere la notazione di Baillie e Wagstaff.

Teorema 3.7 (Teorema di Lucas)**.** *Siano dati P e Q interi positivi tali che il discriminante D dato dall'Equazione 1.18 sia non nullo. Se n è primo, allora*

$$U_{\delta(n)} \equiv 0 \mod n \tag{3.6}$$

Dimostrazione. Segue immediatamente dal Teorema 1.26 che

$$\alpha^{n-\varepsilon(n)} \equiv \begin{cases} 1 \mod n & \text{se } \varepsilon(n) = 1 \\ Q \mod n & \text{se } \varepsilon(n) = -1 \\ P \mod n & \text{se } \varepsilon(n) = 0 \end{cases} \tag{3.7}$$

ed una espressione identica vale per $\beta^{n-\varepsilon(n)}$. Siccome per l'Osservazione 1.19 possiamo scrivere $U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}$ con k intero dato, otteniamo facilmente la tesi. Il denominatore di U_k è ben definito e non-nullo per ipotesi. □

Invertendo logicamente il Teorema 3.7 otteniamo il seguente algoritmo.

Algoritmo 3.8 (Test probabilistico debole di Lucas)**.** *Sia n intero positivo dispari da testare, se esistono P e Q tali che valga l'Equazione 3.6 allora lo diciamo essere un primo probabile. In particolare, se scelgo P e Q tali che $\left(\frac{D}{n}\right) = -1$ il criterio da soddisfare diventa*

$$U_{n+1} \equiv 0 \mod n \tag{3.8}$$

L'insieme degli pseudoprimi del test debole di Lucas sotto i parametri P e Q viene detto $\mathrm{lpsp}(P,Q)$. Baillie e Wagstaff studiano la costruzione di un test più forte partendo dagli stessi principi teorici; si ispireranno al test di Eulero fortificato, che non tratteremo, ma l'idea della costruzione è estremamente simile a quella dietro la fortificazione del test di Fermat.

Algoritmo 3.9 (Test probabilistico forte di Lucas)**.** *Siano dati P e Q interi positivi tali che D discriminante dato dall'equazione 1.18 sia non nullo. Sia n l'intero da testare con D ed n coprimi. Una volta fattorizzato $\delta(n) = 2^s d$ con s valutazione 2-adica di $\delta(n)$, se vale almeno una delle seguenti*

(i) $U_d \equiv 0 \mod n$

(ii) $V_{2^r d} \equiv 0 \mod n$ *per un $r < s$ positivo*

diciamo n essere ***primo probabile forte****.*

La costruzione del test è laboriosa e non costruttiva, rimandiamo a [15] per ulteriori dettagli.
Come prima, l'insieme degli pseudoprimi forti di Lucas sotto i parametri P e Q viene detto $\mathrm{slpsp}(P,Q)$. Possiamo notare che se n appartiene a $\mathrm{slpsp}(P,Q)$ allora è anche in $\mathrm{lpsp}(P,Q)$. Per analogia alla famiglia dei test di Fermat, spesso ci si riferisce a (P,Q) come **base del test**.

Teorema 3.10 (Prima formula di Arnault, 1997)**.** *Siano D un intero fissato ed n un intero composto diverso da 9 e coprimo con $2D$. Definiamo*

$$\mathrm{SL}(n, D) \coloneqq \#\left\{(P, Q) \in \mathbb{Z}^2 \mid (\mathrm{i}), (\mathrm{ii}), (\mathrm{iii}), (\mathrm{iv})\right\} \tag{3.9}$$

dove abbiamo denotato le proprietà

(i) $0 \leq P, Q < n$

(ii) $\gcd(n, Q) = 1$

(iii) $P^2 - 4Q \equiv D \mod n$

(iv) $n \in \mathrm{slpsp}(P, Q)$

Si può dimostrare che $\mathrm{SL}(n, D) \leq {}^{4n}/_{15}$*, a meno che n non sia prodotto di primi gemelli soddisfacenti alcune proprietà. In quel caso qualcosa può ancora essere detto, ma il risultato diventa più complesso.*

Teorema 3.11 (Seconda formula di Arnault, 1997)**.** *Siano D ed n interi qualunque, è sempre vero che* $\mathrm{SL}(n, D) \leq {}^{n}/_{2}$*.*

Rimandiamo all'articolo di Arnault ([22]) per ulteriori dettagli e le dimostrazioni. Soffermandoci sulle proprietà elencate nel Teorema 3.10 possiamo notare che la proprietà (iii) caratterizza la scelta di P e Q partendo da D fissato, (i) e (ii) invece sono uno dei modi possibili per limitare la scelta dei parametri (P, Q). Esistono diversi pareri sulla loro opportuna scelta; al contrario del test di Miller-Rabin, non esiste un buon range prefissato in cui trovarli. Entreremo in seguito nei dettagli di questa scelta e ne discuteremo le motivazioni. Siamo quasi arrivati al nostro traguardo.

3.3 Costruire un test più forte

Il test di Baillie-PSW prende nome dai matematici statunitensi Robert Baillie, Samuel S. Wagstaff, Carl Pomerance e John L. Selfridge, ; i primi due l'hanno formulato nel 1980 ([15]), Wagstaff Pomerance e Selfridge l'hanno perfezionato in seguito ([17]). Si noti che esistono diverse formulazioni dell'Algoritmo 3.9, portando a diversi tipi di test Baillie-PSW. Può essere interessante illustrare Baillie-PSW alla maniera di F. Arnault, ovvero partendo dal test di Fermat. Prendiamo un elemento a piacere di $\mathrm{fpsp}(2)$ - sequenza OEIS A001567 - come ad esempio $n = 341$; si tratta di uno pseudoprimo di Fermat, ovvero un composto che lo passa. Ma possiamo costruire un test di Lucas che lo valuti come composto, difatti basta scegliere

$$D = -7, P = 1, Q = 2$$

ed usare l'Algoritmo 3.8. In seguito sarà possibile capire come abbiamo barato, ovvero come abbiamo scelto i parametri senza colpo ferire. Siccome $\varepsilon(n) = -1$, per ottenere n primo dobbiamo verificare che $U(1, 2)_{n+1} \equiv 0 \pmod n$; questa è la sequenza OEIS A107920, e se "prendiamo in prestito" la tabella dei valori computati ed utilizziamo uno strumento per calcolare il residuo modulare otteniamo 177. Il test probabilistico di Lucas ha effettivamente salvato il test

di Fermat dal cadere in fallo, e questo non sembra essere un caso. Arnault in realtà aveva usato un numero a 397 cifre, ma noi non avremmo spazio sufficiente neanche nel margine della pagina.
Come già noto, il test di Fermat non è esente da problematiche; i numeri di Carmichael ne sono un doloroso (ed infinito) memento. Leggiamo in [15] il seguente teorema.

Teorema 3.12. *Sia dato $n = p_1^{e_1} \dots p_m^{e_m}$ un intero positivo qualsiasi, il numero di basi $a \pmod n$ per cui n appartiene a $\mathrm{fpsp}(a)$ è*

$$\prod_{j=1}^{m} \gcd(n-1, p_j - 1)$$

Da questo segue che ogni intero positivo dispari n è in $\mathrm{fpsp}(a)$ per almeno due basi a non banali - se non è una potenza di 3. Risulta inoltre interessante considerare anche il seguente risultato, sempre dalla stessa fonte.

Teorema 3.13. *Sia D un intero non-nullo fissato. Ogni intero positivo dispari n è in $\mathrm{lpsp}(P, Q)$ per almeno tre coppie (P, Q), dove il calcolo è parametrizzato da distinti valori di $P \pmod n$ e per Q tali che $P^2 - 4Q \equiv D \mod n$.*

La Sezione 5 di [15] sembra suggerire che esista un problema intrinseco ai test di primalità probabilistici: se i due eventi "n è in $\mathrm{fpsp}(a)$" e "n è in $\mathrm{fpsp}(b)$" fossero completamente indipendenti ci aspetteremmo di non incappare nei numeri di Carmichael.

> *"Queste osservazioni sembrano suggerire che sia meglio utilizzare due test probabilistici indipendenti, ovvero dove la probabilità che n sia primo probabile del primo non influenzi la quella che lo sia anche del secondo. In effetti, descriveremo un metodo che pare portare a ben più della mera indipendenza."*
>
> (Baillie e Wagstaff, *Lucas Pseudoprimes*, sez. 5)

Baillie e Wagstaff procedono per osservazioni empiriche, ed individuano due candidati per i test indipendenti che desiderano. Il test di Lucas - ad esempio - determina come composti tutti i primi 50 numeri di Carmichael per una scelta opportuna dei parametri iniziali. Riportano in seguito come i primi 21853 elementi di $\mathrm{fpsp}(2)$ siano stati scartati con successo dal test di Lucas.
Ora sorge una domanda: come scegliere P e Q? Se D fosse un quadrato $\pmod n$ otterremmo solamente una versione alternativa dell'Algoritmo 3.1.

$$\begin{aligned} D &\equiv k \mod n \\ P &\equiv k+2 \mod n \\ Q &\equiv k+1 \mod n \end{aligned}$$

$$U_{n-\varepsilon(n)} = U_{n-1} \equiv \frac{Q^{n-1} - 1}{Q - 1} \mod n$$

Approfondiremo la questione nell'Osservazione 3.17. Per aggirare questo problema è utile considerare $\varepsilon(n) = -1$, ed esistono diversi criteri di scelta per far sì che accada. Nel loro articolo Baillie e Wagstaff ne suggeriscono due:

(A) D viene preso come il primo elemento della sequenza $5, -7, 9, -11, 13, \ldots$ con $\varepsilon(n) = -1$, quindi $P = 1$ e $Q = {}^{(1-D)}/_{4}$

(B) D viene preso come il primo elemento della sequenza $5, 9, 13, 17, 21, \ldots$ con $\varepsilon(n) = -1$, quindi P è il primo dispari dopo $\sqrt{D}$ e $Q = {}^{(P^2-D)}/_{4}$

Il primo metodo, proposto da Selfridge, è il più utilizzato a livello storico. Nell'articolo è suggerita la seguente tabella per paragonarli:

valori minori di x che passano il test

$x =$	10^3	10^4	10^5	10^6	10^7	10^8
metodo (A)						
lpsp	2	9	57	219	659	1911
slpsp	0	2	12	58	178	505
metodo (B)						
lpsp	2	15	70	248	750	2119
slpsp	2	4	23	84	261	711
metodi (A) e (B) insieme						
lpsp	2	4	29	87	246	660
slpsp	0	1	5	17	49	125

Tabella 3.1: dimensioni degli insiemi di pseudoprimi per diversi criteri di scelta

Descriviamo il test di Baillie-PSW nella formulazione originale.

Algoritmo 3.14 (Test di Baillie-PSW)**.** *Sia n un intero positivo dispari da testare,*

(i) *prima di tutto se n è piccolo sfruttiamo altri algoritmi più semplici, ad esempio una fase iniziale di trial division*

(ii) *eseguiamo un test di Fermat fortificato per base 2 (Algoritmo 3.4), se n lo passa procediamo, altrimenti è in* $\mathrm{sfpsp}(2)$

(iii) *verificare se n è un quadrato (facoltativo)*

(iv) *scegliamo i parametri P e Q con il metodo (A) oppure (B), se n passa il test forte di Lucas (Algoritmo 3.9) è quasi sicuramente primo, altrimenti è in* $\mathrm{slpsp}(P, Q)$

Questa viene solitamente detta "versione forte di Baillie-PSW". Il punto (i) è fondamentale, soprattutto per valori di n minori di 1000 - o comunque vicini; infatti il test di Lucas fortificato perde efficienza in questo intervalli. Potrei in realtà implementare varie scorciatoie anche negli altri punti: ad esempio se trovassimo un D con $\varepsilon(n) = 0$ avremmo ottenuto un fattore di n e potremmo fermarci. Si noti che si potrebbe sostituire nel punto (ii) una qualunque base, ma la teoria sviluppata attorno al test classico di Baillie-PSW richiede $a = 2$.
Il punto (iii) verifica l'applicabilità del punto (iv); difatti se n fosse un quadrato di primo non potrei mai trovare D con $\varepsilon(n) = -1$. L'algoritmo (A) per la scelta di D è efficiente?

Lemma 3.15 (Valor medio per la scelta di D)**.** *Sia n un intero positivo non quadrato, il numero medio di D da provare per ottenere $\varepsilon(n) < 1$ è 1.790479091 con il metodo (A), 1.922741874 con il metodo (B).*

Seguono alcune osservazioni che rendono ottimale la scelta dei parametri; si veda [23] per approfondire.

Osservazione 3.16 (Il problema di Q)**.** *Come più volte detto, esistono diversi metodi per scegliere i parametri del test partendo da D. Non tutti i parametri portano ad un test di uguale efficienza , ed esiste un problema associato alla scelta di $Q = \pm 1$. Questo è legato all'ordine di $\alpha \pmod n$, che sicuramente esiste per Teorema 1.26, ed è un caso che genera una probabilità superiore alla norma di generare* ***pseudoprimi quadratici****, ovvero pseudoprimi del test di Lucas con*

$$U_{\delta(n)} \equiv 0 \pmod n \quad \textit{oppure} \quad V_{\delta(n)} \equiv 2Q^{\frac{1-\varepsilon(n)}{2}} \pmod n$$

La ricerca di pseudoprimi quadratici nei casi $Q = \pm 1$ mostra come siano estremamente più numerosi rispetto a tutti gli altri casi:

$Q=-1, P=$	2	3	4	5	6	7	8	9	10
$\mathrm{lpsp}(P,Q)$	50	28	63	28	47	41	26	40	36
$Q=+1, P=$	2	3	4	5	6	7	8	9	10
$\mathrm{lpsp}(P,Q)$	-	61	69	53	105	103	88	86	95
$Q=-2, P=$	2	3	4	5	6	7	8	9	10
$\mathrm{lpsp}(P,Q)$	5	0	2	1	2	2	4	0	10
$Q=+2, P=$	2	3	4	5	6	7	8	9	10
$\mathrm{lpsp}(P,Q)$	43	-	7	3	1	2	3	0	8

Tabella 3.2: numero di pseudoprimi di Lucas minori di 150 000 per diverse scelte di Q e P, dove "-" indica che D è un quadrato (quindi la teoria non si applica)

Osservazione 3.17 (Il problema del quadrato)**.** *Si definisce tale il problema che sorge ponendo $\varepsilon(n) = 1$; questo non necessariamente implica che D sia un quadrato $\pmod n$, ma aumenta la probabilità che avvenga. Infatti $\varepsilon(n)$ per n composto è un simbolo di Jacobi, ed ha vari modi di essere 1, mentre solo in uno di questi si ha che tutte le sue componenti sono 1 e quindi effettivamente D è invertibile.*
Ironicamente scegliere $\varepsilon(n) = 1$ sembra portare ad una quantità decisamente minore di pseudoprimi, ma rende il test di Lucas dipendente dal test di Fermat in base 2 - ed è esattamente questo che non vogliamo.

Riguardo l'Osservazione 3.16, Baillie e Wagstraff forniscono in [15] delle formulazioni alternative per i criteri (A) e (B) che forzano Q ad un valore diverso da ± 1.Se $D = 5$ i due metodi sono equivalenti.

(A*) Scelgo D, P, Q come da (A) ma se $Q = -1$ resetto i loro valori come segue:

$$P < -5, \; Q < -5$$

(B*) Scelgo D, P, Q come da (B) ma se $Q = +1$ resetto i loro valori come segue:

$$Q < -P + Q + 1, \; Q < -P + 2$$

Il test è ben posto, nel senso che se un intero maggiore di 1000 è primo verrà sempre accettato dal test. Baillie e Wagstaff affermano che il test non compie errori per $n < 25 \cdot 10^9$, e proseguono poi l'articolo fornendo ulteriori congruenze

modulari che è possibile utilizzare per costruirne una versione più rapida ed efficiente ; riportiamo gli enunciati da cui questi argomenti derivano, rimandando all'articolo per una trattazione ben più approfondita.

Chiaramente sarebbe possibile aggiungere altre congruenze ancora per tentare di migliorare il test, ma non sempre la complessità computazionale ripaga del lavoro svolto. Il lavoro straordinario di Baillie e Wagstaff (in primis) è stato utilizzare due test operanti su proprietà apparentemente "scorrelate" - nel senso probabilistico che abbiamo visto prima.

Lemma 3.18 (di Hugh Williams)**.** *Se n è primo, $\varepsilon(n) = -1$ e $\gcd(n, 2Q) = 1$ allora*

$$V_{n+1} \equiv 2Q^{\frac{n+1}{2}} \left(\frac{Q}{n}\right) \mod n^2 \tag{3.10}$$

Per n composto e $Q \neq \pm 1$ questa vale raramente.

Lemma 3.19 (Proprietà di divisione semplice delle sequenze di Lucas)**.** *Se n è un primo dispari e $\gcd(n, Q) = 1$*

(i) $V_{\delta(n)} \equiv 2Q^{\frac{1-\varepsilon(n)}{2}} \pmod n$

(ii) $U_n \equiv \varepsilon(n) \pmod n$

(iii) $V_n \equiv V_1 \equiv P \pmod n$

Lemma 3.20. *Sia n un primo, se $\gcd(n, Q) = 1$*

$$Q^{\frac{n+1}{2}} \equiv Q\left(\frac{Q}{n}\right) \pmod n \tag{3.11}$$

Si noti che se $Q = \pm 1$ questa congruenza è triviale, inoltre è facile da verificare con un calcolatore perché sfrutta dati utilizzati per calcolare V_{n+1}:

$$V_{n+1} = \left(V_{\frac{n+1}{2}}\right)^2 - 2Q^{\frac{n+1}{2}}$$

Concludiamo fornendo un'altra tra le tante possibili formulazioni possibili del test di Baillie-PSW, stavolta più forte.

Algoritmo 3.21 (Test fortificato di Baillie-PSW)**.** *Sia n un intero positivo dispari da testare, procediamo come segue e non necessariamente in questo ordine:*

(i) *svolgiamo una fase iniziale di verifiche elementari (ad esempio la trial division)*

(ii) *verifichiamo se n è in $\mathrm{sfpsp}(2)$*

(iii) *scegliamo D, P e Q con (A*) o (B*), verifichiamo se n è in $\mathrm{slpsp}(P, Q)$*

(iv) *verifichiamo la congruenza dell'Equazione 3.10*

(v) *verifichiamo la congruenza (i) del Lemma 3.19*

(vi) *verifichiamo la congruenza dell'Equazione 3.11*

Questo test, per la sua rimarcabile efficienza, viene ancora oggi utilizzato in una versione abbastanza simile all'originale in moltissimi linguaggi di programmazione; ad esempio l'algoritmo di verifica primalità della liberia Python `simpy` sfrutta una formulazione simile di Baillie-PSW - e non è sicuramente l'unico, altri esempi sono Java (classe `BigInteger` con metodo built-in `isProbablePrime`), Mathematica (funzione `PrimeQ`), SageMath (funzione `is_pseudoprime`) e molti altri ancora.

Lo scopo originale di Lucas è sempre stato quello di costruire un test di primalità efficiente per una certa classe di interi, e nel corso del nostro studio abbiamo visto i successi che la sua teoria ha avuto; esempio lampante è il test di Lucas-Lehmer per la classe dei numeri di Mersenne.
Nonostante Lucas non sia mai vissuto per vederlo, possiamo affermare che sia infine riuscito nella sua impresa. Infatti, seppur probabilistico, il test di Baillie-PSW - erede indiretto dei primi lemmi nell'articolo di Lucas - è diventato uno strumento efficace per lo studio della primalità della più grande classe di numeri interi: tutti.

Bibliografia

[1] Marin Mersenne. *Cogitata physico mathematica*. sumptibus Antonij Bertier, via Iacobea, 1644.

[2] B. Boncompagni. *Scritti: Il Liber Abbaci*. v. 1. Tip. delle Scienze Fisiche e Matematiche, 1857. URL: https://books.google.it/books?id=gvRFAAAAcAAJ.

[3] Edouard Lucas. "Théorie des Fonctions Numériques Simplement Périodiques". In: *Comptes Rendus Acad. sci. Paris* 83 (1876), pp. 1286–1288.

[4] P. Pépin. "Sur la formule $2^{(2^n)} + 1$". In: *Comptes rendus de l'Académie des Sciences de Paris* 85 (1877), pp. 329–333.

[5] Edouard Lucas. "Théorie des Fonctions Numériques Simplement Périodiques". In: *American Journal of Mathematics* 1.3 (1878), pp. 197–240. ISSN: 00029327, 10806377. URL: http://www.jstor.org/stable/2369311.

[6] Edouard Lucas. "Théorie des Fonctions Numériques Simplement Périodiques". In: *American Journal of Mathematics* 1.4 (1878), pp. 289–321. ISSN: 00029327, 10806377. URL: http://www.jstor.org/stable/2369373.

[7] R. D. Carmichael. "Note on a new number theory function". In: *Bulletin of the American Mathematical Society* 12 (1910), pp. 232–238. URL: https://www.ams.org/journals/bull/1910-16-05/S0002-9904-1910-01892-9/S0002-9904-1910-01892-9.pdf.

[8] R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha n \pm \beta n$". In: *Annals of Mathematics* 15.1/4 (1913), pp. 30–48. ISSN: 0003486X. URL: http://www.jstor.org/stable/1967797.

[9] R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha n \pm \beta n$ - part II". In: *Annals of Mathematics* 15.1/4 (1913), pp. 49–70. ISSN: 0003486X. URL: http://www.jstor.org/stable/1967798.

[10] Leonard E. Dickson. "History of the theory of numbers". In: (1919). URL: https://archive.org/details/historyoftheoryo01dick/page/398/mode/2up.

[11] D. H. Lehmer. "An extended theory of Lucas' functions". In: *Annals of Mathematics, 2nd Ser.* 31 (1930), pp. 419–448. URL: https://www.jstor.org/stable/1968235.

[12] A. E. Western. "On Lucas' and Pepin's tests for the primeness of Mersenne numbers". In: *London Math. Soc.* 7 (1932), pp. 130–137. URL: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/jlms/s1-7.2.130.

[13] A.H. Beiler. *Recreations in the Theory of Numbers: The Queen of Mathematics Entertains*. Dover Recreational Math Series. Dover Publications, 1964. ISBN: 9780486210964. URL: https://books.google.it/books?id=NbbbL9gMJ88C.

[14] Sidney Kravitz e Douglas Lind. "The theory of simply periodic numerical functions". In: *Fibonacci Association* (1969). traduzione in inglese dell'articolo di Lucas. URL: https://www.mathstat.dal.ca/FQ/Books/Complete/simply-periodic.pdf.

[15] Robert Baillie e Samuel S. Wagstaff Jr. "Lucas Pseudoprimes". In: *Mathematics of Computation* 35.152 (1980), pp. 1391–1417.

[16] L. Monier. "Evaluation and Comparison of Two Efficient Probabilistic Primality Testing Algorithms". In: *Theor. Comput. Sci.* 12 (1980), pp. 97–108.

[17] Carl Pomerance, J. L. Selfridge e Samuel S. Wagstaff Jr. "The pseudoprimes to $25 \cdot 10^9$". In: *Mathematics of Computation* 35.152 (1980), pp. 1391–1417.

[18] Michael O. Rabin. "Probabilistic algorithm for testing primality". In: *Journal of Number Theory* (1980).

[19] M. Rosen. "A proof of the Lucas–Lehmer test". In: *Amer. Math. Monthly* 95 (1988), pp. 855–856.

[20] J. W. Bruce. "A really trivial proof of the Lucas–Lehmer test". In: *Amer. Math. Monthly* 100 (1993), pp. 370–371.

[21] C. Pomerance, A. Granville e W. R. Alford. "There are Infinitely Many Carmichael Numbers". In: *Annals of Mathematics* 3.140 (1994), pp. 703–722. URL: https://math.dartmouth.edu/~carlp/PDF/paper95.pdf.

[22] F. Arnault. "The Rabin-Monier Theorem for Lucas Pseudoprimes". In: *Mathematics of Computation* 66.218 (1997), pp. 869–881. ISSN: 00255718, 10886842. URL: http://www.jstor.org/stable/2153902.

[23] David Bressoud e Stan Wagon. *A Course in Computational Number Theory*. Wiley, 2000.

[24] Paulo Ribenboim. *The little book of bigger primes*. Springer, 2004.

[25] Andrew David Loveless. "Extensions in the theory of Lucas and Lehmer pseudoprimes". Tesi di dott. 2005. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.606.2720&rep=rep1&type=pdf.

[26] T. Koshy. *Elementary Number Theory with Applications*. Elementary Number Theory with Applications. Elsevier Science, 2007. ISBN: 9780080547091. URL: https://books.google.it/books?id=d5Z5I3gnFh0C.

[27] Arturo Garcia. "On Perfect Numbers". In: *Samt Mary's College of California* (2016), p. 2. URL: http://math.stmarys-ca.edu/wp-content/uploads/2017/07/Arturo-Garcia.pdf.

[28] Krzysztof Pietrzak. "Simple Verifiable Delay Functions". In: (2019). URL: https://eprint.iacr.org/2018/627.pdf.

[29] Chris K. Caldwell. *Prime Pages: primes by year*. URL: https://primes.utm.edu/notes/by_year.html.

[30] Chris K. Caldwell. *Prime Pages: the new Mersenne conjecture*. URL: https://primes.utm.edu/mersenne/NewMersenneConjecture.html.

[31] Euclide. *Gli Elementi*. IX. URL: https://books.google.it/books?id=gvRFAAAAcAAJ.

[32] R. D. Silverman. *Mersenne forum*. URL: https://www.mersenneforum.org/showpost.php?p=53533&postcount=3.

[33] George Woltman. *GIMPS: Mathematics and research strategy*. URL: https://www.mersenne.org/various/math.php.

[34] Gary L. Miller. "Riemann's Hypothesis and Tests for Primality". In: (October 1975). URL: https://cs.uwaterloo.ca/research/tr/1975/CS-75-27.pdf.