Pseudoprimi di Fermat e numeri di Carmichael

Umberto Cerruti

1 Il Piccolo Teorema di Fermat

In una lettera a Bernhard Frenicle de Bessy, scritta il 18 Ottobre 1640, Pierre de Fermat asseriva che (traducendo in linguaggio moderno) se il numero primo p non divide a, allora

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\ p) \tag{1}$$

(Ricordiamo che $a \equiv b \,(\mathrm{mod}\ n)$ significa che n divide $a-b$. Rammentiamo anche che la notazione $a|b$ significa che a divide b.)

Questo Teorema (enunciato ma non dimostrato da Fermat) è ora noto come Piccolo Teorema di Fermat (che abbrevieremo con PTF).

Come osserva Qi Han in [21], il PTF, nel caso $a = 2$, è stato sovente attribuito all'antica Cina. Per esempio in [3] lo si fa risalire ai tempi di Confucio, intorno al 500 a.C., e si dice che anche la proposizione inversa era ritenuta vera (se n divide $2^{n-1} - 1$ allora n è primo). In [15] e in [14] si ripete la stessa cosa.

Qi Han nega con decisione che ciò sia possibile. Secondo Qi Han la nozione di numero primo è stata del tutto assente dalla matematica cinese, fino (addirittura) al XVIII secolo.

Quello che è certo è che la prima dimostrazione del PTF, di cui disponiamo, è stata pubblicata da Eulero nel 1736.

Diciamo che, dati due interi a, n, vale la $F(a, n)$ se

$$a^{n-1} \equiv 1 \,(\mathrm{mod}\ n) \tag{2}$$

L'intero a viene chiamato *base*. Si noti che la (2) implica che a ha inverso modulo n e pertanto $(a, n) = 1$, cioè a è coprimo con n (con (a,b) denoteremo sempre il massimo comun divisore degli interi a e b).

L'inverso del PTF è falso, perché la $F(a,n)$ vale anche per alcuni interi n non primi. Gli interi non primi per i quali vale la $F(a,n)$, vengono detti *pseudoprimi di Fermat sulla base a* (abbrevieremo con ppf).

In [15], a pag. 91, inizia una sezione intitolata *Convers of Fermat Theorem*, nella quale si segnalano alcune date storiche nello studio del PTF.

Sarrus, nel 1819, mostrò che è vera $F(2,341)$, dove $341 = 11 \times 31$. Bouniakowsky nel 1839 scoperse $F(3,91)$ ($91 = 7 \times 13$) e Lucas nel 1877 provò $F(2,2701)$, dove $2701 = 37 \times 73$.

Pertanto 341 e 2701 sono ppf su 2, e 91 è ppf su 3.

Fu lo stesso Lucas, nel 1891, a dimostrare quello che si può considerare l'inverso corretto del PTF.

Teorema 1.

Se, per una base $1 < a < n-1$ *vale* $F(a,n)$*, ma, per ogni divisore* d *di* $n-1$*, con* $d < n-1$*, non vale* $a^d \equiv 1\,(mod\ n)$ *allora* n *è primo.*

Utilizzando (1), si può provare che numeri di certe forme speciali sono primi. Si dimostrano, per esempio (vedi ([14]), le due proposizioni.

Teorema 2.

1) Se p *è primo allora* $2p+1$ *è primo se e solo se vale* $F(2,2p+1)$*.*

2) Il numero di Fermat $F_n = 2^{2^n}+1$ *è primo se e solo se*

$$3^{2^{2^n-1}} \equiv -1\,(mod\ F_n)$$

Il Teorema (2)-1 fornisce un criterio per vedere se il primo p è un primo di Sophie Germain, ovvero un primo p tale che anche $2p+1$ è primo.

Nel 1825 Sophie Germain dimostrò che il primo caso dell'ultimo Teorema di Fermat (UTF) è vero se l'esponente è un primo p tale che $2p+1$ è primo.

Ricordiamo che il primo caso dell'UTF è questo:

Non esistono tre interi non nulli e coprimi con p tali che $x^p + y^p = z^p$.

Non si sa se esistano infiniti primi di Sophie Germain.

Sono primi di Sophie Germain (Oeis A005384):

$$2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191 \cdots$$

La parte 2 di (2) è un criterio per stabilire la primalità dei numeri di Fermat F_n (Oeis A000215):

$$3, 5, 17, 257, 65537, 4294967297, 18446744073709551617 \cdots$$

Per esempio $3^{32768} \bmod 65537 = 65536$ e quindi F_4 è primo, mentre F_5 non è primo perché $3^{2147483648} \bmod 4294967297 = 10324303$.

(Naturalmente con $a \bmod n$ si denota il resto della divisione di a per n)

C'è un legame tra i numeri F_n e il PTF?

Per semplificare la notazione, poniamo $k = 2^n$. Pertanto $F_n = 2^k + 1$. Conseguentemente

$$2^{F_n-1} - 1 = 2^{2^k} - 1 =$$

per la formula $(a^2 - b^2) = (a + b)(a - b)$

$$= (2^{2^{k-1}} + 1)(2^{2^{k-1}} - 1) = (2^{2^{k-1}} + 1)(2^{2^{k-2}} + 1)(2^{2^{k-2}} - 1) =$$

e, iterando,

$$= (2^{2^{k-1}} + 1)(2^{2^{k-2}} + 1)(2^{2^{k-3}} + 1) \cdots (2^k + 1) \cdots 5 \times 3 \times 1$$

Quindi $F_n = 2^k + 1$ divide $2^{F_n-1} - 1$, e vale $F(2, F_n)$, per ogni n.

Se Fermat avesse ritenuto vero l'inverso del PTF, il ragionamento fatto sopra sarebbe stata la *dimostrazione* del fatto che tutti gli F_n sono primi!

Quello che abbiamo provato è che gli F_n non primi sono ppf sulla base 2. Questo non dimostra nemmeno ci siano infiniti ppf sulla base 2. Potrebbe essere vero infatti, che da un certo indice in poi tutti gli F_n siano primi! Nessuno ci crede, ma nessuno sa dimostrare il contrario.

E' vero che esistono infiniti ppf su qualsiasi base a. Questo fu dimostrato da Cipolla in ([14]). Per recenti sviluppi sugli pseudoprimi di Cipolla si veda ([33]).

Teorema 3.

Sia a un intero.

Per ogni primo p che non divide $a(a^2 - 1)$ il numero

$$\rho(a, p) = \frac{a^{2p} - 1}{a^2 - 1}$$

è uno ppf sulla base a.

In particolare adesso siamo in grado di produrre infiniti ppf sulla base 2. La lista dei $\rho(2, p)$ con $p = 5, 7, 11, 13, \cdots$ inizia così

$$341, 5461, 1398101, 22369621, 5726623061, 91625968981, 23456248059221, \ldots$$

E' ora spontaneo chiedersi, dato n, per quante basi a vale $F(a, n)$?

2 La grande festa dei primi

Ci sono in tutto $\varphi(n)$ basi possibili, dove φ è la funzione di Eulero e $\varphi(n)$ è il numero degli interi coprimi con n che precedono n. In particolare $\varphi(n) = n - 1$ se e solo se n è primo.

Pensiamo che le basi siano guardiani che sorvegliano l'ingresso ad una grande festa annuale, alla quale soltanto i primi sono invitati.

Molti numeri sono ambiziosi, e desiderano partecipare al party anche non sono primi. Si vestono bene e vanno!

I guardiani sono infiniti, sono tutti i numeri naturali $1, 2, 3, \ldots$, ma c'è una magia. Non appena il numero n si avvicina ad una entrata, gli si fanno incontro esattamente i $\varphi(n)$ guardiani a lui coprimi, e di lui minori.

I guardiani si fermano a rispettosa distanza, e uno di loro viene estratto a sorte. Costui si avvicina a n e lo sottopone ad accurato esame. Se la base-guardiano è a, a lascia passare n *se e soltanto se* vale $F(a, n)$.

I primi naturalmente non temono nulla, sanno che passeranno, e attendono la prova con un sorriso. Gli altri cercano di apparire tranquilli, ma dentro di loro sono preoccupati. Chi verrà, un amico o un avversario?

Se n vede che gli si avvicina 1, è a posto: quello fa passare tutti! Se n è dispari e arriva $n - 1$, n gongola dentro di sé, sarebbe nei guai solo se fosse pari!

Qual è la probabilità che ha n di passare?

Supponiamo che ci siano $\eta(n)$ basi favorevoli a n, ovvero tali che valga $F(a, n)$. Allora la probabilità di cui parliamo è

$$pr(n) = \frac{\eta(n)}{\varphi(n)}$$

L'insieme delle basi favorevoli a n è un sottogruppo del gruppo $\mathbb{Z}_n^*$ formato dalle $\varphi(n)$ basi coprime con n. Infatti, se valgono $F(a, n)$ e $F(b, n)$ allora vale anche $F(ab, n)$. Pertanto il numero $\eta(n)$ delle basi favorevoli è sempre un divisore di $\varphi(n)$. Quindi la probabilità è sempre una frazione della forma $\frac{1}{d}$, dove d è un divisore di $\varphi(n)$.

Questo fatto elimina le sfumature, le differenze sono drastiche. Se esiste anche una sola base che non accetta n, almeno la metà delle basi sarà contraria a n, e $pr(n) \leq \frac{1}{2}$.

Per elencare le probabilità è più comodo utilizzare la funzione reciproca

$$\pi(n) = \frac{1}{pr(n)} = \frac{\varphi(n)}{\eta(n)}$$

E' ben noto che se $n = \prod_{i=1}^{k} p_i^{e_i}$ allora

$$\varphi(n) = \prod_{1=1}^{k} (p_i - 1) p_i^{e_i - 1}$$

Si trova inoltre che

$$\eta(n) = \prod_{1=1}^{k} (p_i - 1, n - 1)$$

Questi sono i valori di $\pi(n)$ per $n = 1 \cdots 37$

$$1, 1, 1, 2, 1, 2, 1, 4, 3, 4, 1, 4, 1, 6, 2, 8, 1, 6, 1, 8, 3, 10, 1, 8, 5, 12, 9, 4, 1, 8, 1, 16, 5, 16, 6, 12, 1$$

Dove appare 2, per esempio, significa che n ha esattamente probabilità $\frac{1}{2}$ di passare. Gli interi che hanno probabilità $\frac{1}{2}$ minori di 50000 sono (Oeis A191311)

$$4, 6, 15, 91, 703, 1891, 2701, 11305, 12403, 13981, 18721, 23001, 30889, 38503, 39865, 49141$$

La probabilità è uguale a 1 per il numero 1 e per tutti i primi.

Se contiamo gli n tra 1 e 1000 per cui $\pi(n) = 1$ troviamo che sono 170. Levato un 1, per il numero 1, che non è primo, ne rimangono 169. Ma i primi minori di 1000 sono 168. C'è un intruso! Lo cerchiamo, e vediamo che si tratta di

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

Controllando bene i risultati (fino a 50000) notiamo che i seguenti signori (Oeis A002997)

$$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657$$

sono accettati da tutte le basi, e possono partecipare alla festa senza ambasce, e senza essere primi!

Chi sono costoro?

3 I numeri di Carmichael

Se per gli interi a, n vale la $F(a, n)$ (ovvero la (2)), moltiplicando per a si ottiene la

$$a^n \equiv a \,(\mathrm{mod}\ n) \tag{3}$$

La (2) e la (3) non sono però equivalenti Per esempio

$$100^{1476} \equiv 100 \,(\mathrm{mod}\ 1476)$$

ma

$$100^{1475} \equiv 1108 \,(\mathrm{mod}\ 1476)$$

Quando n è composto e vale la (3) diciamo che n è uno pseudoprimo debole su a. Ogni n che sia uno ppf sulla base a è uno pseudoprimo debole su a, ma in generale non vale il viceversa.

Sugli pseudoprimi deboli si pongono alcune interessanti questioni. Non è facile, per esempio, trovare pseudoprimi deboli pari su 2. Fino al 1950 non se ne conosceva nemmeno uno. Nel 1950 D.H. Lehmer trovò $161038 = 2 \times 73 \times 1103$. Nel 1951 Beeger dimostrò che esistono infiniti pseudoprimi deboli pari su 2. Per queste problematiche si veda ([31]), dove viene posto anche il seguente problema:

Problema aperto Esiste n tale che sia n che $n+1$ sono pseudoprimi deboli su 2?

Torniamo ai numeri che superano ogni indagine di Fermat.

I numeri composti n tali che

$$\forall a \in \mathbb{Z}_n^* \quad a^{n-1} \equiv 1 \,(\mathrm{mod}\ n) \tag{4}$$

sono detti *numeri di Carmichael*.

Si dimostra che la (4) e equivalente a

$$\forall a \in \mathbb{Z} \quad a^n \equiv a \,(\mathrm{mod}\ n) \tag{5}$$

Riassumendo, assegnato un intero a, vi possono essere n che sono pseudoprimi deboli rispetto ad a ma non sono ppf su a. Però, n verifica la $F(a, n)$ per tutte le basi a coprime con n, se e solo se n è debolmente pseudoprimo su qualsiasi intero a.

I numeri di Carmichael sono anche detti *pseudoprimi assoluti*. Non occorre infatti specificare la base e nemmeno se si tratta di ppf o di pseudoprimi deboli.

Fino all'inizio del 1900 non si credeva che potessero esistere individui così strani e sfuggenti. Tanto è vero che A. Korselt, nel 1899, cercò di caratterizzarli in quache modo. Se uno pseudoprimo n esistesse, come dovrebbe essere fatto?

Ecco la sorprendente risposta di Korselt ([24])

Teorema 4.

Un intero n è uno pseudoprimo assoluto se e solo se
1) n è prodotto di primi distinti, $n = p_1 p_2 \cdots p_k$
2) Per ogni i, $p_i - 1 \mid n - 1$

Si dimostra inoltre che

Teorema 5.

Se n è uno pseudoprimo assoluto, allora
1) n è dispari.
2) n possiede almeno tre fattori primi distinti.

Esistono siffatti numeri? Probabilmente Korselt pensava di no, e non diede alcun esempio. Nel 1910 Carmichael ([6]) trovò il più piccolo esemplare: $561 = 3 \times 11 \times 17$. Ne vennero poi trovati molti, molti altri.

Restava una domanda assillante: *ci sono infiniti numeri di Carmichael?*

Fu necessario attendere fino al 1994 per avere una risposta (affermativa) in ([1]).

Oggi si possono generare facilmente milioni di numeri di Carmichael, a partire da certi particolari insiemi di numeri, ed è possibile costruire pseudoprimi assoluti che possiedono addirittura miliardi di fattori primi. Si tratta di un percorso affascinante, del quale si possono vedere alcune tappe in questi lavori: ([16]), ([28]), ([26]), ([22]), ([2]).

Particolarmente semplice ed efficace il metodo illustrato in ([26]), che si basa sul seguente Teorema

Teorema 6.

Dato un insieme Y di interi definiamo $f(Y)$ il prodotto dei numeri che stanno in Y.

Siano:
$E = \{C_1, C_2, \ldots, C_k\}$ un insieme di numeri di Carmichael coprimi
F l'insieme dei fattori primi di $f(E)$
$S \subseteq E$ un sottoinsieme non vuoto di E
$m = mcm\{p - 1 : p \in F\}$
$n = MCD\{C - 1 : C \in E\}$
Allora:

$$(\forall S\, f(S) \text{ è un numero di Carmichael}) \Longleftrightarrow (m \mid n)$$

Utilizzando il Teorema (6) e un apposito programma, Renaud Lifchitz ha costruito l'insieme

$E = \{7207201, 230630401, 56951294401, 571019248801, 3278310235201,$
$3815902490401, 11943915984001, 129766580143201, 353830002926401,$
$831957935608801, 2210772268504801, 4513636250323201, 5514474572006401,$
$7571362807008001, 26830954437487201, 80222538033237601,$
$828430182206827201, 997651728495021601, 1022994390853955 5201,$
$28430757383895266401, 340866183402412668001,$
$474235364684225944801, 1254602952776990031415201,$
$126171080935116251263092864 01\}$

E contiene 24 numeri di Carmichael.

I 111 fattori primi p del prodotto dei 24 C sono

17, 19, 23, 29, 31, 37, 41, 43, 53, 61, 67, 71, 73, 79, 89, 97, 101, 113, 131, 151, 157, 181, 199, 211, 241, 313, 331, 353, 397, 401, 421, 463, 521, 601, 631, 661, 673, 701, 859, 881, 911, 937, 991, 1009, 1051, 1093, 1171, 1201, 1249, 1301, 1873, 1951, 2003, 2081, 2311, 2521, 2731, 2801, 2861, 3169, 3301, 3361, 3433, 3697, 4201, 4621, 4951, 5851, 6301, 6553, 7151, 7393, 8009, 8191, 11551, 11701, 12601, 13729, 14561, 15401, 16381, 18481, 19801, 20021, 20593, 21841, 25741, 42901, 48049, 50051, 51481, 55441, 72073, 79201, 92401, 93601, 96097, 109201, 110881, 120121, 131041, 180181, 200201, 218401, 257401, 300301, 450451, 600601, 1029601, 1201201, 2402401

Il minimo comune multiplo dei $p - 1$ è 7207200.

Il massimo comun divisore dei $C - 1$ è lo stesso: 7207200.

Si applica quindi il risultato del Teorema (6). Scelto un qualsiasi sottoinsieme non vuoto di E, il prodotto dei numeri di Carmichael che esso contiene è ancora un numero di Carmichael.

Ci sono $2^{24} - 1 = 16777215$ sottoinsiemi non vuoti di E. Si può considerare quindi E come un codice compresso che contiene tutte le informazioni necessarie per generare 16777215 numeri di Carmichael. L'elenco delle cifre decimali di questi interi non starebbe in un CD di $650MB$, come nota l'autore, nemmeno se zippati.

4 Forme universali

Nel 1939, in ([13]), Jack Chernick introdusse il concetto di *forma universale*.

Ci limitiamo qui al caso minimo di 3 fattori.

Sappiamo dal Teorema (5) che un numero di Carmichael deve essere dispari ed avere almeno 3 fattori.

Chernick dimostrò che se n è un numero di Carmichael prodotto di 3 primi, allora esistono h, r_1, r_2, r_3 tali che

$$n = (2r_1h + 1)(2r_2h + 1)(2r_3h + 1) \tag{6}$$

dove gli interi r_1, r_2, r_3 sono coprimi e gli interi $(2r_1h+1)$, $(2r_2h+1)$, $(2r_3h+1)$, sono primi.

Da questo si ottiene

Teorema 7.
Siano dati gli interi positivi r_1, r_2, r_3 coprimi.
Si ponga $r = r_1r_2r_3$.
Sia $k(r_1, r_2, r_3) = (-(r_1 + r_2 + r_3)y) \,(mod\ r)$ dove y è l'inverso di $(r_1r_2 + r_1r_3 + r_2r_3) \,(mod\ r)$.
Siano $v_i(r_1, r_2, r_3, x) = k(r_1, r_2, r_3)r_i + 1 + rr_ix$, con $1 \leq i \leq 3$.
Si ponga

$$U(r_1, r_2, r_3, x) = v_1(r_1, r_2, r_3, x)v_2(r_1, r_2, r_3, x)v_3(r_1, r_2, r_3, x)$$

Allora $U(r_1, r_2, r_3, x)$ è un numero di Carmichael se i $v_i(r_1, r_2, r_3, x)$ sono primi.

Inoltre, se n è un numero di Carmichael prodotto di 3 primi p_1, p_2, p_3, esistono r_1, r_2, r_3, x tali che

$$n = U(r_1, r_2, r_3, x)$$

L'espressione $U(r_1, r_2, r_3, x)$ si dice *forma universale*, proprio perché ogni numero di Carmichael viene trovato specificando opportunamente i parametri r_1, r_2, r_3 e la variabile x. Diciamo *forma* la funzione di x ottenuta assegnado a r_1, r_2, r_3 valori specifici.

Facciamo qualche esempio.

Consideriamo il caso $r_1 = 1, r_2 = 2, r_3 = 3$.
Allora $r = r_1r_2r_3 = 6$. Inoltre $r_1r_2 + r_1r_3 + r_2r_3 = 11 = 5 \,(\text{mod } 6)$. L'inverso y di $5 \,(\text{mod } 6)$ è 5. Poiché $r_1 + r_2 + r_3 = 6 = 0 \,(\text{mod } 6)$, $k(r_1, r_2, r_3) = -0 \times 5 = 0$ e $v_1(1, 2, 3, x) = 1 + 6x$, $v_2(1, 2, 3, x) = 1 + 12x$, $v_3(1, 2, 3, x) = 1 + 18x$. Infine

$$U(1, 2, 3, x) = (1 + 6x)(1 + 12x)(1 + 18x)$$

Questa è la forma più nota ([18]). I numeri di Carmichael che si ottengono sono chiamati *numeri di Chernick*, e la loro sequenza è presente nella Oeis.

Al variare di x, quando i numeri $(1+6x), (1+12x), (1+18x)$ sono tutti primi, si trova il numero di Chernick $U(1,2,3,x)$.

La sequenza è la seguente (A033502)

$$1729, 294409, 56052361, 118901521, 172947529, 216821881, 228842209, \cdots$$

corrispondenti ai valori di x (sequenza A046025)

$$1, 6, 35, 45, 51, 55, 56, \cdots$$

Le forme sono infinite. Consideriamo per esempio $r_1 = 2, r_2 = 3, r_3 = 5$.

Allora $r = r_1 r_2 r_3 = 30$. Inoltre $r_1 r_2 + r_1 r_3 + r_2 r_3 = 31 = 1 \pmod{30}$. L'inverso y di $1 \pmod{30}$ è 1. Poiché $r_1 + r_2 + r_3 = 10 = 10 \pmod{30}$, $k(r_1, r_2, r_3) = -10 \times 1 = -10 \pmod{30} = 20$ e $v_1(2,3,5,x) = 41 + 60x$, $v_2(2,3,5,x) = 61 + 90x$, $v_3(2,3,5,x) = 101 + 150x$. Infine

$$U(2,3,5,x) = (41 + 60x)(61 + 90x)(101 + 150x)$$

Per gli x tali che i numeri $(41+60x), (61+90x), (101+150x)$ sono tutti primi, si trovano, i numeri di Carmichael

$$3828001, 82929001, 366652201, 8251854001, 12173703001, 25749237001, 67495942201, \cdots$$

corrispondenti ai valori di x

$$1, 4, 7, 21, 24, 31, 43, \cdots$$

E' interessante osservare che, se abbiamo la forma universale ternaria (ottenuta dal Teorema (7)),

$$U(r_1, r_2, r_3, x) = (a + bx)(c + dx)(e + fx)$$

al variare di x si ottengono anche numeri di Carmichael

$$n = (a + bx)(c + dx)(e + fx)$$

che *non* sono prodotto di 3 primi, ma di 4 o più primi. Questi numeri non si possono considerare generati dalla forma (la stessa osservazione vale per le forme di ordine superiore).

Questa problematica non è stata ancora studiata, a quanto so.

Per esempio, come descrizione della A033502 si trova la frase *Carmichael numbers of form* $(6k+1)(12k+1)(18k+1)$. Questo non è esatto, perché un numero di Carmichael n appartiene a quella forma se e solo se i tre numeri $6k+1, 12k+1$ e $18k+1$ sono tutti primi, il che ovviamente impedisce che $n=(6k+1)(12k+1)(18k+1)$ abbia altri fattori primi.

Espongo brevemente i risultati di una mia piccola ricerca sperimentale.

Consideriamo proprio la famosa $U(1,2,3,x) = (6k+1)(12k+1)(18k+1)$. Facciamo variare $x = 1, 2, 3, \ldots$. Oltre ai numeri di Carmichael prodotto di 3 primi contenuti nella A033502, otteniamo i numeri di Carmichael

$$172081, 1773289, 4463641, 295643089, 798770161, 1976295241, 122160500281, \cdots$$

che sono prodotti di 4 primi, e corrispondono ai valori di x

$$5, 11, 15, 61, 85, 115, 455, \cdots$$

e poi i numeri di Carmichel

$$13992265, 47006785, 1150270849, 1420379065, 1504651681, 14782305601, 18390744505, \cdots$$

che sono prodotto di 5 primi, e corrispondono ai valori di x

$$22, 33, 96, 103, 105, 225, 242, \cdots$$

e così via...

La sequenza dei valori di x per cui $U(1,2,3,x) = (6k+1)(12k+1)(18k+1)$ è un numero di Carmichael prodotto di 3 o più primi è

$$1, 5, 6, 11, 15, 22, 33, 35, 45, 51, 55, 56, 61, 85, 96, 100, 103, 105, 115, 121, 195, \ldots$$

Questa è la A101187, e si ripartisce nella famiglia di sottosequenze che abbiamo visto (prodotto di $3, 4, 5, \ldots$ primi). A parte il caso di 3 primi, le sottosequenze non sono in Oeis.

Sorge spontaneamente la domanda: si possono caratterizzare i numeri di Carmichael n prodotto di $k > 3$ primi, tali che $n = U(1,2,3,x)$ per un x intero?

Non dimentichiamo poi che il Teorema (7) contiene anche una seconda parte: se n è un numero di Carmichael *prodotto di 3 primi* allora esistono r_1, r_2, r_3, x tali che $n = U(r_1, r_2, r_3, x)$.

La sequenza dei numeri di Carmichael prodotto di 3 primi è (A087788)

$$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 46657, 52633, 115921, \cdots$$

Questi numeri appartengono alle forme $U(r_1, r_2, r_3, x)$, dove le quaterne (r_1, r_2, r_3, x) sono

$$\{1,5,8,0\}, \{1,3,4,0\}, \{1,2,3,1\}, \{1,4,7,0\}, \{1,2,5,0\}, \{3,11,20,0\}, \{1,3,11,0\}, \cdots$$

Moltissimi numeri di Carmichael (prodotto di 3 primi), si trovano, nelle rispettive forme, per $x = 0$. Questo accade quando, con le notazioni del Teorema (7), si ha $p_1 < r_1 r$, $p_2 < r_2 r$ e $p_3 < r_3 r$. In questo caso la forma universale è

$$(p_1 + r_1 r x)(p_2 + r_2 r x)(p_3 + r_3 r x)$$

Potremmo chiamare questi interi *superficiali*, infatti si leggono direttamente dalla loro forma. La loro sequenza inizia così

$$561, 1105, 2465, 10585, 2821, 8911, 6601, 15841, 52633, 29341, 46657, \cdots$$

La forma di un numero superficiale non può mai essere, ovviamente, U(1,2,3,x). Per esempio $46657 = 13 \times 37 \times 97$. Quindi $r_1 = 1, r_2 = 3, r_3 = 8$, e la forma è

$$U(1,3,8,x) = (13 + 24x)(37 + 72x)(97 + 192x)$$

5 La Connessione Egizia

Definizione 8. Diciamo C-insieme un insieme $\{a_1, a_2, \ldots, a_k; S\}$ tale che valgano le condizioni

1. Gli a_i sono interi positivi tutti differenti, e la loro somma è S
2. Ogni a_i divide S

Diciamo che k è l'ordine del C-insieme $\{a_1, a_2, \ldots, a_k; S\}$; Gli insiemi $\{a; a\}$ non sono considerati C-insiemi. E' facile vedere che non esistono C-insiemi con $k = 2$. Il minimo k è pertanto 3. L'insieme $\{1, 2, 3; 6\}$ è un C-insieme di ordine 3.

Se $A = \{a_1, a_2, \ldots, a_k; S\}$ è un C-insieme, anche $A^+ = \{a_1, a_2, \ldots, a_k, S; 2S\}$ è un C-insieme. Esistono quindi C-insiemi con ordine qualsiasi ≥ 3.

In ([17]) si dimostra il seguente risultato

Teorema 9.

Sia $A = \{a_1, a_2, \ldots, a_k; S\}$ un C-insieme.

Supponiamo che esista M tale che tutti i numeri $a_i SM + 1$ siano primi. Allora l'intero N:

$$N = \prod_{i=1}^{k} (a_i SM + 1)$$

è un numero di Carmichael.

Si noti che, dato il C-insieme A, non è detto a priori che esista un M che verifichi le ipotesi del Teorema (9). Tutto quello che abbiamo è un risultato famosissimo di Dirichlet, che assicura la presenza di infiniti primi nella successione $an + b$, al variare di n, se a, b sono coprimi.

Dixon, nel 1904, formulò la seguente congettura

Congettura 10.

Siano dati k polinomi lineari $a_i n + b_i$, nella variabile n.

Supponiamo (è il minimo!) che non esista un p che divida il prodotto degli $a_i n + b_i$ per tutti *gli n.*

Allora esistono infiniti n tali che i numeri $a_i n + b_i$ sono simultaneamente primi.

Il citato Teorema di Dirichlet prova la congettura per $k = 1$. Dimostrarla per $k = 2$ risolverebbe la congettura di Goldbach sui primi gemelli, infatti i polinomi $2n + 1$ e $2n + 3$ sarebbero simultaneamente primi per infiniti valori di n.

Da quanto detto appare chiaro che la congettura (10) è estremamente difficile da provare. Malgrado questo siamo tutti portati a considerarla vera, e molti autori la danno per scontata. Infatti Dubner in ([17]) mette l'esistenza di M nella definizione stessa di C-insieme.

Accetteremo nel seguito la validità della Congettura di Dixon.

Se P è un numero perfetto, P è la somma dei suoi divisori (minori di P), ed è diviso da ognuno di essi. Pertanto si ha il

Teorema 11.

Siano P un numero perfetto e $\{d_1, d_2, \ldots, d_k\}$ i suoi divisori diversi da P.

Allora l'insieme $\{d_1, d_2, \ldots, d_k; P\}$ è un C-insieme.

Possiamo allora ottenere numeri di Carmichael dai numeri perfetti!

Cominciamo con $P = 6$. Il C-insieme è $\{1, 2, 3; 6\}$. Si cercano ora gli M tali che $(6M + 1)$, $(12M + 1)$ e $(18M + 1)$ siano primi. Allora, per il Teoema (9), N=$(6M + 1)(12M + 1)(18M + 1)$ sarà un numero di Carmichael.

Abbiamo già visto questo prodotto, è la forma fondamentale $U(1,2,3,x)$!

Passiamo al secondo numero perfetto $P = 28$.

Il C-insieme relativo è $\{1,2,4,7,14;28\}$. Da questo otteniamo infiniti numeri di Carmichael, prodotto di 5 primi, della forma

$$(1+28M)(1+56M)(1+112M)(1+196M)(1+392M)$$

Il più piccolo si trova per $M = 2136$ ed è 599966117492747584686619009.

Per il terzo numero perfetto 496, abbiamo un prodotto di 9 fattori $(1+496dM)$, e il più piccolo M che li rende simultaneamente primi è 474382033125.

Se prendiamo il quarto, 8128, ci sono 13 fattori, e non è ancora noto alcun M.

Conosciamo ora 47 numeri perfetti pari (derivanti dai primi di Mersenne (([10]), ([9])), alcuni dei quali hanno milioni di cifre. Accettando la congettura di Dixon (10) ognuno di essi genera infiniti numeri di Carmichael.

Vediamo qui molto bene come il finito sia, per noi esseri umani, già infinito. Chi potrà mai trovare per questi 47 numeri, il più piccolo Carmichael associato?

Lo stesso discorso si può fare per i numeri *semiperfetti*. Un numero n è semiperfetto se non è perfetto ed è somma di alcuni suoi divisori (i divisori che appaiono nella somma devono essere tutti diversi).

Il più piccolo semiperfetto è 12

$$12 = 1+2+3+6 \tag{7}$$

Ogni n semiperfetto dà luogo a un C-insieme. Nel caso di 12 si ha $\{1,2,3,6;12\}$. In questo caso i fattori lineari sono $(1+12M), (1+24M), (1+36M), (1+72M)$. Il più piccolo M che li rende primi è 103, al quale corrisponde il numero di Carmichael

$$84154807001953 = 1237 \times 2473 \times 3709 \times 7417$$

Il C-insieme di 12 ha lunghezza 4.

Ci si chiede: **quanti C-insiemi di lunghezza k esistono?**

Si vede facilmente che $\{1,2,3;6\}$ è l'unico C-insieme di lunghezza 3. Ma poi la cosa si complica molto...

Vengono in nostro aiuto le *frazioni egizie*, e, in particolare, le decomposizioni di 1 mediante frazioni egizie ([7]). Ricordiamo che una frazione egizia è un razionale somma di frazioni del tipo $\frac{1}{d}$.

Se $A = \{a_1, a_2, \ldots, a_k; S\}$ è un C-insieme, allora, per definizione (8),

$$S = \sum_{i=1}^{k} a_i$$

Dividendo per S e ricordando, sempre da (8), che ogni a_i divide S si ha

$$1 = \sum_{i=1}^{k} \frac{1}{b_i}$$

dove $a_i b_i = S$.

Vale anche il viceversa. Data la decomposizione, per certi interi d_i tutti diversi

$$1 = \sum_{i=1}^{k} \frac{1}{d_i}$$

poniamo $S = mcm\{d_1, d_2, \ldots, d_k\}$. Allora

$$1 = \sum_{i=1}^{k} \frac{1}{d_i} = \frac{S/d_1 + S/d_2 + \cdots + S/d_k}{S}$$

e questo implica

$$S = \sum_{i=1}^{k} \frac{S}{d_i}$$

Pertanto $\{\frac{S}{d_1}, \frac{S}{d_2}, \ldots, \frac{S}{d_k}\}$ è un C-insieme.

Contare i C-insiemi di lunghezza k equivale quindi a contare le decomposizioni di 1 come somma di k frazioni egizie.

Questo secondo calcolo è facilitato dalla esistenza di un linite superiore per d_k.

E' noto che, se $1 = \sum_{i=1}^{k} \frac{1}{d_i}$, allora ([11], Teorema 5), $d_k \leq AV(k)$, supponendo che gli x_i siano in ordine crescente.

Ricordiamo che $AV(k)$ in ([11]) è la linea ad alta velocità, definita da

$$\mathrm{AV}(1) = 1 \quad \text{e} \quad \mathrm{AV}(n) = \mathrm{AV}(n-1) + (\mathrm{AV}(n-1))^2$$

La funzione $AV(k)$, e pertanto il confine superiore ai d_k, cresce molto velocemente. Di conseguenza, anche con l'uso di computer, non si può andare molto lontano (si veda anche ([27]).

Poniamo V_k uguale al numero di C-insiemi di lunghezza k. La sequenza V_k (A006585) inizia così, partendo da $V_3 = 1, V_4 = 6, \cdots$:

$$1, 6, 72, 2320, 245765, 151182379, \cdots$$

In ([27]) si trova anche l'elenco dei 72 C-insiemi di lunghezza 5.

Recentemente ho scoperto che passeggiare sull'albero $\mathcal{N}$ (presentato in ([11])) produce, forse inconsapevolmente, decomposizioni della unità in frazioni egizie.

Ricordiamo che, se siamo in n, si possono raggiungere tutti e soli i numeri del tipo $n + d$, dove d è un divisore di n^2.

Teorema 12.

Consideriamo la sequenza $a_1, a_2, \ldots, a_i, \ldots, a_k$ *dove per ogni* $1 \leq i \leq k-1$ *si ha*

$a_{i+1} = a_i + d_i$
$a_i^2 = d_i s_i$
Allora, posto $b_i = a_i + s_i$ *si ha*

$$\frac{1}{a_1} - \frac{1}{a_k} = \sum_{j=1}^{k-1} \frac{1}{b_j} \tag{8}$$

Pertanto se sull'albero $\mathcal{N}$ partiamo da 1 e arriviamo in n, percorrendo la strada

$$a_1 = 1, a_2 = 2, a_3, \cdots, a_k = n$$

otteniamo la decomposizione egizia di 1 data da

Teorema 13.

$$1 = \frac{1}{b_1} + \frac{1}{b_2} + \cdots + \frac{1}{b_k}$$

dove:
$b_1 = 2$
$b_h = \frac{a_{h+1} a_h}{a_{h+1} - a_h}$, *per ogni* $2 \leq h \leq k-1$
$b_k = n$

Dalla somma di frazioni egizie si può poi passare al relativo C-insieme,e da questo ai numeri di Carmichael!

Facciamo allora quattro passi su $\mathcal{N}$.

Per esempio, andando piano piano, arriviamo in 8 con questo percorso

$$1, 2, 4, 6, 8$$

Otteniamo la decomposizione di 1:

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{12}+\frac{1}{24}+\frac{1}{8}$$

Il C-insieme corrispondente è

$$\{1,2,3,6,12;24\}$$

Questo, attraverso il Teorema (9), porta a cercare i numeri di Carmichel della forma

$$(1+24x)(1+48x)(1+72x)(1+144x)(1+288x)$$

che si troveranno per i valori di x tali che i 5 fattori sono tutti primi.
Se vale 10 ce ne sono infiniti. I primi tre sono

$$26641259752490421121, 264795586432486070244940 9, 19573613936097310846530892 9$$

ottenuti da $x = 95, 949, 2244$.

Non sempre i percorsi vanno bene. Si ottiene sempre una decomposizione di 1, ma a volte le frazioni si ripetono. In questo caso non si possono ottenere numeri di Carmichael con il procedimento descritto.

Per esempio se il percorso è $\{1,2,6,12\}$ il C-insieme corrispondente è improprio, ha elementi ripetuti, è $\{1,1,4,6,12\}$ e la decomposizione di 1 è $1=\frac{1}{2}+\frac{1}{3}+\frac{1}{12}+\frac{1}{12}$.

Quando va bene si trova una miniera di numeri di Carmichael. Se andiamo di fretta e prendiamo la TAV di $\mathcal{N}$, e ci fermiamo alla quarta stazione, il percorso è $\{1,2,6,42,1806\}$. In questo caso tutto è regolare. Il C-insieme è $\{1,42,258,602,903;1806\}$ e la decomposizione è:

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{7}+\frac{1}{43}+\frac{1}{1806}$$

Ragionando come prima, i numeri di Carmichael da cercare saranno della forma

$$(1+1806x)(1+75852x)(1+465948x)(1+1087212x)(1+1630818x)$$

Il primo x che dà esito positivo è 7425. Il numero di Carmichael trovato è

$$25540199842913177488116557375775307014261648 01$$

prodotto di 5 primi.

Propongo un problema: in $\mathcal{N}$ **quali percorsi portano alle miniere di Carmichael?**

Si noti bene che non conta soltanto il posto ove si giunge, ma anche il percorso fatto!

Non avrebbe senso chiedersi dove si trovino le miniere. Per esempio se si arriva in 12 con $1, 2, 6, 12$, abbiamo appena visto che si fallisce. Ma se percorriamo $1, 2, 4, 12$ troviamo il C-insieme $\{1, 2, 3, 6; 12\}$ già visto (7), con la sua appropriata miniera, data dalla forma

$$(1 + 12x)(1 + 24x)(1 + 36x)(1 + 72x)$$

Ho visto che esiste un percorso che va bene per tutti i numeri > 2 che non sono della forma $k(k + 1)$ (ovvero non sono il doppio di un numero triangolare).

Teorema 14.
Sia n un numero dispari, oppure un numero pari la cui metà non è un numero triangolare.
Allora il percorso $\{1, 2, 3, 4, \ldots, n\}$ (la linea locale di ([11])) fornisce una decomposizione egizia di 1, e quindi un C-insieme con la relativa forma che produce i numeri di Carmichael.

Dimostrazione. Il percorso $\{1, 2, 3, 4, \ldots, n\}$ genera, si veda (13), la sequenza dei b_j

$$b_1 = 1 \times 2 = 2, b_2 = 2 \times 3 = 6, b_3 = 3 \times 4 = 12, \cdots, b_{n-1} = (n-1)n, b_n = n$$

Chiaramente $b_1, \ldots, b_{n-1}$ sono tutti diversi, e, per ipotesi, b_n è diverso da tutti i precedenti, che sono proprio gli interi della forma $k(k + 1)$. Quindi si ha

$$1 = \frac{1}{b_1} + \frac{1}{b_2} + \cdots + \frac{1}{b_n}$$

e questa è una decomposizione senza ripertizioni.
Da ciò, come sappiamo, segue il resto. □

Per esempio il percorso $\{1, 2, 3, 4, 5\}$ dà la decomposizione

$$1 = \frac{1}{2} + \frac{1}{6} + \frac{1}{12} + \frac{1}{20} + \frac{1}{30} + \frac{1}{42} + \frac{1}{7}$$

Il C-insieme è

$$\{10, 14, 21, 35, 60, 70, 210; 420\}$$

la forma generatrice è

$$(1+4200x)(1+5880x)(1+8820x)(1+14700x)(1+25200x)(1+29400x)(1+88200x)$$

Scavando in questa miniera fin a $x = 10^6$ ho trovato 4 numeri di Carmichael, prodotti di 7 primi, per $x = 8194, 13279, 396916, 649198$. Il più grande ha 71 cifre ed è

$$10168788290901386862383225729211845301508433595193743552107585502333601$$

6 Numeri di Carmichael di ordine superiore

Uno dei più recenti sviluppi della teoria dei numeri di Carmichael è l'introduzione del concetto di *numeri di Carmichael di ordine superiore* (si vedano ([23]), ([20])).

Definizione 15. Un intero n è un numero di Carmichael di ordine m se
1) n è prodotto di primi distinti
2) Per ogni p che divide n e per ogni intero positivo $r \leq m$, esiste i tale che

$$p^r - 1 \,|\, n - p^i$$

Osserviamo subito che se n è un numero di Carmichael ordinario, allora n soddisfa le condizioni di (15) con $m = 1$ e $i = 0$.

Un numero di Carmichael di ordine m si dice *rigido* se la condizione 2 vale per $i = 0$. I numeri di Carmichael ordinari sono tutti rigidi.

Il più piccolo numero di Carmichael di ordine 2 è

$$443372888629441 = 17 \times 31 \times 41 \times 43 \times 89 \times 97 \times 167 \times 331$$

Si tratta di un numero rigido.
L'intero z prodotto dei 23 primi
23, 67, 71, 89, 109, 113, 191, 199, 233, 239, 271, 307, 373, 419, 521, 911, 929, 1153, 1217, 1429, 2089, 2729, 23561
è un numero di Carmichael di ordine 2 non rigido. Infatti $p^2 - 1 \,|\, z - 1$ per tutti i primi che lo dividono, tranne $p = 1153$. Infatti $1153^2 - 1$ non divide $z - 1$ ma divide $z - 1153$.

Ecco allora due problemi assai interessanti

Problema 16. Esistono infiniti numeri di Carmichael di ordine 2?

Problema 17. Trovare almeno un numero di Carmichael di ordine 3.

Incredibilmente queste problematiche hanno anche un interesse materiale. Come è ben noto ([8]), determinare la primalità di interi grandi è essenziale per la crittografia moderna. Esistono per questo molti algoritmi, probabilistici e deterministici (vedi ([4]) e ([5]).

Il filtro più semplice, per selezionare i primi, è il PTF, di cui abbiamo parlato. Come ben sappiamo i numeri di Carmichael riescono sempre a superare l'ostacolo. Si è passati allora a sistemi sempre più sofisticati. Uno dei metodi più utilizzati, perché assai veloce, è il cosiddetto test di Baillie-PSW (per una descrizione del test si veda ([4])).

Nel 1984 in ([29]) Carl Pomerance sostenne, attrverso ragionamenti euristici ma assai ben fondati, che devono esistere infiniti interi non primi che superano il test Baillie-PSW. Essi dovrebbero essere assai numerosi, e Pomerance suggerì un metodo per trovarli. Venne anche offerto un premio di 620 dollari.

Fino ad ora nessuno di questi numeri è stato trovato! Ripeto che questo avrebbe implicazioni molto forti sulla pratica crittografica, e non solo.

In seguito le richieste sono state abbassate. Il test di Baillie-PSW applica prima il test di Miller e poi un test di Fibonacci. Ci accontentiamo (vedi ([12])) che l'intero n superi un semplice test di Fermat sulla base 2, al posto del più potente test di Miller, chiediamo cioè che $2^n \equiv 2 \bmod n$. Chiediamo inoltre che n non sia un quadrato modulo 5 (equivalentemente $n \equiv 2, 3 \bmod 5$) e che n divida il numero di Fibonacci F_{n+1}. Se n è un numero di Carmichael rigido di ordine 2 supera ovviamente il test di Fermat e si può dimostrare che, come consegueza del fatto che $p^2 - 1 | n - 1$ per ogni p che divide n, si ha anche che $n | F_{n+1}$.

Il problema è che tutti i numeri di Carmichael rigidi di ordine 2 noti sono congrui a ± 1 modulo 5!

Pertanto invito tutti a cercare un intero di Carmichael rigido di ordine 2 congruo a ± 2 modulo 5.

Più in generale sarebbe di grande interesse trovare un intero n che soddisfi alle condizioni ([12])

- $n \equiv \pm 2 \bmod 5$
- $2^n \equiv 2 \bmod n$
- $F_{n+1} \equiv 0 \bmod n$
- n è composto con fattorizzazione nota

Riferimenti bibliografici

[1] W. R. Alford - A. Granville - C. Pomerance, There are Infinitely Many Carmichael Numbers, Ann. Math. Vol. 139, pp. 703-722, 1994.

[2] W.R. Alford, Jon Grantham, Steven Hayman, Andrew Shallue - Constructing Carmichael numbers through improved subset-product algorithms, arxiv:1203.6664v1, 2012

[3] W. W. Rouse Ball (and H. S. M. Coxeter), Mathematical Recreations and Essays, 13a edizione, Dover, New York 1987; prima edizione pubblicata nel 1892.

[4] Luisella Caire - Umberto Cerruti, Questo numero è primo ? Si, forse, dipende...,

Bollettino U.M.I. Sez.A, La Matematica nella Società e nella Cultura, Serie VIII, Vol IX-A, Dicembre 2006/1, 449-481

[5] Luisella Caire - Umberto Cerruti, Numeri primi: la certezza,

Bollettino U.M.I. Sez.A, La Matematica nella Società e nella Cultura, Serie VIII, Vol X-A, Aprile 2007, 85-117

[6] R. D. Carmichael - Note on a new number theory function. Bulletin of the American Mathematical Society Vol. 16, pp. 232-238, 1910.

[7] U. Cerruti - Frazioni egizie e numeri pratici, (2005)

www.dm.unito.it/ cerruti/marzo-luglio-2005.html

[8] U. Cerruti - Collane colorate, Fermat, Eulero e la crittografia (2008)

www.dm.unito.it/ cerruti/divertimenti/divertiamoci3.html

[9] U. Cerruti - Somme di Interi Consecutivi, Numeri di Mersenne e Numeri di Fermat (2008)

www.dm.unito.it/ cerruti/pdfblog/somme.pdf

[10] U. Cerruti - Nuovi primi di Mersenne, titaniche fattorizzazioni e guerre crittografiche. Fino a quando? (2010)

www.dm.unito.it/ cerruti/mathblog280110.html

[11] U. Cerruti - Percorsi tra i numeri (2011)

www.dm.unito.it/ cerruti/pdfblog/percorsi.pdf

[12] Zhuo Chen, John Greene - Some Comments on Baillie-PSW Pseudoprimes, The Fibonacci Quarterly, Vol. 41, pp. 334-344, 2003.

[13] J. Chernick, On Fermat's simple theorem, Bull. Amer. Math. Soc. 45 (1939), 269-274.

[14] Michele Cipolla, Sui numeri composti p che verificano la congruenza di Fermat, Annali di Matematica 9, pp. 139-160, 1901.

[15] L. E. Dickson, History of the Theory of Numbers, Vol. I: Divisibility and Primality, Carnegie Institute of Washington, 1919; ristampato da Chelsea Publ. Co. New York, 1971.

[16] Harvey Dubner - A new method for producing large Carmichael numbers, Math. Comp. 53 (1989), 411-414.

[17] Harvey Dubner - Carmichael numbers and Egyptian fractions, Mathematica Japonica Vol. 43, pp. 411-419, 1996.

[18] Harvey Dubner - Carmichael Numbers of the form(6m + 1)(12m + 1)(18m + 1) - Journal of Integer Sequences, Vol. 5 (2002), Article 02.2.1

[19] Paul Erdös - On pseudoprimes and Carmichael numbers, Publ. Math. Debrecen 4 (1956), 201-206.

[20] Oleg Eterevsky and Maxim Vsemirnov - On the Number of Prime Divisors of Higher-Order Carmichael Numbers, The Fibonacci Quarterly, Vol. 42, pp. 141-148, 2004.

[21] Qi Han, Man-Keung Siu - On The Myth Of An Ancient Chinese Theorem About Primality - Taiwanese Journal Of Mathematics Vol. 12, No. 4, pp. 941-949, July 2008.

[22] Steven Hayman and Andrew Shallue, Illinois Wesleyan University,

Constructing a ten billion factor Carmichael number, preprint, 2010

[23] Everett W. Howe, Higher-order Carmichael numbers, Math. Comp. 69 (2000), no. 232, 1711-1719.

[24] A. R. Korselt - Problème chinois, L'intermédiaire des mathématiciens Vol. 6 pp. 142-143, 1899.

[25] Erik Lieuwens - Fermat Pseudoprimes - Drukkerij, Hoogland, Delft, 1971.

[26] Renaud Lifchitz - A generalization of the Korselt's criterion,
nested Carmichael numbers, preprint, 2002

[27] Bernard Montaron - Carmichael Polynomials, Pseudo-Perfect Numbers and Egyptian Fractions, preprint, 2003

[28] Löh, G.; Niebuhr, W. (1996). A new algorithm for constructing large Carmichael numbers. Math. Comp. 65: 823-836

[29] Carl Pomerance - Are there counterexamples to the Baillie PSW primality test?, (1984)
cr.yp.to/bib/1984/pomerance.pdf

[30] Poulet - Table des nombres composes verifant le thioreme de Fermat pour le module 2 jusqu'è 100 000 000, Deuxième Congrès Int, Récréation Math. Comptes Rendus, Brussel (1937), pp. 42-52.

[31] A. Rotkiewicz, K. Ziemak - On Even Pseudoprimes, The Fibonacci Quarterly, Vol. 33, pp. 123-125, 1995.

[32] André Weil, Number Theory: An Approach Through History From Hammurapi To Legendre, Birkhäuser, Boston-Basel-Stuttgart, 1984. Traduzione italiana presso Einaudi Paperbacks (1993), con il titolo Teoria dei Numeri.

[33] Y. Hamahata - Y. Kokubun, Cipolla Pseudoprimes,
Journal of Integer Sequences, Vol. 10 Article 07.8.6, (2007).