BOLLETTINO

UNIONE MATEMATICA ITALIANA

Sezione A – La Matematica nella Società e nella Cultura

PAULO RIBENBOIM

1093

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. 6-A—La Matematica nella Società e nella Cultura (2003), n.1, p. 165–182.

Unione Matematica Italiana

http://www.bdim.eu/item?id=BUMI_2003_8_6A_1_165_0

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

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

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

1093.

P. RIBENBOIM

1093! ⁽¹⁾ Se vi domandate di che cosa tratti questo articolo, mi affretto a dire che non tratta della qualità del vino dell'anno 1093. Infatti mancano informazioni storiche circa l'enologia di un'età così remota. È solo a partire dal 1855 che un selezionato gruppo di viticoltori di Bordeaux ha classificato le migliori vigne della propria regione distinguendo fra tutti i fuori classe Chateaux Lafite, Margaux Latur, Haut-Brion, così come il Premier Crus nel Medoc ed il Chateau Yquem nel Sauternes o il Premier Grand Crus. Per non menzionare tutti i meravigliosi vini della Borgogna ... [6]. Questo articolo comunque non tratta di vini.

Infatti l'idea di questo articolo mi è venuta dopo una discussione con F. Le Lionnais a Parigi. Egli è un matematico e letterato, ora ottantenne con un'acuta curiosità (n.d.t. François Le Lionnais è deceduto nel 1984). Subito dopo la guerra, nel 1946, egli pubblicò il libro «Le Grand Courants de la Pensée Mathématique», contenente i contributi di eminenti matematici come André Weil e diversi altri membri del gruppo dei Bourbakisti. L'articolo «L'Avenir des Mathématiques» di Weil merita di essere letto e dà la prospettiva degli ultimi quaranta anni trascorsi. Questo libro è stato tradotto in inglese ed è facilmente reperibile. Ne sono venuto a conoscenza subito dopo la sua apparizione e sono sempre stato impaziente di incontrare Le Lionnais.

Così è stato con immenso piacere che nel 1976 ho fatto la sua conoscenza ad un seminario di storia della matematica. Durante la conversazione ho saputo che stava scrivendo un libro sui numeri

⁽¹⁾ Questo articolo è stato pubblicato una prima volta su *The Mathematical Intelligencer*, 5, 2, 1983, 28-34; è stato, poi, riprodotto, sempre in lingua inglese, come ottavo capitolo del libro P. Ribenboim, *My Numbers, My Friends, Popular lectures on Number Theory*, Springer 2000. La traduzione in italiano è dovuta a Francesco Pappalardi.

«importanti», come 2, 7, π , e , ecc. ... ed egli mi domandò se conoscevo qualche numero con interessanti proprietà che egli potesse includere nel suo libro (nel frattempo, il suo libro è stato pubblicato. F. Le Lionnais. *Les Nombres Remarquables* Hermann Editeurs, Paris, 1983). Dopo averci pensato, ho deciso per «1093», circa il quale egli non aveva ancora sentito nulla.

Vorrei spiegarvi perché considero 1093 un numero interessante (In seguito ho appreso che Le Lionnais ha incluso 1093 nel suo libro sui numeri interessanti. Chiaramente si potrebbe dire che *tutti* i numeri sono interessanti. Dimostrazione: Se così non fosse, poniamo N il più piccolo numero che non è interessante. N è interessante avendo la proprietà di essere «il più piccolo numero non interessante» ...)

Bene ... 1093 è il più piccolo numero primo p che soddisfa la congruenza

$$(1) \quad 2^{p-1} \equiv 1 \pmod{p^2}.$$

Quindi

$$2^{1092} \equiv 1 \pmod{1093^2}.$$

Questa proprietà è stata scoperta da Meissner [18] nel 1913, facendo espressamente il calcolo. Applicando il piccolo teorema di Fermat

$$(2) \quad 2^{p-1} \equiv 1 \pmod{p}.$$

Ma in generale non c'è ragione per aspettarsi che valga la congruenza più forte (1).

Nel Vol. III di [12] Landau dà la seguente dimostrazione di (1) per $p = 1093$:

$$3^7 = 2187 = 2p + 1$$

così elevando al quadrato

$$(3) \quad 3^{14} \equiv 4p + 1 \pmod{p^2}.$$

D'altro canto,

$$2^{14} = 16384 = 15p - 11,$$

quindi

$$2^{28} \equiv -330p + 121 \pmod{p^2}$$

da cui

$$3^2 \times 2^{28} \equiv -1876p - 4 \pmod{p^2}$$

e dividendo per 4

$$3^2 \times 2^{26} \equiv -469p - 1 \pmod{p^2}.$$

Elevando alla 7^a potenza:

$$3^{14} \times 2^{182} \equiv -4p - 1 \pmod{p^2}$$

e dalla (3) risulta

$$2^{182} \equiv -1 \pmod{p^2}$$

Finalmente elevando alla 6^a potenza,

$$2^{1092} \equiv 1 \pmod{p^2}. \quad \text{Q.E.D.}$$

Chiaramente dal momento che la congruenza (1) non vale in generale, qualsiasi dimostrazione valida per $p = 1093$ deve essere *Ad Hoc*.

Beeger [2] scoprì che anche 3511 soddisfa la congruenza (1). È da considerare che egli effettuò i calcoli a mano nel 1921, prima dell'era dei computers. *Che tenacia!* Ancora di più se si pensa che non era noto se esistevano altri esempi con $p > 1093$.

La ricerca fu continuata fino a 6×10^9 da D. H. Lehmer, poi da W. Keller, D. Clark e più recentemente da R. Crandall, K. Dilcher e C. Pomerance fino a 4×10^{12} (vedi [3]). Nessun primo che soddisfa la congruenza (1) fu trovato.

Tutto ciò è bello, ma perchè ci si interessa alla congruenza (1)?

Fu Abel, apparentemente solo per curiosità, che si domandò nel terzo volume del Crelle Journal (1828) se fosse possibile avere

$$(4) \quad a^{p-1} \equiv 1 \pmod{p^m}$$

con $m \geq 2$ e p primo che non divide a .

Jacobi, che era molto abile in calcoli numerici, diede vari esempi

di (4):

$$3^{10} \equiv 1 \pmod{11^2}, 7^4 \equiv 1 \pmod{5^2},$$

$$31^6 \equiv 1 \pmod{7^2}, \text{ e, con}$$

$$m = 3, 19^6 \equiv 1 \pmod{7^3}.$$

Ma il problema non è trovare esempi, ma è rispondere alla seguente domanda:

Ci sono infiniti numeri primi p tali che $2^{p-1} \equiv 1 \pmod{p^2}$?

Per studiare questa domanda riformuliamola in termini del quoziente di Fermat. Sia $a \geq 2$; se p è un primo che non divide a , allora

$$(5) \quad q_p(a) = \frac{a^{p-1} - 1}{p}$$

è un intero (per il piccolo teorema di Fermat) chiamato il *quoziente di Fermat*, con base a e esponente p . Quindi $q_p(a) \equiv 0 \pmod{p}$ se e solo se $a^{p-1} \equiv 1 \pmod{p^2}$.

Ci siamo così condotti a considerare il residuo modulo p di $q_p(a)$. È sorprendente il gran numero di risultati interessanti che legano il quoziente di Fermat a altre quantità aritmetiche interessanti. Vorrei illustrarlo con qualche esempio.

Il residuo modulo p di $q_p(a)$ si comporta come un logaritmo. Questo fatto fu notato da Eisenstein nel 1850:

$$(6) \quad q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}.$$

Determinazione del residuo di $q_p(a)$.

Il primo risultato di cui si hanno tracce è dovuto a Sylvester, che nel 1861 ha dimostrato la graziosa congruenza:

$$(7) \quad q_p(2) \equiv -\frac{1}{2} \left(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{\frac{p-1}{2}} \right) \equiv 1 + \frac{1}{3} + \dots + \frac{1}{p-2} \pmod{p}.$$

Più in generale, per ogni base a :

$$(8) \quad q_p(a) \equiv \sum_{j=1}^{p-1} \frac{a_j}{j} \pmod{p}$$

dove $0 \leq a_j \leq p-1$ e $pa_j + j \equiv 0 \pmod{a}$.

Nel 1910, Mirimanoff ha dimostrato: Se $p = 2^r \pm 1$ è un primo, allora $q_p(2) \equiv \mp 1/r \not\equiv 0 \pmod{p}$.

Più recentemente, Johnson [10] ha ottenuto un modo pratico per il calcolo del quoziente di Fermat. Se r è il più piccolo intero tale che $a^r \equiv \pm 1 \pmod{p}$, scritto $r = \pm 1 + tp$ si ha che

$$(9) \quad q_p(a) \equiv \mp \frac{t}{r} \pmod{p}.$$

Identità e congruenze per il Quoziente di Fermat.

Il primo articolo di rilievo sul quoziente di Fermat è di Lerch (1905) ed oggi è quasi dimenticato. È un piacere cogliere l'occasione per riproporre i suoi risultati.

Per prima cosa egli dimostrò:

$$(10) \quad \sum_{j=1}^{p-1} q_p(j) \equiv W(p) \pmod{p}$$

dove $W(p)$ denota il *quoziente di Wilson* che si definisce in maniera analoga a quella che ha portato alla definizione del quoziente di Fermat. Più precisamente il teorema di Wilson afferma che

$$(11) \quad (p-1)! \equiv -1 \pmod{p}$$

quindi il quoziente

$$(12) \quad W(p) = \frac{(p-1)! + 1}{p}$$

è un intero chiamato il *quoziente di Wilson* di p . Prima di tornare al quoziente di Fermat, vorrei aggiungere che il problema di determinare il residuo di $W(p)$ modulo p è interessante tanto quanto il corrispondente problema per il quoziente di Fermat. In particolare se

$W(p) \equiv 0 \pmod{p}$, allora p si dice *primo di Wilson*. Per esempio, basta un calcolo per verificare che $p = 5, 13$ sono primi di Wilson. La ricerca di nuovi primi di Wilson fino a $p < 4 \times 10^{12}$ (Crandall, Dilcher e Pomerance, [3]) ha reso possibile scoprirne solo un'altro (Golberg): $p = 563$. La domanda se esistano infiniti primi di Wilson sembra essere molto difficile. A tal proposito, Vandiver ha detto nel 1955:

Questa domanda sembra essere così difficile che se io dovessi resuscitare dopo la mia morte e qualche matematico mi dicesse di averla completamente risolta, ricadrei morto di nuovo.

Ritorniamo al problema di determinare il residuo del quoziente di Wilson.

Lerch ha dimostrato che

$$(13) \quad W(p) \equiv B_{2(p-1)} - B_{p-1} \pmod{p}$$

dove B_n denota l' n -esimo numero di Bernoulli. Tali numeri sono generati dalla funzione

$$(14) \quad \frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}.$$

Quindi $B_0 = 1$, $B_1 = -1/2$ e i numeri di Bernoulli soddisfano la relazione ricorsiva:

$$(15) \quad \binom{n+1}{1} B_n + \binom{n+1}{2} B_{n-1} + \binom{n+1}{3} B_{n-2} + \dots + \binom{n+1}{1} B_1 + 1 = 0.$$

Questa formula può essere scritta in modo simbolico mediante la formula:

$$(16) \quad (B+1)^{n+1} - B^{n+1} = 0.$$

(Si tratta B come una indeterminata e dopo aver calcolato il polinomio sul lato sinistro, si sostituisce B^k con B_k . Ricordare che $B_n = 0$ per ogni n dispari, $n \geq 3$.)

Un'importante proprietà dei numeri di Bernoulli, scoperta da Eulero, collega questi numeri alla funzione zeta di Riemann:

$$(17) \quad B_{2n} = (-1)^{n-1} \frac{2(2n)!}{(2\pi)^{2n}} \zeta(2n) \quad (\text{per } n \geq 1)$$

dove

$$(18) \quad \zeta(s) = \sum_{j=1}^{\infty} \frac{1}{j^s}, \quad s \text{ complesso e } \Re(s) > 1.$$

Usando l'equazione funzionale della funzione zeta di Riemann, si ha

$$(19) \quad \zeta(1-n) = -\frac{B_n}{n} \quad (\text{per } n \geq 2)$$

ed anche $\zeta(0) = -\frac{1}{2}$.

Tornando alla formula di Lerch (10) il punto è il seguente: poichè il calcolo del quoziente di Fermat è difficile, è più naturale trovare una relazione tra somme dei quozienti di Fermat su tutte le classi modulo p , a quantità definite per p .

Questo è stato fatto anche per somme con pesi. In una lettera del 1909 a Hensel, Friedman e Tamarkine dimostrarono: Se $1 \leq n \leq p-1$ allora:

$$(20) \quad \sum_{j=1}^{p-1} j^n q_p(j) \equiv (-1)^{\left[\frac{n}{2}\right]} \frac{B_n}{n} \pmod{p}.$$

Da (19) segue che se $1 \leq n \leq p-1$ allora:

$$(21) \quad \sum_{j=1}^{p-1} j^n q_p(j) \equiv (-1)^{\left[\frac{n-2}{2}\right]} \zeta(1-n) \pmod{p}.$$

e anche

$$\sum_{j=1}^{p-1} j q_p(j) \equiv -\frac{1}{2} = \zeta(0) \pmod{p}.$$

Lerch ha anche scoperto un collegamento tra il quoziente di Fer-

mat e il *quoziente di Legendre*

$$(22) \quad \lambda_p(j) = \frac{j^{\frac{p-1}{2}} - \left(\frac{j}{p}\right)}{p}.$$

Si rammenti che se $p \nmid j$ e $\left(\frac{j}{p}\right)$ è il simbolo di Legendre, allora

$$(23) \quad \left(\frac{j}{p}\right) \equiv j^{\frac{p-1}{2}} \pmod{p}$$

quindi $\lambda_p(j)$ è un intero.

Lerch ha dimostrato che:

$$(24) \quad q_p(j) \equiv 2 \left(\frac{j}{p}\right) \lambda_p(j) \pmod{p}.$$

Un'altra bella relazione coinvolge la distribuzione dei residui quadratici, e il numero di classe dei campi quadratici.

Denotiamo $H(a)$ il numero di classe di un campo quadratico $\mathbf{Q}(\sqrt{a})$ (dove a è un intero privo di fattori quadratici). Dirichlet provò la famosa formula per $p \equiv 3 \pmod{4}$

$$(25) \quad H(-p) = -\frac{1}{p} \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) j = \frac{\varrho - \varrho'}{2 - \left(\frac{2}{p}\right)}$$

dove

ϱ = numero dei residui quadratici tra 0 e $p/2$;

ϱ' = numero dei residui non-quadratici tra 0 e $p/2$.

È noto che $\varrho > \varrho'$ quando $p \equiv 3 \pmod{4}$. Questo è un teorema difficile. Le dimostrazioni fin ora conosciute fanno uso dell'analisi, nonostante l'enunciato sia di natura puramente aritmetica.

Friedman e Tamarkine notarono inoltre che

$$(26) \quad \varrho - \varrho' \equiv \left[2 - \left(\frac{2}{p}\right)\right] 2B_{\frac{p+1}{2}} \pmod{p}$$

da cui si ricava che

$$(27) \quad H(-p) \equiv 2B_{\frac{p+1}{2}} \pmod{p}.$$

Lerch ha inoltre dimostrato:

$$(28) \quad \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) jq_p(j) \equiv \begin{cases} 0 & \text{quando } p \equiv 1 \pmod{4} \\ H(-p) & \text{quando } p \equiv 3 \pmod{4}. \end{cases}$$

Passiamo ora a un teorema che ha suscitato interesse intorno al quoziente di Fermat aprendo nuove aree di ricerca.

I risultati che seguono hanno importanza storica. Non hanno perso il loro interesse dopo la dimostrazione dell'*Ultimo Teorema di Fermat* fornita da Wiles, perchè i metodi che ne derivano si possono applicare a altre equazioni diofantee. Per esempio *l'equazione di Catalan*

$$(29) \quad X^m - Y^n = 1.$$

Nel 1909, Wieferich dimostrò che se esistono interi x, y, z non multipli del numero primo dispari p e tali che $x^p + y^p + z^p = 0$ (in questa situazione diremo che il primo caso dell'ultimo teorema di Fermat è falso per p), allora

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Quindi, per quanto detto sopra, il primo caso dell'Ultimo Teorema di Fermat (=FLT) è vero per ogni esponente $p < 4 \times 10^{12}$ con le possibili eccezioni $p = 1093, 3511$.

La dimostrazione di Wieferich è molto difficile e tecnica. Essa è basata sul seguente profondo risultato di Kummer: Se il primo caso di FLT è falso per l'esponente p , con $x^p + y^p + z^p = 0$, p non divide xyz , allora

$$(30) \quad \left[\frac{d^{2s} \log(x + e^v y)}{dv^{2s}} \right] \times B_{2s} \equiv 0 \pmod{p}$$

per $2s = 2, 4, \dots, p-3$. (e simili congruenze per le coppie $(x, z), (y, z), (z, y), (x, z), (z, x)$).

Inoltre, Wieferich usa complicate congruenze soddisfatte dai numeri di Bernoulli. Nel 1912, Furtwängler ha trovato un'altra dimo-

strazione del Teorema di Wieferich. Questa dimostrazione usa la teoria del campo di classe ad ulteriore conferma della potenza di questa tecnica. Il Teorema di Wieferich è il primo di una serie di criteri che coinvolgono i quozienti di Fermat.

Nel 1910 Mirimanoff ha mostrato:

Se il primo caso di *FLT* è falso per un esponente p allora $q_p(3) \equiv 0 \pmod{p}$.

Dal momento che 1093 e 3511 non soddisfano la precedente congruenza, questo risolve il primo caso per tutti i primi minori di 4×10^{12} .

Questo lavoro è stato continuato da Frobenius, Vandiver, Morishima, Pollaczek, Rosser e più recentemente da Granville e Monagan.

Oggi si sa che se il primo caso è falso per p allora

$$(31) \quad q_p(l) \equiv 0 \pmod{p}, \quad \text{per } l \text{ primo, } l \leq 89.$$

Un corollario dovuto a Spunar che vale la pena ricordare è il seguente:

Sia p un primo dispari che soddisfa la seguente proprietà: (P₈₉)

Se esiste k , non multiplo di p tale che $kp = a \pm b$, dove tutti i fattori primi di a , b sono al più uguali a 89, allora il primo caso di FLT vale per l'esponente p .

La dimostrazione è così semplice che la darò adesso.

Se il primo caso è falso per l'esponente p allora per ogni primo l , $l \leq 89$, si ha $l^{p-1} \equiv 1 \pmod{p^2}$, per la formula (31). Quindi $a^{p-1} \equiv 1 \pmod{p^2}$ e $b^{p-1} \equiv 1 \pmod{p^2}$. Ne segue che $a^p \equiv a \pmod{p^2}$, e $b^p \equiv b \pmod{p^2}$.

Ma $a = \mp b + kp$ perciò $a^p \equiv \mp b^p \pmod{p^2}$. Da $kp = a \pm b \equiv a^p \pm b^p \equiv 0 \pmod{p^2}$ segue che p divide k e ciò è contro le ipotesi. Q.E.D.

In questo ambito c'è il seguente problema ancora aperto: Sono infiniti i primi con la proprietà (P₈₉)?

Puccioni ha dimostrato nel 1969: Se l'insieme sopra descritto

è finito allora per ogni primo l , $l \leq 89$, $l \not\equiv \pm 1 \pmod{8}$, l'insieme $M_l = \{p \mid l^{p-1} \equiv 1 \pmod{p^2}\}$ è infinito.

Sfortunatamente questo teorema potrebbe non significare nulla dal momento che entrambi gli insiemi in questione, che sembrano essere sparsi, potrebbero risultare infiniti.

Un corollario al risultato di Spunar, già dato da Mirimanoff, è il seguente:

Il primo caso di *FLT* vale per gli esponenti primi p della forma $p = 2^m \pm 1$.

È un semplice esercizio verificare che:

Se $2^m + 1$ è un numero primo allora $m = 2^n$ ($n \geq 0$).

I numeri

$$F_n = 2^{2^n} + 1$$

sono stati considerati per la prima volta da Fermat, ed oggi vengono appunto chiamati *numeri di Fermat*.

In modo simile se $2^m - 1$ è un numero primo allora $m = p$ è un primo. I numeri

$$M_p = 2^p - 1 \quad (p \text{ primo})$$

si chiamano *numeri di Mersenne*.

Fermat credeva che tutti i numeri di Fermat fossero primi. Infatti

$$F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

Tuttavia F_5 che è molto più grande, con circa 10 cifre, risulta composto. Eulero ha dimostrato nel 1747 il seguente criterio: Se p divide F_n ($n \geq 2$) allora $p = 2^{n+1}k + 1$ (con $k \geq 1$).

Egli ha applicato questo criterio ad F_5 provando che 641 divide F_5 , che quindi non è un numero primo.

Questo può essere verificato anche nella seguente maniera:

$$\begin{aligned} 641 &= 2^4 + 5^4 = 5 \times 2^7 + 1, \\ 2^{32} &= 2^4 \times 2^{28} = (641 - 5^4) \times 2^{28} = \\ &= 641 \times 2^{28} - (5 \times 2^7)^4 = \\ &= 641 \times 2^{28} - (641 - 1)^4 \equiv -1 \pmod{641}. \end{aligned}$$

Quindi 641 divide $2^{32} + 1 = F_5$.

Lo studio dei numeri di Fermat e dei numeri di Mersenne ha portato alla scoperta dei primi *test di primalità* per verificare quando dei grandi numeri sono o no primi.

Il primo criterio è dovuto a Lucas, sotto la forma di un inverso del piccolo teorema di Fermat:

Sia $n \geq 3$ dispari e supponiamo che esista a , $1 \leq a \leq n$ tale che

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

se per un qualsiasi primo p che divide $n-1$, risulta

$$a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$$

allora n è primo.

Basandosi su questo criterio Pepin ha dimostrato:

Il numero di Fermat F_n è primo se e soltanto se

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Una ricerca ad ampio raggio è stata effettuata sui primi di Fermat. Secondo le mie informazioni, che possono essere già superate, il più grande numero di Fermat esaminato è $F_{5050446}$ (composto).

Di solito sono necessari calcoli lunghi per stabilire se un numero di Fermat è composto. Al contrario di ciò che riteneva Fermat gli unici primi di Fermat conosciuti sono quelli che egli già conosceva!

Le seguenti congetture sono in successione meno forti delle affermazioni originali di Fermat:

(a) Eisenstein (1944): Esistono infiniti primi di Fermat;

(b) Schinzel (1963): Esistono infiniti numeri di Fermat privi di fattori quadratici (cioè prodotto di primi distinti).

Anche per i numeri di Mersenne, Eulero ha dato un primo criterio per determinarne i fattori: Se p è un primo, $p > 3$, $p \equiv 3 \pmod{4}$, allora $2p+1$ divide M_p se e soltanto se $2p+1$ è primo.

Con questo metodo Eulero ha concluso che 23 divide M_{11} , ..., 503 divide M_{251} , ecc ...

Il problema diventa quello di determinare i primi p tali che $2p + 1$ è ancora primo. Tali primi, non a caso, vengono chiamati *primi di Sophie Germain*. Sono stati presi in considerazione per la prima volta attorno al 1820, quando Sophie Germain ha dimostrato il seguente bel teorema che era di natura totalmente nuova: Se p e $2p + 1$ sono primi allora il primo caso di *FLT* è vero per l'esponente p .

Un problema aperto è il seguente: Esistono infiniti primi di Sophie Germain?

Confrontiamo questa domanda con la seguente (il problema dei primi gemelli): Esistono infiniti primi p tali che $p + 2$ è ancora primo?

In entrambi i casi si hanno polinomi lineari $2X + 1$ e $X + 2$ rispettivamente e la domanda è se essi assumono infiniti valori primi sui primi.

Vorrei descrivere un test di primalità molto efficace per i numeri di Fermat e di Mersenne scoperto da Lucas nel 1878. Esso usa le ricorrenze lineari del secondo ordine, o più precisamente, i numeri di Fibonacci e Lucas.

Nel secolo tredicesimo, Fibonacci ha considerato la seguente successione di numeri $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$, ... e più genericamente

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

(Spero che la notazione precedente non porti confusione con quella usata per i numeri di Fermat.)

I numeri di Fibonacci hanno un forte interesse aritmetico. Sono stati scritti libri in proposito, e esiste una rivista trimestrale che ha questi numeri come suo principale argomento.

Un'altra successione collegata è quella dei numeri di Lucas: $L_0 = 2$, $L_1 = 1$, $L_2 = 3$, $L_3 = 4$, $L_4 = 7$, $L_5 = 11$, ... e per $n \geq 2$

$$L_n = L_{n-1} + L_{n-2}.$$

Più in generale, dati due numeri U_0 e U_1 e $\alpha, \beta \in \mathbf{Q}$, poniamo

$$(32) \quad U_n = \alpha U_{n-1} + \beta U_{n-2}.$$

L'equazione $X^2 - \alpha X + \beta = 0$ ha come radici

$$a = \frac{\alpha + \sqrt{\alpha^2 - 4\beta}}{2}, \quad b = \frac{\alpha - \sqrt{\alpha^2 - 4\beta}}{2}$$

così che

$$\alpha = a + b, \quad \beta = ab$$

e

$$(33) \quad U_n = (a + b) U_{n-1} - ab U_{n-2}.$$

Per i numeri di Fibonacci e Lucas, $\alpha = 1$, $\beta = -1$, quindi $a = \frac{1 + \sqrt{5}}{2}$ (il numero aureo), $b = \frac{1 - \sqrt{5}}{2}$.

Dalla formula di Binet segue che

$$(34) \quad U_n = \frac{a^n - b^n}{a - b}$$

e definiamo *la successione compagna*:

$$(35) \quad V_n = a^n + b^n.$$

Ponendo:

$$(36) \quad W_n = \frac{V_{2^{n-1}}}{(ab)^{2^{n-2}}} \quad (\text{per } n \geq 2)$$

otteniamo

$$(37) \quad W_2 = \frac{\alpha^2 - 2\beta}{\beta}, \quad W_{n+1} = W_n^2 - 2.$$

Con una appropriata scelta di α e β , Lucas ha ottenuto l'utile «successione di prova»:

Nel caso in cui $p \equiv 1 \pmod{4}$, sia $W_2 = -4$, $W_{n+1} = W_n^2 - 2$; pertanto la successione è

$$-4, 14, 194, \dots$$

Il suo criterio è il seguente:

$M_p = 2^p - 1$ è primo se e soltanto se M_p divide W_p .

Se invece $p \equiv 3 \pmod{4}$, sia $W_2 = -3$, $W_{n+1} = W_n^2 - 2$, cosicché la

successione è

$$-3, 7, 47, \dots$$

Il suo criterio in questo caso è:

$M_n = 2^p - 1$ è primo se e soltanto se M_p divide W_p .

Questo è il metodo che viene ancora oggi usato per verificare se i numeri di Mersenne sono primi o no.

Nel 1644, Mersenne sapeva che per $p = 2, 3, 5, 7, 13, 17, 19, 31$, M_p è un primo di Mersenne.

Nel 1868, Lucas ha mostrato che se $p = 61, 89, 107, 127$, M_p è un primo di Mersenne.

Con l'avvento del computer, oggi conosciamo 39 primi di Mersenne di cui il più grande è $M_{13466917}$ che ha 4053946 cifre (scoperto nel 2001 da Cameron, Woltman e Kurowski e GIMPS (=Great Internet Mersenne Prime Search)).

Schinzel ha congetturato ciò che segue:

Esistono infiniti numeri di Mersenne privi di fattori quadratici. Ancora oggi nessun numero di Mersenne o Fermat con fattori quadratici è mai stato scoperto.

Nel 1965, Rotkiewicz ha considerato la precedente congettura dimostrando:

Se la congettura di Schinzel sui numeri di Mersenne è vera, allora esiste un numero infinito di primi p tale che $2^{p-1} \equiv 1 \pmod{p^2}$.

A questo proposito Rotkiewicz fece uso dell'interessante teorema, più volte riscoperto, di Zsigmondy (1892):

Se $n \neq 6$, $n \geq 3$, $a \geq 2$ allora esiste un primo p tale che l'ordine di a modulo p è uguale a n . Equivalentemente, esiste un primo p tale che p divide $a^n - 1$, ma p non divide $a^m - 1$ per $m < n$.

Questo teorema è stato scoperto da Zsigmondy (per $a = 2$), Kano, Artin, Pomerance, e ... chi altro? Mi piacerebbe saperlo.

Dal teorema di Rotkiewicz segue una sorprendente e, desidero dirlo, profonda connessione tra argomenti così dissimili come l'ultimo teorema di Fermat, la congruenza $2^{p-1} \equiv 1 \pmod{p^2}$ e la fattorizzazione di numeri di Mersenne.

Però mi sono allontanato dalla domanda principale.

C'è un ragionamento euristico che suggerisce che esistono infiniti numeri primi p tali che $2^{p-1} \equiv 1 \pmod{p^2}$. L'argomentazione è la seguente: Dato che non c'è nessuna ragione per credere il contrario, possiamo assumere (euristicamente) che per ogni numero primo p , la probabilità che $\frac{2^{p-1}-1}{p} \equiv 0 \pmod{p}$ sia $\frac{1}{p}$ dato che ci sono p classi resto modulo p . Se x è un qualunque numero reale positivo, allora il numero di numeri primi $p \leq x$ con $2^{p-1} \equiv 1 \pmod{p^2}$ dovrebbe essere

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + \text{errore}.$$

Quindi dovrebbero esistere infiniti numeri primi p che soddisfanno la precedente congruenza. Purtroppo questo argomento non si può rendere rigoroso.

Dai calcoli svolti, con solo due eccezioni, risulta sempre che $2^{p-1} \not\equiv 1 \pmod{p^2}$, quindi ci si aspetta che ci siano infiniti numeri primi p che soddisfano

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Questo non è ancora stato dimostrato, ma segue dalla importante e intrigante congettura (ABC) di Masser e Oesterlé: Per ogni $\varepsilon > 0$, esiste un numero $K(\varepsilon) > 0$ tale che per ogni A, B, C interi positivi con $\text{mcd}(A, B, C) = 1$ e $A + B = C$, risulta

$$(38) \quad C \leq K(\varepsilon) r^{1+\varepsilon}$$

dove r (il radicale di $A \cdot B \cdot C$) è il prodotto dei fattori primi distinti di $A \cdot B \cdot C$.

Per esempio se $\varepsilon = \frac{1}{2}$, $A = 2^m$, $B = 3^n$ (con m, n sufficientemente grandi), $C = 2^m + 3^n$ quindi da $C < K(1/2) r^{3/2}$ e $r = 6 \prod_{p|C} p$ ne segue che C deve avere un radicale molto grande.

La congettura (ABC) è divenuta subito un argomento «caldo». Effettivamente, è quasi immediato verificare che la congettura (ABC) implica l'ultimo teorema di Fermat.

Silverman ha dimostrato in [25]: Se la congettura (ABC) si

assume vera, allora esistono infiniti numeri primi p tali che $2^{p-1} \not\equiv 1 \pmod{p^2}$.

A momento c'è un grande interesse intorno alla congettura (ABC). Sarebbe estremamente importante se qualcuno la dimostrasse.

Il numero 1093, è interessante dopotutto...

BIBLIOGRAFIA

- [1] N. H. ABEL, *Aufgabe von Herrn N. H. Abel zu Christiania* in Norvegese, J. reine u. angew. Math., **3** (1828), 212.
- [2] N. G. W. H. BEEGER, *On a new case of the congruence $2^{p-1} \equiv 1 \pmod{p^2}$* , Messenger of Math., **51** (1922) 149-150.
- [3] R. CRANDALL - K. DILCHER - C. POMERANCE, *A search for Wieferich and Wilson primes*, Math. Comp., **66** (1997), 433-449.
- [4] F. G. EISENSTEIN, *Aufgaben*, J. reine u. angew. Math., **27** (1844), 87 (Ristampato su *Mathematische Werke*, Vol. 1, No. 3, Chelsea, New York 1975).
- [5] F. G. EISENSTEIN, *Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktionalgleichungen definiert werden*, Ber. über Verhandl. der Königl. Preuß. Akad. d. Wiss. zu Berlin, 36-42, 1850 (Ristampato su *Mathematische Werke*, Vol. 2, 705-712, Chelsea, New York, 1975).
- [6] C. FADIMAN - S. AARON, *The Joys of Wine*, Galahad Books, New York, 1981.
- [7] A. FREIDMANN - J. TAMARKINE, *Quelques formules concernant la théorie de la fonction $[x]$ et des nombres de Bernoulli*, J. reine u. angew. Math., **135** (1909), 146-156.
- [8] K. GOLDBERG, *A table of Wilson quotients and the third Wilson prime*, J. London Math. Soc., **28** (1953), 252-256.
- [9] R. K. GUY, *The primes 1093 and 3511*, Math. Student, **35** (1967), 204-206.
- [10] C. G. J. JACOBI, *Beantwortung der Aufgabe S. 212 dieses Bandes: «Kann $\alpha^{\mu-1} - 1$ wenn μ eine Primzahl und α eine ganze Zahl und kleiner als μ und größer als 1 ist, durch $\mu\alpha$ theilbar sein»*, J. reine u. angew. Math., **3** (1828), 301-303.
- [11] W. JOHNSON, *On the non-vanishing of Fermat's quotient $(\text{mod } p)$* , J. reine u. angew. Math., **292** (1977), 196-200.
- [12] E. LANDAU, *Vorlesungen über Zahltheorie*, Vol. 3. S. Hirzel, Leipzig, 1927 (Ristampato dal Chelsea, New York, 1969).

- [13] F. LE LIONNAIS, *Les grands courants de la pensée mathématique*, A. Blanchard, Paris, 1946.
- [14] M. LERCH, *Zur Theorie der Fermatschen Quotienten $(a^{p-1} - 1)/p \equiv q(a)$* , Math. Ann., **60** (1905), 471-490.
- [15] E. LUCAS, *Sur la recherche des grands nombres premiers*, Congrès de l'Assoc. Française pour l'Avancement des Sciences. Clermont-Ferrand, **5** (1876), 61-68.
- [16] E. LUCAS, *Théorie des fonctions numériques simplement périodiques*, Amer. J. of Math., **1** (1878), 184-240; 289-321.
- [17] D. MIRIMANOFF, *Sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **150** (1910), 204-206.
- [18] W. MEISSNER, *Über die Teilbarkeit von $2^p - 2$ durch das Quadrat der Primzahl $p = 1093$* , Sitzungsber. Akad. d. Wiss., Berlin, 1913, 663-667.
- [19] T. PEPIN, *Sur la formule $2^{2^n} + 1$* , C. R. Acad. Sci. Paris, **85** (1877), 329-331.
- [20] S. PUCCIONI, *Un teorema per una risoluzione parziale del famoso problema di Fermat*, Archimede, **20** (1968), 219-220.
- [21] P. RIBENBOIM, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.
- [22] A. ROTKIEWICZ, *Sur les nombres de Mersenne dépourvus de diviseurs carrés et sur les nombres naturels n tels que $n^2 | 2^n - 2$* , Matem. Vesnik **2**, **17** (1965), 78-80.
- [23] A. SCHINZEL, *Remarque au travail de W. Sierpiński sur les nombres $a^{2^n} + 1$* , Colloquium Math., **10** (1963), 137-138.
- [24] W. SIERPIŃSKI, *Sur les nombres composés de la forme $a^{2^n} + 1$* , Colloquium Math., **10** (1963), 133-135.
- [25] J. H. SILVERMAN, *Wieferich's criterion and the abc-conjecture*, J. Number Theory, **30** (1988), 226-227.
- [26] J. J. SYLVESTER, *Sur une propriété des nombres premiers qui se rattache au théorème de Fermat*, C. R. Acad. Sci. Paris, **52** (1861), 161-163 (Ristampato su *Math. Papers*, Vol. 2, 229-231, Cambridge Univ. Press, 1908).
- [27] J. J. SYLVESTER, *Note relative aux communications faites dans les séances du 28 Janvier et 4 Février 1861*, C. R. Acad. Sci. Paris, **52** (1861), 307-308 (Ristampato su *Math. Papers*, Vol. 2, 234-235; e Corrigenda, 241 Cambridge Univ. Press, 1908).
- [28] H. S. VANDIVER, *Extension of the criteria of Wieferich and Mirimanoff in connection with Fermat's last theorem*, J. reine u. angew. Math., **144** (1914), 314-318.
- [29] H. S. VANDIVER, *Divisibility problems in number theory*, Scripta Math., **21** (1955), 15-19.