Bollettino
Unione Matematica Italiana

Sezione A – La Matematica nella Società e nella Cultura

Paulo Ribenboim

Galimatias Arithmeticae

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **10-A**—*La Matematica nella Società e nella Cultura* (2007), n.1, p. 119–135.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2007_8_10A_1_119_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2007.

Bollettino U. M. I.
La matematica nella Società e nella Cultura
Serie VIII, Vol. X-A, Aprile 2007, 119-135

Galimatias Arithmeticæ (*)

Paulo Ribenboim

Nell'*Oxford English Dictionary* potete leggere che *galimatias* significa linguaggio confuso, discorso senza senso. Questo è quanto dovrete attendervi da questo discorso ([1]). Come segno di ammirazione per Gauss, mi permetto di inserire la parola *Arithmeticae* nel titolo. Senza offesa per il Principe, che a 24 anni pubblicò *Disquisitiones Arithmeticae*, l'imperituro capolavoro.

Avendo raggiunto la pensione (o, meglio, essendo stato raggiunto dal pensionamento), è arrivato il momento di riconsiderare gli eventi della mia carriera. A differenza di quanto fanno i più, io preferisco parlare di proprietà matematiche e di problemi su alcuni numeri connessi con le fasi salienti della mia vita. Riservo per il finale la più singolare di tali congiunzioni.

Inizierò con il numero 11, pieno di speranze, e finirò con l'inquietante 65.

(*) Questo lavoro è stato pubblicato originariamente in lingua inglese con lo stesso titolo Galimatias Arithmeticae sulla rivista Mathematics Magazine, **71**, n. 5, 1998, 331-340. Si ringrazia la Mathematical Association of America per averci concesso la autorizzazione alla traduzione ed alla riproduzione dell'articolo.

La traduzione è dovuta a Maurizio Laporta.

In accordo con l'autore, nel testo sono stati inclusi alcuni nuovi dati e sono state operate leggere modifiche per aggiornare le informazioni contenute nell'articolo originale del 1998.

([1]) Questo articolo è una versione modificata di un seminario tenuto all'Università di Monaco nel novembre del 1994 durante un festoso incontro in onore della Prof.ssa Sibylla Priess-Crampe.

11.

• All'età di 11 anni imparai ad usare la x per rappresentare quantità incognite allo scopo di risolvere problemi come questo: «La somma delle età di tre fratelli, nati a distanza di due anni, è uguale a 33. Quali sono le loro età?». La potenza del metodo mi fu immediatamente chiara e fu decisiva nel farmi interessare ai numeri, anche quando la mia età avrebbe superato il doppio della somma delle età dei tre fratelli.

Ma 11 è interessante per tante ragioni più valide.

• 11 è la più piccola repunità che è un numero primo. Un numero con n cifre tutte uguali ad 1 è detto *repunità* e denotato con R_n. Così $11 = R_2$. Le seguenti repunità sono note per essere numeri primi: R_n per $n = 2, 19, 23, 317, 1031$. Non si sa se vi siano infiniti numeri primi tra le repunità.

• Se $n > 11$, allora esiste un primo $p > 11$ tale che

$$p \quad \text{divide} \quad n(n+1)(n+2)(n+3)\ .$$

Solo una curiosità? Non proprio. Un bel teorema (di Mahler) asserisce che, se $f(x)$ è un polinomio a coefficienti interi di grado due o più (nel caso di grado 2 il teorema è dovuto a Pólya) e se H è un insieme finito di numeri primi (come $\{2, 3, 5, 7, 11\}$), allora esiste n_0 tale che dal fatto che tutti i fattori primi di $f(n)$ appartengano ad H segue che $n \leq n_0$.

Un altro modo di esprimere ciò è il seguente: $\lim_{n\to\infty} P[f(n)] = \infty$, dove $P[f(n)]$ denota il più grande fattore primo di $f(n)$. Mediante la teoria di Baker sulle forme lineari nei logaritmi, Coates fornì una stima effettiva per n_0. Nel caso particolare del polinomio $f(x) = x(x+1)(x+2)(x+3)$, la dimostrazione è elementare.

• 11 è il più grande tra gli interi positivi d, liberi da quadrati, tali che l'anello degli interi di $\mathbb{Q}(\sqrt{-d})$ sia euclideo. Gli altri campi siffatti sono quelli con $d = 1, 2, 3, 7$. Ciò vuol dire che, se $\alpha, \beta \in \mathbb{Z}[\sqrt{-d}]$, allora esistono $\gamma, \delta \in \mathbb{Z}[\sqrt{-d}]$ tali che $\alpha = \beta\gamma + \delta$, dove $\delta = 0$ oppure $N(\delta) < N(\beta)$. Qui si sia posto la *norma* $N(\alpha) = a^2 + db^2$ per ogni $\alpha = a + b\sqrt{-d}$. La situazione è del tutto simile a quella della divisione euclidea nell'anello $\mathbb{Z}$ degli interi usuali.

• Non è noto se esista un parallelepipedo rettangolo con lati le cui misure, a, b e c, siano intere, così come quelle delle diagonali. In altri

termini, non si sa se il seguente sistema abbia soluzione in interi non nulli:

$$\begin{cases} & a^2+b^2=d^2 \\ & b^2+c^2=e^2 \\ & c^2+a^2=f^2 \\ a^2+ & b^2+c^2=g^2 \end{cases}$$

Se tali interi esistono, allora 11 divide abc.

• 11 è il più piccolo intero che non è un *numerus idoneus*.

Non sapete cos'è un *numerus idoneus*? Anch'io ho dovuto compiere i 65 anni prima di capire come quest'età e i numeri *idonei* fossero in relazione. Quindi pazientate un poco.

• Secondo la teoria delle supersimmetrie il mondo è a 11 dimensioni: 3 per la posizione nello spazio, 1 per il tempo e 7 per descrivere le varie possibili superstringhe e i loro differenti modi di vibrazione, spiegando così il comportamento delle particelle subatomiche.

Si tratta di una burla o di un nuova teoria per descrivere il mondo?

• I numeri di Mersenne sono gli interi $M_q = 2^q - 1$, dove q è primo. Grosso problema: alcuni sono primi, altri sono composti. Problema più grosso: quanti di ciascun tipo? Mistero totale!

$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 28$. Questo è il più piccolo numero composto di Mersenne. Il più grande numero di Mersenne noto per essere composto è M_q, con

$$q = 137211941292195 \times 2^{171960} - 1\,.$$

19.

• Uno dei miei numeri preferiti è sempre stato il 19. A questa età Napoleone vinceva le battaglie — questo lo possiamo anche scordare. Alla stessa età, Gauss scopriva la legge di reciprocità quadratica — questa, una volta che l'abbiamo conosciuta, non la possiamo dimenticare.

• Prima una curiosità riguardante il numero 19. È il numero più grande n tale che

$$n! - (n-1)! + (n-2)! - \ldots \pm 1!$$

è un numero primo. Gli altri interi con questa proprietà sono

$$n = 3, 4, 5, 6, 7, 8, 9, 10, 15\,.$$

• Sia la repunità R_{19} sia il numero di Mersenne M_{19} sono numeri primi.

• Poniamo $U_0 = 0$, $U_1 = 1$ e $U_n = U_{n-1} + U_{n-2}$, per $n \geq 2$; questi sono i numeri di Fibonacci. Se U_n è primo, allora anche n deve essere primo, ma non viceversa. 19 è il più piccolo indice primo che fornisce un controesempio: $U_{19} = 4181 = 37 \cdot 113$.

• I campi $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{19})$ hanno numero di classi 1 (il numero di classi è un numero naturale che si associa ad ogni campo numerico; per il campo dei razionali è 1; pure per il campo dei numeri gaussiani è 1 e così per ogni campo le cui proprietà aritmetiche assomigliano a quelle dei numeri razionali; più è grande il numero di classi di un campo numerico, più le sue proprietà aritmetiche «deviano» da quelle dei razionali; per saperne di più si veda [3]). L'anello degli interi di $\mathbb{Q}(\sqrt{19})$ è euclideo, mentre quello di $\mathbb{Q}(\sqrt{-19})$ non lo è.

• Sia $n > 2$, $n \not\equiv 2 \pmod 4$, e si denoti con $\zeta_n = e^{2\pi i/n}$ una radice primitiva n-esima dell'unità. Il numero 19 è il più grande primo p tale che $\mathbb{Q}(\zeta_p)$ abbia numero di classi 1. Ciò fu importante per le ricerche di Kummer sull'Ultimo Teorema di Fermat.

Nel 1976 Masley e Montgomery determinarono tutti gli interi $n \not\equiv 2 \pmod 4$ tali che $\mathbb{Q}(\zeta_n)$ abbia numero di classi 1, vale a dire:

$$n = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28,$$
$$32, 33, 35, 36, 40, 44, 45, 48, 60, 84\,.$$

• Nel 1986 Balasubramanian, Dress e Deshouillers dimostrarono che ogni numero naturale è la somma di al più 19 quarte potenze. Davenport aveva dimostrato nel 1939 che ogni numero naturale sufficientemente grande è la somma di al più 16 quarte potenze. Ciò consentì una soluzione completa delle due forme del problema di Waring per le quarte potenze.

29.

• Primi gemelli, ad esempio 29 e 31, non sono come le età dei gemelli: la loro differenza è 2. Perché? Ci sono molte persone gemelle e molti numeri primi gemelli, ma in entrambi i casi non si sa se siano infiniti...

Eulero dimostrò che

$$\sum_{p \text{ primo}} \frac{1}{p} = \infty \ .$$

D'altra parte, Brun provò che

$$\sum_{p,\, p+2 \text{ primi}} \frac{1}{p} < \infty \ .$$

Il risultato di Brun ci dice che: o i primi gemelli sono in numero finito oppure che, se essi sono infiniti, allora il loro ordine di grandezza deve crescere così rapidamente che le suddette somme risultano limitate. Tutto ciò è ampiamente trattato nel mio libro sui numeri primi [5].

• Una curiosità notata da Eulero: se 29 divide la somma $a^4 + b^4 + c^4$, allora 29 divide il m.c.d.(a, b, c).

• Sia p un numero primo. Il *primoriale* di p è

$$p\sharp = \prod_{q \le p,\ q \text{ primo}} q \ ;$$

$29 = 5\sharp - 1$. Le espressioni $p\sharp + 1$ e $p\sharp - 1$ sono state considerate in relazione ad alcune varianti della dimostrazione di Euclide del fatto che esistono infiniti numeri primi. I seguenti primi p sono gli unici minori di 11213 tali che $p\sharp - 1$ sia primo:

$$p = 3, 5, 11, 13, 41, 89, 317, 991, 1873, 2053 \ .$$

Per questa e per sequenze simili si veda [5].

• $2 \cdot 29^2 - 1 = \square$ (un quadrato); similmente $2 \cdot 1^2 - 1 = \square$, $2 \cdot 5^2 - -1 = \square$. In realtà, ci sono infiniti numeri naturali x tali che $2x^2 - 1 = \square$. Ecco come ricavare tutte le coppie di numeri naturali (t, x) tali che $t^2 - 2x^2 = -1$. Da $(t + \sqrt{2}x)(t - \sqrt{2}x) = -1$, segue che $t + \sqrt{2}x$ è un'unità del campo $\mathbb{Q}(\sqrt{2})$. L'unità fondamentale è $1 + \sqrt{2}$ con norma $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$, così $t + \sqrt{2}x = (1 + \sqrt{2})^n$ per un dispari n. Quindi abbiamo

$$(1 + \sqrt{2})^2 = 3 + 2\sqrt{2};\ (1 + \sqrt{2})^3 = 7 + 5\sqrt{2};\ (1 + \sqrt{2})^5 = 41 + 29\sqrt{2} \ .$$

La soluzione successiva si ottiene da

$$(1 + \sqrt{2})^7 = 239 + 169\sqrt{2} \ ,$$

vale a dire $2 \cdot 169^2 - 1 = 239^2$.

• L'anello degli interi di $\mathbb{Q}(\sqrt{29})$ è euclideo. Ci sono 16 campi quadratici reali $\mathbb{Q}(\sqrt{d})$ con anello degli interi euclideo, corrispondenti a

$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73 \ .$$

• $2X^2 + 29$ è un *polinomio generatore ottimale di primi*. Questi polinomi furono considerati per la prima volta da Eulero. Sono polinomi $f \in \mathbb{Z}[X]$ che assumono come valori gli iniziali numeri primi, tanti quanti ne sono possibili. Più precisamente, sia $f \in \mathbb{Z}[X]$ con coefficiente direttore positivo e sia $f(0) = q$ un numero primo. Esiste il minimo $r > 0$ tale che $f(r) > q$ e $q | f(r)$. Il polinomio si dice *generatore ottimale di primi* se $f(k)$ è primo per $k = 0, 1, \ldots, r-1$.

Eulero notò che $X^2 + X + 41$ è un polinomio generatore ottimale di primi, giacché assume valori primi per $k = 0, 1, \ldots, 39$, ma $40^2 + 40 + 41 = 41^2$.

Nel 1912 Rabinovitch dimostrò che $f(X) = X^2 + X + q$ (con q primo) è un polinomio generatore ottimale di primi se e solo se il campo $\mathbb{Q}(\sqrt{1-4q})$ ha numero di classi uguale ad 1.

Heegner, Stark e Baker hanno determinato tutti i campi quadratici immaginari $\mathbb{Q}(\sqrt{d})$ (dove $d < 0$ è libero da quadrati) con numero di classi uguale ad 1:

$$d = -1, -2, -5, -7, -11, -19, -43, -67, -163 \ .$$

Questi corrispondono ai soli polinomi generatori ottimali di primi della forma $X^2 + X + q$, cioè $q = 2, 3, 5, 11, 17, 41$. Dei polinomi generatori di primi della forma $X^2 + X + q$ il record è $X^2 + X + 41$.

Frobenius (1912) e Hendy (1974) studiarono i polinomi generatori ottimali di primi in relazione ai campi quadratici immaginari con numero di classi 2. Ci sono tre tipi di tali campi:

(i) $\mathbb{Q}(\sqrt{-2p})$, dove p è un primo dispari;

(ii) $\mathbb{Q}(\sqrt{-p})$, dove p è primo e $p \equiv 1 \pmod 4$;

(iii) $\mathbb{Q}(\sqrt{-pq})$, dove p, q sono primi dispari, con $p < q$ e $pq \equiv 3 \pmod 4$.

Per campi dei tipi suddetti vale il seguente teorema:

(i) $\mathbb{Q}(\sqrt{-2p})$ ha numero di classi 2 se e solo se $2X^2 + p$ assume valori primi per $k = 0, 1, \ldots, p-1$.

(ii) $\mathbb{Q}(\sqrt{-p})$ ha numero di classi 2 se e solo se $2X^2 + 2X + \frac{p+1}{2}$ assume valori primi per $k = 0, 1, \ldots, \frac{p-3}{2}$.

(iii) $\mathbb{Q}(\sqrt{-pq})$ ha numero di classi 2 se e solo se $pX^2 + pX + \frac{p+q}{4}$ assume valori primi per $k = 0, 1, \ldots, \frac{p+q}{4} - 2$.

Stark e Baker classificarono i campi quadratici immaginari $\mathbb{Q}(\sqrt{d})$ (con $d < 0$ libero da quadrati) che hanno numero di classi 2. A seconda del loro tipo, essi sono:

(i) $d = -6, -10, -22, -58$

(ii) $d = -5, -13, -37$

(iii) $d = -15, -35, -51, -91, -115, -123, -187, -235, -267, -403, -427$.

Con tali valori di d si ottengono polinomi generatori ottimali di primi.

In particolare, $2X^2 + 29$ è un polinomio generatore ottimale di primi, con valori primi per $k = 0, 1, \ldots, 28$; esso corrisponde al campo $\mathbb{Q}(\sqrt{-58})$ che ha numero di classi 2.

• 29 è il numero delle topologie distinte su un insieme con 3 elementi. Si denoti con τ_n il numero delle topologie su un insieme con n elementi; così $\tau_1 = 1$ e $\tau_2 = 2$. Si conoscono i valori di τ_n per $n \leq 9$ (Radoux, 1975).

Avvicinandomi alla trentina (l'età della fiducia in se stessi), la vita mi sorrideva. Raggiunsi i 29 anni, che fu la prima età ad essere un numero primo gemello da quando ero diventato un matematico professionista. Così ora scelgo il numero

30.

• A quest'età ero a Bahia Blanca in Argentina, dove lavoravo ad un libro che si distingue, credo, per essere il libro di matematica pubblicato più a sud di tutti (almeno questo è vero per i libri su i gruppi ordinati, ma il mio non è il libro pubblicato più a nord tra tutti quelli su questa materia).

• Esiste solo un triangolo pitagorico primitivo con area uguale al suo perimetro; vale a dire $(5, 12, 13)$ con perimetro 30.

• 30 è il più grande intero d tale che, se $1 < a < d$ e m.c.d.$(a, d) = 1$, allora a è primo. Altri numeri con questa proprietà sono 3, 4, 6, 8, 12, 18, 24. Questo fu dimostrato la prima volta da Schatunowsky nel 1893 e

indipendentemente da Wolfskehl nel 1901 (Wolfskehl è quel ricco matematico che donò 100000 marchi d'oro da assegnarsi all'autore della prima dimostrazione dell'Ultimo Teorema di Fermat che fosse stata pubblicata in un'autorevole rivista di matematica).

Questo risultato ha la seguente interpretazione. Dati $d > 1$ e a tali che $1 \leq a < d$ e m.c.d. $(a, d) = 1$, dal teorema di Dirichlet si ha che esistono infiniti primi della forma $a + kd$ $(k \geq 0)$. Sia $p(a, d)$ il più piccolo primo siffatto e sia

$$p(d) = \max\{p(a, d) |\ 1 \leq a < d\,,\ \text{m.c.d.}\,(a, d) = 1\}\ .$$

Se $d > 30$, allora $p(d) > d + 1$. In particolare,

$$\liminf \frac{p(d)}{d+1} > 1\ .$$

Pomerance ha dimostrato che:

$$\liminf \frac{p(d)}{\varphi(d)\log d} \geq e^{\gamma}\ ,$$

dove $\varphi(d)$ è la funzione di Eulero in d e γ la costante di Eulero-Mascheroni.

D'altra parte, come fu mostrato da Linnik, per d sufficientemente grande si ha $p(d) \leq d^L$, dove L una costante. Heath-Brown ha dimostrato che $L \leq 5.5$.

32.

• 32 è il più piccolo intero n tale che il numero γ_n dei gruppi di ordine n (a meno di isomorfismi) sia più grande di n: $\gamma_{32} = 51$.

Odio il numero 32. A 32 gradi Fahrenheit l'acqua diventa ghiaccio e la neve inizia a cadere. Cambiamo argomento!

Le persone anziane ricordano meglio gli eventi della loro giovinezza e gli eventi del passato più recente. Io non ho dimenticato niente che non avessi voluto dimenticare, cosicché potrei raccontarvi a proposito degli anni 33, 34, ... Ma vorrei piuttosto concentrarmi sui 60.

60.

• 60 era la base nel sistema di numerazione dei Sumeri (circa nel 3500 a.C.). Oggi noi usiamo ancora il sistema sessagesimale in astronomia e per suddividere l'ora.

• 60 è un *numero altamente composto*. Questi numeri furono introdotti e studiati da Ramanujan (1915): il numero naturale n è *altamente composto* se $d(n) > d(m)$ per ogni m, $1 \leq m < n$, dove $d(n) =$ numero dei divisori di n. Così $d(60) = d(2^2 \cdot 3 \cdot 5) = 3 \cdot 2 \cdot 2 = 12$. I più piccoli numeri altamente composti sono:

$$2, 4, 6, 12, 24, 32, 48, 60, 120, 180, 240, 360, 720, 840, \ldots \ .$$

• 60 è un *numero unitariamente perfetto* secondo la prossima definizione. Un numero d è un *divisore unitario* di n se $d|n$ e m.c.d. $(d, n/d) = 1$; n è *unitariamente perfetto* se

$$n = \sum_{\substack{d=1 \\ d \text{ divisore} \\ \text{unitario di } n}}^{n-1} d \ .$$

Divisori unitari di 60 sono $1, 3, 4, 5, 12, 15, 20$ e la loro somma è effettivamente 60.

Congettura: esiste solo un numero finito di numeri unitariamente perfetti.

Tra i numeri unitariamente perfetti gli unici noti sono

$$6, 60, 90, 87360 \qquad \text{e} \qquad 2^{18} \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 37 \cdot 79 \cdot 109 \cdot 157 \cdot 313 \ .$$

• 60 è il numero di rette che sono intersezioni di coppie di piani delle facce di un dodecaedro.

• 60 è l'ordine del gruppo di isometrie dell'icosaedro. Questo è il gruppo alterno di 5 lettere. È il gruppo semplice non-abeliano di ordine minimo. I gruppi semplici sono stati classificati: una grande conquista! Esistono 18 famiglie infinite:

— gruppi ciclici di ordine primo;
— gruppi alterni A_n con $n \geq 5$;
— sei famiglie associate ai gruppi classici;
— dieci famiglie associate alle algebre di Lie (scoperte da Dickson, Chevalley, Suzuki, Ree e Steinberg).

Ci sono anche 26 gruppi «sporadici» che non appartengono alle suddette famiglie. Il gruppo sporadico con l'ordine più grande è il mostro di Fischer che ha

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \geq 8 \cdot 10^{53}$$

elementi.

61.

• Una curiosità: sia $k \geq 0$ e si considerino delle cifre $a_1, \ldots, a_k, x, y$. Se il numero (in notazione decimale)

$$a_1 a_2 \ldots a_k xyxyxyxyxy$$

è un quadrato, allora xy è uguale a 21, a 61 o a 84. Esempi:

$$1739288516161616161 = 1318820881^2;$$
$$258932382121212121 = 508853989^2.$$

• Il numero di Mersenne $M_{61} = 2^{61} - 1$ è un primo. Oggi sono noti 44 numeri primi di Mersenne $M_p = 2^p - 1$. Ecco la lista di tali numeri primi con i nomi degli scopritori nei casi significativi e con l'anno della scoperta ([2]). A tutt'oggi $2^{32582657} - 1$ è anche il più grande numero primo conosciuto.

p	Anno	Autore della scoperta
2	—	—
3	—	—
5	—	—
7	—	—
13	1461	Sconosciuto
17	1588	P.A. Cataldi
19	1588	P.A. Cataldi
31	1750	L. Euler
61	1883	I.M. Pervushin

([2]) Lo scopritore di $M_{13} = 1461$ è sconosciuto. Per saperne di più si veda L.E. Dickson, *History of the Theory of Numbers*, Vol. **I**, p. 6. Facciamo notare che $M_{13466917}$ è effettivamente il trentanovesimo numero primo di Mersenne, mentre non è ancora noto al momento se vi sono altri numeri primi di Mersenne compresi tra $M_{13466917}$ e $M_{32582657}$ oltre a $M_{20996011}$, $M_{24036583}$, $M_{25964951}$ e $M_{30402457}$ (ved. www.mersenne.org/status.htm) [NdT].

89	1911	R.E. Powers
107	1913	E. Fauquembergue
127	1876	E. Lucas
521	1952	R.M. Robinson
607	1952	R.M. Robinson
1279	1952	R.M. Robinson
2203	1952	R.M. Robinson
2281	1952	R.M. Robinson
3217	1957	H. Riesel
4253	1961	A. Hurwitz
4423	1961	A. Hurwitz
9689	1963	D.B. Gillies
9941	1963	D.B. Gillies
11213	1963	D.B. Gillies
19937	1971	B. Tuckerman
21701	1978	L.C. Noll e L. Nickel
23209	1979	L.C. Noll
44497	1979	H. Nelson e D. Slowinski
86243	1982	D. Slowinski
110503	1988	W.N. Colquitt e L. Welsh, Jr.
132049	1983	D. Slowinski
216091	1985	D. Slowinski
756839	1992	D. Slowinski e P. Gage
859433	1993	D. Slowinski e P. Gage
1257787	1996	D. Slowinski e P. Gage
1398269	1996	J. Armengaud, G.F. Woltman e GIMPS
2976221	1997	G. Spence, G.F. Woltman e GIMPS
3021377	1998	R. Clarkson, G.F. Woltman, S. Kurowski e GIMPS
6972593	1999	N. Hajratwala, G.F. Woltman, S. Kurowski e GIMPS
13466917	2001	M. Cameron, G.F. Woltman, S. Kurowski e GIMPS
20996011	2003	M. Shafer, G.F. Woltman, S. Kurowski e GIMPS
24036583	2004	J. Findley, G.F. Woltman, S. Kurowski e GIMPS
25964951	2005	M. Nowak, G.F. Woltman, S. Kurowski e GIMPS
30402457	2005	C. Cooper, S.R. Boone, G.F. Woltman, S. Kurowski e GIMPS
32582657	2006	C. Cooper, S.R. Boone, G.F. Woltman, S. Kurowski e GIMPS

62.

Questo numero è notevole per non essere interessante affatto. In verità supponiamo che, per una ragione o per l'altra, esista qualche numero che non sia notevole. Allora esiste il minimo numero non

notevole, che è dunque notevole per il fatto di essere il più piccolo numero non notevole.

Ma questo è solo un altro esempio di paradosso di Russell...

63.

• Questo numero appare in un ciclo associato all'*algoritmo di Kaprekar* per numeri a 2 cifre. Quest'algoritmo funziona come segue per numeri con k cifre: date k cifre $a_1 \dots a_k$ non tutte uguali, con $a_1 \geq a_2 \geq \dots \geq a_k \geq 0$, si considerino due numeri costituiti da queste cifre: $a_1 a_2 \dots a_k$ e $a_k a_{k-1} \dots a_1$. Si calcoli la loro differenza e si ripeta il processo con le k cifre così ottenute.

L'algoritmo di Kaprekar per 2, 3, 4 e 5 cifre conduce a punti fissi o ai cicli seguenti.

2 cifre	$\rightarrow$	ciclo:	$63-27-45-09-81$
3 cifre	$\rightarrow$	495	
4 cifre	$\rightarrow$	6174	
5 cifre	$\rightarrow$	uno dei tre cicli:	$99954-95553$
			$98532-97443-96642-97731$
			$98622-97533-96543-97641$

Esempio: $\{3, 5\}$: 53-35=18, 81-18=63, 63-36=27, 72-27=45, 54-45=09, 90-09=81.

• 63 è l'unico intero $n > 1$ tale che $2^n - 1$ non possieda un *fattore primo primitivo*. Spiegazione: se $1 \leq b < a$ con m.c.d. $(a, b) = 1$, si consideri la successione dei binomi $a^n - b^n$ per $n \geq 1$. Il primo p si dice che è un *fattore primitivo* di $a^n - b^n$ se $p | a^n - b^n$ e $p \not| a^m - b^m$ per $1 \leq m < n$.

Zsigmondy ha dimostrato, sotto le precedenti ipotesi, che ogni binomio $a^n - b^n$ possiede un fattore primo primitivo, eccetto nei casi seguenti:

(i) $n = 1$, $a - b = 1$;

(ii) $n = 2$, a e b dispari e $a + b$ una potenza di 2;

(iii) $n = 6$, $a = 2$ e $b = 1$.

Questo teorema ha molte applicazioni nello studio delle equazioni esponenziali diofantee (ved. [4]). Esplicitamente, quando $a = 2$ e $b = 1$,

la successione è:

$$1, 3, 7, 15 = 3 \cdot 5, 31, 63 = 3^2 \cdot 7, 127, 257, 511, 1023 = 3 \cdot 11 \cdot 31, \ldots$$

64.

64 è quasi 65, un numero di anni che ho detestato per averlo raggiunto, ma che, ciò nonostante, ha molti risvolti interessanti.

65.

65 è il più piccolo numero che è somma di 2 quadrati di numeri naturali in 2 modi differenti (a meno dell'ordine degli addendi):

$$65 = 8^2 + 1^2 = 7^2 + 4^2 \,.$$

Si ricordi il risultato di Fermat: n è somma di 2 quadrati se e solo se $v_p(n)$ è pari per ogni primo $p \equiv 3 \pmod 4$ (qui $v_p(n)$ denota il valore p-adico di n, cioè $p^{v_p(n)} | n$ e $p^{v_p(n)+1}$ non divide n). Il numero

$$r(n) = \#\{(a, b) : 0 \leq b \leq a \text{ e } n = a^2 + b^2\}$$

si esprime mediante la formula che segue. Per ogni $d \geq 1$, sia

$$\chi(d) = \begin{cases} (-1)^{\frac{d-1}{2}} & \text{se } d \text{ è dispari} \\ 0 & \text{se } d \text{ è pari} \,. \end{cases}$$

Sia $R(n) = \sum_{d|n} \chi(d)$. Allora

$$r(n) = \begin{cases} \dfrac{R(n)}{2} & \text{se } R(n) \text{ è pari} \\ \dfrac{R(n)+1}{2} & \text{se } R(n) \text{ è dispari} \,. \end{cases}$$

Esempio: $65 = 5 \cdot 13$ ha divisori $1, 5, 13, 65$ e $R(65) = \sum\limits_{d|65} \chi(d) = 4$, da cui $r(65) = 2$.

- 65 è la più piccola ipotenusa in comune a due triangoli pitagorici. Ciò segue dalla parametrizzazione dei lati dei triangoli pitagorici: se $0 < x, y, z$ con y pari e $x^2 + y^2 = z^2$, allora esistono a e b,

$1 \leq b < a$, tali che

$$x = a^2 - b^2\,; \qquad y = 2ab\,; \qquad z = a^2 + b^2\ .$$

Inoltre il triangolo è primitivo (cioè m.c.d. $(x, y, z) = 1$) se e solo se m.c.d. $(a, b) = 1$. Da $65 = 8^2 + 1^2 = 7^2 + 4^2$ si ricavano i triangoli pitagorici $(63, 16, 65)$ e $(33, 56, 65)$.

• Una curiosità: 65 è l'unico numero a 2 cifre d, e, con $0 \leq e < d \leq 9$, tali che $(de)^2 - (ed)^2 = \square$, un quadrato. Infatti, $65^2 - 56^2 = 33^2$, mentre l'unicità segue dalla parametrizzazione introdotta prima.

• 65 è anche un numero notevole di *seconda specie*, cioè esso conta i numeri notevoli che verificano qualche proprietà assegnata. In questo caso, 65 è forse il numero dei *numeri idonei* di Eulero. Dico «forse» perché si tratta ancora di un problema aperto, e invece di 65 potrebbero esistere anche 66 numeri siffatti.

Numeri idonei

Cosa sono questi *numeri idonei* di Eulero? Detti pure *numeri convenienti*, essi venivano usati convenientemente da Eulero per generare numeri primi.

Ora spiego cosa sono i *numeri idonei*. Sia $n \geq 1$. Se q è un primo dispari ed esistono interi $x, y \geq 0$ tali che $q = x^2 + ny^2$, allora:

(i) m.c.d$(x, ny) = 1$;

(ii) se $q = x_1^2 + ny_1^2$ con interi $x_1, y_1 \geq 0$, allora $x = x_1$ e $y = y_1$.

Ci possiamo porre la questione seguente. *Supponiamo che q sia un intero dispari e che $q = x^2 + ny^2$ con interi $x, y \geq 0$, in modo che le condizioni suddette (i) e (ii) siano soddisfatte. Allora q è un numero primo?*

La risposta dipende da n. Se $n = 1$, la risposta è «sì», come era noto a Fermat. Per $n = 11$ la risposta è «no»: $15 = 2^2 + 11 \cdot 1^2$ e le condizioni (i) e (ii) sono soddisfatte, ma 15 è composto. Eulero chiamava n un *numerus idoneus* se la risposta alla precedente questione è «sì».

Eulero fornì un criterio per stabilire in un numero finito di passi se

un assegnato numero fosse conveniente, tuttavia la sua dimostrazione aveva qualche falla. Gauss interpretò i numeri convenienti in termini della sua teoria delle forme quadratiche binarie: il numero n è conveniente se e solo se ogni genere della forma $x^2 + ny^2$ ha una sola classe. In seguito, nel 1874 Grube ([3]) scoprì il seguente criterio, impiegando nella dimostrazione il risultato di Gauss. Così, n è un numero conveniente se e solo se, per ogni $x \geq 0$ tale che $q = n + x^2 \leq \frac{4n}{3}$, dal fatto che $q = rs$ e $2x \leq r \leq s$ segue che $r = s$ oppure $r = 2x$.

Per esempio, 60 è un numero conveniente poiché

$$\begin{aligned} 60 + 1^2 &= 61\star\,, \\ 60 + 2^2 &= 64 = 4 \cdot 16 = 8 \cdot 8\,, \\ 60 + 3^2 &= 69\star\,, \\ 60 + 4^2 &= 76\star \end{aligned}$$

e i numeri segnati con $\star$ non hanno una fattorizzazione della forma indicata.

Per esempio, Eulero dimostrò che 1848 è un numero conveniente e che

$$q = 18518809 = 197^2 + 1848 \cdot 100^2$$

è un numero primo. Ai tempi di Eulero questo fu un risultato di un certo rilievo.

Ecco una lista dei 65 numeri convenienti scoperti da Eulero:

$$\begin{aligned} &1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, \\ &37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, \\ &130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, \\ &357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848\,. \end{aligned}$$

Ci sono altri numeri convenienti? Chowla dimostrò che esiste solo un numero finito di numeri convenienti; in seguito, un più raffinato studio analitico (ad esempio, di Briggs, Grosswald e Weinberger) rivelò che ci sono al più 66 numeri convenienti.

([3]) Il riferimento bibliografico del risultato di F. Grube è *Zeitschrift für Mathematik und Physik*, Vol. **19** (1874), 492-519 [NdT].

Il problema è difficile. L'esclusione di un *numerus idoneus* supplementare è di natura simile all'esclusione di un ipotetico decimo campo quadratico immaginario (di Heegner, Stark e Baker) di cui ho detto già.

Una straordinaria congiunzione.

Nel caso la vostra curiosità non sia stata ancora appagata, nel 1989 ad Atene, in occasione delle mie «Lezioni greche sull'Ultimo Teorema di Fermat», fui colpito da una straordinaria congiunzione di numeri. Una sola volta nella vita, e che non si ripeterà prima di...

Quell'anno mia moglie ed io avevamo 59 e 61 anni, primi gemelli (ma noi non siamo gemelli); quello stesso anno noi eravamo sposati da 37 anni, il più piccolo numero primo irregolare. Se siete ancora interessati, Kummer dimostrò che l'Ultimo Teorema di Fermat è vero per tutti gli esponenti dati da numeri primi dispari che sono regolari. Questi sono i primi p che non dividono il numero di classi dei campi ciclotomici generati dalla p-esima radice di 1. Kummer scoprì anche che 37 è il più piccolo primo irregolare. Peccato che il 1989 (l'anno delle mie lezioni ad Atene) non sia primo.

Così siete sfidati a trovare la prossima occorrenza di numeri come $37, 59, 61$, purché in un anno che corrisponda ad un numero primo.

NOTE. – Questo articolo sui numeri notevoli non sarebbe stato possibile se non fosse stato per l'originalissimo libro di F. Le Lionnais, *Les Nombres Remarquables*, pubblicato nel 1983 da Hermann a Parigi.

François Le Lionnais non era un matematico di professione, ma uno scrittore scientifico e, come tale, molto bene informato. Il suo libro *Les Grands Courants de la Pensée Mathématique* è molto impegnativo da leggere ancora oggi. Appena dopo la guerra egli racchiuse in questo libro le idee di alcuni giovani matematici francesi — ancora poco noti a quel tempo — che ben presto si sarebbero distinti. Una traduzione in inglese e l'originale sono disponibili nelle migliori biblioteche. Io posseggo una copia autografata del libro sui numeri notevoli con i ringraziamenti di Le Lionnais per aver richiamato la sua attenzione sul

numero 1093. A proposito di questo numero potete leggere il mio articolo, 1093, *Math. Intelligencer* **5** (1983), 28-34 ([4]).

Un altro libro dello stesso tipo, che mi è servito molto, è: D. Wells, *The Penguin Dictionary of Curious and Interesting Numbers*, Penguin, London, UK, 1986.

Per i risultati sui numeri algebrici, niente è più facile per me di citare il mio testo [3]. Per i *numeri idonei* si veda [1]. Riguardo ai fattori primitivi dei binomi si veda [4]. Per i numeri primi, i numeri di Fibonacci e argomenti simili, si veda [5]. Si veda [2] per ulteriori riferimenti.

Inutile dire che il seguente elenco di referimenti bibliografici è incompleto.

BIBLIOGRAFIA

[1] G. Frei, *Les nombres convenables de Leonhard Euler*, Publ. Math. Fac. Sci. Besançon, Théorie des Nombres, 1983-1984 (1985), 1-58.

[2] R.K. Guy, *Unsolved Problems in Number Theory*, 2nd edition, Springer-Verlag, New York, NY, 1994.

[3] P. Ribenboim, *Classical theory of algebraic numbers*, Springer-Verlag, New York, 2001.

[4] P. Ribenboim, *Catalan's Conjecture*, Academic Press, Boston, MA, 1994.

[5] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, NY, 1995.

Paulo Ribenboim: Department of Math. & Stats.
Queen's University, Kingston, Ontario
Canada K7L 3N6

([4]) Una traduzione in italiano di questo articolo è stata pubblicata sul *Bollettino U.M.I.*, Vol. **VI-A**, (2003), 165-182 [NdT].