Numeri di Mersenne

Marin Mersenne

Al giorno d'oggi è conosciuto soprattutto per i numeri che portano il suo nome, ma Marin Mersenne (1588-1648), frate dell'ordine dei Minimi, oltre che di questioni di matematica si occupò anche di filosofia, teologia, linguistica, astronomia, geometria, cosmologia, meccanica, acustica, ottica e musica, e fu probabilmente il più importante polo di raccolta e distribuzione di conoscenze del suo tempo. Finché visse infatti fu instancabile nel tessere una fittissima corrispondenza con tutti gli uomini di scienza dell'epoca (Cartesio, Hobbes, Fermat, Galilei, Huygens, Torricelli, Gassendi ed altri), mettendo in contatto l'uno con l'altro e promuovendo il dibattito e la cooperazione scientifica, contribuendo in modo determinante a diffondere nel continente europeo la conoscenza delle nuove scoperte scientifiche.

Fra le altre cose, si fece anche promotore di incontri settimanali, ai quali erano soliti intervenire molti degli intellettuali dell'epoca, per dibattere di argomenti scientifici o per ascoltare le relazioni dei soci o una comunicazione degli scienziati con cui Mersenne era in corrispondenza. Il principio ispiratore di questo cenacolo, dal quale sarebbe successivamente nata l'Accademia francese delle Scienze, era la completa autonomia della ricerca scientifica basata sulla metodologia sperimentale (oltre all'ortodossia in materia religiosa).

Nel suo libro "Cogitata physico-mathematica" del 1644 Mersenne si dedica allo studio dei numeri esprimibili nella forma $2^n - 1$, normalmente detti numeri di Mersenne e indicati col simbolo M_n.

Si tratta di numeri che godono di alcune interessanti proprietà: innanzi tutto, ognuno di loro equivale alla somma di tutte le potenze del 2, da 2^0 a 2^{n-1}. Ad esempio se n = 7, $M_7 = 2^7 - 1 = 128 - 1 = 127 = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 = 1 + 2 + 4 + 8 + 16 + 32 + 64$. Molti di loro sono numeri primi, anche se non tutti. Per *n* = 2, 3, 5, 7, 13 i relativi numeri di Mersenne valgono 3, 7, 31, 127, 8191, tutti numeri primi, ma per *n* = 4, 6, 8, 9, 10, 11, 12 il corrispondente numero di Mersenne non è primo. È facile dimostrare che se $2^n - 1$ è un numero primo, allora deve esserlo anche *n*, ma non è detto che il viceversa sia vero. Per questa loro proprietà la formula dei numeri di Mersenne viene utilizzata tutt'ora per cercare numeri primi di grandi dimensioni, dando a *n* soltanto valori primi.

Un'altra notevole caratteristica dei numeri di Mersenne è che essi sono legati ai numeri perfetti. Euclide aveva dimostrato che i numeri perfetti sono della forma $2^{n-1} \times (2^n-1)$ quando $2^n - 1$ è un numero primo, quindi per trovare i numeri perfetti occorre trovare per quali valori di *n* M_n è primo.

Mersenne studia tutti i valori di *n* fino a *n* = 257 sostenendo che M_1, M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}, M_{67}, M_{127}, M_{257} sono primi. Ai nostri occhi ha dell'incredibile il fatto che qualcuno abbia potuto imbarcarsi in un'impresa simile senza disporre di altri strumenti di calcolo all'infuori di carta e penna, basti pensare che M_{257} ha la bellezza di 78 cifre, e verificare se esso sia o meno primo ha dell'allucinante. In realtà, Mersenne aveva commesso qualche errore (perdonabile del resto data la complessità dei calcoli): aveva dimenticato M_{89} e M_{107} e aveva incluso M_{67} che non è primo al pari di M_{257} che egualmente non è primo essendo divisibile per tre numeri, rispettivamente di 15, 25 e 39 cifre.

A Mersenne comunque spetta il merito di aver trovato il più grande numero primo conosciuto senza ricorrere all'uso dei moderni strumenti di calcolo, esso è $2^{127} - 1$, un numero di 39 cifre. Il più grande numero primo di Mersenne attualmente conosciuto (ma forse questo primato oggi è già stato battuto) è $2^{57885161} - 1$, un numero mostruoso che ha diciassette milioni di cifre.

Nella tabella successiva *(vedi Immagine 42, pagina seguente)* sono indicati i numeri di Mersenne da 1 a 13, è precisato se essi sono primi, e quali di essi danno origine ai numeri perfetti: come si vede, cinque di loro sono primi e danno luogo ad altrettanti numeri perfetti.

I successivi cinque numeri perfetti, dei quarantotto finora scoperti, hanno i seguenti valori (per ovvie ragioni, facciamo grazia al lettore dei valori dei numeri perfetti successivi):

17	8.589.869.056
19	137.438.691.328
31	2.305.843.008.139.952.128
61	2.658.455.991.569.831.744.654.692.615.953.842.176
89	191.561.942.608.236.107.294.793.378.084.303.638.130.997.321.548.169.216

I matematici ritengono (ma non sono in grado di dimostrarlo, per cui si

n	2^{n-1}	2^n-1		$2^{n-1}\times(2^n-1)$	
1	1	1		1	
2	2	3	numero primo	6	numero perfetto
3	4	7	numero primo	28	numero perfetto
4	8	15	numero non primo	120	
5	16	31	numero primo	496	numero perfetto
6	32	63	numero non primo	2016	
7	64	127	numero primo	8128	numero perfetto
8	128	255	numero non primo	32640	
9	256	511	numero non primo	130816	
10	512	1023	numero non primo	523776	
11	1024	2047	numero non primo	2096128	
12	2048	4095	numero non primo	8386560	
13	4096	8191	numero primo	33550336	numero perfetto

Immagine 42

tratta di una congettura) che i numeri primi di Mersenne siano infiniti, al pari dei numeri perfetti. Altra cosa che si ignora è se esistano numeri perfetti dispari, tutti quelli conosciuti infatti sono pari, e finiscono con 6 oppure 8.

La scoperta dei più grandi numeri primi di Mersenne, e dei relativi numeri perfetti, ha appassionato per secoli i matematici; al giorno d'oggi ci si avvale di computer. Nel 1996 è stata creata negli Stati Uniti un'associazione, la Great Internet Mersenne Prime Search (GIMPS), con l'obbiettivo di scoprire nuovi numeri primi di Mersenne servendosi di migliaia di computer di volontari sparsi in tutto il mondo e connessi in rete; ai giorni nostri sono centinaia di migliaia quelli che partecipano al progetto. Dal 1996 a oggi (ma può darsi che questo primato sia già stato battuto), sono stati trovati quattordici nuovi numeri primi di Mersenne, da $2^{1398269}-1$ a $2^{57885161}-1$.

La Electronic Frontier Foundation aveva offerto un premio di centomila dollari alla prima persona che avesse scoperto un numero primo di Mersenne con dieci milioni di cifre, ed il premio è stato regolarmente assegnato a un matematico dilettante nel 2001. Dopo di allora, GIMPS ha scoperto altri nove numeri primi di Mersenne.

Può sembrare inconcepibile che matematici di vaglia (e anche dilettanti) dedichino il loro tempo a ricerche così particolari e, apparentemente, inutili. In effetti, gli amanti della matematica trovano che ricerche di questo tipo hanno un fascino unico e ineguagliabile.

La caccia ai numeri primi di Mersenne di dimensioni colossali continua, e sono ancora disponibili premi in denaro della Electronic Frontier Foundation per chi ne trova: centocinquantamila dollari a chi scoprirà un numero primo con cento milioni di cifre, e duecentocinquantamila per un numero primo con un miliardo di cifre. Se il cortese lettore vuole cimentarsi…

Fermat, il principe dei dilettanti

Pierre de Fermat

La vita

È singolare il fatto che uno dei più grandi matematici del periodo post-rinascimentale, forse il più grande fra quelli che precedettero l'arrivo di Newton e Leibniz, non fosse un uomo di scienza bensì un uomo di legge; la professione di Pierre Fermat (1601-65) infatti fu quella di giudice.

Della sua vita non sappiamo molto: egli nasce a Beaumont de Lomagne, in Francia, figlio di Dominique Fermat, commerciante di pellami abbastanza agiato da consentire a Pierre un'istruzione universitaria presso l'ateneo di Tolosa. Grazie ai suoi studi di giurisprudenza, nel 1631 Pierre è nominato consigliere presso il parlamento di Tolosa con l'incarico di vagliare le locali esigenze da sottoporre al consiglio della corona, far rispettare i regi decreti ed amministrare la giustizia in qualità di giudice. Fermat fa una rapida carriera nella pubblica amministrazione, in parte per il prestigio personale che sa conquistarsi e in parte per l'epidemia di peste scoppiata intorno alla metà del XVII secolo, che non risparmia molti dei suoi concorrenti in carriera. Fermat sopravvive e conquista una prestigiosa posizione sociale, con il diritto di usare il "de" come parte integrante del cognome.

Ad un giudice, anche se importante come lui, non è consentito di tenere relazioni sociali o familiarizzare con chicchessia, nel timore che un domani, in caso di processi in cui siano coinvolti dei conoscenti, manchi di imparzialità. Questa fu una fortuna per la matematica perché Pierre de Fermat è costretto a fare vita piuttosto ritirata, probabilmente monotona e priva di avvenimenti importanti. Ma ciò non gli è di peso, caratterialmente infatti egli è un uomo riservato anche se affabile, insensibile alle critiche ed agli elogi, la sua vita è illuminata soltanto da una grande passione, lo studio della matematica inteso come un hobby al quale dedica sempre tutto il proprio tempo libero.

Nonostante questa sua grande passione però Fermat non rende mai, o quasi mai, pubbliche le proprie scoperte; i risultati dei suoi studi ci sono noti perché pubblicati postumi da uno dei suoi figli, Clément Samuel, che in cinque anni di paziente lavoro raggruppa e mette ordine in tutti gli appunti del padre. Queste due caratteristiche – la matematica intesa come hobby e l'indifferenza a divulgare le proprie scoperte – sono tipiche della personalità di Fermat: quando egli scopre o intuisce una qualche verità matematica, oppure riesce a dimostrare un qualche teorema, non si preoccupa di farlo sapere ad alcuno; anzi, pago del risultato raggiunto, dedica subito la propria attenzione ad altri problemi. Per lui la soddisfazione consiste nell'affrontare e risolvere problemi nuovi, non negli elogi che potrebbe ricevere pubblicandone le soluzioni o rendendone partecipi gli altri, nemmeno i pochi matematici coi quali è in contatto epistolare.

Questo fa sì che probabilmente non conosciamo la totalità delle sue intuizioni e scoperte, e anche quel poco che ha rivelato ai matematici con cui è in contatto, o scrive da qualche parte come appunto personale, è quasi sempre senza spiegazioni né dimostrazioni, e spesso anche espresso in forma quanto mai oscura. Si pensi che nei propri appunti Fermat aveva annotato, senza darne dimostrazione alcuna, la bellezza di ben quarantotto enunciati. La dimostrazione delle sue geniali intuizioni verrà data da altri matematici ad anni (talvolta secoli) di distanza. Tipico al riguardo è il cosiddetto "ultimo teorema di Fermat" del quale ci occuperemo tra poco; in questo, come in altri casi, egli aveva scarabocchiato – senza dimostrazione o giustificazione alcuna – la sua tesi sul margine della pagina di un libro. Un altro esempio è la sua affermazione che qualsiasi numero naturale è sempre la somma di al massimo quattro quadrati perfetti (la dimostrazione fu trovata un secolo dopo da Lagrange).

Ci si è chiesti più volte il motivo di questa sua indifferenza alla divulgazione delle dimostrazioni delle proprie scoperte matematiche. Voleva tenerle solo per sé, era forse una forma di gelosia? Oppure sopravvalutava le capacittà dei colleghi matematici? O anche si divertiva a sfidarli? Probabilmente, nulla di tutto questo. Considerando la matematica un piacevole hobby, non sentiva la necessità di confidarsi con altri, né tantomeno gloriarsene, l'unico piacere per lui era la scoperta, e nient'altro.

È facilmente immaginabile come i matematici a lui posteriori fossero presi dal panico quando si imbattevano in una qualche sua affermazione, e si ponessero domande del tipo: l'avrà dimostrata? Sarà soltanto una congettura? E se avesse commesso un errore?

Da chi, o da cosa, ha tratto ispirazione Fermat nel coltivare gli studi matematici? Stranamente, non è stato un suo contemporaneo, bensì qualcuno vissuto quasi 1400 anni prima, o meglio un suo libro, l'Arithmetica di Diofanto di Alessandria, pervenutagli nella traduzione latina del suo contemporaneo Claude Gaspar Bachet de Méziriac. Il libro contiene, sotto forma di problemi e relative soluzioni, tutto lo scibile nel campo della teoria dei numeri ai tempi di Diofanto, conoscenze andate perdute o dimenticate nei secoli successivi. Dopo diciassette secoli di decadenza matematica, e a quasi quattordici dalla morte di Diofanto, Fermat non solo riscopre ma anche amplia, generalizza e trova nuovi significati nella sua opera. È da notare che Fermat, a differenza di altri matematici (come ad esempio Newton per il quale la matematica sarà uno strumento di esplorazione scientifica), è un matematico puro, che ama la matematica a prescindere dalle sue applicazioni pratiche. Infatti, la disciplina prediletta da Fermat è la <u>teoria dei numeri</u>, cioè quella parte della matematica che cerca di scoprire le proprietà dei numeri in se stessi e la ricerca delle loro relazioni reciproche (quella che i greci chiamavano <u>aritmetica</u>, per distinguerla dalla <u>logistica</u>, che riguardava le applicazioni pratiche dei calcoli al commercio).

Ma Fermat non si limita a questo: i suoi studi lo portano a elaborare alcune idee fondamentali del calcolo infinitesimale ben prima di Newton e Leibnitz, scopre un metodo generale per trattare problemi di massimo e minimo delle curve, è il primo ad applicare la geometria analitica allo spazio a tre dimensioni, assieme a Pascal è uno degli ideatori della teoria delle probabilità, affronta problemi di fisica ricavando le leggi della riflessione ottica (l'angolo di incidenza è eguale all'angolo di riflessione) e rifrazione (nel passaggio da un mezzo all'altro il seno dell'angolo di incidenza ha un rapporto costante col seno dell'angolo di rifrazione), si diletta perfino dello studio dei cosiddetti "quadrati magici".

I cosiddetti "quadrati magici"

Cosa sono i quadrati magici? Ne diamo qualche cenno.

Un quadrato composto da n^2 quadrati minori, entro i quali siano sistemati dei numeri tali che la loro somma per riga, per colonna e lungo le diagonali principali sia sempre la stessa è detto quadrato magico di ordine *n*, e la somma costante è detta costante magica del quadrato.

Si deduce immediatamente che qualsiasi quadrato magico rimane tale se ad ogni elemento si somma o si sottrae uno stesso numero o se lo si moltiplica o divide per uno stesso numero; la costante magica però non sarà più la stessa (anche se sarà facile calcolarla). Una volta trovato un quadrato magico, quindi, da questo se ne possono ricavare infiniti altri semplicemente aggiungendo, sottraendo, moltiplicando o dividendo i suoi termini per uno stesso numero.

Esiste (a parte rotazioni o riflessioni) un unico quadrato magico di ordine 3 in cui compaiono le cifre dall'1 al 9, la sua costante magica è 15 in quanto la somma dei primi nove numeri naturali vale 45, quindi la somma di ognuna delle tre righe o colonne deve essere 45 : 3 = 15; lo rappresentiamo qui sotto.

8	3	4
1	5	9
6	7	2

Esistono invece ben sedici quadrati magici di ordine quattro aventi come elementi i primi sedici numeri naturali, la loro costante magica vale 34. Uno di questi è il "quadrato di Dürer", cosiddetto perché è raffigurato in un quadro di Albrecht Dürer dal titolo: la melanconia.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

In esso la costante magica può essere ottenuta, oltre che per riga, colonna e diagonali principali, in ben altri ottantaquattro modi differenti (la somma dei quattro vertici, delle quattro caselle centrali, delle quattro caselle accanto ai vertici opposti, ecc.); di questi, trentasei sono ottenuti sommando posizioni chiaramente simmetriche come quelle descritte, altri ventiquattro godono di una qualche simmetria (ad esempio, 1, 8, 11, 14 oppure 5, 11, 4, 14), ed altri ventiquattro non godono di simmetrie evidenti (ad esempio 4, 7, 8, 15 oppure 5, 6, 9, 14).

Dürer ha evidenziato la data dell'opera, il 1514, al centro dell'ultima riga.

Se i numeri del quadrato magico di ordine n sono i primi n^2 numeri naturali, da 1 a n^2, la loro somma vale $n^2 \times {(n^2+1)}/{2}$; essendo n le righe, la somma costante di ogni riga deve valere $n \times {(n^2+1)}/{2}$. Inoltre, per i quadrati magici di ordine dispari, il numero centrale deve valere ${(n^2+1)}/{2}$. Ad esempio, la somma di tutti i numeri compresi in un quadrato magico di ordine 5 vale 325, la somma costante di ogni riga o colonna vale 65, e il numero centrale vale 13.

L'origine dei quadrati magici si perde nella notte dei tempi. Il primo quadrato magico è descritto in un manoscritto cinese del 3000 a.C., dalla Cina il loro utilizzo come amuleti si diffuse poi in India, nei paesi arabi, e infine nell'Europa medievale, dove probabilmente furono introdotti da cultori dell'astrologia, ed acquisirono subito proprietà magiche. Gli antichi infatti attribuivano virtù cabalistiche a certi numeri, è quindi logico che essi attribuissero virtù ancora maggiori a quadrati in cui la disposizione dei numeri offriva caratteristiche singolari.

Cornelio Agrippa (1486-1535) costruì quadrati magici di ordine 3, 4, 5, 6, 7, 8, 9; egli sosteneva che questi sette tipi di quadrati rappresentavano simbolicamente i sette pianeti allora conosciuti (compreso il Sole e la Luna, considerati alla stregua di pianeti nella visione tolemaica, non erano ancora conosciuti Urano e Nettuno). Dal fatto che non fosse possibile costruire un quadrato magico di ordine 2, cioè con quattro caselle, egli deduceva l'imperfezione dei quattro elementi aria, terra, acqua e fuoco. Partendo da queste cervellotiche ipotesi, un suo discepolo dedusse che non era possibile costruire il quadrato magico di ordine due perché era il simbolo del peccato originale.

Nel Medioevo un quadrato magico inciso su una lastra d'argento serviva a preservare chi lo portava dalla peste, e tuttora in alcune regioni d'oriente esso viene considerato come un talismano. Non è da stupirsi quindi che i quadrati magici avessero attirato la curiosità di molti dotti del tempo, ne fa fede la cospicua letteratura sull'argomento.

La soluzione generale del problema di disporre su un quadrato magico di ordine n i primi n^2 numeri naturali in modo da rendere costante la somma per riga, per colonna e per diagonale principale fu risolto da Fermat per i quadrati con un numero pari di righe, e da Pascal per i quadrati con un numero di righe dispari.

Lo studio dei quadrati magici ha portato alla scoperta di quadrati dalle caratteristiche particolari: ad esempio, esistono quadrati non magici che però diventano tali innalzando a potenza i loro elementi (sono detti "semplicemente magici), ci sono quadrati magici che rimangono tali sostituendo a ciascun numero lo stesso numero elevato ad una certa potenza (vengono detti "satanici" , ne esistono di ordine 8, 9, 10 e 14), sono detti "magici fino al grado n"

quei quadrati magici che rimangono tali per le loro prime, seconde,… n-sime potenze. Sono detti "diabolici" quei quadrati magici in cui la somma costante per riga, colonna e diagonale principale può essere ottenuta anche in altri modi, ad esempio (come nel quadrato di Dürer) sommando i quattro vertici o le quattro caselle centrali; sono detti, infine, "cabalistici" quei quadrati magici che siano al tempo stesso satanici e diabolici (ne esistono di ordine 8 e 9).

Nonostante gli studi sull'argomento, non è stata ancora scoperta la formula che dà il numero di quadrati magici di ogni ordine, si sa solo che tale numero "esplode" molto rapidamente (sono già 275.305.224 per il quinto ordine, senza contare rotazioni e riflessioni).

Accanto ai quadrati magici esistono anche i poligoni magici, che però hanno goduto di minori attenzioni per le loro inferiori doti di simmetria: i triangoli magici sono costituiti da un certo numero di triangoli equilateri concentrici in cui è costante la somma dei numeri posti sui lati di ciascun triangolo; i rettangoli magici hanno somme costanti per riga e per colonna; ci sono poi pentagoni magici, esagoni magici, e così via.

Esistono infine anche i cosiddetti "cubi magici", l'equivalente a tre dimensioni dei quadrati magici. Il più piccolo cubo magico esistente è stato scoperto il 13 novembre 2003 da due matematici, il francese Christian Boyer e il tedesco Walter Trump, con l'ausilio del computer. Si tratta di un cubo con cinque caselle di lato su cui sono disposti i numeri da 1 a 125, con 63 nel cubo centrale, che dà la somma di 315 in 109 modi diversi: per ciascuna riga (le righe sono 25), per ciascuna colonna (altre 25), e per ciascuna "profondità" (altre 25, in tutto 75 modi), per ogni diagonale (altri 30 modi) e infine nelle quattro diagonali che collegano i vertici opposti del cubo (altri 4 modi).

Il cosiddetto "ultimo teorema di Fermat"

Un teorema che per secoli ha appassionato i matematici è il cosiddetto "ultimo teorema di Fermat". Si tratta di un teorema dalla formulazione semplicissima, tale che anche un bambino è in grado di capirlo senza difficoltà; per questa sua apparente semplicità ci si sono appassionate persone dei più diversi livelli di cultura, e credo non esista un solo studente universitario di matematica che non abbia cercato – senza successo – di dimostrarlo.

Per capire meglio questo "ultimo teorema di Fermat" partiamo dal teorema di Pitagora che, come noto, dice che, se a e b sono i cateti di un triangolo rettangolo e c ne è l'ipotenusa, vale la relazione: $a^2 + b^2 = c^2$, relazione che è soddisfatta da numeri interi come 3, 4, 5 ($3^2 + 4^2 = 5^2$) e da tutte le cosiddette terne pitagoriche. Ciò significa che, se disponiamo di due quadrati costruiti sui cateti di un triangolo rettangolo, ad esempio di lati 3 e 4, e li scomponiamo in quadratini minori di lato 1, possiamo ricomporli per formare un quadrato di lato 5. La domanda che ci si può porre è allora: può valere una relazione analoga anche per i cubi, oltreché per i quadrati? In altre parole, esistono tre numeri interi tali che la somma dei cubi dei primi due sia eguale al cubo del terzo, $a^3 + b^3 = c^3$? Ciò equivarrebbe, in pratica, a trovare tre cubi geometrici a lati interi tali che scomponendo i primi due e ricomponendoli si ottenga esattamente il terzo cubo. E, proseguendo di questo passo, esistono numeri interi che soddisfino una relazione analoga anche per potenze superiori, ad esempio $a^4 + b^4 = c^4$, oppure $a^5 + b^5 = c^5$?

Verso la metà del '600 Pierre de Fermat scrisse sul margine di un foglio della propria copia del testo Arithmetica di Diofanto: "… generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere", cioè: "in generale, nessun numero che sia una potenza maggiore di due può esser scritto come somma di due potenze dello stesso valore". È questa l'enunciazione del cosiddetto "<u>ultimo teorema di Fermat</u>", che possiamo anche esprimere così: se n è un numero intero maggiore di 2, non esistono numeri naturali a, b, c tali che $a^n + b^n = c^n$. O, se si preferisce, la relazione $a^n + b^n = c^n$ è soddisfatta da numeri interi <u>soltanto</u> se $n = 2$ (ne sono esempi i numeri 3, 4, 5 oppure 5, 12, 13), oppure se $n = 1$ (caso banale). Quindi, nel caso dei tre cubi di cui abbiamo parlato, Fermat non solo esclude che essi possano esistere, ma afferma altresì che la relazione $a^n + b^n = c^n$ non può essere soddisfatta per alcun valore intero di n eccetto il 2.

Per quale motivo la dimostrazione di questo teorema ha appassionato (ma sarebbe più giusto dire ossessionato) tanto i matematici? Perché Fermat aggiunse alla sua nota a margine anche la seguente scritta: "cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet", cioè: "dispongo di una meravigliosa dimostrazione di questo teorema, che non può essere contenuta nel margine troppo esiguo della pagina".

Quando scrisse questa frase, Fermat aveva trentasei anni, e non tornò più sull'argomento per i rimanenti ventotto della sua vita, né per confermarla, né per smentirla. La domanda che sorge spontanea è allora: quale può essere questa "meravigliosa" dimostrazione? Domanda complicata dal fatto che non si ha nessuna idea di quale possibile strada logica abbia seguito Fermat: aveva tratto ispirazione dall'Arithmetica di Diofanto? Dalla teoria dei numeri? Era arrivato alla conclusione per via algebrica? Per via geometrica? In quale altro modo? D'altra parte, Fermat non era certo uomo da sbandierare le sue scoperte, egli faceva matematica per puro diletto personale, indifferente alla divulgazione delle proprie geniali intuizioni.

Dopo la sua morte, quando venne alla luce la copia dell'Arithmetica di Diofanto su cui era scritta la frase incriminata, iniziò la gara a trovare la "meravigliosa dimostrazione", e l'affermazione di Fermat prese il nome di "ultimo teorema di Fermat". Nessuno, infatti, era mai riuscito a trovare numeri naturali a, b, c, n (con $n>2$) tali che $a^n + b^n = c^n$, e tutto lasciava pensare che non ne esistessero, ma fino alla dimostrazione non se ne poteva essere sicuri. Mancando quest'ultima, più che di "teorema" di Fermat molti parlavano di "congettura" di Fermat.

Nel corso degli anni però alcuni risultati si erano ottenuti: Fermat stesso, anche se nel suo solito modo criptico, aveva dimostrato che il teorema era valido per $n = 4$ (cioè, non possono esistere numeri interi a, b, c tali che $a^4 + b^4 = c^4$); cent'anni dopo Eulero dimostrò che il teorema era valido anche per $n = 3$. In queste affermazioni è implicita la validità del teorema anche per tutti i multipli di 4 e 3, infatti se fosse possibile la relazione $a^8 + b^8 = c^8$ varrebbe anche quella $(a^2)^4+(b^2)^4=(c^2)^4$; quindi bastava limitarsi a dimostrare il teorema se n era un numero primo. Nel 1825 Dirichlet e Legendre dimostrarono valido il teorema anche per $n = 5$, nel 1839 Lamé per $n = 7$, Kummer fra il 1847 e il 1857 per qualsiasi n inferiore a cento, nel 1980 il teorema fu dimostrato valido per qualsiasi intero inferiore a 125000, mancava però sempre la dimostrazione generale.

La dimostrazione generale che Fermat aveva detto di aver dato si dimostrò talmente elusiva che furono promessi ricchi premi a chi fosse riuscito a trovarla, ed è curioso invece il fatto che non si offriva nulla a chi l'avesse invalidata (cioè, se qualcuno avesse trovato quattro numeri interi a, b, c, n, con $n>2$, tali che $a^n + b^n = c^n$). Nel 1853 l'Accademia Francese delle Scienze bandì un concorso tra matematici, con in premio tremila franchi e una medaglia d'oro. Furono presentate undici memorie nessuna delle quali risolveva il problema, ma ognuna delle quali portava un contributo alla sua soluzione. Nel 1908 la Regia Società delle Scienze di Gottinga promise un premio di centomila marchi tedeschi dell'epoca a chi, matematico o dilettante, fosse riuscito a dimostrare l'ultimo teorema di Fermat. Ma nemmeno questo incentivo ottenne risultati, anche se molti, soprattutto dilettanti, inviarono "dimostrazioni" che alla prova dei fatti si dimostrarono tutte errate: seicentoventuno nel primo anno, e molte migliaia gli anni successivi.

Tutte le "dimostrazioni" venivano vagliate dagli esaminatori, e divise in due categorie: le soluzioni "eretiche", cioè fuori della grazia di Dio, e quelle che avevano una qualche parvenza di serietà, ma alla fine anche in queste ultime si scopriva l'errore. A tutte veniva data risposta, ma all'aumentare del numero delle "dimostrazioni" del primo tipo (quelle eretiche) gli esaminatori ricorsero a sistemi più spicci, ad esempio uno di loro mandava ai concorrenti risposte del tipo: "Dispongo di una meravigliosa confutazione della sua dimostrazione, ma purtroppo questa pagina non è abbastanza grande per contenerla". Un altro, invece, rispondeva di dichiararsi incompetente a esaminare la dimostrazione, tuttavia consigliava di rivolgersi ad un esperto in grado di farlo, e gli forniva i dati di un altro dilettante eretico.

Fu solo nel settembre 1994 che un matematico inglese, Andrew Wiles, finalmente riuscì a raggiungere lo scopo dopo otto anni di lavoro, fornendo una dimostrazione talmente iperspecialistica che, come disse qualcuno, soltanto un matematico su mille era in grado di capirla.

Anzi, a dire la verità, la dimostrazione – che nella formulazione iniziale conteneva un errore, successivamente corretto da Wiles – fu resa pubblica nel giugno del 1993, a un congresso tenutosi presso il Sir Isaac Newton Institute for Mathematical Sciences di Cambridge. Wiles fece i suoi interventi in tre conferenze di un'ora ciascuna, senza comunicare a nessuno dove voleva andare a parare. Quando finalmente il terzo giorno arrivò alla conclusione: "Così questo dimostra l'ultimo teorema di Fermat", dopo un secondo di silenzio allibito, scoppiò un'ovazione da parte dei congressisti, notevolmente aumentati in quei tre giorni, essendosi sparsa la voce della possibile conclusione della relazione di Wiles.

La notizia fu ripresa da tutta la stampa mondiale: Il Washington Post definì Wiles "l'uccisore del drago matematico", il New York Times annunciava in prima pagina: "Finalmente un grido, Eureka! risolve un antico mistero matematico".

La dimostrazione di Wiles era basata su teoremi sviluppati almeno trecento anni dopo l'epoca di Fermat, era quindi sicuramente diversa da quella ideata da lui. Restano allora soltanto due ipotesi: esiste una bellissima dimostrazione che aspetta ancora di essere trovata, oppure Fermat aveva preso un abbaglio? Questo interrogativo probabilmente rimarrà per sempre avvolto nel mistero.

Del resto, anche Fermat aveva preso qualche cantonata. Ad esempio, aveva affermato che tutti i numeri del tipo: 1 + (2 elevato ad una potenza di 2) (cioè, $1 + 2^1 = 3$, $1 + 2^2 = 5$, $1 + 2^4 = 17$, $1 + 2^8 = 257$, $1 + 2^{16} = 65537$ ecc.) erano primi. Eulero, cento anni dopo, dimostrò che Fermat si era sbagliato, infatti $1 + 2^{32} = 4294967297$ non è un numero primo, essendo divisibile per 641. Ma anche Eulero, a sua volta, aveva fatto un'affermazione dimostratasi falsa: nel 1769 egli aveva sostenuto: "per ogni numero <u>intero</u> $n > 2$, la somma di $n - 1$ potenze n-esime di interi positivi non può uguagliare una potenza n-esima"; cioè, per dirla con parole più semplici: non possono esserci tre numeri interi che elevati alla quarta potenza diano un intero elevato alla quarta potenza. Questa affermazione si rivelò errata, infatti: $95800^4 + 217519^4 + 414560^4 = 422481^4$.

Accanto all'ultimo teorema, esiste anche un cosiddetto "<u>piccolo teorema di Fermat</u>". Anche di questo la formulazione è semplicissima, e neppure di questo Fermat aveva dato dimostrazione, tanto che essa fu trovata soltanto una cinquantina d'anni dopo da Leibnitz. Il piccolo teorema dice questo: se n è un numero primo, per ogni intero a il numero $a^n - a$ è un multiplo di n. Una formulazione tanto semplice quanto invece difficile ne è la dimostrazione.

Il "teorema di Natale"

Abbiamo già detto come Pierre de Fermat abbia messo in crisi generazioni di matematici con l'enunciazione del suo indimostrato teorema, e come anche il cosiddetto "piccolo teorema di Fermat" abbia fatto sudare i matematici prima di essere dimostrato. Ma esiste un altro teorema in cui Fermat ha dimostrato il proprio genio e assieme la propria avversità a dare dimostrazioni esplicite ed esaurienti: è giunta fino a noi una sua lettera datata 25 dicembre 1640, indirizzata a Marin Mersenne, nella quale viene descritta una scoperta notevole a proposito dei numeri primi. Dato che la lettera fu inviata il giorno di Natale, il teorema venne chiamato "il teorema di Natale".

Fermat aveva notato che alcuni numeri primi si potevano scrivere come somma di due quadrati, come ad esempio 53, risultato di $2^2 + 7^2$, mentre per altri tale proprietà non sussisteva, come ad esempio per il numero 31. Egli scrisse in quella lettera che aveva scoperto per quale motivo vi fosse quel diverso comportamento, senza però darne una spiegazione esauriente.

Una spiegazione completa fu trovata soltanto cento anni più tardi da Eulero, e successivamente da Minkowski. Comunque sia, l'intuizione di Fermat fu notevole, e il ragionamento (qui lo presenteremo in forma incompleta) che lo portò alla conclusione fu questo: ogni numero primo (se si esclude il 2 che è l'unico numero primo pari e come tale di comportamento anomalo) deve essere dispari, cioè del tipo $4k + 1$ oppure $4k + 3$ (con k numero intero). Tutti i quadrati di numeri interi devono essere della forma $4k$ oppure $4k + 1$, a seconda che provengano dall'elevamento di un numero pari oppure dispari [un numero pari n può essere scritto come $2k$ il cui quadrato è $4k^2$; un numero dispari può essere scritto come $2k + 1$ il cui quadrato è $4 \times (k^2 + k) + 1$]; d'altra parte se si sommano due quadrati, il risultato può essere multiplo di 4 (se proviene da due numeri pari), oppure multiplo di 4 + 1 (uno pari e uno dispari), oppure multiplo di 4 + 2, (due dispari), ma mai multiplo di 4 + 3. Quindi nessun numero primo nella forma $4k + 3$ può essere somma di due quadrati.

Naturalmente, ciò non dimostra che tutti i numeri primi del tipo $4k+1$ siano sempre somma di due quadrati, ma come detto tale fatto fu avvalorato più tardi. Si potrebbe dire che Fermat aveva dimostrato che affinché un numero primo sia somma di due quadrati è necessario che sia del tipo $4k + 1$, senza aver dimostrato (o almeno senza aver esplicitato la dimostrazione) che ciò è anche sufficiente.

Niccolò Fontana, detto Tartaglia

Niccolò Tartaglia, come appare sulla copertina di un libro a lui dedicato

La vita

Pochi conoscono questo matematico col suo vero nome di Niccolò Fontana (1500-57), dai più è noto col soprannome di Tartaglia, attribuitogli per la sua balbuzie. In realtà, egli non era nato con questo difetto, la causa fu una ferita infertagli dai soldati francesi nel duomo di Brescia durante il "sacco di Brescia" del 1511. Come scrive egli stesso nella sua autobiografia: "io ve dirò quando che li Franzesi saccheggiorno Bressa… essendo io fugito nel domo di Bressa insieme con mia madre et mia sorella et molti altri huomini, credendone in tal luogo esser salvi … mi fur date cinque ferite mortali, cioè tre sulla testa (che in cadauna la panna del cervello si vedeva) et due sulla fazza, che se la barba non me le occultasse io pareria un mostro, fra le quali una ve ne aveva a traverso la bocca et denti, la qual della massella e del palato superiore me ne fece due parti, et el medesimo della inferiore. Per la qual ferita non solamente io non poteva parlare (salvo che in gorga come fanno le gazzole), ma neanche poteva manzare, perché io non poteva movere la bocca né le masselle in conto alcuno, per essere quelle (come detto) insieme con li denti tutte fracassate…".

Fortunatamente, e grazie alle cure della madre, Niccolò riesce a sopravvivere, sia pur deformato dalle ferite, e prosegue nel racconto: "or essendo io quasi guarito di tali ferite, stetti un tempo che io non poteva ben profferire parole, ma sempre balbutava nel parlare per causa di quella ferita a traverso la bocca et denti (non ancora ben consolidata), per il che i putti della mia età con chi conversava me imposero per sopra nome Tartaglia". Niccolò accetta di buon grado questo soprannome, tanto che non esita a firmarsi Tartaglia.

La famiglia di Tartaglia è povera, il padre muore quando Niccolò ha appena sei anni, egli impara da solo a leggere, scrivere e far di conto, attività quest'ultima in cui eccelle tanto che si guadagna da vivere dando lezioni private e consulenze come maestro d'abaco. Nel 1518 si trasferisce a Verona e nel 1534 a Venezia dove insegna matematica e scopre la soluzione dell'equazione di terzo grado, che però non pubblica. Si dedica invece alla pubblicazione di altre opere, tra le quali: *General trattato di numeri e misure* (opera enciclopedica di matematica elementare, dove compare il triangolo che porta il suo nome), *Nova scientia* (che tratta di balistica), e *Euclide megarense*, opera divulgativa degli elementi di Euclide.

La parte finale della sua vita è amareggiata dalla lunga disputa con Girolamo Cardano e il suo allievo Ludovico Ferrari per la priorità della scoperta della soluzione delle equazioni di terzo grado, soluzione pubblicata da Cardano.

Il triangolo di Tartaglia

Il cosiddetto "triangolo di Tartaglia" è il seguente:

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1
1 9 36 84 126 126 84 36 9 1
1 10 45 120 210 252 210 120 45 10 1
1 11 55 165 330 462 462 330 165 55 11 1
1 12 66 220 495 792 924 792 495 220 66 12 1
…………………………………………………………………

Immagine 43

Come si può verificare, ogni numero è pari alla somma dei due che gli stanno immediatamente sopra.

Il triangolo gode di alcune proprietà: innanzitutto, ogni riga dà i coefficienti numerici dello sviluppo del binomio $(a+b)$ elevato ad una qualsiasi potenza. Vediamolo subito in pratica:

$(a+b)^0 = 1$
$(a+b)^1 = a + b$
$(a+b)^2 = a^2 + 2ab + b^2$
$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$
$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$
ecc.

In generale, nella riga $n + 1$ del triangolo si trovano i coefficienti della potenza n-esima del binomio $a + b$; per questo motivo i numeri del triangolo di Tartaglia sono anche detti coefficienti binomiali.

Ma le proprietà del triangolo di Tartaglia sono altre, molte di esse furono scoperte da Blaise Pascal, tanto che il triangolo è anche conosciuto col nome di "triangolo di Pascal". Per comprendere meglio tali proprietà, rappresentiamo il triangolo nella forma indicata di seguito, come faceva Pascal:

riga													
0	1												
1	1	1											
2	1	2	1										
3	1	3	3	1									
4	1	4	6	4	1								
5	1	5	10	10	5	1							
6	1	6	15	20	15	6	1						
7	1	7	21	35	35	21	7	1					
8	1	8	28	56	70	56	28	8	1				
9	1	9	36	84	126	126	84	36	9	1			
10	1	10	45	120	210	252	210	120	45	10	1		
11	1	11	55	165	330	462	462	330	165	55	11	1	
12	1	12	66	220	495	792	924	792	495	220	66	12	1

....

Si vede che:

Numerando le righe come indicato in figura, la somma dei termini di ogni riga è la successione delle potenze del 2: $1 = 2^0$, $1+1=2^1$,$1+2+1=2^2$, $1+3+3+1= 2^3$, ecc; il che equivale a dire che la somma dei termini della n-esima riga è 2^n, che la somma dei termini di ogni riga è il doppio della precedente, e che la somma dei termini di ogni riga è uguale alla somma dei termini di tutte le righe che la precedono, aumentata di 1.

La prima colonna è formata tutta da 1, la seconda è la successione dei numeri naturali, la terza dà i numeri triangolari. Per gli amanti del difficile, la formula che dà l'*n*-esimo termine di una qualsiasi colonna è la seguente:

colonna 1 1
colonna 2 n
colonna 3 $n(n+1)/2$
colonna 4 $n(n+1)(n+2)/6$
colonna 5 $n(n+1)(n+2)(n+3)/24$
colonna 6 $n(n+1)(n+2)(n+3)(n+4)/120$, ecc.

Facciamo la somma, a partire da 1, di quanti termini successivi si vuole di una qualsiasi colonna: il totale è il numero che si trova a destra e nella riga successiva dell'ultimo addendo. Ad esempio: 1+4+10+20+35=70.

Facciamo ora la somma in diagonale, partendo dal primo numero di una qualsiasi riga, andando verso il basso e sommando quanti addendi si vuole: si ottiene proprio il numero che si trova sotto l'ultimo addendo. Ad esempio: 1+4+10+20+35+56=126, oppure: 1+8+36+120=165.

Facciamo ora la somma, sempre in diagonale, partendo dal primo numero di ogni riga ma andando verso l'alto, e sommando tutti i numeri di quella diagonale: 1, 1, 1+1=2, 1+2=3, 1+3+1=5, 1+4+3=8, 1+5+6+1=13, 1+6+10+4=21, 1+7+15+10+1=34 ecc. I valori di queste somme ricordano qualcosa? Certamente, si tratta della successione di Fibonacci.

Consideriamo la riga *n* e la colonna *k*: l'elemento che vi compare è eguale al numero di combinazioni (senza ripetizioni) di *n* elementi a *k* a *k*: $n!/k!(n-k)!$ (vedremo fra poco di cosa si tratta). Ad esempio sulla riga 8 e colonna 5 compare il numero 56, che è proprio il numero di combinazioni di 8 elementi a 5 a 5: $8!/5!3! = 56$.

Se il lettore vuole scoprire qualche altra curiosità del triangolo di Tartaglia, colori i numeri pari in modo diverso da quelli dispari: se il triangolo è abbastanza esteso, scoprirà che si crea una quantità di triangoli di notevole simmetria con la punta rivolta verso il basso per i numeri pari, e verso l'alto per i numeri dispari.

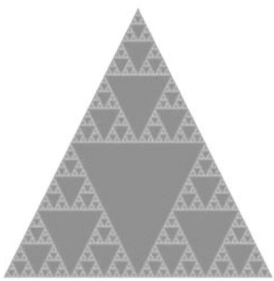

Immagine 44