La mosca di Hilbert.
L'ultimo Teorema di Fermat da Fermat ai giorni nostri.

Una storia con molti protagonisti, un Prologo, e un Epilogo che non c'è.

Letterio Gatto

Dipartimento di Matematica, Politecnico di Torino.

Sommario.

1 Introduzione

Negli ultimi due anni è successo per i manuali di matematica qualcosa di analogo a quanto è capitato per gli atlanti geografici. Muri sono caduti, frontiere sono cambiate, mutano i nomi di stati e città. E gli atlanti, anche solo quelli di un paio d'anni fa, già vecchi, altro non sono che una testimonianza di ciò che era e che non è più.

Chi si interessa di matematica, professionalmente e non, può avvertire una simile sensazione sfogliando libri di teoria algebrica dei numeri o di analisi diofantea o, più semplicemente, un (neanche troppo) vecchio numero di una rivista di matematica ricreativa. Un nuovo muro è stato abbattuto, nuove frontiere si sono aperte e la "congettura di Fermat", da oltre trecento anni impropriamente chiamata "teorema" (e, per la precisione, *Ultimo Teorema di Fermat*), è stata finalmente dimostrata. Essa è ora un teorema a pieno titolo o, più precisamente, un corollario del teorema di Wiles il quale afferma che *tutte le curve ellittiche semistabili definite su* $\mathbf{Q}$ *sono modulari*. In questo breve rapporto si intende raccontare la storia recente della congettura di Fermat, fino ai giorni della dimostrazione, rimandando, salvo una breve sinopsi, a collaudati testi classici per la prima fase di questa affascinante e entusiasmante vicenda. Una storia con un prologo e un epilogo. E con un epilogo naturalmente scontato.

2 PROLOGO

All'inizio del '900, un pomeriggio in casa Hilbert, all'ora del té. Si chiacchiera piacevolmente del più e del meno, e un amico domanda al già illustre matematico tedesco:
"Qual è il traguardo più importante per il progresso tecnologico del nuovo secolo?"
"Catturare una mosca sulla Luna".
"Perché?"
"Perché la soluzione dei problemi ausiliari che, a tal fine, occorre risolvere, implica la soluzione di quasi tutte le difficoltà materiali del genere umano".

3 La Storia.

3.0.1 L'inizio della storia.

Nato nel 250 d.C. circa, Diofanto di Alessandria fu uno dei più famosi *aritmetici* dell'antichità. Visse presumibilmente 84 anni, come documenterebbe un indovinello compendiato in una raccolta greca di problemi algebrici: "La giovinezza durò 1/6 della vita, la barba crebbe 1/12 della vita, si sposò ad 1/7 della vita e gli nacque un figlio dopo 5 anni. Il figlio visse metà degli anni del padre e il padre morì 4 anni dopo il figlio."

Per quanto ne sappiamo, il cronometro della nostra storia potrebbe proprio partire intorno al 300 d.C. circa, quando Diofanto cominciò a compilare la sua monumentale *Arithmetica*. Le vicende, però, iniziano a movimentarsi solo 1400 anni più tardi circa, ai tempi in cui per le strade di Tolosa passeggiava il giudice Pierre de Fermat (1601-1665), matematico e fisico per diletto. A lui si deve il celebre *principio di Fermat*, una sorta di principio variazionale *ante litteram*, fondamento dell'ottica geometrica, secondo il quale un raggio luminoso che congiunge due punti dello spazio descrive la traiettoria che richiede il tempo minimo. E a lui, oltre alla famosissima congettura che porta il suo nome, e di cui si vuol riferire, si devono molti altri risultati di teoria dei numeri, forse meno noti ma non perciò meno interessanti. Come esempio valga per tutti la bella proposizione nota come "primo teorema di Fermat". Essa afferma che se p è un qualsiasi numero primo, allora $n^p - n$ è divisibile per p, qualunque sia l'intero n. Per esempio, $13^7 - 13$ è divisibile per 7, $8^{17} - 8$ è divisibile per 17 e così via. Vale la pena, a proposito di questo "primo teorema di Fermat", di richiamare l'attenzione sul carattere *universale* dell'enunciato: esso non afferma che p divide $n^p - n$ per particolari valori di n (per esempio i numeri pari, o i numeri interi minori o uguali a 100) o per particolari valori di p. Al contrario, si tratta di un enunciato che afferma una proprietà verificata da *tutti* i numeri interi e *tutti* i numeri primi.

Il cosiddetto *Ultimo Teorema di Fermat* è anch'esso costituito da una proposizione universale che, essenzialmente per tale motivo, si è rivelata estremamente resistente ai ripetuti tentativi di dimostrazione operati, negli ultimi due secoli, dai migliori matematici del mondo. Una fatica a dir poco sproporzionata, se si pensa che il buon Fermat si dichiarava in possesso della chiave del rebus, cui non pareva attribuire maggior difficoltà di quella necessaria per schiacciare una nocciolina. Sembra infatti che, nel 1637, studiando l'edizione di Bachet dell'*Arithmetica* di Diofanto, accanto a un problema concernente le terne pitagoriche, il giudice di Tolosa annotasse, in un margine indubitabilmente angusto, che:

Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem

mirabilem sane detexi. Hanc marginis exiguitas non caparet.[1]

In realtà, se si vuol essere precisi, il volume contenente la preziosa quanto sibillina annotazione è andato perso e pare che nessuno l'abbia mai potuto consultare. Nessuno eccetto il figlio di Pierre, Samuel che, nel 1679, curerà un'edizione delle opere del padre, trascrivendo il testo - e non è ragionevole sospettarne alterazioni - della summenzionata annotazione.

In linguaggio moderno, la congettura di Fermat può essere enunciata affermando che, se $n > 2$, l'equazione:

$$x^n + y^n = z^n \qquad\qquad (F_n),$$

non ha soluzioni intere a, b, c tali che $abc \neq 0$ (ossia tali che a, b e c siano simultaneamente diversi da zero). Si osservi che la (F_2)[2] ammette infinite soluzioni: $3^2 + 4^2 = 5^2$ non è che uno degli esempi più noti. Nel seguito si dirà semplicemente che la congettura di Fermat è vera per l'intero n, se, fissato l'intero $n > 2$, l'equazione $x^n + y^n = z^n$ non ha soluzioni intere a, b e c tali che $abc \neq 0$. Si noti che se la congettura fosse falsa per un particolare intero $n > 2$, allora esisterebbero infinite soluzioni intere dell'equazione (F_n). Se infatti $(a, b, c) \in \mathbf{Z}^3$ fosse una soluzione di (F_n) con $abc \neq 0$, (ma, mb, mc) sarebbe essa stessa una soluzione non banale della (F_n), per ogni intero $m \neq 0$. Ovviamente (ma, mb, mc) non sarebbe una terna di interi relativamente primi. Ciò significa che la congettura di Fermat per l'intero n è vera se e solo se non esistono *soluzioni primitive* della (F_n), ossia soluzioni intere (a, b, c) tali che $abc \neq 0$ e $MCD(a, b, c) = 1$.

Il lettore non avrà difficoltà ad osservare che l'enunciato della proposizione pare avere un aspetto del tutto innocuo. E l'appunto riportato a margine da chi, come il giudice di Tolosa, non avvertì alcuna esigenza di documentarne con dovizia di dettagli la tanto "meravigliosa dimostrazione", aveva il sapore forte di una provocazione che cominciò ad assumere dimensioni sproporzionate man mano che, col passare del tempo, le più brillanti menti matematiche si scoprivano incapaci a ricostruire la (presunta) dimostrazione di Fermat.

Lo stesso Fermat, comunque, dimostrò completamente la sua congettura per $n = 4$. Sfruttando note proprietà delle terne pitagoriche e l'ingegnoso metodo della *discesa infinita*, egli provò che l'equazione:

$$x^4 + y^4 = z^4,$$

non ha soluzioni intere a, b, c tali che $abc \neq 0$. Non si ha, tuttavia, traccia della soluzione *universale* del problema (cioè per *ogni* n) anche se pare che lo stesso Fermat si rendesse conto che per dimostrare la proposizione in generale, sarebbe stato sufficiente dimostrarla per $n = 4$ e per ogni $n = p$, con p un numero primo dispari. Infatti, se la proposizione fosse vera per un primo $p \neq 2$ essa sarebbe vera per qualsiasi multiplo N di p, poiché, in caso contrario, esisterebbero x, y e z interi e tutti diversi da zero tali che:

$$x^N + y^N = z^N,$$

ossia:

$$(x^{N/p})^p + (y^{N/p})^p = (z^{N/p})^p,$$

contraddicendo la validità del teorema per $n = p$. Se N fosse un multiplo di 4, si ragionerebbe esattamente come sopra.

[1] "E' impossibile separare un cubo in due cubi, o una quarta potenza in due quarte potenze, o in generale, ogni potenza superiore alla seconda in due potenze dello stesso ordine. Ho scoperto una prova davvero meravigliosa di ciò, che questo margine è però troppo stretto per contenere."

[2] Cioè la F_n per $n = 2$.

3.1 La storia continua. Il teorema di Fermat è una mosca di Hilbert

Dopo la morte di Fermat e la pubblicazione delle sue opere curate dal figlio Samuel, i migliori matematici d'Europa cominciarono ad interessarsi del problema. Probabilmente non si trattava di vero interesse scientifico per la questione in sé, ma piuttosto di un modo per reagire ad una implicita sfida resa intrigante dalla semplicità di formulazione della questione e dal fatto che un dilettante, sia pur il principe dei dilettanti, avesse affermato di essere già in possesso di una "soluzione meravigliosa". Nessuno parve in grado, però, di ricostruire la soluzione di Fermat, nonostante ripetuti e autorevoli tentativi. Per quale motivo si ritenesse, pur in assenza di una dimostrazione, di dover credere alla non esistenza di soluzioni intere simultaneamente non nulle dell'equazione $x^n + y^n = z^n$, per $n > 2$, è in un certo senso un mistero. Una delle ragioni è senz'altro da attribuire all'ottima fama di cui godeva Fermat (già si sono ricordati alcuni dei suoi più importanti contributi): pareva ragionevole credere che, se diceva qualcosa, aveva una grande probabilità di azzeccarci.

Ed ecco una rapida rassegna dei primi importanti tentativi di dimostrare la congettura di Fermat. Si rimanda al testo di Paulo Ribemboim ([10]) per ulteriori e saporiti dettagli.

Eulero pubblicò nel 1822, nel suo libro di Algebra, la dimostrazione che la congettura è vera per $n = 3$. La dimostrazione si basava su alcune non banali proprietà dei numeri interi della forma $a^2 + 3b^2$ (il cui studio è omesso nel suo trattato) e viene conclusa usando, come Fermat fece per $n = 4$, il metodo della *discesa infinita*. Si osservi che, per quanto detto nel paragrafo precedente, aver dimostrato la proposizione per $n = 3$ significa averla dimostrata per tutti gli interi multipli di 3. Quindi, quanto meno, la proposizione di Fermat si sapeva essere vera per infiniti n (i multipli di 3 e i multipli di 4). Essenzialmente la stessa prova di Eulero fu riprodotta da Legendre ma il salto di qualità nella comprensione della stessa fu compiuto da Gauss (1777-1855) che, proprio motivato dalla congettura, introdusse particolari numeri complessi oggi noti, nei testi di algebra, come *interi di Gauss*. Più precisamente, Gauss inquadrò la dimostrazione di Eulero lavorando nel naturalissimo ambiente $\mathbf{Q}[\sqrt{-3}]$ (una particolare estensione quadratica immaginaria di $\mathbf{Q}$). Egli osservò, in quest'ambito, che $\mathbf{Z}[\sqrt{-3}]$ (ossia i numeri complessi della forma $a + b\sqrt{-3}$ con $a, b \in \mathbf{Z}$) è un dominio di integrità con algoritmo di divisione e interpretò gli interi del tipo $a^2 + 3b^2$ come *norme* di siffatti numeri.

Fu così che, accidentalmente, Gauss si trovò tra i primi esploratori del meraviglioso mondo abitato dai campi di numeri algebrici (estensioni algebriche finite di $\mathbf{Q}$), che avrebbero nutrito un filone ricchissimo di ricerca e di bella matematica. Dal 1820 in poi, come racconta Ribemboim, matematici francesi e tedeschi cominciarono a provare intensivamente il teorema di Fermat. A Legendre (1752-1833) e Dirichlet (1805-59) è dovuta la dimostrazione per $n = 5$ e quest'ultimo dimostrò il caso $n = 14$. Altri contributi sono dovuti a Lamé (1795-1870), la cui dimostrazione del caso $n = 7$ fu successivamente semplificata da Lebesgue (1857-1941). Importanti contributi provennero anche da Sophie Germaine (1776-1831), la quale dimostrò che se *p è un primo dispari tale che anche $2p + 1$ è primo, allora non esistono interi x, y, z non divisibili per p tali che $x^p + y^p = z^p$.*

Il progresso di maggior rilievo verso la dimostrazione della congettura di Fermat, comunque, fu compiuto da E. E. Kummer (1810-93) che, proprio ispirato dalla dimostrazione di Gauss, fu indotto a studiare sistematicamente le estensioni ciclotomiche di $\mathbf{Q}$ (ossia del minimo campo contenente $\mathbf{Q}$ e una radice p-esima dell'unità diversa da 1. [3]). Di fatto, lavorando in codeste estensioni ciclotomiche, i cui elementi egli denominava *interi complessi*, Kummer credette di aver ottenuto la dimostrazione generale della congettura per ogni n. La sua dimostrazione conteneva tuttavia un errore, segnalato da Dirichlet: essa infatti assumeva la proprietà di fattorizzazione unica in un

[3] Una radice p-esima dell'unità è un numero complesso z tale che $z^p = 1$.

campo ciclotomico che non la verificava. Per porre rimedio a questa lacuna della sua dimostrazione, Kummer fu indotto ad introdurre i cosiddetti *numeri ideali* (non necessariamente interi complessi), che recuperarono i vantaggi dell'unicità della fattorizzazione nei campi ciclotomici che ne erano sprovvisti. E la felice invenzione dei numeri ideali consentì a Kummer di dimostrare la congettura di Fermat per tutti i primi minori di 100 con le sole eccezioni di 37, 59 e 67.

La morale è quasi scontata: sebbene Kummer non fosse riuscito a dimostrare la congettura nella sua universalità, le sue ricerche a tal fine stimolarono decisamente lo sviluppo dell'algebra commutativa. Di lì a poco, Dedekind avrebbe cominciato a studiare sistematicamente gli anelli che portano il suo nome, i *numeri ideali* sarebbero stati interpretati in termini di *ideali frazionari* degli *anelli di Dedekind* e questi ideali avrebbero trovato un corrispettivo geometrico nel concetto di *divisore su una curva algebrica*.

Ancora ben lontano da una sua completa dimostrazione, già nell'Ottocento il Teorema di Fermat aveva stimolato nuove ricerche e la creazione di nuove teorie che avrebbero orientato in modo determinante lo sviluppo futuro della matematica. Eppure, quando Gauss ricevette informazioni sul premio che l'Accademia di Parigi aveva bandito, nel 1816, per chi fosse stato capace di dimostrare la celebre congettura, la risposta che il "Princeps Mathematicorum" indirizzò a W. M. Olbers (1758-1840) suonava press'a poco così: "Sono molto obbligato per le vostre notizie concernenti il premio di Parigi. Ma confesso che il teorema di Fermat, come proposizione isolata ha davvero scarso interesse per me, poiché potrei facilmente formulare una gran quantità di tali proposizioni, che non si potrebbero né provare né confutare". Pareva a Gauss, per dirla in breve, che dimostrare quel teorema non fosse molto più importante di quanto non gli sarebbe sembrato, a quel tempo, il cercar di catturare una mosca sulla Luna. Ma gli incontenibili sviluppi della matematica, stimolati dallo studio di quel "piccolo" problema, non possono non richiamare alla mente la metafora hilbertiana.

Il teorema di Fermat, insomma, era una mosca di Hilbert che volava sulla Luna dell'universo matematico.

2.3. Un'altra mosca di Hilbert: gli integrali ellittici

Se $f(x)$ è una funzione reale definita su un intervallo della retta reale, una sua primitiva è una funzione $F(x)$, definita e derivabile nel medesimo intervallo, la cui derivata prima, $F'(x)$, è uguale a $f(x)$. Il teorema fondamentale del calcolo integrale assicura che se f è continua in un intervallo chiuso e limitato della retta reale, $[a, b]$, allora la *funzione integrale*:

$$F(x) = \int_a^x f(t)dt$$

è una primitiva di $f(x)$ nell'assegnato intervallo. Per una ampia classe di funzioni, le primitive sono esprimibili in termini di funzioni elementari (polinomi, esponenziali, logaritmi, funzioni trigonometriche e loro inverse...). Per esempio, la funzione $arctg(x)$ (*arcotangente* di x) è una primitiva della funzione $1/(1 + x^2)$, che è definita per ogni x reale. Le primitive di una funzione $f(x)$ si indicano convenzionalmente con la scrittura:

$$\int f(x)dx + C,$$

dove C è una costante reale arbitraria. Il primo addendo si dice l'*integrale indefinito* di $f(x)$. "Calcolare" l'integrale indefinito di una funzione $f(x)$ significa determinarne una primitiva in termini di funzioni note.

Un integrale ellittico è un integrale indefinito della forma:

$$\int \frac{dx}{\sqrt{P_3(x)}},$$

dove $P_3(x)$ è un polinomio di terzo grado con radici tutte distinte e si chiama così perché esso interviene nel calcolo della lunghezza di un arco d'ellisse tra due estremi fissati. Il problema di *integrare* (ossia risolvere) l'equazione differenziale del pendolo non linearizzata:

$$\ddot{\theta} + \omega^2 sin(\theta) = 0,$$

è anche riconducibile alla valutazione di un integrale ellittico. Per cercare di illustrare le peculiarità di tali integrali ci si riferirà, nel seguito, al semplice esempio :

$$\int \frac{dx}{\sqrt{x^3 - x}}. \tag{1}$$

Prima di Abel e Jacobi, i matematici tentarono per decenni di esprimere la primitiva della funzione integranda in termini di funzioni elementari, ma senza successo. Naturalmente, in ogni intervallo chiuso $[a, b]$ tale che $\{0, 1, -1\} \cap [a, b] = \emptyset$, esiste una primitiva (e quindi infinite) di tale funzione. Infatti, essendo la funzione continua in tale intervallo, il teorema fondamentale del calcolo integrale garantisce che:

$$F(x) = \int_a^x \frac{dt}{\sqrt{t^3 - t}}, \quad x \in [a, b] \tag{2}$$

è una primitiva di $1/\sqrt{x^3 - x}$. Dal punto di vista teorico, quindi, il calcolo esplicito di una primitiva che già si sa esistere, potrebbe apparire un risibile, per quanto difficile, problema pratico, non più interessante del voler catturare una mosca sulla Luna. Stupiva, però che, viceversa, una primitiva della funzione:

$$x \mapsto \frac{1}{\sqrt{x^3 - x^2}}, \tag{3}$$

fosse facilmente esprimibile in termini di funzioni elementari. Infatti, operando la sostituzione $x = m^2 - 1$, la ricerca può essere ricondotta allo studio dell'integrale:

$$\int \frac{dm}{m(m^2 - 1)},$$

facilmente valutabile utilizzando la cosiddetta *decomposizione in fratti semplici*.

La parametrizzazione razionale della x, utilizzata per calcolare (E2), ha una semplice interpretazione geometrica, più profonda di quanto non possa cogliersi a prima vista. Infatti, nel piano cartesiano Oxy, l'espressione $\sqrt{x^3 - x^2}$, o la sua opposta, può essere pensata come il valore dell'ordinata di un punto della curva definita dall'equazione:

$$y^2 = x^3 - x^2. \tag{4}$$

Questa curva, nota anche in letteratura come *curva ad alfa* [figg. 1a), 1b)], ha un nodo nell'origine.

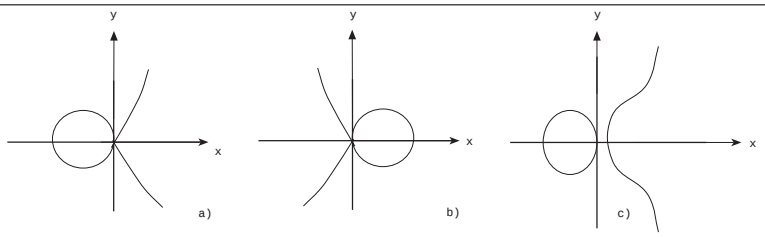

fig. 1a) La *curva ad alfa* $y^2 = x^3 + x^2$;
fig. 1b) La *curva ad alfa* $y^2 = x^3 - x^2$;
fig. 1c) Il grafico reale $E(\mathbb{R})$ della curva ellittica, definita su $\mathbf{Q}$, $y^2 = x^3 - x$. Ogni retta passante per

l'origine interseca la curva in tre punti, di cui due coincidenti in $(0, 0)$ e un terzo che è esprimibile in funzione del coefficiente angolare m della retta $y = mx$. In altri termini, la curva (E4) è una cubica razionale, cioè le coordinate dei suoi punti possono esprimersi in forma parametrica con funzioni razionali [4], ossia $x = m^2 - 1$ e $y = m(m^2 - 1)$.

Se l'integrale (E1) fosse dunque valutabile attraverso una parametrizzazione razionale della x, ciò significherebbe che la curva:

$$y^2 = x^3 - x,$$

dovrebbe essere essa stessa razionale. In altri termini, esisterebbero funzioni razionali $x = \phi(m)$ e $y = \psi(m)$ tali che:

$$[\psi(m)]^2 = [\phi(m)]^3 - \phi(m).$$

In questo caso l'integrale (E1) risulterebbe facilmente calcolabile, ricorrendo al già invocato metodo della decomposizione in fratti semplici.

Gli studi di C. G. Jacobi (1804-1851), di N. H. Abel (1802-1829) e di K. Weierstrass (1815-1897) chiarirono definitivamente la natura dell'ostacolo nel trovare un'espressione della primitiva di $1/\sqrt{x^3 - x}$ in termini di funzioni elementari. Essi mostrarono, infatti, che se $P_3(x)$ è un polinomio di terzo grado a coefficienti complessi, con radici tutte distinte, tutte le curve di equazione $y^2 = P_3(x)$ non sono razionali nel senso dianzi chiarito.

E' naturalmente difficile (e, forse, persino sconveniente) essere più precisi in questa sede. Si può dimostrare, tuttavia, che se si considerassero tutte le soluzioni (x, y), reali e complesse, dell'equazione $y^2 - P_3(x) = 0$ e si aggiungesse loro un punto (il cosiddetto *punto all'infinito*), si descriverebbe un *toro* [cfr. fig. 2b)] in $\mathbb{R}^4$. In omaggio alla loro storia, le curve del tipo $y^2 - P_3(x) = 0$ si dicono *curve ellittiche* giacché sono state scoperte nel tentativo di affrontare praticamente il problema di calcolare la lunghezza d'arco di un ellisse. La teoria delle curve elittiche è tra le più ricche di tutta la matematica (si veda [2], [14], [15], [8], [7] per approfondimenti) e si è sviluppata in molteplici direzioni, influenzando nettamente l'Analisi Complessa, la Teoria Algebrica e Analitica dei Numeri, la Fisica Matematica e la Geometria Algebrica. Per quanto riguarda quest'ultima, essa conduce a due naturali generalizzazioni: da una parte alle curve algebriche complesse di genere maggiore di 1, che sono topologicamente equivalenti (fig. 2) ad una sfera con $n > 1$ manici, dall'altra alle varietà abeliane che imitano, in dimensione > 1, lo sbalorditivo *interplay* tra algebra e geometria che rende

[4] Cioè funzioni esprimibili come quozienti di polinomi.

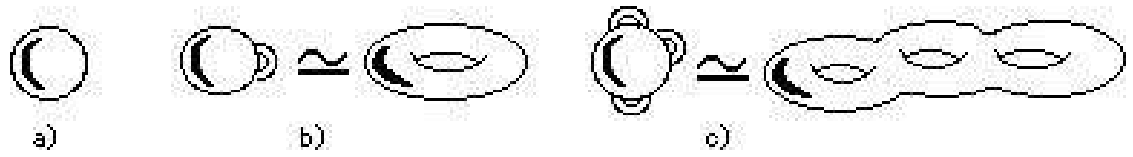

fig. 2a) sfera;

fig. 2b) un *toro* e una sfera con un manico sono topologicamente equivalenti;

fig. 2c) una sfera con 3 manici, topologicamente equivalente ad una *ciambella con* 3 *"buchi"*. la teoria

delle curve ellittiche tra le più ricche e feconde di tutta la matematica.

Anche l'integrale ellittico, insomma, era una mosca di Hilbert. L'importanza di esprimerlo in termini di funzioni elementari sarebbe potuto apparire un problema di infima importanza. Esso ha invece impresso un fortissimo impulso alla nascita e allo sviluppo di nuove branche della matematica, i cui contorni ne disegnano tutt'oggi la geografia delle più avanzate frontiere di ricerca.

3.2 Digressioni aneddotiche

Come il lettore già saprà, a parte i dettagli che ancora hanno da essere narrati, la proposizione di Fermat è stata dimostrata dopo aver mobilitato gli sforzi dei più begli ingegni di tutti i tempi. Ciò che, però, rende singolare la storia di questa congettura rispetto a quella di altre non meno importanti (come la congettura di Mordell dimostrata da Faltings o le congetture di Weil dimostrate da Deligne, e altre ancora che potrebbero citarsi a iosa), è il fatto che la mobilitazione non ha riguardato solo truppe specializzate, ma anche un vero e proprio esercito di dilettanti (sia detto senza alcun intendimento dispregiativo) della matematica. La principale ragione di ciò va, ovviamente, individuata nella estrema semplicità del suo enunciato: esso può essere compreso perfino da un ragazzino al primo o second'anno di scuola media.

Tale semplicità enunciativa è stata peraltro fraintesa e confusa con la presunta esistenza di una dimostrazione semplice (ossia accessibile a dilettanti digiuni delle teorie più avanzate) ma geniale.

Già Gauss aveva compreso che tale apparente semplicità è propria della teoria dei numeri. Talvolta le proposizioni di teoria dei numeri paiono addirittura intuitive, di facile scoperta, ma, come affermava il "Princeps Mathematicorum": "L'aritmetica superiore ha la speciale caratteristica che la maggior parte dei suoi bellissimi teoremi possono essere facilmente scoperti per induzione, mentre qualsiasi vera dimostrazione può essere solo ottenuta con enorme difficoltà". Non meno importante, però, è un altro aspetto che, nella storia della congettura di Fermat, ha contribuito non poco a colpire ed eccitare la fantasia dei non professionisti, incoraggiandone i tentativi di soluzione. Si tratta dell'inusuale proliferare di premi in denaro banditi a vantaggio di coloro che avessero eventualmente dimostrato o provato la falsità della congettura.

Dopo quello dell'Accademia di Parigi, dal quale Gauss, come già si è ricordato, preferì tenersi a debita distanza, reputando il problema poco interessante per i suoi sforzi, il premio più importante bandito a tal fine è stato il Wolfskhel Prize, che consisteva nel 1906 di una somma in denaro che ammontava a circa 100000 marchi, patrocinato dalla Reale Accademia delle Scienze di Gottingen, sulla base del lascito testamentario di tal Paul Wolfskhel. Le ultime volontà di costui prevedevano che la somma in denaro dovesse essere corrisposta a chi, seguendo le idee di Fermat o di Kummer, fosse stato in grado di offrire una dimostrazione completa della congettura per ogni intero n dell'esponente.

Il regolamento del premio che, a norma di bando, dovrebbe scadere il 13 Settembre del 2007 (se Wiles non fosse intenzionato a ritirare la modesta somma risparmiata dall'erosione di un'inesorabile inflazione), prevedeva che, anno per anno, in assenza di vincitori, gli interessi sarebbero stati devoluti all'Università di Gottingen, per invitare professori stranieri. Per esempio Hilbert utilizzò quel denaro per invitare a Gottingen sia Poincaré che il suo buon amico Minkowski.

A proposito di Hilbert, il premio Wolfskhel e la congettura di Fermat, circola una curiosa storia secondo la quale egli si affermava in grado di dimostrare la proposizione e di averla, di fatto, dimostrata. Tuttavia, sosteneva, si sarebbe ben guardato dal pubblicarla, per non uccidere "quella gallina che ci fa delle uova d'oro così belle". Il riferimento all'incasso degli interessi annuali, maturati dalla somma lasciata da quel tal "benefattore della matematica" di nome Wolfskhel, è evidente. Alle parole di Hilbert, però, non sembra che nessuno abbia mai dato, o dia, più che il peso di un' allegra *boutade*.

E' comunque fuor di dubbio che il Premio Wolfskhel abbia davvero eccitato la fantasia e l'entusiasmo di migliaia e migliaia di dilettanti che, inseguendo sogni di gloria, hanno prodotto, tutti insieme, una massa incredibile di dimostrazioni rivelatisi errate, nella migliore delle ipotesi, se non del tutto insensate. Questo è, almeno, quanto si darebbe ad intendere in una lettera con cui il dr. F. Schlichting, dell'Università di Gottinga, rispose, nel 1974, ad una richiesta di informazioni di Paulo Ribemboim.

Gottinga, 23 Marzo 1974.

Caro Signore,

la prego di scusare il ritardo con il quale rispondo alla sua lettera. Allego una copia dell'annuncio originale del premio, che stabilisce le regole principali, e una nota dell'"Akademie" abitualmente inviata alle persone che si iscrivono al premio e che ammonta ora a poco più di 10000 marchi. Non vi è alcuna stima del numero totale di "soluzioni" presentate fin'ora. Nel primo anno (1906-1907) sono state raccolte 621 soluzioni negli archivi dell'accademia e, a tutt'oggi, sono conservate circa 3 metri di corrispondenza concernenti il problema di Fermat.

([4])

Negli ultimi lustri ci si è comportati alla maniera seguente: il segretario dell'Akademie divide i manoscritti pervenuti in (1) complete nonsense (assolutamente insensati) che sono immediatamente rispediti al mittente; (2) materiale che assomiglia a matematica. La seconda parte è consegnata al dipartimento di matematica e, lì, il lavoro di lettura, di caccia agli errori e risposte è delegato a uno degli assistenti scientifici (nelle università tedesche questi sono dei laureati che lavorano alla tesi di Ph.D. o all'abilitazione e che aiutano i professori nell'insegnamento e nella supervisione). Al momento io sono la vittima a ciò designata. Vi sono

circa tre o quattro lettere a cui rispondere ogni mese, e c'è un sacco di materiale curioso e divertente, come, per esempio, quello di quel tipo che invia la prima parte della sua soluzione e che promette la seconda se paghiamo mille marchi in anticipo; o un altro, che mi promette il 10 percento del suo profitto derivante da pubblicazioni e interviste radio-televisive quando sarà diventato famoso, a patto che io lo appoggi da subito; se no, minaccia, manderebbe tutto ad un dipartimento di matematica russo per privarci della gloria di averlo scoperto.

Di tanto in tanto qualcuno arriva a Gottinga e insiste per discussioni personali. Essenzialmente tutte le "soluzioni" sono scritte ad un livello davvero elementare (usando le nozioni della matematica della scuola superiore e forse qualche lavoro di teoria dei numeri mal digerito), ma può ciononostante essere di difficile comprensione.

Socialmente, coloro che inviano i propri lavori sono spesso persone con un'educazione tecnica ma con una carriera mancata e che cercano successo con una dimostrazione del teorema di Fermat. Ho dato alcuni dei loro manoscritti a dei medici che hanno diagnosticato una pesante schizofrenia.
Una condizione nelle ultime volontà di Wolfskehl era che l'Akademie dovesse pubblicare annualmente l'annuncio del premio nei più importanti periodici matematici. Ma già dopo i primi anni i periodici rifiutarono di stampare l'annuncio, perché sommersi da lettere e manoscritti demenziali.

Sicché il miglior effetto è stato ottenuto da un altro regolamento del premio: vale a dire, che l'interesse degli originali 100000 marchi potesse essere usato dall'Akademie. Per esempio, nel 1910 i leader del dipartimento di matematica di Gottinga (Klein, Hilbert, Minkowski) usarono il proprio denaro per invitare Poincaré a dare sei lezioni a Gottinga.

Dal 1948 comunque il denaro rimanente non è più stato toccato. Spero che Lei possa usare queste informazioni e sarei lieto di rispondere ad ogni altra sua questione.

sinceramente Suo, F. Schlichting

La lettera di Schlichting, quantunque seria, è innegabilmente divertente se non comica. Anche l'Italia ha dato i natali a centinaia e centinaia di "solutori" del problema di Fermat e, anzi, qualche anno fa, la rivista "L'ingegnere italiano" ([6]) ha pubblicato una "dimostrazione" della congettura elaborata da un improvvisato matematico che, da quanto si legge nell'articolo, ha spedito la soluzione anche all'accademia di Gottingen per il premio Wolfskhel. La dimostrazione esposta nel suddetto articolo è naturalmente errata, basata com'è su un grave fraintendimento delle proprietà dell'aritmetica delle classi di resto. L'esposizione ha, tuttavia,il pregio di essere così comica (sia detto senza malignità), da far persino dubitare che l'articolo stesso altro non sia che una mattacchionata dell'autore, figura ben nota nell'ambiente degli ingegneri. Citiamo a caso alcuni passi: "Il grande matematico francese de Fermat, alcuni anni prima di morire, adirato con i matematici universitari dei suoi tempi, lanciò un cartello di sfida e li invitò a dimostrare che:

$$x^n + y^n = z^n$$

con x,y,z interi e $>$ di 0 ed n intero $>$ di 2 è impossibile.

[...] Dalla morte di Fermat molti matematici hanno tentato di trovare la soluzione, senza però mai arrivare ad una soluzione generale. Ricordiamo Gauss, Cauchy, Riemann etc. Questi grandi matematici ci provarono in media per 10 anni e abbandonarono la dimostrazione dicendo: "Maledetto Fermat!!".

Divertente vero? E ancora:

"Sembra però che altri matematici abbiano trovato la soluzione del teorema, ma non l'abbiano voluta rendere pubblica, sia per la semplicità che per rispetto a Fermat. Un esempio ne sono alcuni matematici dell'800 che dopo aver trovato la soluzione usavano poggiare un teschio, a mo' di fermacarte su di essa ed alla loro morte doveva essere bruciata." Divertente al limite del paradosso è, però, il passo in cui l'illustre

ingegnere sostiene d'essere stato "agevolato", nella ricerca della soluzione, "dal sopraggiungere di una grave malattia" per cui, continua l'autore, ..."potei dedicarmi incessantemente al teorema di Fermat e feci passi avanti, dato che potevo solo lavorare col cervello, non potendo usare né penna né carta per scrivere".

Vera fortuna o un brutto scherzo giocato da una smodata - e, quindi, pericolosa - passione per la matematica? Ognuno è certamente in grado di giudicare da sé.

Nessun dubiti, comunque, dell'esistenza in circolazione di migliaia e migliaia di simili storie. A differenza di molte altre, però, questa ha l'indiscutibile pregio di essere documentata e documentabile.

2.5. La fine della storia? Storia recente

La fine della storia, se una fine c'è, è la storia degli ultimi vent'anni, quella che ha determinato, poco tempo fa, la riuscita di Wiles nell'impresa per tanto tempo fallita: dimostrare l'asserzione di Fermat annotata in quel margine così angusto. Il Novecento si apre con una importante congettura, la congettura di Mordell (1888-1972), formulata nel 1923, secondo la quale la cardinalità dei punti razionali di una curva definita su $\mathbf{Q}$ e di genere maggiore di 2 è finita. La dimostrazione della congettura di Mordell è stata ottenuta nel 1983 ed è dovuta a G. Faltings che, per tale risultato, è stato insignito dell'ambita Field Medal, l'omologo del premio Nobel per la matematica. Per comprendere il significato di tale affermazione e la sua rilevanza per il teorema di Fermat, occorre sapere che una curva complessa si può pensare come il luogo dei punti di uno spazio proiettivo di dimensione $N \geq 2$ le cui coordinate omogenee annullano $N-1$ polinomi omogenei di assegnato grado. La curva complessa si dice definita su $\mathbf{Q}$ se tutti i coefficienti delle equazioni da cui è determinata sono razionali. Un punto su una curva siffatta si dice inoltre razionale se le sue coordinate omogenee possono essere rappresentate da una $(N+1)$-pla di numeri interi. Si potrebbe dimostrare, per esempio, che il luogo dei punti $(x : y : z) \in \mathbb{P}^2_{\mathbb{C}}$ che annullano il polinomio omogeneo $x^3 + y^3 - z^3$, definisce una curva ellittica. Esiste, cioè, una trasformazione lineare di coordinate tale che l'equazione $x^3 + y^3 = 1$ può rappresentarsi nella forma $Y^2 = P_3(X)$, dove $P_3(X)$ è un polinomio di terzo grado con radici tutte distinte. Le curve ellittiche hanno genere 1 (esse possono essere rappresentate, topologicamente, come una sfera con un manico). Inoltre, l'equazione di Fermat $x^n + y^n = z^n$, con $n \geq 4$, rappresenta l'equazione di una curva (ovviamente definita su $\mathbf{Q}$) di genere maggiore di 2. In altri termini, per ogni $n > 3$, l'equazione di Fermat ha solo un numero finito di soluzioni *primitive* intere, in virtù del teorema di Mordell-Faltings.

La dimostrazione di Faltings della congettura di Mordell rappresentò un grosso passo avanti nel campo della geometria algebrica aritmetica e destò profonda emozione e scalpore. Persino l'inserto settimanale de "La Stampa", TUTTOSCIENZE, dedicò all'evento quasi mezza pagina, enfatizzando principalmente le implicazioni riguardanti la soluzione del problema di Fermat. Faltings, come allora si diceva, ha dimostrato che il numero delle soluzioni primitive dell'equazione di Fermat è finito per ogni $n > 3$ e sarebbe bastato, dunque, far vedere che tale numero è effettivamente zero. E, invero, cos'altro poteva farsi? Ma la strada seguita non fu la prosecuzione naturale lungo la direzione indicata dal risultato di Faltings. Improvvisamente ci si rese conto che la dimostrazione poteva basarsi interamente sulla ricchissima teoria aritmetica delle curve ellittiche, evitando di ricorrere alle proprietà di curve di genere superiore.

Si è ormai ai giorni nostri, al 23 Giugno 1993. Andrew Wiles, al termine di un ciclo di tre seminari intitolato "Forme modulari, curve ellittiche e rappresentazioni di Galois", nell'ambito del workshop "p-adic Galois representations, Iwasawa Theory and the Taniyama number of motives",

scrive sulla lavagna di un'aula del Newton Institute di Cambridge:

$$x^p + y^p + z^p = 0 \quad x, y, z \in \mathbf{Z} \quad \Leftarrow xyz = 0.$$

Si trattava della teatrale affermazione con la quale Wiles comunicava ai suoi colleghi di aver risolto il problema di Fermat, come caso particolare di un teorema molto più forte che risolve parte di una congettura dovuta a Weil, Shimura e Taniyama: *ogni curva ellittica definita su* $\mathbf{Q}$ *è modulare*. La notizia rimbalzò negli ambienti matematici di tutto il mondo come una pallina da tennis. L'entusiasmo era grande ed era opinione diffusa, tra i massimi esperti mondiali nel campo, che si trattasse, come si leggeva in un messaggio di posta elettronica che, all'epoca, fece il giro del mondo, "of an amazing piece of mathematics".

Grande ottimismo che, in breve, parve effimero e affrettato. Circa sei mesi più tardi dal primo storico annuncio si scoprì che la dimostrazione di Wiles conteneva un "baco". I pessimisti pensarono subito ad uno dei tanti fuochi di paglia a cui la storia di tre secoli di infruttuosi tentativi li aveva già abituati, e la congettura, dal canto suo, pareva essersi arroccata nuovamente dietro i propri bastioni d'impenetrabilità. Si trattava solo, però, degli ultimi colpi di coda: essa era ormai sotto assedio. Wiles chiese rinforzi ad un suo brillantissimo ex-allievo, Richard Taylor, con l'aiuto del quale riuscì ad aggirare l'ostacolo che ancora si ergeva a disperata difesa della congettura. Essa capitolò definitivamente sotto l'attacco sferrato da Wiles e Taylor in [17], sicché il manoscritto [18] costituisce la resa formale e definitiva della congettura di Shimura e Taniyama nonché la dichiarazione solenne con la quale la Congettura di Fermat veniva annessa per sempre alla Landa dei Teoremi.

Aldilà della drammatizzazione, val la pena di ricordare che Wiles ha dimostrato solo un caso particolare della congettura, ossia che *ogni curva ellittica a riduzione semistabile è modulare*. Ovviamente non si ha alcuna pretesa di spiegare la dimostrazione, che è molto difficile e sicuramente non alla portata di chi scrive. Per dare un'idea della difficoltà, si può però ricordare che Gerd Faltings si vantò di essere stato l'unico matematico al mondo ad aver capito la dimostrazione di Wiles in una sola settimana. Per il lettore interessato, le righe che seguono costituiscono un vocabolario essenziale e il tentativo di dare un'idea della dimostrazione del teorema di Fermat come conseguenza del teorema di Wiles. Chi non lo fosse, può semplicemente saltarne la lettura, senza alcun rischio di perdersi il succo finale della storia.

Una curva ellittica E si dice essere definita su $\mathbf{Q}$ se e solo se può essere rappresentata come luogo di zeri di un polinomio di terzo grado della forma:

$$y^2 = P_3(x),$$

dove $P(X)$ è un polinomio a radici distinte a coefficienti in $\mathbf{Q}$.

Sia $y^2 = ax^3 + bx^2 + cx + d$ l'equazione esplicita di un tale polinomio. Si può sempre operare un opportuno cambio di variabili in modo da supporre che a, b, c, d siano interi.

Se K è un campo, si indichi con $E(K)$ il luogo dei punti di E che sono K-razionali, ossia tali che le coordinate siano tutte in K.

Per esempio $E(\mathbb{C})$ rappresenta tutti i punti di E a coordinate complesse, mentre $E(\mathbf{Q})$ tutti i punti a coordinate razionali. Ovviamente $E(\mathbf{Q}) \subset E(\mathbb{R}) \subset E(\mathbb{C})$. Per chi sa che E è un gruppo algebrico, la precedente inclusione è in effetti un'inclusione di gruppi algebrici.

Se E è definita su $\mathbf{Q}$, e trovata una rappresentazione in cui tutti i coefficienti sono interi, questi possono essere ridotti modulo un numero primo p. Riducendo modulo p si ottiene una curva definita su $\mathbb{F}_p$, il campo a p-elementi, che verrà indicata con $E \otimes \mathbb{F}_p$. Un primo p si dice primo di riduzione semistabile se i) o $E \otimes \mathbb{F}_p$ è ancora una curva ellittica, ossia $E \otimes \mathbb{F}_p$ non ha punti singolari (nel qual caso si dice anche che p è un primo di *buona riduzione*); ii) o $E \otimes \mathbb{F}_p$ ha un nodo, ossia un punto singolare ma con tangenti distinte (le figure 1a), 1b) possono aiutare l'immaginazione).

Sia ora $\sharp(E(\mathbb{F}_p))$ la cardinalità dei punti $\mathbb{F}_p$ razionali di $E \otimes \mathbb{F}_p$, ossia soluzione dell'equazione a coordinate nel campo $\mathbb{F}_p$.

Un reticolo Λ_τ di $\mathbb{C}$ è un sottogruppo di $\mathbb{C}$ tale che $\Lambda_\tau = \mathbf{Z}\tau + \mathbf{Z} \cdot 1$, dove $\tau \in \mathbb{C}$ è scelto in modo tale che $Im(\tau) > 0$.

Di fatto, ogni curva ellittica E definita su $\mathbb{C}$ si può realizzare come un quoziente del tipo $\mathbb{C}/\Lambda_\tau$ (si veda, per esempio, [1]).

Una forma modulare di peso k è una funzione f definita su $H = \{z \in \mathbb{C}/Im(z) > 0\}$ tale che:

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = \left(\frac{1}{c\tau + d}\right)^k \cdot f(\tau),$$

per ogni $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl_2(\mathbf{Z})$ (ossia i coefficienti della matrice sono interi e il determinante è uguale a 1).

E' facile dimostrare che tale funzione è periodica di periodo 1. Essa ammette quindi uno sviluppo di Fourier convergente della forma:

$$f(\tau) = \sum_n a_n q^n,$$

con $q = e^{2\pi i \tau}$.

Una curva ellittica definita su $\mathbf{Q}$ si dice modulare se e solo se esiste una forma modulare [5] $\sum a_n q^n$ tale che:

$$a_p = p + 1 - \sharp(E(F_q)).$$

Qual è la relazione tra il teorema di Wiles e la congettura di Fermat? Nei tardi anni Sessanta, Yves Hellegouarch collega $a^n + b^n = c^n$ con curve ellittiche del tipo:

$$y^2 = x(x + a^n)(x - b^n).$$

E' però solo nel 1985 che tale legame viene chiarito completamente: Gerhard Frey, in una conferenza a Oberwolfach, avanza a titolo congetturale l'ipotesi che curve ellittiche costruite da controesempi del teorema di Fermat *non possono essere modulari*. Tale congettura verrà provata da Ribet nel 1990 (che pubblicherà la dimostrazione in un articolo sulla rivista "Inventiones Mathematicae" ([11])). Era inoltre ben noto che la cosiddetta curva di Frey $y^2 = x(x + a^n)(x - b^n)$, (con a, b e c interi non nulli tali che $a^p + b^p = c^p$) è semistabile. L'importanza del teorema di Wiles è allora chiara: esso costituisce il tassello mancante del complicato mosaico: *ogni curva ellittica a riduzione semistabile è modulare* e, dunque, l'equazione $a^n + b^n = c^n$ non può essere soddisfatta da nessuna terna di interi (a, b, c) a meno che $abc = 0$. In caso contrario si potrebbe trovare una curva ellittica (la curva di Frey) che è semistabile e non modulare e ciò, come dimostra Wiles, non è possibile. Quello seguito da Wiles, e che si è cercato di descrivere, non è comunque l'unico itinerario possibile al fine di dimostrare la congettura di Fermat, ora teorema a pieno titolo. E il futuro sembra promettere nuovi e importanti sviluppi che, in prospettiva, contribuiranno a chiarire maggiormente la stessa dimostrazione di Wiles e la natura profonda dell'enunciato di Fermat. Per non citare che uno degli esempi più importanti, basterà ricordare che nel 1985 Masser e Oesterlé formularono la cosiddetta *Congettura abc*. Essa asserisce che *per ogni* $\epsilon > 0$*, esiste una costante* $C(\epsilon) > 0$ *tale che* $sup(|a|, |b|, |c|) \leq C(\epsilon)\,(Rad(abc))^{1+\epsilon}$*, qualunque sia la terna (a, b, c) di interi primi tra loro e tali che* $a + b + c = 0$.

[5] Tale forma deve essere autofunzione di particolari operatori detti "operatori di Hecke" e sulla definizione dei quali si sorvolerà per ovvie ragioni. Il lettore interessato può consultare [7] o [15]).

In [16] si prova che la congettura *abc* implica il teorema di Fermat, sicché una dimostrazione della prima fornirebbe una (nuova) dimostrazione del secondo. Non ci sarebbe da stupirsi se la congettura *abc* si rivelasse un'altra di quelle magiche proposizioni matematiche di facile formulazione e di difficile dimostrazione. Una congettura, insomma, di quelle che dovrebbero procurare ancora molto lavoro e filo da torcere ai matematici, obbligandoli a inventarsi nuovi potentissimi strumenti tecnici dai quali la matematica stessa non potrebbe non trarre un salutare giovamento.

La storia, dunque, continua?

3. Epilogo.

Come scrive Paulo Ribemboim:

> *"Non c'è alcun epilogo. La ricerca continua. Nuovi metodi verranno inventati per risolvere nuovi problemi. O, al contrario, nuovi problemi motiveranno la ricerca di nuovi metodi. Ciò è quanto di meglio possa accadere, poiché è proprio il provare e riprovare, alla ricerca delle risposte alle sue questioni più profonde, che nutre la matematica."*

* * *

Per favorire la nascita e la crescita delle idee matematiche non c'è alcuna specie di insetti, nel giardino della ricerca, tanto utile quanto le mosche di Hilbert.

References

[1] H. Cartan, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*, Hermann, Paris, 1960.

[2] J. W. S. Cassels,*Lectures on Elliptic Curves*, **LMSST 24**, Cambridge University Press, Cambridge, 1995.

[3] H. Darmon, *The Shimura-Taniyama Conjecture (d'après Wiles)*, Lecture Notes, Monographies CICMA, 1994.

[4] Darinka Mignatta, *Vignetta gentilmente disegnata su richiesta dell'autore*

[5] G. Faltings, *The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles*, Notices of the AMS, **42**, 1995, 743–746.

[6] , *Teorema di de Fermat*, L'Ingegnere Italiano, n. **181**, giugno 1987, 13–15.

[7] , S. Lang, *Introduction to modular forms*, Springer-Verlag, 1976.

[8] , D. Husemöller, *Elliptic Curves*, **GTM 111**, Springer-Verlag, 1987.

[9] , M. Kline, *Storia del Pensiero Matematico*, Einaudi, 1990.

[10] P. Ribemboim, 13 Lectures on Fermat's last Theorem, Springer-Verlag, 1979.

[11] K. Ribet, *On modular representations of* $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math., **100**, 1990, 431–476.

[12] K. Rubin, A. Silverberg, *Wiles' Proof of Fermat's Last Theorem*, Manoscritto, 1994.

[13] J. P. Serre, *A course in Arithmetic*, **GTM 7**, Springer-Verlag, 1973.

[14] J. Silverman, *The arithmetic of elliptic curves*, **GTM 106**, Springer-Verlag, 1986.

[15] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, **GTM 151**, Springer-Verlag, 1994.

[16] J. Oesterlé ,*Nouvelles approaches du "Théorème" de Fermat*, Astérisque, **161-162**, 1988.

[17] R. Taylor, A. Wiles, *Ring Theoretic Properties of Certain Hecke Algebras*, Ann. of Math., (2), **141**, 1995, 552–.

[18] A. Wiles, *Modular Elliptic Curves and Fermat's Last Theorem*, Ann. of Math. (2), **141**, 1995, 443–551.

Torino, 7 Marzo 1996