Un aspetto dei contributi di Poincaré alla Teoria dei numeri

Aldo Scimone*

Con l'abito del matematico Poincaré si cimentò sull'intero arco delle questioni scientificamente cruciali del proprio tempo, nelle discipline matematiche elaborò le soluzioni più originali; dalla matematica prese le mosse per interrogarsi sui fondamenti della stessa ed elaborare una propria epistemologia (e, per certi aspetti, anche una filosofia generale).

Gaspare Polizzi, *Henri Poincaré, tra Matematica ed Epistemologia*, Introduzione a "Il valore della Scienza", La Nuova Italia, 1994, p. IX.

Introduzione

H. Poincaré

Al IV Congresso Internazionale dei Matematici, che venne tenuto a Roma dal 6 all'11 aprile 1908, Henri Poincaré aveva accettato di tenere

* GRIM-Dipartimento di Matematica dell'Università degli Studi di Palermo, via Archirafi, 34 90123 Palermo.

una conferenza su *L'Avvenire delle Matematiche*[1], ma, a causa d'una indisposizione, il testo della conferenza venne letto da Gaston Darboux (1842-1917).

La conferenza iniziava con un'affermazione che è diventata una di quelle più riportate da chi si occupa di Storia della Matematica, soprattutto perché proviene non solo da parte di un matematico attivo nella ricerca ma soprattutto di un matematico di razza (in particolare di un genio); e ciò in netto contrasto con l'opinione di quei matematici che solo perché impegnati nella ricerca, mostrano un malcelato (ma a volte aperto) disprezzo per tutto ciò che non rientra nell'orizzonte del loro campo di indagine. La citazione, che è stata il punto di partenza per molte riflessioni di carattere storico-epistemologico è la seguente:

"Se vogliamo prevedere il futuro della matematica, la via da seguire è quella di studiare la storia e le attuali condizioni della nostra scienza."

La parte della *Conferenza* relativa alla Teoria dei numeri commenta e chiarisce le idee generali che hanno guidato Poincaré nelle sue ricerche aritmetiche, idee che appaiono singolarmente profetiche e caratterizzano il suo pensiero matematico, più sensibile alla ricchezza ed alla potenza dei metodi impiegati che ai dettagli tecnici che lo potevano condurre ai risultati.

L'Aritmetica

Poincaré inizia questa parte della sua *Conferenza* chiedendosi perché mai l'Aritmetica abbia fatto meno progressi di quanti ne abbia segnato invece l'Analisi, e individua il motivo di ciò nel fatto che mentre l'Aritmetica procede essenzialmente su un campo discreto (l'insieme degli interi), l'Analisi, di contro, utilizza l'insieme dei numeri reali, che, essendo molto più vasto, permette di fare un maggior numero di scoperte matematiche.

"I progressi dell'Aritmetica sono stati più lenti di quelli dell'Algebra e dell'Analisi, ed è facile comprendere perché. Il sentimento della continuità è una guida preziosa che difetta all'aritmetico; ciascun numero intero è separato dagli altri, ha per così dire una sua individualità propria; ciascuno d'essi è una sorta d'eccezione ed è per questo che i teoremi generali saranno più rari in teoria dei numeri, è anche per questo che quelli che esistono saranno più nascosti e sfuggiranno a lungo ai ricercatori."

[1] H. Poincaré, *L'Avenir des Mathématiques*, Atti del IV Congresso Internazionale dei Matematici, Roma, Regia Accademia dei Lincei, 1909, pp. 167-182.

Secondo Poincaré, se l'Aritmetica vorrà fare dei progressi, dovrà cercare di prendere come modello proprio l'Algebra, il cui linguaggio mostra delle forti analogie con quello della teoria dei numeri. Poincaré ricorre, in questa parte, alla sua visione della matematica, in cui i progressi sono segnati più dai collegamenti tra le diverse discipline che dalla ricerca di proprietà all'interno di un solo campo d'indagine.

"Se l'Aritmetica è in ritardo sull'Algebra e sull'Analisi, è che essa ha meglio da fare che cercare di modellarsi su tali scienze, per profittare del loro progresso. ***L'Aritmetico deve dunque prendere per guida le analogie con l'Algebra.*** *Queste analogie sono numerose e se, in molti casi, esse non sono state ancora studiate da vicino per divenire utilizzabili, sono nondimeno presenti da lungo tempo e il linguaggio delle due discipline mostra che vi sono dei legami.* ***E' così che si parla di numeri trascendenti, e che ci si rende conto che la classificazione futura di questi numeri ha già per immagine la classificazione delle funzioni trascendenti****, e innanzitutto non si vede ancora bene come si possa passare da una classificazione ad un'altra; ma se si fosse visto, ciò sarebbe già fatto e non sarebbe più opera del futuro.*
Il primo esempio che mi viene in mente è la teoria delle congruenze, dove si trova un parallellismo perfetto con quella delle equazioni algebriche. Certamente si arriverà a completare questo parallellismo che deve sussistere per esempio tra la teoria delle curve algebriche e quella delle congruenze a due variabili. ***E quando i problemi relativi alle congruenze a più variabili saranno risolti, ciò sarà un primo passo nella soluzione di molte questioni d'analisi***[2] ***indeterminata****."*

Quest'ultimo passo non poteva essere più profetico, perché i progressi della teoria delle equazioni diofantine nel secolo XX hanno accompagnato quelli della teoria delle congruenze a più variabili [Cfr. Weil]:

"Un altro esempio, dove l'analogia però non è stata intuita che solo dopo, ci è fornita dalla teoria dei corpi e degli ideali. Per averne la controparte, consideriamo le curve tracciate su una superficie; ai numeri esistenti corrispondono le intersezioni complete, agli ideali primi le curve non scomponibili; le diverse classi d'ideali hanno così le loro analoghe."
Nessuno dubita che questa analogia possa chiarire la teoria degli ideali, o quella delle superfici, o anche entrambe[3]***.."***

---

[2] Considerazioni di questo tipo hanno permesso molti progressi nella teoria delle equazioni diofantine. (nota di A.Chatelet)

[3] Si sa l'importanza odierna della teoria degli ideali di polinomi e delle teorie recenti delle funzioni algebriche. Se ne può vedere una consacrazione della profezia di H. Poincaré. (nota di A.Chatelet)

Il passo che segue è significativo perché, per tracciare una via di ricerca da seguire, Poincaré prende spunto anche dai risultati delle sue ricerche.

*"**La teoria delle forme, e in particolare quella delle forme quadratiche, è intimamente legata a quella degli ideali**. Se tra le teorie aritmetiche essa è stata una delle prime a prendere forma, è quando si è giunti a introdurvi l'unità con la considerazione dei gruppi di trasformazioni lineari.*

Queste trasformazioni hanno permesso la classificazione e di conseguenza l'introduzione dell'ordine. Può darsi che se ne siano tratti tutti i frutti che se ne potevano sperare; ma se queste trasformazioni lineari sono in Geometria parenti della prospettiva, la Geometria analitica ci fornisce ben altre trasformazioni (come per esempio le trasformazioni birazionali d'una curva algebrica) di cui si avrà vantaggio nel cercare le analoghe aritmetiche. Quelle lì formeranno senza alcun dubbio dei gruppi discontinui di cui si dovrà dapprima studiare il dominio fondamentale che sarà la chiave di tutto. In questo studio, io non dubito che si dovrà servirsi della Geometrie der Zahlen *di Minkowski.*

***Un'idea dalla quale non si è ancora tratto tutto ciò che essa contiene è l'introduzione da parte di Hermite delle variabili continue nella teoria dei numeri.** Ora si sa ciò che essa significa. Prendiamo come punto di partenza due forme F e F', la seconda quadratica definita, e applichiamo ad esse una stessa trasformazione; se la forma F' trasformata è ridotta, si dirà che la trasformazione è ridotta, e anche che la forma F trasformata è ridotta. Ne risulta che se la forma F può trasformarsi in se stessa, essa potrà avere parecchie ridotte; ma questo incoveniente è essenziale e non può essere evitato da alcun sotterfugio; esso non impedisce d'altronde che queste ridotte non permettano la classificazione delle forme. **E' chiaro che questa idea, che fino ad oggi non è stata applicata che a delle forme e a delle trasformazioni molto particolari, possa essere estesa a dei gruppi di trasformazioni non lineari; essa ha una portata sempre più grande e non è stata esaurita**[4]."*

Nell'ultima parte Poincaré affronta l'argomento dei numeri primi, ed è chiaro che quando egli si riferisce ad una mancanza di unità nello studio di tali numeri, vuole riferirsi al fatto che lo studio della loro distribuzione, che d'altronde costituiva (e costituisce) il cuore di ogni questione che gravita attorno ad essi, non avrebbe potuto fare a meno di utilizzare strumenti analitici. Oggi sappiamo bene che i maggiori progressi nello studio della distribuzione dei numeri primi sono stati ottenuti dai risultati conseguiti nel tentativo, da parte della comunità matematica mondiale, di

[4] Lo stesso Poincaré ha dato esempi di tali gruppi di trasformazioni non lineari, il cui studio è stato sviluppato dopo di lui (Memoria 348,) (nota di A.Chatelet)

dimostrare la famosa congettura di Riemann, riguardante, com'è noto, la distribuzione degli zeri non banali della cosiddetta *funzione zeta di Riemann*, $\zeta(s)$ (s, variabile complessa), introdotta per primo da Euler per s reale, e utilizzata appunto da Riemann in un memorabile lavoro di teoria dei numeri del 1859. Inoltre, quando scrisse quello che segue, Poincaré aveva certamente in mente l'elenco dei 23 problemi presentati da Hilbert nel 1900 al Congresso mondiale dei matematici di Parigi, nonché gli strumenti analitici usati da Dirichlet per la dimostrazione del suo famoso teorema della progressione aritmetica.

Un dominio aritmetico dove l'unità sembra fare assolutamente difetto, è la teoria dei numeri primi; non si sono trovate che delle leggi asintotiche e non si può sperare altro; ma queste leggi sono isolate e non ci si può arrivare che con dei percorsi differenti che non sembrano poter comunicare tra loro. ***Io credo d'intravvedere da dove uscirà l'unità desiderata, ma non l'intravedo che molto vagamente; tutto si ricondurrà senza dubbio allo studio di una famiglia di funzioni trascendenti che permetteranno, con lo studio dei loro punti singolari e con l'applicazione del metodo di Darboux, di calcolare asintoticamente***[5] ***certe funzioni di numeri molto grandi.***

I lavori di Teoria dei numeri di Poincaré

Questo elenco è tratto dal V volume delle *Oeuvres de Henri Poincaré*, Paris, 1950, e comprende 21 lavori.
I numeri in grassetto corrispondono ai lavori dedicati alla Teoria delle forme, che in tutto sono16 su 21; un lavoro è dedicato alla distribuzione dei numeri primi, uno ad una estensione dei metodi di Tchebychev, un altro alla congettura di Goldbach, e l'ultimo alle curve ellittiche.
Curiosamente, il lavoro relativo alla congettura di Goldbach, è una semplice domanda fatta in concomitanza ad Eugène-Charles Catalan (1814-1894) nella quale si chiedeva ai lettori dell'*Intermediaire des Mathématiciens* la data della celebre congettura di Goldbach sul fatto che ogni numero pari maggiore di 2 possa essere espresso come somma di due primi. Come è noto, tale congettura, a tutt'oggi non risolta, venne formulata da Christian Goldbach (1690-1764) in una lettera a Leonhard Euler (1707-1783) del 7 giugno 1742.

[5] Si sa che i progressi più importanti nella teoria dei numeri primi risultano dallo studio analitico della funzione $\zeta(s)$ di Riemann. (nota di A.Chatelet)

Comunque la domanda congiunta di Poincaré e Catalan rimase senza risposta!
Il lavoro evidenziato sarà oggetto del mio intervento. La maggior parte delle ricerche di Teoria dei numeri di Poincarè riguarda le forme quadratiche binarie, ternarie, quelle cubiche ternarie e quaternarie.

1] Sur quelques propriétés des formes quadratiques, *Comptes Rendu des séances de l'Académie des Sciences*, 1879.

2] Sur les formes quadratiques, *Comptes Rendu des séances de l'Académie des Sciences*, 1879.

3] Sur les formes cubiques ternaires, *Comptes Rendu des séances de l'Académie des Sciences*, 1880.

4] Sur la réduction simultanée d'une forme quadratique et d'une forme linéaire, *Comptes Rendu des séances de l'Académie des Sciences*, 1880.

5] Sur un mode nouveau de représentation géométrique des formes quadratiques définies ou indéfinies, *Journal de l'Ecole Polytechique* [XLVII^{e} *Cahier*, 1880, pp. 177-245].

6] Sur la raprésentation des nombres par les formes, *Comptes Rendu des séances de l'Académie des Sciences*, 1881.

7] Sur les invariants arithmétiques, *Association française pour l'avancement des Sciences (Congrès d'Alge)*, 1881, t. X, 1881, pp. 109-117.

8] Sur les applications de la Géométrie non-euclidienne à la théorie des formes quadratiques, *Association française pour l'avancement des Sciences (Congrès d'Alg.)*, t. X, 1881, pp. 109-117.

9] Sur une extension de la notion arithmétique de genre, *Comptes Rendu des séances de l'Académie des Sciences*, 1882.

10] Sur les formes cubiques ternaires et quaternaires, *Journal de l'Ecole Polytechique*, Seconde Partie (LI^{e} Cahier, 1882, pp. 45-91).

11] Sur une généralisation des fractions continue, *Comptes Rendu des séances de l'Académie des Sciences*, 1884.

12] Sur la représentation des nombres par les formes, *Bulletin de la Société Mathématique de France*, t. XIII, 1885, pp. 162-194.

13] Réduction simultanée d'une forme quadratique et d'une forme linéaire, *Journal de l'Ecole Polytechique* (LVI[e] Cahier, 1886, pp. 79-142).

14] Sur les fonctions fuchsiennes et les formes quadratiques ternaires indéfinies, *Comptes Rendu des séances de l'Académie des Sciences*, 1886 [Oeuvres, t. II, pp. 64-66].

15] Sur les déterminants d'ordre infini, *Bulletin de la Société Mathématique de France*, t. XIV, 1886, pp. 77-90.

16] Les Fonctions fuchsiennes et l'Arithmétique, *Journal de Mathématiques pures et appliquées*, 4[e] série, t. 3, 1887 [Oeuvres, t. 2, pp. 463-511].

17] Extension aux nombres premiers complexes des théorèmes de M. Tchebicheff, *Journal de Mathématiques pures et appliquées*, 4[e] série, t. 8, 1891, pp. 25-68.

18] Sur la distribution des nombres premiers, *Comptes Rendu des séances de l'Académie des Sciences*, 1891.

19] Sur le théorème de Goldbach relatif aux nombres premiers (Question proposée en commun avec E. Catalan), Intérmédiaire Mathématiciens, 1894, t. 91.

20] Sur les propriétés arithmétiques des courbes algébriques**, *Journal de Mathématiques pures et appliquées***, 5[e] série, t. 7, fasc. 2, 1901, pp. 161-233.

21] Sur les invariants arithmétiques, *Journal für die reine und angewandte Mathematik*, Bd. 129, Ht. 2, 1905, pp. 89-150.

Parte prima

Osservazioni generali sulle ricerche aritmetiche di Poincaré sulla Teoria delle forme

Sulle ricerche di Poincaré relative alla Teoria delle forme mi limiterò ad una panoramica generale, in quanto, per approfondirne i metodi impiegati e i risultati ottenuti, sarebbe necessario premettere i risultati conseguiti in quest'ambito da altri matematici prima di lui e in particolare dal suo Maestro, Charles Hermite (1822-1901).
Infatti, come rimarcò André Weil (1906-1998) nella Conferenza[6] *Poincaré et l'Arithmétique*, tenuta all'Aja in occasione del centenario

[6] A. Weil, *Poincaré et l'Arithmétique*, in Oeuvres de Henri Poincaré, tome XI, 1956, cinquiéme partie, pp. 206-212.

della nascita del grande matematico francese, molti dei suoi primi lavori sulle forme quadratiche binarie e su quelle ternarie mostrano quanto sia stato meticoloso da parte di Poincaré lo studio dell'opera di Hermite, di cui egli era stato allievo, e come ne abbia assimilato metodi e risultati.

C. Hermite

Ricordiamo brevemente che Hermite ha lasciato importanti contributi nella teoria dei numeri, nell'algebra, nei polinomi ortogonali e nelle funzioni ellittiche, oltre che, beninteso, nella teoria delle forme quadratiche.
Le ricerche effettuate in questo campo lo portarono allo studio della Teoria degli invarianti, nonché alla scoperta di una legge di reciprocità relativa alle forme binarie. Nel 1855, forte delle conoscenze acquisite nella teoria delle forme quadratiche e degli invarianti, Hermite creò una teoria delle trasformazioni, giungendo a risultati che fornivano connessioni tra la teoria dei numeri, le funzioni *theta* e le cosiddette funzioni abeliane. [Cfr. Houzel]
Fu proprio sotto l'influenza di Hermite che Poincaré dedicò la maggior parte delle sue ricerche aritmetiche alla teoria algebrica e aritmetica delle forme, e in particolare delle forme cubiche ternarie e quaternarie.
Tali ricerche lo condussero ad una dimostrazione e ad una estensione del teorema di Camille Jordan (1838-1922) secondo il quale non vi è che un numero finito di classi di forme algebricamente equivalenti a una forma data di discriminante non nullo [C. Jordan, *Oeuvres*, t. V, pp. 299-305].

In generale, data una forma, per esempio *quadratica binaria*, del tipo (scritta nel modo lagrangiano):

$$f(x, y) = ax^2 + bxy + cy^2$$

con $a, b, c \in \mathbf{Z}$, sono due i problemi fondamentali che si pongono:

a) trovare gli interi *n rappresentabili* per mezzo di *f*, cioè quei numeri interi per i quali esistono degli interi *x* e *y* per cui

$$n=f(x, y)$$

b) se *n* è rappresentabile per mezzo di *f*, determinare in quanti modi ciò può essere fatto.

Inoltre, due forme *f=(a,b,c)* e *g=(a',b',c')* sono *equivalenti* e si scrive $f \sim g$, se esiste una *matrice unimodulare S*, cioè con determinante $\Delta = \pm 1$, tale che

$$g(x', y') = f(\alpha x'+\beta y', \gamma x'+\delta y')$$

L'equivalenza delle forme è una relazione di equivalenza, per cui l'insieme delle forme viene suddiviso in classi di equivalenza.
Ebbene, detto $D=b^2-4ac$ il discriminante di una forma *f*, si dimostra che se due forme sono equivalenti allora i loro discriminanti, D e D', sono uguali, cioè:

$$f \sim g \implies D=D'$$

per cui il discriminante è un invariante delle classi di equivalenza, e a volte può essere usato proprio per distinguere una classe dall'altra.
Ma l'inverso non è vero. Per esempio, è vero che le forme x^2+y^2 e $-x^2-y^2$ hanno lo stesso discriminante D = -4, ma mentre la prima rappresenta il numero $2=1^2+1^2$, la seconda $-x^2-y^2 \leq 0$ non può.
Ebbene, un'altra distinzione tra le forme, dovuta a Lagrange, riguarda proprio il segno del discriminante. Infatti, ogni forma

$$f(x, y)= ax^2+bxy+cy^2$$

di discriminante $D=b^2-4ac$ può essere scritta nel modo seguente:

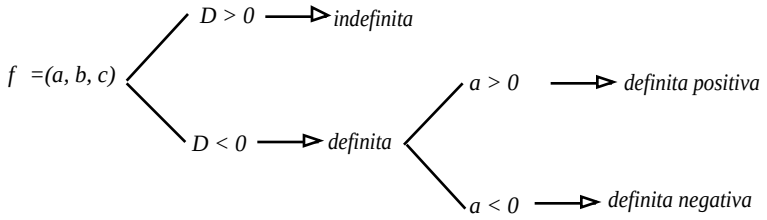
$$f(x, y)= ax^2+bxy+cy^2 = y^2 \cdot \left(a\left(\frac{x}{y} \right)^2 + b\frac{x}{y} + c \right)$$

per cui possiamo associare ad essa il polinomio quadratico az^2+bz+c, con $z=x/y$. Ebbene, se consideriamo la parabola $w = az^2+bz+c$, allora, com'è noto, si possono presentare i seguenti casi:
1] se D > 0, allora l'equazione $az^2+bz+c=0$ ha due radici distinte e la parabola attraversa l'asse *z*.
In questo caso la forma *f*=(*a, b, c*) prende sia valori positivi che negativi per appropriati valori interi di *x* e *y* (corrispondenti a valori razionali di *w* e *z*), e viene detta *indefinita*.

Se D, in particolare, è un quadrato, la teoria della rappresentazione e dell'equivalenza non è particolarmente profonda ed è stata risolta da Gauss nelle sezioni 206-212 delle *Disquisitiones*, dove peraltro il matematico tedesco affronta alcune questioni interessanti relative al valore del prodotto di due o più forme lineari, per valori interi delle variabili.

2] se D < 0, allora l'equazione $az^2+bz+c=0$ non ha due radici reali e la parabola giace tutta o sopra o sotto l'asse *z*, e la *f* viene detta *definita*.
In particolare:
- se $a > 0$ la parabola giace sopra l'asse *z* e la forma corrispondente prende solo valori positivi per $(x, y) \neq (0, 0)$, e si chiamerà *forma definita positiva*;
- se $a < 0$ la parabola giace sotto l'asse *z* e la forma corrispondente prende solo valori negativi per $(x, y) \neq (0, 0)$, e si chiamerà *forma definita negativa*.

Possiamo sintetizzare questi casi con il seguente schema:



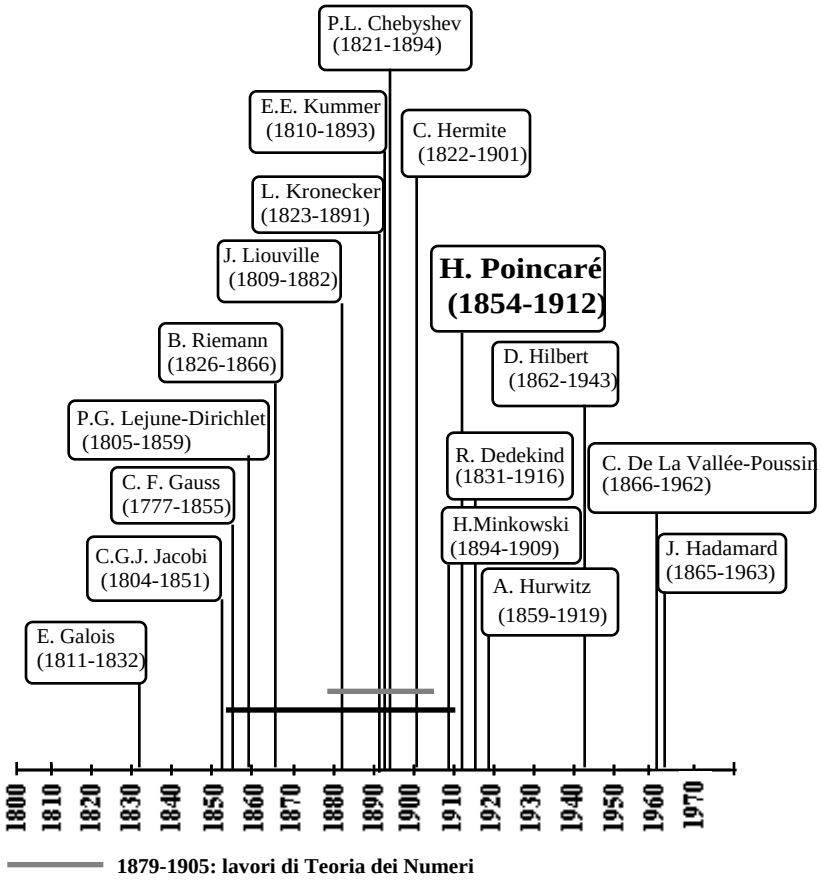
3] Se D = 0, allora la parabola sarà tangente all'asse *z*, ed $f(x, y) \geq 0$ se $a>0$, e $f(x, y) \leq 0$ se $a <0$. In questo caso ci si riduce al quadrato di una forma lineare e il problema della rappresentazione si riduce a quello semplice delle forme lineari.

Le sue ricerche sulle forme quadratiche ternarie indefinite condussero Poincaré ad una delle sue scoperte più celebri, quella delle funzioni da lui chiamate *fuchsiane*, com'egli stesso raccontò in *Scienza e metodo*. Tali funzioni godono di una proprietà che, scoperta in seguito sempre da Poincaré, doveva colpirlo vivamente: ovvero quella di dare luogo ad una generalizzazione della teoria della trasformazione delle *funzioni modulari*. Prendendo a prestito una efficace esemplificazione di Kenneth A. Ribet, al quale si deve il passo decisivo che ha permesso a Wiles di dimostrare il cosiddetto*Ultimo teorema di Fermat* (cioè, che esso discende dalla congettura di Shimura-Taniyama).
Si può dire che una funzione modulare è una particolarissima funzione di variabile complessa che ha un alto grado di simmetria, nel senso che,

trasformando in vario modo un numero complesso in cui la funzione assume un dato valore, essa conserva sempre lo stesso risultato.
Un esempio analogo e familiare di simmetria lo riscontriamo nelle funzioni trigonometriche elementari come sen *x* che ogni 2π riprende lo stesso valore preso in *x*, per cui si dice che è periodica di periodo 2π.
Il livello di simmetria delle funzioni modulari è così eccezionale che quando Poincaré le scoprì, raccontò ai suoi colleghi che, non credendo ai propri occhi, tutti i giorni, per due settimane, si era alzato di notte per cercare un errore nei calcoli, finché, al quindicesimo giorno, si arrese, accettando il fatto che le funzioni che aveva scoperto fossero estremamente simmetriche.
Come sottolinea Weil, nella citata *Conferenza*, l'ultimo lavoro di Poincaré di Teoria dei numeri, riguardante lo studio delle curve ellittiche di genere 1, ebbe evidentemente origine dalle sue riflessioni sulla Teoria delle forme. Infatti, fu il suo lavoro sulle funzioni fuchsiane e l'influenza di Felix Klein (1849-1925) a condurlo allo studio dell'opera di Riemann, dove domina la nozione di *invarianza birazionale*; per cui egli non poteva non accorgersi -dice Weil- che alcune delle proprietà essenziali di una forma ternaria *f* (x, y, z), come per esempio quella di potere rappresentare lo zero, fossero in realtà delle proprietà intrinseche della curva *f* (x, y, z) = 0, che sono invarianti non solo rispetto a trasformazioni proiettive ma anche rispetto alle corrispondenze birazionali a coefficienti razionali.
Fu proprio su questo soggetto che egli pubblicò nel 1901 la sua grande memoria sulle curve ellittiche di genere uno, aprendo un vasto orizzonte di ricerche.

La teoria dei numeri nell'epoca di Poincaré

E' bene cercare di inquadrare l'opera di Poincaré in Teoria dei numeri nel panorama delle ricerche relative a questo settore durante la sua epoca.
Nel grafico che segue sono stati indicati i matematici più significativi che precedettero l'epoca di Poincaré e quelli che seguirono immediatamente dopo di lui.



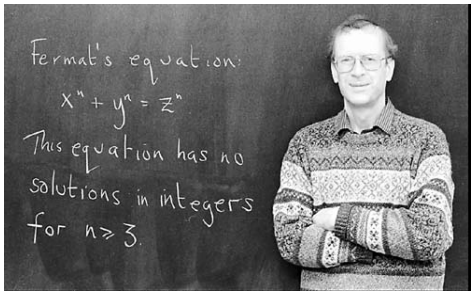
Se si dovesse tracciare un profilo cronologico dello sviluppo della moderna Teoria dei numeri si noterebbero, in generale, tre grandi periodi dall'epoca di Fermat a quella in cui operò Poincaré.

Il **primo periodo** è appunto quello di Pierre de Fermat (1601-1665) al quale fanno capo tutti i matematici suoi contemporanei che si interessarono alla Teoria dei numeri, come C.G. Bachet De Méziriac

(1581-1683), M. Mersenne (1588-1648), Lord Brouncker (1620-1684), J. Wallis (1616-1703), F. de Bessy (1612?-1675), Pierre de Carcavi (1600-1684), R. Descartes (1596-1650), J. de Billy (1602-1679).

Pierre de Fermat

Questo è un periodo di **grande creazione e innovazione**; la moderna Teoria dei numeri riceve, per così dire, l'***imprinting***.
Fermat getta le basi per la teoria delle forme e delle curve ellittiche, inventa il metodo di dimostrazione della discesa infinita, dimostra qualche teorema importante, pone questioni profonde, scopre proprietà nascoste degli interi, dei primi e lascia in eredità alle generazioni future alcune congetture che verranno o dimostrate o confutate.
Il cosiddetto "ultimo teorema" che egli lasciò solo enunciato e che ha resistito agli sforzi dei matematici successivi è stato finalmente dimostrato, per via indiretta, dall'inglese A. Wiles dell'Università di Princeton nel 1995, per cui viene giustamente chiamato il teorema di Fermat-Wiles.



Andrew Wiles

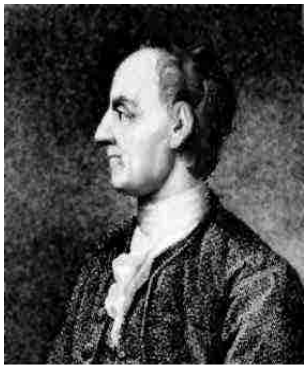
Wiles ha dimostrato in realtà la verità della congettura detta di Goro Shimura e Yutaka Tanijama, che ha come corollario la verità del Teorema di Fermat, e come hanno scritto Simon Singh e Kenneth A. Ribet in un delizioso articolo divulgativo intitolato *La dimostrazione dell'ultimo teorema di Fermat* [Le Scienze, gennaio 1998, pp. 74-79]:

"... tutti concordano sul fatto che la dimostrazione di Wiles è decisamente troppo complessa e moderna per essere ciò che aveva in mente Fermat quando scrisse la sua nota a margine. I casi sono due: o Fermat aveva preso un abbaglio, oppure esiste una dimostrazione semplice e brillante che aspetta ancora di essere scoperta."

Morto Fermat, la Teoria dei numeri ricade nuovamente nell'ombra, anche perché, nel frattempo va prendendo sempre più piede il nuovo calcolo, del quale, peraltro, Fermat e Pascal avevano preannunciato, con le loro ricerche, alcuni dei concetti più importanti. Esplode l'epoca di Newton (*"Let Newton be! "*), di Leibniz e dei Bernoulli.

Per **il secondo periodo** bisognerà attendere L. Euler (1707-1783) perché le ricerche di teoria dei numeri tornino in auge, per merito suo e di altri matematici minori, fra cui spicca il suo amico e corrispondente C. Goldbach (1690-1764), al quale si deve la famosa congettura (1742), ancora irrisolta, sul fatto che ogni numero pari maggiore di 2 può essere scritto come somma di due primi.
Per quanto riguarda il complesso delle sue ricerche e dei risultati raggiunti in Teoria dei numeri, mi limito a sottolineare ciò che giustamente scrive A. Weil, al quale rimando per una bella panoramica della produzione aritmetica del grande matematico svizzero (Cap. terzo):

"... già da solo, sebbene occupi soltanto quattro dei settanta e più volumi delle sue opere, sarebbe sufficiente, anche se egli non avesse fatto altro, a garantirgli un posto di rilievo nella storia della matematica."



L. Euler

Sulla scia di Euler si pongono J.L. Lagrange (1736-1813) e A.M. Legendre (1752-1833).

Lagrange *Legendre*

La maggior parte dei contributi di Lagrange alla Teoria dei numeri hanno a che fare con problemi già affrontati da Fermat e da Euler. I contributi più originali Lagrange li apportò alla teoria delle forme quadratiche con il concetto di equivalenza tra forme in base al quale le forme di discriminante assegnato si suddividono in classi di equivalenza, dimostrando inoltre, mediante un processo di riduzione, che il numero di tali classi è finito. [Cfr. A. Weil, Teoria dei numeri, Einaudi, 1993, pp. 288-301]

Di Legendre voglio ricordare (perché si basa su una proprietà riposta) un algoritmo che permette di decidere, in un numero finito di passi, se una conica razionale ha un punto razionale. Egli considera una conica razionale generica e mostra che per mezzo di manipolazioni algebriche elementari questo problema può essere ricondotto a quello di trovare un punto razionale su una curva della forma $ax^2 + by^2 + c = 0$, con a, b, c interi non divisibili per un quadrato, non tutti dello stesso segno e $abc \neq 0$.
Ponendo

$$x = X/Z \qquad y = Y/Z$$

ciò equivale a trovare una soluzione intera non nulla per l'equazione

$$aX^2 + bY^2 + cZ^2 = 0;$$

e questo problema viene risolto proprio dal suo teorema che si può enunciare nel modo seguente:

"Siano a, b, c interi non divisibili per un quadrato, non tutti dello stesso segno, con abc ≠ 0. Allora la curva

$$F(X, Y, Z) = aX^2 + bY^2 + cZ^2 = 0$$

ha una soluzione intera non banale (X, Y, Z) ≠ (0, 0, 0), se e solo se -bc, -ca, -ab sono residui quadratici rispettivamente modulo a, b e c."

E' nota inoltre la fama di Legendre per la sua congettura sulla distribuzione dei primi; e degno di nota rimanse il suo tentativo di dare una sistemazione organica alla Teoria dei numeri con la pubblicazione nel 1798 del libro *Essai sur la Théorie des Nombres*, che ebbe diverse edizioni, l'ultima delle quali, la terza, nel 1830.
[Cfr. A. Weil, Teoria dei numeri, Einaudi, 1993, pp. 301-315]

Il **terzo periodo** viene inaugurato dalla grande opera di C.F. Gauss (1777-1855), con il quale la Teoria dei numeri riceve il suo *status* disciplinare.

C.F. Gauss

I contributi che Gauss apportò alla Teoria dei numeri, profondi, a volte difficili da leggere, e altamente originali sono noti a tutti i cultori della Storia della Teoria dei numeri, per cui voglio ricordare solo la sua prima grande opera che segna lo spartiacque tra quel che s'era fatto prima di lui

e l'epoca che si potrebbe chiamare “l'era gaussiana” della teoria dei numeri, cioè, le *Disquisitiones Arithmeticae* apparse nel 1801.
Quest'opera di Gauss, come scrive Morris Kline (1908-1992) è basata su tre idee principali: la teoria delle congruenze, l'introduzione dei numeri algebrici e la teoria delle forme come guida per l'analisi diofantina.
Il grande Lagrange, in una lettera a Gauss del 31 maggio 1804, così gli scrisse:

“Le vostre Disquisitiones vi hanno sollevato di colpo all'altezza dei sommi matematici, e io giudico che la loro ultima parte racchiuda le più belle scoperte analitiche che siano state fatte da moltissimo tempo in qua ... Credete, signore, che nessuno applaude ai vostri successi più sinceramente di me.”

I sette capitoli (che Gauss chiama «Sezioni», alla maniera latina) che formano l'opera trattano i seguenti argomenti:
- Teoria delle congruenze: Sezz. I-IV

- Teoria delle forme quadratiche: Sezz. V-VI

- Ciclotomia: Sez. VII

In quest'ultima parte, Gauss espone la celebre costruzione con riga e compasso del poligono regolare di 17 lati.
Diretti continuatori di Gauss nelle ricerche di Teoria dei numeri furono: Carl Gustav Jacob Jacobi (1804-1851), Ferdinand Gotthold Eisenstein (1823-1852), Peter Gustav Lejeune Dirichlet (1805-1859), Richard Dedekind (1835-1916).
Per quanto riguarda i contributi principali di Jacobi alla Teoria dei numeri, essi sono:

C.G.J. Jacobi

Il teorema di reciprocità cubica (Lezioni del 1837) [pubblicato nel 1844 da F.G. Eisenstein (1832-1852), ciò che causò una leggera disputa di priorità tra i due matematici]; il teorema per cui ogni numero intero è la somma di quattro quadrati, dimostrato con l'uso delle funzioni ellittiche; il lavoro sull'applicazione della teoria degli integrali ellittici e abeliani all'Analisi diofantina [*De usu Theoriae Integralium Ellipticorum et Integralium Abelianorum in Analysi Diophantea*, Journal de Crelle, bd. 13, pp. 353-355] (1835) in cui mostrò il legame tra l'analisi diofantina e il calcolo integrale, e di cui parlerò in seguito.
Dirichlet apportò contributi fondamentali a parecchie parti della Teoria dei numeri: le equazioni diofantine, la legge di reciprocità quadratica, la teoria dei numeri algebrici, l'approssimazione diofantina, il principio della "piccionaia", la formula del numero della classe per le forme quadratiche, il teorema sui primi in una progressione aritmetica. Per dimostrare quest'ultimo teorema egli, com'è noto, introdusse tecniche di analisi complessa, e nuovi oggetti matematici quali quelle che ora sono chiamate “serie di Dirichlet”.
E' proprio in relazione alla dimostrazione di questo teorema che si fa risalire l'inizio della cosiddetta *teoria analitica dei numeri*, anche se, in verità, bisognerebbe darne il merito ad Euler che fu proprio il primo ad usare metodi analitici nelle sue ricerche aritmetiche.

P.G. Lejune-Dirichlet

Com'è noto, la posizione di Riemann nei confronti della Teoria dei numeri è un po' anomala, in quanto egli scrisse nel 1859 una sola breve memoria sull'argomento, *Über die Anzhal der Primzahlen unter einer gegebener Grösse,* (Sul numero dei numeri primi inferiori a una grandezza data) pubblicata sul «Monatsberichte der Berlinen Akademie» (Bollettino

mensile dell'Accademia di Berlino) in occasione della sua nomina di membro corrispondente da parte dell'Accademia berlinese.
A onore del vero, c'è da dire che Riemann continuò a interessarsi dell'argomento, soprattutto della sua funzione zeta, anche in seguito.
Infatti, nel 1926 vennero ritrovati alcuni suoi appunti contenenti alcuni calcoli sul comportamento della funzione zeta, ed essi vennero pubblicati nel 1932 dopo essere stati rivisti e completati dal matematico Karl Ludwig Siegel (1896-1981), che fu uno dei teorici dei numeri più importanti del XX secolo.
Tornando alla breve memoria del 1859 (unica!) di Riemann ("l'articolo più geniale e fecondo" sui numeri primi, secondo il parere di Edmund Landau), c'è da ricordare che essa ha dato luogo a una messe inesauribile, che dura tuttora, di ricerche da parte dei teorici dei numeri primi.
L'introduzione della *funzione zeta* di Riemann, $\zeta(s)$, per valori complessi di s, e della congettura, ad essa collegata (e a tuttoggi non risolta), relativa alla parte reale degli zeri non banali della sua funzione che dovrebbero giacere tutti sulla retta $x=1/2$, è stata una delle pietre miliari nello studio della distribuzione dei numeri primi.
[Cfr. R. Tazzioli, *Riemann*, Le Scienze, aprile 2000]

B. Riemann

Molti furono i contributi di J. Liouville (1809-1882) alla Teoria dei numeri, ma, forse, il suo nome rimane oggi legato al cosiddetto Teorema di "non approssimazione" (1844), che ammette l'esistenza di un limite all'approssimazione di un qualsiasi numero algebrico:

Se α *è algebrico di grado* $n\geq 2$*, allora esiste un* $c(\alpha)>0$ *dipendente solo da* α *tale che per tutti i numeri razionali* p/q *di Q, si ha:*

$$|\alpha - p/q| > c(\alpha)/q^n$$

Tale teorema gli permise di dimostrare per primo l'esistenza di numeri trascendenti tali da poter essere approssimati con il grado di approssimazione che si vuole. Quindi, un numero α è un numero di Liouville se esiste una successione di numeri razionali distinti p_1/q_1, p_2/q_2, ... tali che, per qualche costante $k > 0$ si abbia:

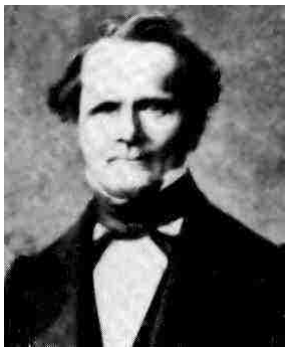
$$|\alpha - p_r/q_r| < k/q_r^r$$

- Un esempio di numero trascendente dato dallo stesso Liouville":

$$\alpha = \sum 1/10^{k!} = 0{,}11000100000...$$

J. Liouville

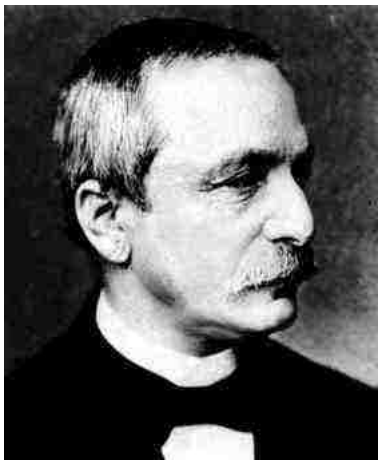
Nella teoria dei numeri la fama di E.E. Kummer (1810-1893), come si sa, rimane legata all'introduzione dei numeri "ideali" nella teoria dei domini algebrici di razionalità (1846).



E.E. Kummer

Egli giunse a tale teoria in parte cercando di dimostrare l'Ultimo teorema di Fermat, anche se un'altra motivazione per essa va ricercata in parte nella teoria dei residui biquadratici di Gauss che aveva introdotto il concetto di fattore primo nel campo dei numeri complessi- E' noto come l'introduzione di Kummer dei fattori "ideali" permise la scomposizione di un numero in fattori primi all'interno di un dominio di razionalità qualunque, e come questa scoperta rese possibile grandi passi in avanti nell'aritmetica dei numeri algebrici

Per quanto riguarda L. Kronecker (1823-1891), com'è noto, i suoi contributi principali riguardano le funzioni ellittiche, la teoria degli ideali e l'aritmetica delle forme quadratiche. Le sue lezioni sulla teoria dei numeri si caratterizzano per l'esposizione accurata delle sue scoperte e di quelle degli altri matematici, e rivelano la sua profonda convinzione di aritmetizzare tutta la matematica, che per lui significava rigorizzazione.



L. Kronecker

Così, per esempio, invece di definire il numero π con l'usuale procedimento geometrico, egli preferiva definirlo mediante la serie

$$1 - 1/3 + 1/5 - \ldots$$

cioè su una combinazione di interi.

Memorabile rimane il suo grande lavoro del 1881: *Grundzüge einer aritmetischen Theorie der algebraischen Grössen* (Lineamenti di una teoria aritmetica delle grandezze algebriche) in cui raccolse i risultati dovuti a vent'anni di ricerche, presentando la generalizzazione della teoria dei numeri ideali di Kummer a campi di numeri algebrici qualunque. Con questo grande lavoro Kronecker voleva fornire fondamenti rigorosi

(cioè aritmetici) sia alla teoria dei numeri che a quella delle funzioni algebriche.
Solo recentemente i suoi lavori hanno ricevuto una maggiore attenzione da parte della comunità matematica, perché all'epoca della loro pubblicazione furono giudicati difficili da leggere.

Per ciò che concerne i risultati di P.L.Chebycev (1821-1894) in Teoria dei numeri, fondamentale rimane la sua grande memoria ***Sulla funzione che determina la totalità dei numeri primi inferiori a un limite dato***, Memorie dell'Accademia delle Scienze di San Pietroburgo, 1851, pp. 366-390.

P.L. Chebycev

Il teorema che Chebycev dimostrò in questa sua memoria fondamentale rappresentò il primo passo veramente significativo per determinare l'andamento asintotico di $\pi(x)$ per x tendente all'infinito:

$$0{,}92129\, x/\log x < \pi(x) < 1.105548\, x/\log x$$

Come corollario del suo teorema egli ottenne la dimostrazione di un'altra celebre congettura sui numeri primi, la congettura di Joseph Louis François Bertrand (1822-1900):

Esiste, per ogni intero n, un numero primo tra n e 2n?.

Chebycev dimostrò pure che se il rapporto

$$\pi(x)/x/\log x$$

tende ad un limite, quando *x* tende a infinito, dev'essere necessariamente 1.

Per quanto riguarda Hermite, si è già accennato ai suoi contributi alla teoria delle forme e a quella delle trasformazioni.

C. Hermite

Voglio ricordare ancora che a lui si deve la dimostrazione (1873) della trascendenza del numero $e = 2,\ 7182818459045\ ...$, la base dei cosiddetti logaritmi naturali.

Proprio ispirandosi ai suoi metodi, Ferdinand Lindemann (1852-1939) dimostrò nel 1882 che anche π è trascendente. Così veniva posta la parola fine al problema millenario della quadratura del cerchio, uno dei tre problemi classici dell'antichità, con grave scorno per tutti i cosiddetti "quadratori".

Un altro risultato famoso di Hermite fu la risoluzione dell'equazione di quinto grado mediante le funzioni ellittiche che egli usò anche per risolvere la cosiddetta equazione differenziale di Lamé.

Richard Dedekind (1831-1916), che per trentun anni insegnò alla scuola tecnica superiore di Brunswick, è rimasto soprattutto famoso per due fondamentali tematiche delle sue ricerche: la costruzione di una teoria rigorosa degli irrazionali, con il concetto di *sezione* [*Stetigkeit und irrationale Zahlen* del 1872 e *Was sind und was sollen die Zahlen* del 1882], e il suo *Supplement "Über die Theorie der ganzen algebraischen Zahlen"* (Sulla teoria dei numeri interi algebrici) alla 4° edizione del 1894 delle *Vorlesungen über Zahlentheorie* (Lezioni sulla teoria dei numeri) di P.G.L. Dirichlet, che esercitarono un'influenza enorme sulla teoria dei numeri e sulla nascita dell'algebra moderna.

R. Dedekind

A detta di B.L. van der Waerden (11903-1996), questo *Supplement* di Dedekind era per la grande Emmy Noether (1882-1935) una fonte inesauribile di idee e di metodi.
Purtroppo, solo negli anni '20 del XX secolo le ricerche algebriche di Dedekind poterono essere apprezzate compiutamente in tutta la loro profondità e modernità, in quanto all'inizio la loro estrema astrattezza incontrò una forte resistenza da parte dei matematici contemporanei.

Parte Seconda

Breve excursus sulla storia precedente alla Memoria di Poincaré:

Sur les propriétés arithmétiques des courbes algébriques
***Journal de Mathématiques pures et appliquées*, 5e série, t. 7, fasc. 2, 1901, pp. 161-233.**

Poiché la memoria di Poincaré sulle curve ellittiche di genere uno rappresenta l'inizio della moderna teoria aritmetica sulle curve, è opportuno riassumere la storia che conduce al lavoro del matematico francese.

1. Diofanto d'Alessandria (circa 350 d.C.)

Com'è noto, non si sa praticamente nulla della sua vita. Un cenno si ha nel Libro XIV dell'*Antologia Palatina*, in cui un epigramma contiene un problema di aritmetica elementare la cui soluzione ci informa su quanto è vissuto Diofanto. Si può dire che egli sia una figura alquanto isolata nel panorama della matematica greca.
Di Diofanto si conosce un'opera intitolata l'*Aritmetica* e un opuscolo sui numeri poligonali, inoltre gli si attribuiscono dei *Porismi* che sono andati perduti. Dei 13 libri originari dell'*Aritmetica*, oggi se ne conoscono 10: i primi 3 in greco, gli altri 4 in arabo, identificati nel 1971 e pubblicati nel 1984, e gli ultimi 3 in greco.
E' noto che Diofanto lavorava su problemi particolari, in un modo puramente algebrico, senza alcuna notazione algebrica .
Come già aveva notato Zeuthen, nel 1896, oggi è chiaro che Diofanto conosceva un metodo generale per risolvere equazioni del tipo

$$y^2 = ax^2 + bx + c$$

quando o a o c era un quadrato perfetto.
Se con il simbolismo moderno rappresentiamo con la scrittura $f_2(x, y)$ un polinomio irriducibile di secondo grado nel campo razionale **Q**, e supponiamo di conoscere una soluzione razionale dell'equazione

$$f_2(x, y)=0$$

si può dire che Diofanto aveva scoperto un metodo per rappresentare x e y mediante funzioni razionali $x=\varphi(t)$, $y=\psi(t)$ tali che

$$f_2[x=\varphi(t), \qquad y=\psi(t)]=0.$$

Allora tutte le soluzioni dell'equazione potevano essere calcolate assegnando a *t* diversi valori razionali.
Oggi si dice che *una curva razionale di secondo grado o non contiene affatto alcun punto razionale; oppure che essa è birazionalmente equivalente ad una retta*.
Comunque, solo in due esempi (i lemmi ai problemi VI_{12} e VI_{15}) dell'*Aritmetica* egli formulò le sue scoperte in modo generale. Per esempio, nel problema VI_{12}, secondo lemma, si propone:

Dati due numeri, la somma dei quali sia un quadrato, si può trovare un numero infinito di quadrati tali che, quando il quadrato è moltiplicato per uno dei dati numeri e il prodotto è aggiunto all'altro, il risultato è un quadrato.

Usando il nostro simbolismo, Diofanto cercava tutte le soluzioni razionali dell'equazione

$$ax^2+b=y^2, \text{ con } a+b =$$

La restrizione che $a+b$ sia un quadrato, $a+b=m^2$, comporta che l'equazione abbia una soluzione razionale $(1, m)$. Diofanto pone:

$$x=t+1,\ y=y$$

ottenendo l'equazione

$$at^2+2at+m^2=y^2$$

il cui termine noto è un quadrato perfetto. Le altre soluzioni razionali dell'equazione si possono determinare con la sostituzione $y=kt-m$:

$$t = 2\ \frac{a+km}{k^2-a}$$

per cui x e y sono funzioni razionali del parametro k.
A ciascun valore di questo parametro corrisponde una e una sola soluzione del problema.
I metodi usati da Diofanto si possono interpretare geometricamente in maniera semplice: si supponga che l'equazione $f_2(x, y)=0$ determini una curva L in un piano dove la soluzione (x, y) è un punto situato sulla curva. Se x e y sono razionali, si dice che il punto è razionale. Non è difficile rendersi conto che ciascuna delle sostituzioni che Diofanto usa per risolvere problemi del tipo di quello che abbiamo visto è equivalente alla costruzione di un fascio di rette passanti per un punto razionale $A(x_0, y_0)$ situato sulla curva L e avente una pendenza k razionale. Ciascuna retta del fascio intersecherà la curva in un punto ancora razionale.

Nel Libro IV dell'*Aritmetica* Diofanto affrontò la risoluzione di problemi che portavano a equazioni indeterminate di terzo, quarto e sesto grado, e

poiché dapprima queste equazioni davano luogo a curve di *genere zero*, Diofanto sapeva rappresentare le incognite come funzioni razionali del parametro. Ma in problemi successivi, apparvero le prime curve di *genere uno*, e Diofanto anticipò i *metodi moderni della secante e della tangente* per determinare i punti.
Accenniamo a questi due metodi. Sia L una data equazione di terzo grado

$$f_3(x, y)=0$$

dove $f_3(x, y)$ è un polinomio di terzo grado, irriducibile in **Q**. Supponiamo anche che su L esistano due punti razionali $A(x_1, y_1)$ e $B(x_2, y_2)$.
- Il primo metodo, quello della secante, consiste nel tracciare la retta che passa per A e B, la quale intersecherà la curva L in un terzo punto che sarà anche razionale.

- Il secondo metodo, quello della tangente, si applica quando si conosce un solo punto $A(x_1, y_1)$ della curva L. In tal caso si traccia la retta tangente a L in A:

$$y - y_1 = k\,(x - x_1)$$

$$\text{con } k = \frac{dy}{dx} = -\frac{\dfrac{\partial f_3}{\partial x}}{\dfrac{\partial f_3}{\partial y}}(x_1, y_1)\ .$$

Poiché il punto di tangenza è un punto doppio, la tangente intersecherà la curva L in un altro punto che sarà ancora razionale.
Così, nei problemi IV_{24} e VI_{18} egli considera rispettivamente le equazioni

$$x\,(a - x) = y^3 - y$$

$$y^2 = x^3 - 3x^2 + 3x + 1$$

che risolve con il metodo della tangente; mentre applica il metodo della secante nella risoluzione del problema IV_{26}, in cui perviene all'equazione:

$$y^3 = 8x^3 + x^2 - 8x - 1.$$

Tutti questi esempi testimoniano che Diofanto arrivò a comprendere che non è possibile rappresentare le incognite *x* e *y* di equazioni indeterminate di terzo grado come funzioni razionali di un parametro.

2. Il secolo XVI

In questo secolo gli studiosi europei riscoprono l'*Aritmetica* di Diofanto, la cui prima traduzione latina venne fatta nel 1575 da *Xylander*, ovvero

Wilhelm Holzmann (1532-1576); ma bisogna ricordare che già tre anni prima Raffaele Bombelli (1526-dopo1572) aveva incluso ben *143* problemi dell'*Aritmetica* nella sua *Algebra*, apparsa nel 1572.
Come rimarca la Bashmakova, è abbastanza curioso il fatto che *prima* della traduzione latina dell'*Aritmetica*, a nessun matematico europeo venga in mente di applicare la dottrina delle equazioni indeterminate per risolvere i problemi dell'analisi diofantina, che venivano risolti in maniera puramente aritmetica, ed è solo *dopo*, quando essi si sono già familiarizzati con l'*Aritmetica*, che si cominciano a padroneggiare i metodi di Diofanto.
Proprio usando i metodi di Diofanto, lo stesso Bombelli introdusse i numeri negativi e quelli complessi. Egli pose molta attenzione al metodo della tangente e riuscì ad applicarlo alla soluzione dell'equazione:

$$x^3 + y^3 = a^3 - b^3$$

con $a=4$ e $b=3$.
Nella sua *Zetetica*, F. Viète (1540-1603) impiegò il suo nuovo calcolo letterale per la soluzione di problemi diofantini, e risolvette l'equazione

$$x^3 + y^3 = a^3 - b^3$$

nel caso generale, ma con la restrizione che $a^3 > 2b^3$.

3. Il secolo XVII- Pierre de Fermat

Fermat, come prima di lui al-Kaezin, distingue tra l'analisi diofantina *intera*, propriamente aritmetica e l'analisi diofantina *razionale*, che è più algebrica, come risulta chiaramente quando, nel 1657, egli sfidò Lord William Brouncker e John Wallis a trovare soluzioni intere di alcune equazioni indeterminate.
Fermat ;fu il primo ad asserire che l'equazione $x^2 - N y^2 = 1$ ammette sempre un numero infinito di soluzioni intere (un fatto veramente notevole) in una lettera scritta a Frénicle de Bessy{ XE "Frénicle de Bessy" } nel febbraio del 1657 [P. de Fermat, *Oeuvres*, publiées par les soins de MM. Paul Tannery et Charles Henry, Paris, 1894, vol. II, pp. 333-335], nella quale gli chiese, appunto, di trovare una regola generale per determinare, dato un qualunque numero che non fosse un quadrato, dei numeri quadrati tali che, moltiplicati per il numero dato e sommando l'unità al prodotto ottenuto, fornissero un quadrato.
Passando ad un esempio concreto, Fermat{ XE "Fermat" } propose a Frénicle { XE "Frénicle " }di fornire il più piccolo valore di y che potesse soddisfare le equazioni:

$$61y^2 + 1 = x^2, \qquad 109y^2 + 1 = x^2.$$

La sfida venne raccolta anche in Inghilterra da Lord William Brouncker (1620-1684)**{** XE "Lord William Brouncker (1620-1684)" **}**, che fu anche il primo Presidente della Royal Society, e dal matematico John Wallis (1616-1703), che fu una delle personalità scientifiche più importanti dell'epoca di Newton**{** XE "John Wallis (1616-1703)" **}**.
A proposito di Lord Brouncker, come ricorda H. Davenport (1907-1969) nella sua magistrale opera *Higher Arithmetic*[7], non erano pochi quelli che avevano una bassa opinione della sua statura morale, tuttavia le sue conquiste matematiche meritavano parecchio credito.
Dapprima, forse per qualche malinteso, essi credettero di dovere cercare solo soluzioni razionali, e non necessariamente intere, dell'equazione proposta, per cui risolvettero facilmente il problema.
Ma Fermat**{** XE "Fermat" **}** non rimase naturalmente soddisfatto di questa soluzione, e Brouncker**{** XE "Brouncker" **}**, affrontando nuovamente il problema, riuscì finalmente a risolverlo, anche se in maniera complicata.
Il metodo venne esposto in due lettere di Wallis**{** XE "Wallis" **}** del 17 dicembre 1657 e del 30 gennaio 1658, nonché nel capitolo XCVIII della sua *Algebra*.
I due matematici inglesi, come s'è detto, risposero subito risolvendo le equazioni mediante soluzioni razionali, al che Fermat replicò che egli non aveva inteso che gli si presentassero soluzioni di quel tipo che ogni novizio avrebbe potuto trovare, bensì soluzioni intere, il che era un'altra cosa.
16116116116116116150161161161161505016116116150505Sappiamo come andò la storia: Lord Brouncker rispose esibendo per la seconda equazione la coppia (126862368, 7170685) e Wallis la coppia (1728148040, 140634693) per la prima equazione: e sappiamo anche come queste equazioni siano passate alla storia con il nome *di equazioni di Pell*, e ciò per un errore di attribuzione dovuto a Euler; infatti, dovrebbero essere chiamate giustamente equazioni di Fermat.
Il principio unificatore dell'analisi intera di Fermat sembra essere stato il suo metodo della ***discesa infinita***, e i problemi principali che egli ha risolto con questo metodo si trovano già enunciati in una lettera a Mersenne degli inizi del mese di giugno 1638:

- Trovare un triangolo rettangolo in numeri la cui area sia un quadrato;

[7] H. Davenport, The Higher Arithmetic. An Introduction to the Theory of Numbers, Dover, 1983, p. 108.

- Trovare due quadrati-quadrati la cui somma sia un quadrato-quadrato, o due cubi la cui somma sia un cubo;

- Trovare tre quadrati in progressione aritmetica sotto la condizione che la differenza della progressione sia un quadrato.

Ritratto di Fermat eseguito da Antoine Durant nel 1600

A questi problemi Fermat aggiunse alcuni teoremi, come:

-«Ogni numero è somma di uno, due o tre triangoli; di uno, 2, 3, 4 quadrati; di uno, 2, 3, 4, 5 pentagoni; di uno, 2, 3, 4, 5, 6 esagoni; d'uno, di 2, 3, 4, 5, 6, 7 eptagoni e così di seguito indefinitamente...»
-«Un multiplo di 8 diminuito d'una unità si compone solamente di 4 quadrati, non solo in interi ma anche in frazioni»

Altri sono enunciati in una lettera a Carcavi dell'agosto 1659.
E' meno noto il fatto che Fermat abbia fatto un passo decisivo in avanti rispetto a Diofanto nell'affrontare la risoluzione dei problemi diofantini, perché egli ha mostrato che i calcoli derivanti dai metodi della tangente e della secante di Diofanto potevano essere ripetuti consecutivamente in

modo da fornire un'infinità di soluzioni razionali per le equazioni che determinano curve ellittiche.
Nelle sue osservazioni all'*Aritmetica* di Diofanto egli parla appunto di *"ma méthode"* e *"la méthode que je inventée"*.
J. De Billy spiegò il metodo di Fermat in maniera più dettagliata. Nell'Introduzione all'*Inventum Novum*, che come è noto si basa sulle lettere di Fermat, egli scrisse con enfasi e un po' di retorica:

"...chi ha mai fornito tante soluzioni quante se ne vuole ad espressioni composte di cinque termini di gradi successivi [cioè, a equazioni del tipo $y^2=ax^4+bx^3+cx^2+dx+c$*]? Chi, dalle radici primitive, ha saputo ricavare quelle derivate del primo ordine, del secondo, del terzo e così di seguito indefinitamente? Una persona senza dubbio; è a Fermat che appartiene questa scoperta."*

Per un esempio del metodo di Fermat rimando a Bashmakova.

4. Il secolo XVIII

Newton e Leibniz si interessarono all'analisi diofantina. In uno scritto del 1670 Newton interpreta l'equazione diofantina $y^2=P(x)$, con P polinomio di terzo grado, come la ricerca dei punti a coordinate razionali sulla cubica piana definita da questa equazione; Newton spiega come una secante che congiunge due punti razionali incontra la curva in un terzo punto razionale. Ma a quel tempo la sua interpretazione attraverso la geometria algebrica è rimasta isolata.

Isaac Newton

Leibniz s'era accorto invece che alcune manipolazioni impiegate nell'analisi diofantina gli permettevano di poter esprimere razionalmente

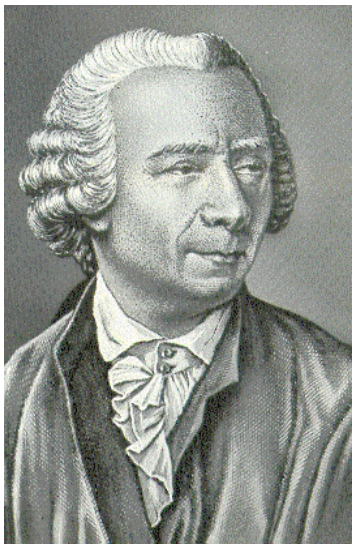
in funzione di un parametro delle quantità x e y, legate da una relazione algebrica f (x, y) =0.
Egli si accorse che poteva utilizzare le stesse manipolazioni nel calcolo integrale per ottenere degli integrali del tipo [Houzel]

$$\int y\, dx.$$

Leonhard Euler introdusse essenzialmente nuove idee nell'analisi diofantina. Egli sistematizzò [1770, *Vollständige Anleitungzur Algebra*, *Opera Omnia* 1 (1) pp. 209-498] e sviluppò tutte le ricerche precedenti relative alle curve

$$y^2=f_3(x), \qquad y^2=f_4(x), \qquad y^3=f_3(x),$$

dove $f_n(x)$ è un polinomio di grado n a coefficienti razionali interi. Determinò i punti razionali su queste curve per mezzo del metodo della tangente e applicò il metodo della secante in alcuni esempi come quelli portati da Diofanto.



L. Euler

Scoprì anche la condizione che assicurava che tutte le soluzioni razionali dell'equazione

$$y^2=ax^3+bx^2+cx+d$$

potessero essere rappresentate mediante funzioni razionali di un parametro.

5. Il secolo XIX

Generalmente, si crede che soltanto Poincaré notò la connessione tra l'analisi diofantina e il teorema di addizione degli integrali ellittici; invece, era stato già preceduto da una breve nota di Jacobi del 1835: "*De usu theoriae integralium ellipticorum et integralium abelianorum in analysi Diophantea*, Journal für die reine und angewandte Mathematik 13, pp. 353-355; in C.G.J. Jacobi, *Gesammelte Werke* 2, Berlino 1882, pp. 53-55." (*Sull'applicazione della Teoria degli integrali ellittici e abeliani all'Analisi diofantina*), in cui il matematico tedesco formulava in modo nuovo i problemi di analisi diofantina studiati dal grande Euler.
Spunto del lavoro di Jacobi fu proprio l'avere ricevuto dall'Accademia Petropolitana un volume postumo di memorie di Euler, in cui si affrontava il seguente problema:

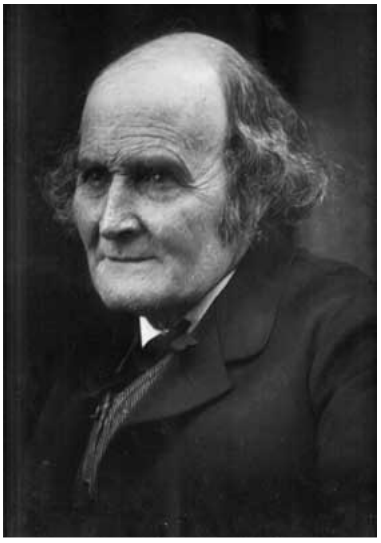
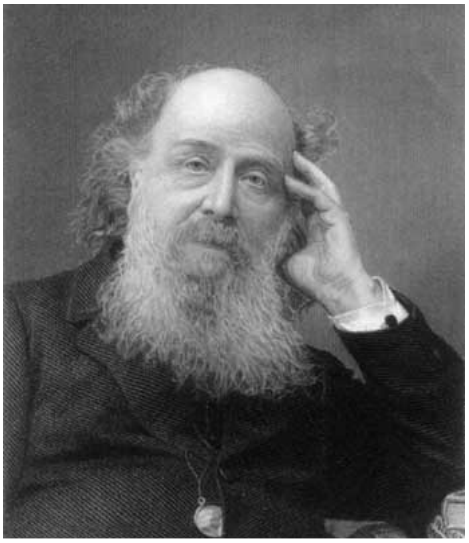
Dato un numero razionale x che rende l'espressione

$$(a + bx + cx^2 + dx^3 + ex^4)^{1/2}$$

razionale, trovare un'infinità di altri valori di x della stessa specie.

Jacobi fece rilevare come il metodo di Euler di analizzare problemi del tipo di quello riportato coincideva esattamente con il procedimento usato per scoprire il teorema di addizione per gli integrali ellittici. Benché Euler non avesse fatto rilevare questa coincidenza, Jacobi credeva che difficilmente egli avrebbe potuto non notarla.
In sostanza, Jacobi scoprì la connessione tra i problemi di analisi diofantina per le curve ellittiche e i teoremi d'addizione di Euler per gli integrali ellittici. Egli effettuò uno studio profondo della struttura dei punti razionali sulle curve ellittiche ma non indovinò la generazione finita dei punti razionali né ebbe la nozione di equivalenza birazionale. Studiò anche curve di genere superiore, e abbozzò un piano per costruire una teoria per esse. Egli terminò il suo lavoro con alcune generalizzazioni con lo scopo di accertare la connessione tra l'analisi diofantina e il teorema d'addizione di Abel.
Come sottolinea la Bashmakova, Jacobi generalizzò i risultati relativi alle curve ellittiche per includere quelle che oggi vengono chiamate *varietà jacobiane arbitrarie*. [Brigaglia-Ciliberto]
Comunque, resta il fatto che questo lavoro di Jacobi, breve ma succoso, passò inosservato, tanto che nemmmeno Poincaré ne era a conoscenza.

Nel periodo successivo al 1835 i matematici cominciarono a studiare le curve algebriche con interesse crescente. Riemann, com'è noto, classificò le equazioni del tipop $f(x, y) = 0$ [f polinomio a coefficienti complessi] prendendo come fondamento le trasformazioni birazionali; egli scoprì così il loro invariante più importante: il *genere* della curva. Poi A.
Clebsch (1833-1872) e altri studiosi dell'ultima metà del XIX secolo algebraizzarono i metodi di Riemann [Houzel], dando origine, con ciò, alla geometria algebrica delle curve.
Joseph James Sylvester (1814-1897), insieme a Arthur Cayley (1821-1895), fu il matematico inglese più importante del suo tempo. Il suo nome rimane legato soprattutto alla teoria degli invarianti che accomuna i suoi lavori sia a quelli di Cayley che a quelli di Hermite. Famosi furono i suoi lavori sulla distribuzione dei numeri primi e specialmente sulla partizione dei numeri.

A. Cayley *J.J. Sylvester*

Ma anche all'analisi diofantina Sylvester dedicò alcuni lavori molto interessanti, studiando le equazioni diofantine di terzo grado con i metodi della geometria algebrica. I risultati delle sue ricerche furono dapprima annunziati in una nota del 1858 (rif. bibl.) e poi sviluppati in una serie di memorie dal 1879 al 1880, proprio nel periodo in cui Poincaré iniziava a interessarsi di ricerche aritmetiche. In questi lavori Sylvester non usa mai la parametrizzazione della cubica mediante le funzioni ellittiche, e il suo metodo consiste nel costruire dei punti razionali della cubica partendo da un punto razionale dato e servendosi del metodo della tangente e della secante. [Houzel]

Nel 1890 Hilbert e Hurwitz pubblicarono su *Acta Mathematica* (v. 14, pp. 217-224) un lavoro dal titolo *Über die diophantischen Gleichungen von Geschlecht null* (Sulle equazioni diofantine di genere zero), in cui per la prima volta, il *genere*, nella sua qualità di invariante, tratto dal lavoro di Riemann sugli integrali abeliani e introdotto in geometria algebrica da Clebsh [seminari di Houzel], compariva in una questione d'analisi diofantina.
Hilbert e Hurwitz stabilirono in sostanza che una curva di genere zero e di grado *n* definita su **Q** era birazionalmente equivalente, sempre su **Q**, o ad una retta proiettiva o ad una conica. Generalizzando il metodo della secante, essi costruivano una curva birazionalmente equivalente alla curva data, di grado *n*-2 e ciò era sufficiente per ricominciare il procedimento.
Sembra che Poincaré non fosse a conoscenza nemmeno di questo risultato importante (Weil attribuisce tale lacuna alla poco dimestichezza di Poincaré con la lingua tedesca).

Alcuni concetti sulle Curve ellittiche

Prima di passare alla memoria di Poincaré mi sembra opportuno premettere alcuni concetti e risultati sulle curve ellittiche, che renderanno più chiaro il contenuto della memoria.

1] *Innanzitutto il nome*: tali curve si chiamano *ellittiche* non perché abbiano qualche legame con l'ellisse (che è una curva di genere zero e quindi non è una *curva ellittica*) ma semplicemente perché possono essere parametrizzate solo mediante le funzioni ellittiche.

2] *Genere di una curva ellittica*

Il genere di una curva algebrica piana può essere descritto in termini dei suoi punti singolari e del grado dell'equazione che la definisce.
Ricordiamo che un *p*-esimo punto singolare di ordine r_p di una curva di equazione $f(x, y)=0$ è un punto per cui si annullano le derivate parziali f_x ed f_y fino all'ordine *r*-1.
Nello spazio proiettivo avviene la stessa cosa, e si dimostra che:

Se C, di equazione implicita f(X, Y, Z) = 0, è una curva irriducibile nello spazio proiettivo, e di grado n, allora il suo genere è dato da

$$g(C) = \frac{(n - 1)(n - 2)}{2} - \sum_p \frac{r_P (r_P - 1)}{2}$$

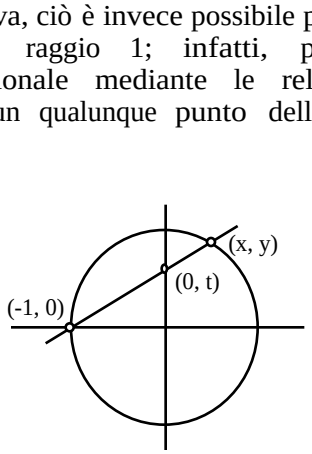
dove la somma è presa su tutti i punti singolari P di C.

Il numero (n-1) (n-2)/2 è il massimo numero possibile di punti singolari di una curva di grado *n*.
Classicamente il genere venne chiamato *difetto*, poiché misura la deviazione della curva dal numero massimo dei suoi punti singolari, come nodi o cuspidi che si ottengono, com'è noto, risolvendo il sistema dato annullando le derivate parziali f'_x ed f'_y della curva *f*.
Per esempio, una cubica piana senza punti doppi è di genere 1; se ha un punto doppio è di genere zero, nel qual caso la curva viene anche detta *unicursale* perché le sue coordinate sono esprimibili razionalmente in funzione di un parametro.
E' dovuto a A. Clebsch (1833-1872) il teorema secondo il quale *una curva razionale non riducibile è di genere zero e viceversa.*
Sempre a Clebsch è dovuto un altro fondamentale teorema (1863-64) per le curve di genere 1, secondo il quale *le coordinate di una qualunque curva di genere 1 si esprimono come funzioni ellittiche di un parametro.*

Si dimostra il seguente importante teorema:

Se C_1 è birazionalmente equivalente a C_2 (cioè se le due curve sono equivalenti in base ad una trasformazione birazionale), allora $g(C_1)=g(C_2)$.

Ma ***l'inverso non è vero***, perché due curve possono avere lo stesso genere, ma non essere birazionalmente equivalenti.
Per esempio, le due curve $x^2 + y^2 = 1$ e $x^2 + y^2 = 3$ sono due curve non singolari di genere zero, ma non sono birazionalmente equivalenti, perché la prima ha punti razionali, mentre la seconda no. La ragione di ciò risiede nel fatto che mentre non è possibile esprimere mediante espressioni razionali di un certo parametro le coordinate di un qualsiasi punto della seconda curva, ciò è invece possibile per la prima curva, che è una circonferenza di raggio 1; infatti, possiamo trovare una parametrizzazione razionale mediante le relazioni che legano le coordinate *x* e *y* di un qualunque punto della circonferenza ad un parametro *t*:



$$x = \frac{1 - t^2}{1 + t^2} \ , \qquad y = \frac{2\,t}{1 + t^2}$$

Come ulteriore esempio, la curva $y=x^3$ ha la parametrizzazione $x=t$ e $y=t^3$ e ha genere zero, che può essere calcolato direttamente con la formula. Infatti, nel piano affine la curva non ha punti singolari, mentre nel piano proiettivo, in cui la sua equazione si scrive $YZ^2 - X^3 = 0$, il punto Y_∞ (0, 1, 0) è un punto singolare di ordine 2 sulla curva, per cui il genere è:

$$g = \frac{(3 - 1)(3 - 2)}{2} - \frac{2(2 - 1)}{2} = 0$$

Una *curva ellittica* è una curva non singolare di genere uno che contiene un punto razionale O.
Se E denota una curva ellittica nella forma normale:

$$E: y^2 = f(x) = x^3 + ax^2 + bx + c$$

E(K) denoterà l'insieme dei punti di E a coefficienti nel campo K **1** **C**.

3] *Curve ellittiche e funzioni ellittiche*

Le curve ellittiche non possono essere parametrizzate mediante funzioni razionali, ma possono esserlo nella cosiddetta *forma normale di Weierstrass*:

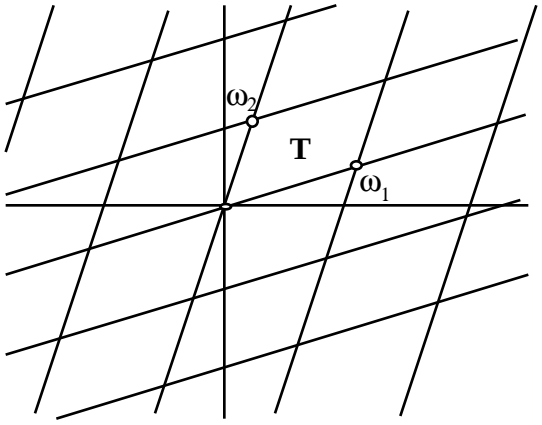
$$y^2 = 4x^3 - g_2 x - g_3$$

K. Weierstrass

Nella teoria delle funzioni ellittiche dovuta a Weierstrass si dimostra che ognivolta che si hanno due numeri complessi g_2, g_3 tali che il polinomio $4x^3 - g_2x - g_3$ ammette radici distinte (cioè, in modo che $g^3{}_2 - 27\, g^2{}_3 \neq 0$), allora si possono trovare nel piano complesso dei numeri complessi ω_1, ω_2 (chiamati *periodi*) mediante il calcolo di alcuni integrali definiti. Questi periodi sono linearmente indipendenti su **R**, e si considera il gruppo ottenuto prendendo tutte le loro combinazioni lineari su **Z**:

$$L = Z\,\omega_1 + Z\,\omega_2 = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbf{Z}\}$$

Questo sottogruppo del piano complesso si chiama *reticolo*.



Ebbene, benché vi siano molte scelte per i generatori ω_1 e ω_2 di L, nondimeno si ha che i coefficienti g_2, g_3 determinano in maniera unica il gruppo L; e inversamente, il gruppo L determina in maniera unica g_2, g_3 mediante le formule:

$$g_2 = 60 \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^4} \qquad\qquad g_3 = 140 \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^6}$$

I periodi si usano per definire una funzione $\wp(z)$, della variabile complessa z, definita dalla serie:

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left\{ \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right\}$$

Questa funzione meromorfa è chiamata la funzione $\wp(z)$ di Weierstrass. Essa ha poli solo nei punti di L e nessun altro polo nel piano complesso, ed è doppiamente periodica, cioè:

$$\wp(z + \omega_1) = \wp(z) \text{ e } \wp(z + \omega_2) = \wp(z)$$

Ebbene, si dimostra che $\wp(z)$ e $\wp'(z)$ soddisfano l'equazione differenziale:

$$\wp'(z)^2 = 4\,\wp(z)^3 - g_2\wp(z) - g_3$$

con

$$\wp'(z) = \frac{d\wp}{dz}.$$

Ciò significa allora che $(\wp(z), \wp'(z))$ è un punto della curva:

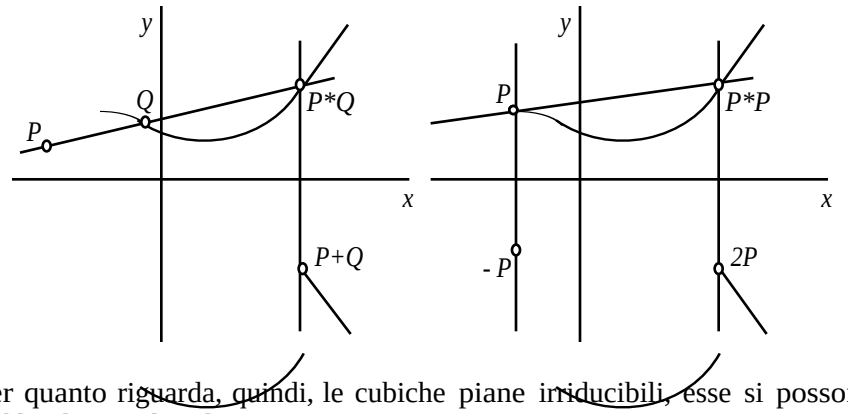
$$y^2 = 4x^3 - g_2x - g_3$$

Poiché, come dimostrò Weierstrass, ogni funzione ellittica può essere espressa semplicemente in termini di $\wp(z)$ e della sua derivata $\wp'(z)$, ne deriva che le funzioni ellittiche parametrizzano le curve ellittiche.
Inversamente, ogni curva ellittica nella forma normale di Weierstrass determina un reticolo L tale che $\wp(z)$ e $\wp'(z)$ parametrizzano la curva.

4] Si può mostrare che ogni cubica ellittica è birazionalmente equivalente (nel senso precisato prima) ad una cubica nella forma normale di Weierstrass o all'equazione leggermente più generale:

$$y^2 = x^3 + a\,x^2 + bx + c$$

Ebbene, l'insieme dei punti razionali sulla cubica è un gruppo, con una operazione di somma ben definita. Poiché una cubica nella forma di Weierstrass ha un solo punto O all'infinito, si assumerà questo come elemento neutro del gruppo, per cui per trovare i punti razionali sulla curva ellittica, noti un punto o una coppia di punti, si procederà come indicato nelle figure seguenti:



Per quanto riguarda, quindi, le cubiche piane irriducibili, esse si possono suddividere in due classi:

1) Le *cubiche dotate di un punto doppio*, che hanno genere zero e sono rappresentabili parametricamente mediante equazioni del tipo $x=f(t)$, $y=g(t)$, con $f(t)$ e $g(t)$ funzioni razionali del parametro t. Se la cubica è definita da un'equazione $P(x, y) = 0$, con P polinomio a coefficienti razionali, allora f e g sono quozienti di polinomi in t a coefficienti anch'essi razionali, per cui a ogni valore razionale del parametro t corrisponde sulla cubica un punto razionale, di coordinate $x=f(t)$ e $y=g(t)$, e viceversa.

I punti razionali delle cubiche di genere zero si ottengono dando a t valori razionali.

2) Le cubiche prive di punti doppi, dette *cubiche ellittiche*, che sono di genere uno e non sono curve razionali, cioè non possono essere rappresentate parametricamente da funzioni razionali di qualche parametro. I punti razionali sulle curve ellittiche si possono determinare, in generale mediante un procedimento di costruzione che viene detto per "secanti o tangenti" e che consiste in questo:

a) Se su una cubica ellittica a coefficienti razionali si conosce un punto razionale (x_0,y_0), un altro punto razionale su di essa potrà essere determinato intersecando la cubica con la retta tangente ad essa in (x_0,y_0).Tale intersezione è razionale perché la retta tangente ha coefficienti razionali; le ascisse dei tre punti di intersezione (due dei quali coincidenti) sono le tre radici di un'equazione di terzo grado a coefficienti razionali e la loro somma e il loro prodotto si esprimono razionalmente mediante i loro coefficienti, quindi anche la terza radice è razionale poiché lo sono le prime due.

b) Se su una cubica ellittica a coefficienti razionali si conoscono due punti razionali distinti (x_1,y_1) e (x_2,y_2) se ne può determinare un terzo come ulteriore intersezione della cubica con la retta passante per i due punti:

A questo procedimento di costruzione per "tangenti o secanti" di punti razionali su una curva ellittica si associa in modo naturale una "legge di composizione" mediante la quale tale insieme (includendo punti all'infinito esprimibili con coordinate omogenee razionali) è un gruppo, detto il gruppo di Mordell-Weil della cubica.
In particolare il teorema di Mordell afferma che tale gruppo ha sempre un numero finito di generatori; cioè, l'insieme dei punti razionali su una cubica ellittica o è finito oppure ogni punto razionale su di essa si può ottenere partendo da un numero finito di punti razionali con successive applicazioni del metodo per secanti o tangenti.

La memoria di Poincaré sulle curve ellittiche

Nell'*Introduzione* alla sua memoria del 1901, Poincaré la presentava più come un programma di studio che come una vera teoria:

"Le proprietà aritmetiche di alcune espressioni e, in particolare, quelle delle forme quadratiche binarie, si ricollegano nella maniera più stretta alla trasformazione di tali forme per mezzo di sostituzioni lineari a coefficienti interi. Io non devo insistere qui sulla parte che è stata oggetto di studio di queste sostituzioni e che è molto conosciuta da coloro che si interessano alla Teoria dei numeri. Si può supoporre che lo studio dei gruppi di trasformazioni analoghe sia chiamato a rendere grandi servizi alla Teoria dei numeri. E' ciò che mi ha spinto a pubblicare le considerazioni seguenti benché esse costituiscano piuttosto un programma di studio che una vera teoria.
("plutôt un programme d'étude qu'une véritable théorie" [Poincaré 1901, p. 161]).
Mi sono chiesto se molti dei problemi d'Analisi indeterminata non possano essere ricollegati gli uni agli altri mediante un legame sistematico, grazie a una nuova classificazione dei polinomi omogenei d'ordine superiore di tre variabili, analoghi, per certi aspetti, alla classificazione delle forme quadratiche.
Tale classificazione avrebbe per base il gruppo delle trasformazioni birazionali, a coefficienti razionali, che può subire una curva algebrica."

Per sistemare un gran numero di problemi dell'analisi diofantina, Poincaré ideò una nuova classificazione dei polinomi omogenei di grado superiore, una classificazione simile a quella che Gauss aveva adottato per le forme quadratiche.
Egli definì le curve per mezzo delle coordinate omogenee e chiamò due curve *equivalenti* o appartenenti alla stessa classe se esse potevano essere cambiate l'una nell'altra per mezzo di una trasformazione birazionale.

Poincaré condusse la sua ricerca sulle curve ellittiche usando il campo dei numeri razionali, e a paragone del lavoro di Jacobi, l'avere introdotto la classificazione delle curve mediante la trasformazione birazionale rappresentò, come sottolineò Chatelet, un nuovo passo nella direzione giusta.

II. **Curve unicursali**.

Poincaré considerò quindi curve razionali di genere 0, cioè rette, coniche e cubiche *unicursali*, aventi cioè un punto doppio. Per tali curve egli dimostra il seguente teorema [p. 487]:

Una curva unicursale razionale è sempre equivalente a un'altra curva unicursale, il cui grado è più piccolo di due unità. Da ciò segue che una curva unicursale razionale è sempre equivalente o a una retta o a una conica.

In Matematica è un fenomeno normale che un risultato già noto venga riscoperto da un altro matematico che ne era all'oscuro. Questo è il caso di Poincaré che non sapeva che il suo teorema relativo alle curve di genere zero, era già stato stabilito, prima da Max Noether con un linguaggio differente in un lavoro apparso sui Mathematische Annalen, v. 23, p. 311, dal titolo *Rationale Ausführung der Operationen in der Theorie der algebraischen Funktionen*; e che tale teorema era stato in seguito precisato meglio da Hilbert e Hurwitz nel 1890, in un lavoro dal titolo *Über die diophantischen Gleichungen von Geschlecht null*, apparso sugli Acta Mathematica, v. 14, pp. 217-224.

David Hilbert

Andrè Weil, nella sua conferenza data all'Aia per il centenario della nascita di Poincaré suppone che Poincaré masticasse poco tedesco, per cui non era al corrente di molti lavori tedeschi: *"... sans doute ne lisait-il l'allemand qu'avec beaucoup de peine; ..."*.

Poiché -continua Poincaré- su una retta o su una conica razionale vi è un'infinità di coppie di punti tali che ogni funzione simmetrica delle loro coordinate sia razionale, allora queste coppie si otterranno su una conica intersecando la conica con una qualunque retta razionale. Dunque, su una qualsiasi curva unicursale razionale, c'è sempre un'infinità di coppie razionali; e poiché su una retta razionale vi sono sempre infiniti punti razionali, allora su una curva unicursale razionale qualunque di grado dispari vi sono infiniti punti razionali.
In sostanza, Poincaré, in questo primo punto, introduce per le curve algebriche proiettive l'equivalenza birazionale. Questo punto merita, forse, una precisazione maggiore.
Due curve C_1, C_2 a coefficienti razionali, sono birazionalmente equivalenti se esistono delle funzioni razionali di due variabili a coefficienti razionali che definiscono delle corrispondenze biunivoche di punti da C_1 a C_2 e da C_2 a C_1, e che sono l'una inversa dell'altra, con la possibile eccezione di un numero finito di punti su ciascuna curva. (Le eccezioni si riferiscono sia ai domini delle funzioni che alle relazioni inverse). Fatto ciò, Poincaré reinterpreta tutto mediante il concetto di *gruppo razionale* che egli definisce come un gruppo di punti tali che ogni funzione simmetrica delle loro coordinate sia razionale.

III. Punti razionali delle cubiche

Quindi, per le curve di genere 0 lo studio della struttura dell'insieme dei suoi punti razionali si riduceva all'esame dei punti razionali di una conica, problema già risolto, com'è noto, da Diofanto.
In questa terza parte che rappresenta il "cuore" della memoria Poincaré introduce vari concetti importanti che andiamo ad esaminare.
Innanzitutto, egli prende in considerazione le più semplici tra le curve ellittiche di genere 1, cioè le cubiche, di cui intende studiare proprio la distribuzione dei punti razionali. Ma egli assume che esse possano essere parametrizzate mediante funzioni ellittiche, senza peraltro stabilire quando tali curve abbiano un punto razionale, né in che modo esse siano birazionalmente equivalenti a curve nella forma normale di Weierstrass. Sono appunto questi particolari, lasciati agli altri, che caratterizzano questa memoria di Poincaré, come altre memorie in cui si nota, come è stato più volte rilevato anche da altri studiosi delle sue opere, come questo grande matematico miri alla cima senza preoccuparsi tanto di alcuni dettagli che egli ritiene secondari. Ciò comporta che la lettura di alcune parti della memoria non è agevole se a monte non cè una conoscenza almeno di base di ciò che Poincaré ritiene *evidente*.
Egli considera il caso in cui gli argomenti ellittici di tutti i punti razionali della cubica si ottengono per combinazione d'un numero finito di valori

ed introduce il valore minimo di questo numero con il nome di *rango*. Come il genere il rango è un invariante per trasformazioni birazionali.
Poincaré afferma, a questo punto, che il rango è un elemento molto importante per la classificazione delle cubiche razionali (“*c'est évidenmment un élement très important de la classification des cubiques rationnelles*”, p. 493), anche se -tenendo fede al suo stile matematico- non dimostra che esso è un invariante per ogni trasformazione birazionale della cubica in un'altra cubica o in una curva di genere 1.
Nell'introdurre il concetto di rango, egli chiama l'insieme dei punti razionali il cui numero costuisce il rango della cubica *sistema di punti razionali fondamentali*, ma ammettendo implicitamente che di tali punti fondamentali ne esista *un numero finito*. Fu proprio questa affermazione implicita a costituire la cosiddetta *congettura di Poincaré* sul gruppo dei punti razionali di una cubica ellittica. Si notò subito che la sua dimostrazione era difficile, e solo nel 1922 l'insigne matematico L.J. Mordell (1888-1872) riuscì a dimostrare [*On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Philos. Soc:, t. 21, 1922, pp. 179-192] che data una curva cubica non singolare nella forma normale di Weierstrass allora l'insieme dei punti razionali della curva è un gruppo abeliano generato in maniera finita; per cui si possono ottenere tutti i punti razionali di una cubica non singolare avendo a disposizione solo un insieme finito di tali punti e usando la legge del gruppo, cioè i metodi geometrici della tangente e della secante.

L.J. Mordell

In seguito, nel 1930, il teorema di Mordell sarebbe stato generalizzato da A. Weil.
Passa, quindi, a classificare le cubiche razionali secondo che siano formate da un solo ramo; o due rami ma con punti razionali solo su uno dei due; infine da due rami e con punti razionali su entrambi.
Relativamente a tale classificazione, alla fine di questa sezione, Poincaré pone alcune questioni che fino ad oggi non sono state completamente risolte (p. 495):

"*Quelles valeurs peut-on attribuer au nombre entier que nous avons appelé le rang d'une cubique rationelle? Quelles sont, parmi les catégories que nous venons d'énumérer et qui sont jusqu'ici logiquement possibles, celles qui existent réellement?*"

IV. Altre curve di genere 1

In questa sezione Poincaré passa alla trattazione di qualsiasi curva di genere 1, come per esempio, le quartiche, e si pone il problema di determinare in quali casi vi possa essere equivalenza tra una quartica o una curva di grado superiore e una cubica. Dimostra così un bel teorema, secondo il quale

Condizione necessaria e sufficiente affinché una quartica razionale sia equivalente ad una cubica è che essa abbia un punto razionale.
Condizione necessaria e sufficiente affinché una cubica razionale sia equivalente ad una quartica è che essa abbia un punto razionale.

Passa quindi a trattare la questione ancora più generale:

"Sia $f = 0$ una curva piana di genere 1 e di grado m. Qual è la condizione perché essa sia equivalente ad una curva di grado p, la cui equazione è $f_1 = 0$?"

Alla questione Poincaré risponde dimostrando il teorema:

"Affinché una curva razionale di genere 1 e di grado m sia equivalente ad una curva di grado $p>3$, è necessario e sufficiente che essa possieda un gruppo razionale di p punti"

Poiché un gruppo razionale di punti sulla curva può essere determinato, come s'è detto, non appena si conosca un punto razionale o una coppia di punti razionali (applicando il metodo della tangente e della secante), allora questi risultati di Poincaré si possono completare dicendo che:

Affinché una curva razionale piana, di genere 1, sia equivalente ad una cubica di equazione

$$y^2=x^3+px+q \qquad (p, q \text{ razionali})$$

è necessario e sufficiente che sulla curva esista un punto razionale; affinché essa sia equivalente ad una quartica d'equazione

$$y^2=x^4+ax^2+bx+c \qquad (a, b, c \text{ razionali})$$

è necessario e sufficiente che sulla curva esista una coppia di punti razionali.

V. Studio di alcune trasformazioni

In questo paragrafo Poincaré studia, nel caso dell'esistenza di due punti razionali su una cubica di genere 1, una certa trasformazione della cubica in se stessa. Questa trasformazione può essere considerata come l'applicazione sulla cubica d'una trasformazione di Cremona del piano. I punti base di questa trasformazione e quelli della sua inversa formano un esagono inscritto in una conica, i cui punti di Pascal sono dei punti allineati della cubica. Questo paragrafo pieno di spirito geometrico serve in realtà a Poincaré per introdurre la ricerca generale del paragrafo seguente.

VI. Suddivisione delle classi in sottoclassi

L'interesse di questo paragrafo risiede nel fatto che teoricamente le cubiche possono ripartirsi in sottoclassi. Scrive Poincaré (p. 513):

"Una questione si pone dopo. Secondo le nostre definizioni, due cubiche sono equivalenti o appartengono alla stessa classe se si può passare dall'una all'altra mediante una trasformazione birazionale a coefficienti razionali. Io dirò che esse appartengono alla stessa sottoclasse se si può passare dall'una all'altra nediante una trasformazione lineare a coefficienti razionali (io non dico interi)."

Ebbene -dice Poincaré- ci si può accorgere se due cubiche appartengono alla stessa sottoclasse, perché non esiste che un numero finito di trasformazioni lineari che permettono di passare da una cubica all'altra; per cui è sufficiente cercare se fra esse ve ne sia una a coefficienti razionali.
Purtroppo, come sottolinea Chatelet in una nota a pie' di pagina, la difficoltà, non ancora eliminata, della classificazione delle cubiche, e in generale delle curve di genere 1, risiede proprio nel raggruppamento delle sottoclassi (o delle curve definite da una trasformazione lineare, a coefficienti razionali) in classi.

VIII. Cubiche derivate

In questo penultimo paragrafo Poincaré considera il caso di una cubica *C* con tre punti di flesso razionali in linea retta, di equazione

$$A^3 = X\ Y\ Z$$

con A, X, Y, Z polinomi di primo grado in *x, y, z* a coefficienti interi. Da essa, mediante opportune trasformazioni su A, X, Y e Z, del tipo:

$$X=h_1\,\xi^3,\ Y=h_2\,\eta^3,\ Z=h_3\,\zeta^3,\ A=k\,\xi\eta\zeta$$

eliminando *x, y, z* tra esse, egli ottiene una relazione lineare e omogenea a coefficienti interi tra ξ^3, η^3, ζ^3, che è l'equazione di una cubica razionale *C'* sulla quale si trova il punto di coordinate ξ, η, ζ, e che egli chiama una *derivata* di *C.* Poiché tra gli interi *h* e *k* -dice Poincaré- non si può fare che un numero finito di ipotesi segue che *C* non ha che un numero finito di cubiche derivate; inoltre, a ciascun punto razionale di C corrisponde un punto razionale d'una delle sue derivate, e se C ha un'infinità di punti razionali, la stessa cosa avviene almeno per una delle sue derivate.
Quindi, passa a dimostrare che le funzioni ellittiche relative a C' si deducono da quelle che sono relative a C mediante una trasformazione del terzo ordine.
Infine, generalizza questi risultati validi nel caso in cui i tre punti di flesso di C siano razionali, aggiungendo al dominio di razionalità le coordinate dei tre punti in linea retta, per cui l'equazione della cubica (p. 534) si scriverà

$$X\,Y\,Z = A^3$$

con X, Y, Z, A polinomi di primo grado i cui coefficienti sono degli interi algebrici del corpo algebrico ottenuto mediante l'aggiunta di prima.
Dopo avere chiarito nuovamente come definire anche in questo caso una cubica derivata da quella data, egli stabilisce i seguenti risultati (p. 537):

Una cubica C non ha che un numero finito di derivate.

Ad ogni punto razionale di C corrisponde su una delle sue derivate un punto razionale, in modo che se C ha una infinità di numeri razionali, lo stesso deve accadere per almeno una delle sue derivate.

Le funzioni ellittiche relative alla derivata si deducono da quelle della cubica C mediante una trasformazione del terzo ordine.

Si può sintetizzare il contenuto di questo paragrafo dicendo che se si estende il dominio di razionalità aggiungendogli i numeri che formano la base di un certo corpo algebrico, due cubiche che non erano equivalenti possono divenirlo; due cubiche equivalenti che erano di sottoclassi differenti potranno divenire della stessa sottoclasse. Donde nuovi criteri per la classificazione delle cubiche.

IX: Curve di genere superiore

"Je ne dirai que quelques mots des courbes de genre supérieur à 1. Il n'est plus vrai que de la connaissance d'un point rationnel on puisse

déduire celle d'une infinité d'autres points rationnels. Mais de la connaissance d'un groupe rationnel (et par conséquent de celle d'un point rationnel) on peut déduire celle d'une infinité d'autres groupes rationnels. "

In realtà, in sole due pagine Poincaré auspica che anche per le curve di genere superiore, vi sia la possibilità di costruire una teoria analoga a quella delle cubiche, partendo dai gruppi razionali di punti situati sulla curva.

Epilogo

Scrive Albert Chatelet, a commento della grande memoria di Poincaré:

"Sembra che questa Memoria d'Aritmetica di H.Poincaré sia quella che ha dato origine alla maggior parte delle ricerche e dei lavori successivi. Essa ha messo in evidenza la relazione stretta tra i due problemi diofantini:
1° la ricerca dei punti di coordinate razionali che si trovano su una curva algebrica definita attraverso un'equazione a coefficienti razionali;
2° la costruzione della classe delle curve (chiamate equivalenti) dedotte da una d'esse attraverso le trasformazioni birazionali a coefficienti razionali. [...] Dal 1910 la Memoria di Henri Poincaré, che egli stesso modestamente chiama un "programma di studi", ispira numerosi lavori. Alcuni dei risultati sono stati precisati e completati da Nagell, Mordell, Maillet, ecc. Altri sono stati generalizzti anche in Francia, così le curve di genere superiore a 1 sono state studiate da Weil. I gruppi dei punti eccezionali d'una cubica e le molteplicità unicursali sono state studiate da François Chatelet. Alcune precisazioni sul rango di una curva sono state ottenute da Neròn.
Una esposizione di queste diverse ricerche si trova nel fascicolo XXXIX (1929) del Memorial de Sciences mathématiques su L'Analyse Indeterminée de degrée superieur redatto da M. Nagell. "

Io voglio concludere ricordando come lo studio delle curve ellittiche costituisca oggi un vasto campo di ricerca, anche perché ormai nelle nuove indagini intervengono metodi e concetti di analisi, di algebra e di geometria algebrica.
Per esempio, nella fattorizzazione di grandi interi, che è uno dei temi di ricerca più all'avanguardia nell'attuale Teoria dei numeri, soprattutto per le sue applicazioni crittografiche, uno degli algoritmi più usati è quello dovuto a H.W. Lenstra Junior [*Factoring Integers with Elliptic Curves*, Annals of Mathematics, (2) 126, 1987, pp. 649-673], in cui si calcolano ricorsivamente i punti razionali del gruppo abbinato ad una curva ellittica, considerata nella forma di Peter Montgomery:

$$By^2 = x^3 + A\,x^2 + x \quad \text{con } B\,(A^2 - 4) \neq 0$$

Per finire, riporto uno stralcio di lettera che il nipote di Poincaré, Pierre Boutroux scrisse a G. Mittag-Leffler (1846-1927) dopo la morte dello zio, e che venne pubblicata negli Acta Mathematica, 38, 1921, pp. 197-201.

[...] *Nella quiete del suo studio in rue Claude Bernard o sotto le ombrose fronde del suo giardino di Lozère, ogni giorno, per alcune ore, Henrì Poincaré si sedeva davanti a un quinterno di fogli a righe, e si vedevano allora le pagine riempirsi, con sorprendente rapidità e regolarità, della sua scrittura fine e angolosa. Quasi mai una cancellatura, molto di rado un'esitazione. In pochi giorni ecco terminata una lunga memoria, pronta per essere data alle stampe, e mio zio non se ne interessava ormai più, se non come a un evento del passato.*
[...] *Egli pensava per strada mentre si recava alla Sorbona, quando doveva assistere a qualche riunione scientifica, o quando, dopo pranzo, faceva, com'era solito, una delle sue lunghe passeggiate a piedi. Egli pensava nella sua anticamera, o nella sala delle sedute dell'Institut, quando passeggiava a piccoli passi, la fisionomia tesa, agitando il suo mazzo di chiavi. Egli pensava a tavola, nelle riunioni familiari, perfino nei salotti, interrompendosi spesso bruscamente nel mezzo d'una conversazione, e piantando il suo interlocutore, per cogliere al volo un pensiero che gli attraversava lo spirito.*
In mio zio tutto il lavoro di scoperta avveniva mentalmente, senza ch'egli, nella maggior parte dei casi, avesse bisogno di controllare i suoi calcoli per iscritto o di fissare le sue dimostrazioni sulla carta. Egli attendeva che la verità lo colpisse come il tuono, e per ricordarla contava sulla sua memoria eccellente.

Bibliografia di riferimento

1. **A. Brigaglia-C. Ciliberto**, *Geometria algebrica*, in La Matematica Italiana dopo l'unità. Gli anni tra le due guerre mondiali, 1998, Marcos y Marcos.

2. **I. G. Bashmakova**, *Arithmetic of Algebraic Curves from Diophantus to Poincaré*, Historia Mathematica 8 (1981), pp. 393-416;

3. **U. Bottazzini**, *Il flauto di Hilbert. Storia della matematica moderna e contemporanea*, Utet, 1990.

4. **U. Bottazzini**, *Poincaré. il cervello delle scienze razionali*, Le Scienze, 1999.

5. **W. e F. Ellison**, *Théorie des nombres*, in Abrégé d'histoire des Mathématiques 1700-1900 (a cura di J. Dieudonné), Hermann, tome I, 1978, pp. 165-333.

6. **Ch. Houzel**, *Théoreme de Fermat. A travers l'histoire de l'analyse diophantienne*, Société de mathématique de France, 1995, pp. 1-17;

7. **Ch. Houzel**, *Fonctions elliptiques et intégrales abéliennes*, in Abrégé d'histoire des Mathématiques 1700-1900 (a cura di J. Dieudonné), Hermann, tome II, 1978, pp. 1-113.

8. **D. Husemöller**, *Elliptic Curves*, Springer-Verlag, 1987.

9. **A. W. Knapp**, *Elliptic Curves*, Princeton University Press, 1992.

10. **S. Lang**, *Elliptic Curves: Diophantine Analysis*, Springer-Verlag, 1978.

11. **L.J. Mordell**, *Diophantine Equations*, Academic Press, 1969.

12. **H. Poincaré**, *Oeuvres*, tome V, Gauthier-Villars, 1950.

13. **K. A. Ribet, B. Hayes**, *Fermat's Last Theorem and Modern Arithmetic*, American Scientist, vol. 82, march-april 1994, pp. 144-156.

14. **G. M. Scarpello**, *On the Legendre's steps. Elliptic functions, Geometry and nonlinear Mechanics in the Eighteenth Century* (inedito).

15. **J. H. Silvermann & John Tate**, *Rational points on elliptic curves*, Springer-Verlag, 1992.

16. **C. Viola**, *Commento al n. 44 delle "Osservazioni su Diofanto" di Fermat*, Archimede, 1984, pp. 178-185.

17. **A. Weil**, *Teoria dei Numeri*, Einaudi, 1993, (in particolare modo le *Appendici al capitolo secondo*, pp. 119-147).