Joseph-Louis Lagrange e il teorema dei quattro quadrati

Jenny Boucard

JOSEPH-LOUIS LAGRANGE E IL TEOREMA DEI QUATTRO QUADRATI

di Jenny Boucard

Jenny Boucard

È "maître de conférences" in Storia della Matematica all'Università di Nantes. I suoi contributi vertono sulla storia della Teoria dei numeri tra il 1750 e il 1850. È autrice di una tesi (discussa nel 2011) intitolata "Un «rapprochement curieux de l'algèbre et de la théorie des nombres»: études sur l'utilisation des congruences en France de 1801 à 1850".

Conosciuto in particolare per i lavori di Analisi e la *Mécanique analytique*, Joseph-Louis Lagrange non è forse altrettanto considerato per le ricerche aritmetiche, spesso trascurate nelle descrizioni del suo lavoro matematico. Lagrange è in realtà uno degli studiosi che maggiormente hanno contribuito alla rinascita di questo campo matematico nel XVIII secolo: "*Avec Euler, Lagrange remet en honneur la théorie des nombres, négligée depuis Fermat; il démontre pour la première fois quantité de théorèmes que les arithméticiens du dix-septième siècle s'étaient contentés d'énoncer, et aussi le théorème de J. Wilson, communiqué par Waring; ses travaux sur l'équation de Pell et sur l'analyse indéterminée générale du second degré, où le rôle du discriminant des formes quadratiques est mis en lumière, préparant les voies à Legendre et à Gauss*" (Andoyer et Humbert 1924, p. 69).
[*Insieme a Eulero, Lagrange, che ha dato lustro alla teoria dei numeri, trascurata dopo Fermat, ha dimostrato per la prima volta una grande quantità di teoremi che gli aritmetici del XVII secolo si limitavano a enunciare, fra i quali anche il teorema di J. Wilson, riportato da Waring; il suo lavoro sulla equazione di Pell e l'analisi generale delle forme indeterminate di secondo grado, in cui viene evidenziato il ruolo del discriminante delle forme quadratiche, aprì la strada a Legendre e Gauss*].

Il teorema dei quattro quadrati

> Nel XVIII secolo alcuni nomi ricorrono sistematicamente nella storia di questa teoria come quelli di Goldbach ed Eulero che si scambiarono alcune lettere sull'Aritmetica nel 1730.

Le ricerche in ambito aritmetico affrontate da Lagrange sono solitamente descritte come la sintesi di una serie di risultati ottenuti da Fermat ed Eulero e l'anticipazione della teoria delle forme quadratiche sviluppata da Legendre e Gauss all'inizio del XIX secolo. Dopo una breve presentazione del lavoro aritmetico di Lagrange, l'obiettivo di questo articolo sarà quello di fornire una visione concreta dei metodi e delle tecniche utilizzate dal grande matematico torinese nella Teoria dei numeri e di individuare la sua attività aritmetica nella seconda metà del Settecento con particolare attenzione alla dimostrazione del teorema dei quattro quadrati [1] e ad alcuni lavori che ci permetteranno di comprendere al meglio la realizzazione di questa dimostrazione.

1 Lagrange e la Teoria dei numeri: una panoramica

Con i lavori di Eulero, Lagrange e Legendre, la seconda metà del Settecento può essere considerata un'epoca di transizione nella storia della Teoria dei numeri [2]. Tra il XVI e il XVII secolo [3], molti giudici, nobili, diplomatici e religiosi si interessarono a questioni inerenti a tale teoria e si confrontarono per lo più attraverso scambi di lettere o vere e proprie sfide. Il magistrato di Tolosa Fermat è noto in modo particolare per le questioni aritmetiche che pose. Rese così l'Aritmetica un vero e proprio oggetto di studio e incoraggiò i suoi contemporanei ad affrontarla: "*Cependant l'arithmétique a un domaine qui lui est propre, la théorie des nombres entiers; cette théorie n'a été que très légèrement ébauchée par Euclide et n'a pas été assez cultivée par ses successeurs* […]*; les arithméticiens ont donc à la développer ou à la renouveler*".

[*Per quanto riguarda l'Aritmetica, questa ha un campo di studio che gli è proprio, ovvero la teoria dei numeri interi; questa teoria è stata solo delineata in superficie da Euclide e non è stata sufficientemente approfondita dai suoi successori* […]; *gli aritmetici devono perciò svilupparla o quanto meno rinnovarla*].

Alcuni presero questo invito come un gioco, altri al contrario – la maggior parte – lo declinarono. Così John Wallis scriveva a Kenelm Digby: "*Confesso che per, quanto mi riguarda,* [le questioni sui numeri] *non suscitano in me un interesse così grande da rendermi propenso a dedicare loro troppo tempo e fatica. Non le ritengo abbastanza importanti da trascurare altre ricerche in Geometria che mi interessano maggiormente*".

Come vedremo con Lagrange, commenti simili appariranno anche nelle corrispondenze dei secoli successivi. La situazione cambia però in modo significativo nel XIX secolo: l'ultimo teorema di Fermat diventa oggetto di un premio da parte dell'Accademia delle Scienze e alcuni studiosi, fra i quali Kummer, ottengono riconoscimenti ufficiali per i loro contributi alla Teoria dei numeri.

Nel XVIII secolo alcuni nomi [4] ricorrono sistematicamente nella storia della teoria dei numeri. Per cominciare, Christian Goldbach ed Eulero scambiarono alcune lettere sull'Aritmetica a partire dal 1730. Quest'ultimo pubblicò inoltre numerosi articoli su questo tema [5]. Alla fine del secolo, Legendre pubblicò l'Essai sur la théorie des nombres, nel quale riassume diversi risultati di Analisi indeterminata studiati dai suoi predecessori. Per parte sua, Lagrange presentò una dozzina di Memorie sull'Aritmetica tra il 1768 e il 1777.

È proprio a Berlino che Lagrange produsse tutte le sue ricerche di Aritmetica [6]. Lo scienziato si trovava in una posizione molto favorevole che gli permetteva di dedicarsi completamente al lavoro scientifico. All'epoca poi, sempre all'Accademia di Berlino, c'era anche Johann Heinrich Lambert che, a partire dal 1770, mise a punto un progetto per la costruzione di una tavola di fattori e sollecitò l'ambiente accademico a sviluppare una autonoma teoria dei numeri [7]. Lagrange operava dunque in un clima in cui la Teoria dei numeri non era del tutto ignorata e mantenne inoltre una regolare corrispondenza con d'Alembert e Eulero proprio su alcune questioni aritmetiche.

Fra gli scritti I lavori di Aritmetica di Lagrange più famosi e più citati nella storia della Teoria dei numeri sono senza dubbio quelli che trattano dei problemi indeterminati di secondo grado e delle forme quadratiche [8]. Dal 1768 al 1771, Lagrange fornì alcuni metodi per risolvere l'equazione di Pell-Fermat e più in generale i problemi indeterminati di secondo grado. Erano questioni già studiate in precedenza. Ad esempio, nel caso dell'equazione di Pell-Fermat, Eulero aveva dimostrato l'esistenza di infinite soluzioni partendo da una soluzione data. La grande originalità di Lagrange, nel caso delle equazioni indeterminate, consiste nel determinare (se esiste) una soluzione particolare e da questa dedurre l'insieme delle soluzioni. Inoltre, in diverse opere, Lagrange si impegnò a semplificare i suoi metodi di risoluzione [10]. Nel 1775 e nel 1777 Lagrange pubblicò uno studio dei numeri che possono essere rappresentati nella forma $Bt^2+Ctu+Du^2$. Spesso considerato come il contributo più interessante di Lagrange alla teoria dei numeri, questo lavoro viene di solito letto alla luce dei lavori successivi di Legendre e di Gauss sulle forme quadratiche [11]. Un commento a questo suo lavoro si trova nella lettera che Lagrange scrisse a d'Alembert il 6 luglio 1775: "*Je ne serais pas surpris que vous fussiez peu satisfait de ce que j'ai donné dans ce Volume, car je ne l'en suis guère moi-même. Les recherches d'Arithmétique sont ce qui m'a coûté les plus de peine et ce qui vaut peut-être le moins*".

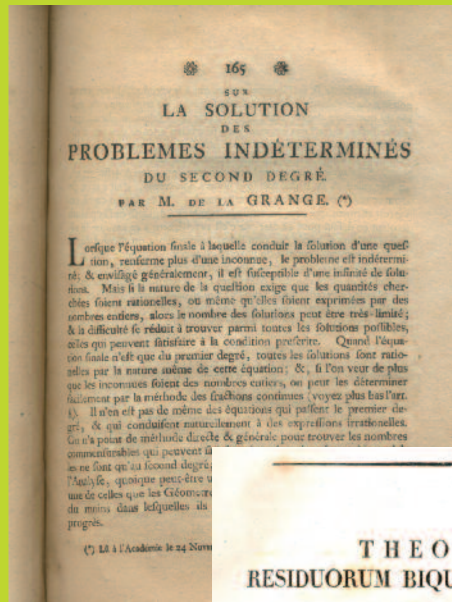
[*Non sarei sorpreso se tu fossi insoddisfatto di quello che troverai in questo volume, perché non mi rappresenta del tutto. Le ricerche d'Aritmetica sono la cosa che più mi è costata in termini di fatica e forse non ne è valsa la pena*]. Lagrange pubblicò infine anche la prima dimostrazione completa di alcuni risultati specifici, fra cui il teorema dei quattro quadrati [12], il teorema di Wilson [13] e la risoluzione dell'equazione diofantea $z^2 = 2x^4 - y^4$ [14]. Queste Memorie sono più brevi rispetto alle altre e possono apparire isolate. Noi comunque dimostreremo come, nel caso del teorema dei quattro quadrati, Lagrange si sia basato su strumenti e metodi già approntati durante le ricerche sui problemi indeterminati di secondo grado e su alcuni scritti di Eulero. Allo stesso modo, quest'ultimo si baserà a sua volta sui lavori di Lagrange per proporre una nuova dimostrazione.

2 *Démonstration d'un théorème arithmétique* di Lagrange (1770)

2.1 Il teorema dei quattro quadrati da Bachet a Lagrange: alcuni riferimenti storici

La Memoria intitolata *Démonstration d'un théorème arithmétique*, pubblicata da Lagrange nel 1772 nelle *Mémoires* dell'Accademia di Berlino, inizia così: "*C'est un théorème connu depuis longtemps* que tout nombre entier non carrés peut toujours se décomposer en deux, ou trois, ou quatre carrés entiers*; mais personne, que je sache, n'en a encore donné la démonstration*" (Lagrange 1772, p. 189).
[*È un teorema noto da tempo quello secondo cui,* dato un qualsiasi numero intero non quadrato, questo può sempre essere diviso in due, tre, o quattro quadrati interi*; ancora nessuno, a mia conoscenza, ne ha però mai fornito la dimostrazione*].
In questo lavoro di una dozzina di pagine, Lagrange presenta una prima dimostrazione del teorema dei quattro quadrati dopo aver tratteggiato una breve analisi storica degli studi precedenti sul "*teorema di M. Bachet*". Anche noi, inizieremo citando alcuni autori che hanno parlato di questo teorema nei loro lavori.
Claude Gaspard de Bachet Méziriac, membro dell'Accademia di Francia dal 1634, è celebre per il volume *Problèmes plaisants et délectables qui se font par les nombres*,

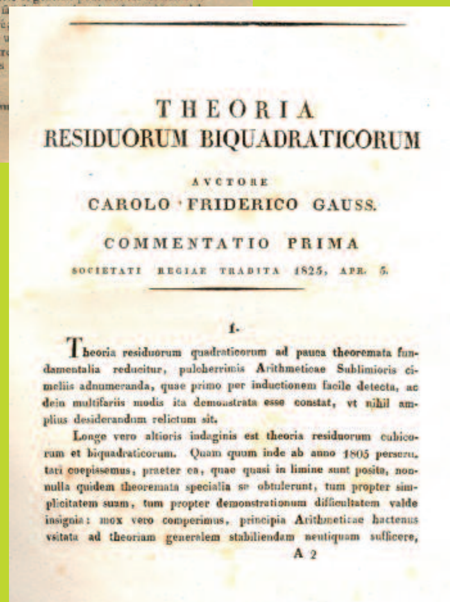
> La grande originalità di Lagrange, nel caso delle equazioni indeterminate, consiste nel determinare (se esiste) una soluzione particolare e da questa dedurre l'insieme delle soluzioni. Inoltre, in diverse opere, Lagrange si impegnò a semplificare i suoi metodi di risoluzione.


165

SUR
LA SOLUTION
DES
PROBLEMES INDÉTERMINÉS
DU SECOND DEGRÉ.
PAR M. DE LA GRANGE. (*)

Lorsque l'équation finale à laquelle conduit la solution d'une question, renferme plus d'une inconnue, le problème est indéterminé, & envisagé généralement, il est susceptible d'une infinité de solutions. Mais si la nature de la question exige que les quantités cherchées soient rationelles, ou même qu'elles soient exprimées par des nombres entiers, alors le nombre des solutions peut être très-limité; & la difficulté se réduit à trouver parmi toutes les solutions possibles, celles qui peuvent satisfaire à la condition prescrite. Quand l'équation finale n'est que du premier degré, toutes les solutions sont rationelles par la nature même de cette équation; &, si l'on veut de plus que les inconnues soient des nombres entiers, on peut les déterminer facilement par la méthode des fractions continues (voyez plus bas l'art. 6). Il n'en est pas de même des équations qui passent le premier degré, & qui conduisent naturellement à des expressions irrationelles. On n'a point de méthode directe & générale pour trouver les nombres commensurables qui peuvent ...

LA PRIMA MEMORIA DI LAGRANGE SULLA TEORIA DEI NUMERI (1769) (Copyright: Accademia delle Scienze di Torino)


THEORIA
RESIDUORUM BIQUADRATICORUM

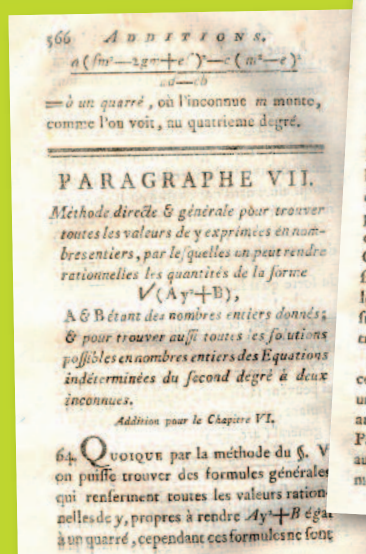
AUCTORE
CAROLO FRIDERICO GAUSS.

COMMENTATIO PRIMA
SOCIETATI REGIAE TRADITA 1825. APR. 5.

1.

Theoria residuorum quadraticorum ad pauca theoremata fundamentalia reducitur, pulcherrimis Arithmeticae Sublimioris cimeliis adnumeranda, quae primo per inductionem facile detecta, ac dein multifariis modis ita demonstrata esse constat, vt nihil amplius desiderandum relictum sit.
Longe vero altioris indaginis est theoria residuorum cubicorum et biquadraticorum. Quam quum inde ab anno 1805 perscrutari coepissemus, praeter ea, quae quasi in limine sunt posita, nonnulla quidem theoremata specialia se obtulerunt, tum propter simplicitatem suam, tum propter demonstrationum difficultatem valde insignia: mox vero comperimus, principia Arithmeticae hactenus vsitata ad theoriam generalem stabiliendam neutiquam sufficere,
A 2

GAUSS SUI PROBLEMI INDETERMINATI DI QUARTO GRADO (1828) (Cortesia di Sandro Caparrini)


566 ADDITIONS.

= à un quarré, où l'inconnue *m* monte, comme l'on voit, au quatrieme degré.

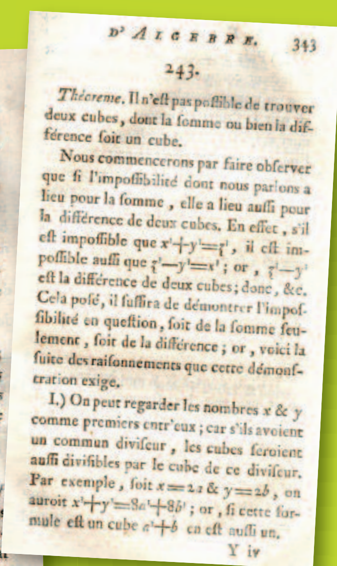
PARAGRAPHE VII.

Méthode directe & générale pour trouver toutes les valeurs de y exprimées en nombres entiers, par lesquelles on peut rendre rationnelles les quantités de la forme $\sqrt{(Ay^2+B)}$, *A & B étant des nombres entiers donnés; & pour trouver aussi toutes les solutions possibles en nombres entiers des Equations indéterminées du second degré à deux inconnues.*

Addition pour le Chapitre VI.

64. Quoique par la méthode du §. V on puisse trouver des formules générales qui renferment toutes les valeurs rationnelles de y, propres à rendre Ay^2+B égal à un quarré, cependant ces formules ne sont

L'ANALISI INDETERMINATA NELLE *ADDITIONS* DI LAGRANGE ALL'ALGEBRA DI EULERO (1773) (Cortesia di Sandro Caparrini)


D'ALGEBRE. 343

243.

Théoreme. Il n'est pas possible de trouver deux cubes, dont la somme ou bien la différence soit un cube.
Nous commencerons par faire observer que si l'impossibilité dont nous parlons a lieu pour la somme, elle a lieu aussi pour la différence de deux cubes. En effet, s'il est impossible que $x^3+y^3=z^3$, il est impossible aussi que $z^3-y^3=x^3$; or, z^3-y^3 est la différence de deux cubes; donc, &c. Cela posé, il suffira de démontrer l'impossibilité en question, soit de la somme seulement, soit de la différence; or, voici la suite des raisonnements que cette démonstration exige.
I.) On peut regarder les nombres *x* & *y* comme premiers entr'eux; car s'ils avoient un commun diviseur, les cubes seroient aussi divisibles par le cube de ce diviseur. Par exemple, soit $x=ma$ & $y=mb$, on auroit $x^3+y^3=m^3a^3+m^3b^3$; or, si cette formule est un cube a^3+b^3 en est aussi un.
Y iv

EULERO SUL PROBLEMA DI FERMAT NELL'*ALGEBRA* (1770) (Cortesia di Sandro Caparrini)

pubblicato nel 1612 e riedito nel 1624, che costituirà una fonte fondamentale nei secoli successivi sulle questioni aritmetiche. Ha inoltre pubblicato, nel 1621, una traduzione dal latino dell'*Arithmétiques* di Diofanto a cui ha aggiunto un commento nel quale si sofferma su un problema diofanteo enunciando a questo proposito il teorema dei quattro quadrati e verificandolo per gli interi da 1 a 325.
Qualche anno più tardi Fermat si procurò questo volume, lo studiò e lo arricchì di annotazioni di proprio pugno: è proprio su queste pagine che il matematico scrisse la famosa affermazione: "*Preuve véritablement merveilleuse que la marge est trop étroite pour contenir* [13]".
[*Dispongo di una meravigliosa dimostrazione di questo teorema che però non può essere contenuta nel margine troppo stretto della pagina*].
È da questo libro che Fermat venne a conoscenza dell'enunciato del teorema dei quattro quadrati. Come dimostra la sua corrispondenza a partire dal 1630 con Marin Mersenne e soprattutto con sir Kenelm Digby, Fermat si occupò a fondo del problema. Così scrisse, nel 1658, a Digby: "*J'annonce à vos éminents correspondants que j'en ai trouvé une démonstration complète*".
[*Annuncio alla vostra eminente persona che ho trovato una dimostrazione completa*]. Anche se non è stata trovata nessuna dimostrazione, l'insieme delle note sulle questioni numeriche che Fermat aveva inviato al suo collega Pierre de Carcavi nel 1659 contiene delle indicazioni metodologiche. Tuttavia l'insieme delle note sulle questioni numeriche che Fermat aveva inviato al suo collega Pierre de Carcavi nel 1659 contiene una traccia per una possibile dimostrazione. Fermat afferma che il teorema dei quattro quadrati ricade in una serie di questioni aritmetiche, *a priori* diverse le une dalle altre, che possono essere dimostrate con quello che lui chiama *metodo della discesa infinita* [14], metodo che descrive nel caso di una proposizione negativa [15]. Si tratta di supporre che il problema ammetta una soluzione intera positiva da cui sia possibile dedurre un'altra soluzione intera positiva, strettamente minore: in questo modo si costruisce una successione decrescente di numeri interi positivi, che porta ad una contraddizione. Fermat propone di applicare questo metodo anche al caso di affermazioni positive e fornisce un esempio con il cosiddetto teorema dei due quadrati [16]: "*Si un nombre premier pris à discrétion, qui surpasse de l'unité un multiple de 4, n'est point composé de deux carrés, il y aura un nombre premier de même nature, moindre que le précédent, et ensuite un troisième encore moindre, etc. En descendant à l'infini jusques ce que vous arriviez au nombre 5, qui est le moindre de tous ceux de cette nature, lequel il s'ensuivrait n'être pas composé de deux quarrés, ce qu'il est pourtant. D'où on doit inférer, par la déduction à l'impossible, que tous ceux de cette nature sont par conséquent composés de deux carrés*".
[*Se un numero primo preso a discrezione, che supera di un'unità un multiplo di 4, non è decomponibile nella somma di due quadrati, allora ci sarà un numero primo minore del precedente della stessa natura e ancora un terzo minore del secondo e così via. E così all'infinito, fino ad arrivare al numero 5 che è il più piccolo dei primi siffatti: ne consegue che neanche lui non può essere decomposto in due quadrati, che è una contraddizione. Quindi dobbiamo dedurre, essendo giunti a una conclusione impossibile, che tutti i numeri primi di questa natura si decompongono nella somma di due quadrati*].

> "Prendendo in considerazione l'insieme delle Memorie di Eulero e Lagrange, appaiono evidenti le reciproche influenze ma anche le differenti posizioni nell'ambito della Teoria dei numeri."

Fermat esplicita il principio del suo metodo, ma non mostra alcun dettaglio per costruire la successione decrescente di numeri interi che soddisfi le condizioni richieste. Vedremo in seguito che questo metodo è al centro delle dimostrazioni date da Lagrange ed Eulero nei loro lavori sulle somme dei quadrati.
Come abbiamo accennato in precedenza, le ricerche in Teoria dei numeri di Eulero iniziano con la sua corrispondenza con Goldbach. In una lettera del 1 dicembre 1729, Goldbach comunica a Eulero alcuni risultati contenuti negli scritti di Fermat, con particolare riferimento ad una congettura di Fermat che affermava che tutti i numeri della forma $2^{2^n}+1$ sono primi [17]. Il 22 maggio 1730, scrive nuovamente a Eulero osservando che i resti dei quadrati dei termini di una progressione aritmetica ottenuti da una divisione per un numero primo formano una sequenza periodica. Eulero risponde a Goldbach il 4 giugno 1730 confermando il proprio interesse per la Teoria dei numeri e in particolare per un "*teorema elegante*" che afferma che ogni numero può essere scritto sotto forma di quattro quadrati. Dal 1730 al 1750, i due studiosi discussero regolarmente i risultati relativi alla somma dei quadrati. Tra il 1749 e il 1751, Eulero presentò diverse Memorie sulle somme di quadrati, nelle quali si trova una dimostrazione di una versione debole del teorema dei quattro quadrati [20]: ogni intero è somma di al più quattro numeri quadrati interi o razionali.
È soltanto nella *Démonstration d'un théorème arithmétique*, pubblicata nel 1772, che Lagrange presenta una dimostrazione completa del teorema dei quattro quadrati [18]. Lagrange ed Eulero avevano in quel periodo [19] una corrispondenza regolare e si confrontavano spesso su questioni aritmetiche, ma mai lo fecero sul teorema dei quattro quadrati. Lagrange non pubblicò alcun articolo intermedio ed espose la sua dimostrazione in una dozzina di pagine, un fatto che rende difficile la comprensione della sua costruzione. La sua lettura non è facile ma soffermarsi proprio sulla dimostrazione permette da un lato di coglie-

re le difficoltà che si presentano quando si guardano da vicino gli scritti di Lagrange e, in secondo luogo, di evidenziare la diversità dei metodi – algebrico, analitico, aritmetico – usati da Lagrange nei suoi scritti in particolare di Teoria dei numeri. Prendendo in considerazione l'insieme delle Memorie di Eulero e Lagrange, appaiono evidenti le reciproche influenze ma anche le differenti posizioni nell'ambito della Teoria dei numeri.

2.2 Punti chiave della dimostrazione del teorema dei quattro quadrati di Lagrange

In generale, il lavoro utilizza una lunga serie di operazioni algebriche che ne rendono difficile la lettura. Come ricorda lo stesso Lagrange nell'introduzione alla sua Memoria, la struttura della dimostrazione si basa su alcuni lavori dedicati da Eulero alla somma dei quadrati. Viene impiegata anzitutto l'affermazione che il prodotto di due somme di quattro quadrati è una somma di quattro quadrati, che consente di limitare il ragionamento ai numeri primi. La dimostrazione che ciascun numero primo è scomponibile nella somma di quattro quadrati è condotta da Lagrange alla maniera di Eulero e presenta due passi:

(I) qualsiasi numero primo divide la somma di due o tre quadrati e il quoziente risultante è minore di p;

(II) se un prodotto è somma di quattro quadrati e uno dei fattori è anch'esso di questa forma, allora anche il secondo fattore sarà una somma di quattro quadrati [20].

Come ricorda lo stesso Lagrange, Eulero aveva già fornito una dimostrazione della preposizione (I). Lagrange fornisce una dimostrazione di questi due passi, partendo però da enunciati leggermente diversi.

2.3 Il metodo della discesa infinita di Lagrange

Lagrange dimostra inizialmente che ogni numero primo che divide la somma di quattro quadrati, senza dividere ogni quadrato, è necessariamente anche lui la somma di quattro quadrati. Per fare questo dimostra che, "*si la somme de quatre carrés est divisible par un nombre premier plus grand que la racine carrée de la même somme, ce nombre sera nécessairement égal à la somme de quatre carrés*" (Lagrange 1772, p. 193) [*se la somma dei quattro quadrati è divisibile per un numero primo maggiore della radice quadrata della loro somma, questo numero sarà necessariamente uguale alla somma di quattro quadrati*]. A questo scopo, Lagrange utilizza il metodo della discesa infinita di cui abbiamo parlato in precedenza a proposito di Fermat. La grande differenza è che Lagrange non ricorre al ragionamento per assurdo. Così, dopo aver dimostrato che ci si potrebbe limitare ai casi in cui i numeri che compongono la somma di quattro quadrati sono primi, considera l'equazione $Aa = p^2 + q^2 + r^2 + s^2$, dove p, q, r, s sono primi tra loro e A è un numero primo tale che:

$$A > \sqrt{p^2 + q^2 + r^2 + s^2}.$$

Seguono tre pagine di operazioni, attraverso identità algebriche e varie considerazioni sulla divisibilità, che gli consentono di ricavare l'esistenza dei numeri interi a', p', q', r' e s' tali che $Aa' = p'^2 + q'^2 + r'^2 + s'^2$ con $a'<a$ se è $a>1$. L'applicazione del metodo della discesa gli permette di concludere: "*Il s'ensuit de là que si Aa est la somme de quatre carrés, Aa' sera aussi la somme de quatre carrés* [...]*; ainsi, si a est plus grand que 1, a' sera nécessairement plus petit que a ; et si a' est encore plus grand que 1, on prouvera de la même manière que Aa" sera aussi la somme de quatre carrés, a" étant plus petit que a' ; et ainsi de suite; donc comme les nombres a, a', a" sont des nombres entiers, dont aucun ne peut être égal à zéro* [...] *et que ces nombres vont en diminuant, il est clair qu'on parviendra nécessairement à un de ces nombres qui sera égal à l'unité, et alors on aura A égal à la somme de quatre carrés entiers*" (Lagrange 1772, p. 197).
[*Ne consegue che, se Aa è la somma di quattro quadrati, allora anche Aa' è la somma di quattro quadrati* [...]*; così, se a è maggiore di 1, a' è necessariamente più piccolo di a; se a' è ancora maggiore di 1, si dimostra nello stesso modo che Aa" è somma di quattro quadrati con a" ancora più piccolo di a', e così via. Poiché i numeri a, a', a" sono numeri interi, così nessuno di questi può essere uguale a zero; pertanto i numeri a, a' e a" sono numeri interi diversi da zero* [...] *e questi numeri sono decrescenti. Quindi è chiaro che si otterrà necessariamente che uno di questi numeri sarà uguale a uno e A sarà allora uguale alla somma di quattro quadrati interi*].

2.4 Le differenze finite

Contrariamente a quello che si conosce dei lavori di Fermat, il metodo della discesa infinita permette dunque a Lagrange di dimostrare che il numero A è proprio una somma di quattro quadrati senza utilizzare il ragionamento per assurdo.

Lagrange dimostra il primo passo ottenendo un risultato più generale di quello di Eulero: "*Si A est un nombre premier et que B et C sont des nombres quelconques positifs ou négatifs non divisibles par A, je dis qu'on pourra toujours trouver deux nombres p et q tels que le nombre $p^2 - Bq^2 - C$ soit divisible par A*" (Lagrange 1772, p. 198).
[*Se A è un numero primo e B e C sono numeri arbitrari positivi o negativi non divisibili per A, possiamo sempre trovare due numeri p e q tali che il numero $p^2 - Bq^2 - C$ sia divisibile per A*].

> "Lagrange dimostra inizialmente che ogni numero primo che divide la somma di quattro quadrati, senza dividere ogni quadrato, è necessariamente anche lui la somma di quattro quadrati."

È sufficiente considerare $B = C = -1$ per ottenere un teorema simile a quello dimostrato da Eulero.
Lagrange distingue due casi: in primo luogo, se riusciamo a trovare q tale che $Bq^2 + C$ sia divisibile per A, allora possiamo prendere $p = 0$ oppure p divisibile per A. Poi suppone che non esista alcun q tale che $Bq^2 + C$ sia divisibile per A e pone $Bq^2 + C = b$. A questo punto, introduce le seguenti espressioni dipendenti da b e p:

$$P = p^{A-3} + bp^{A-5} + b^2p^{A-7} + \ldots + b^{\frac{A-3}{2}}$$

e:

$$Q = b^{\frac{A-1}{2}} + 1$$

ottenendo:

$$(p^2 - Bq^2 - C)PQ = Q(p^{A-1} - 1) - (b^{A-1} - 1).$$

Secondo il piccolo teorema di Fermat, i membri di questa uguaglianza sono divisibili per A e quindi la questione si riduce a mostrare che esistono degli interi p e q tali che A non divide né P né Q; in questo caso, i numeri p e q sono tali che A divide $p^2 - Bq^2 - C$. Lagrange si appella allora alla "*nota teoria delle differenze*" [21] (Lagrange 1772, p.199): "*Car si l'on substitue successivement dans l'expression de P les nombres 1, 2, 3,... jusqu'à A – 2 inclusivement à la place de p, et qu'on nomme P', P", P''',..., P^(A-2) les valeurs résultantes de P, on aura, par la théorie connue des différences,*

$$P' - (A-3)P'' + \frac{(A-3)(A-4)}{2}P''' - \ldots + P^{(A-2)} = 1.2.3.4\ldots(A-3).$$

Or, si tous les nombres P', P", P''',... jusqu'à P^(A-2) étaient divisibles par A, il faudrait que le nombre 1·2·3 . . . (A – 3) le fût aussi ; ce qui ne pouvant être à cause que A est premier, il s'ensuit que parmi les nombres P', P",..., P^(A-2) il s'en trouvera nécessairement quelqu'un qui ne sera pas divisible par A; donc, etc".
[*Infatti, se vengono successivamente sostituiti nell'espressione di P, al posto di p, i numeri 1, 2, 3, ... fino ad A-2 compreso e si chiamano P', P", P''', ... , i valori ottenuti da P, si otterrà, grazie alla nota teoria delle differenze che:*

$$P' - (A-3)P'' + \frac{(A-3)(A-4)}{2}P''' - \ldots + P^{(A-2)} = 1.2.3.4\ldots(A-3).$$

Tuttavia, se tutti i numeri P', P", P''', ... fino a P^(A-2) fossero divisibili per A, anche il numero 1·2·3... (A – 3) lo sarebbe stato come avrebbero dovuto essere ma ciò non è possibile perché A è primo. Ne segue che tra i numeri P', P", ... P^(A-2) se ne dovrà necessariamente trovare qualcuno che non sia divisibile per A; pertanto, ecc"].
Vi è quindi un numero intero p tale che P non è divisibile per A. Si fa lo stesso per Q e questo conclude la dimostrazione.

> È innegabile che, presa da sola, è difficile capire come Lagrange abbia costruito la sua *Démonstration d'un théorème d'arithmétique* ottenuta in effetti attraverso lunghi calcoli e a priori poco intuitiva.

3 Verso la dimostrazione del teorema dei quattro quadrati da Lagrange

Nella Memoria intitolata *Novae demonstrationes circa resolutionem numerorum in quadrata*, presentata all'Accademia di San Pietroburgo nel 1772 (ma pubblicata solamente negli *Acta eruditorum* del 1780), Eulero annuncia con gioia di essere finalmente in grado di produrre una dimostrazione completa del teorema dei quattro quadrati, ben diversa da quella di Lagrange e certamente meno laboriosa. Prima di presentare il proprio lavoro, richiama brevemente le fasi della dimostrazione presentata da Lagrange e sottolinea il suo scopo: proporre una nuova dimostrazione che sia più chiara e concisa.
È innegabile che, presa da sola, è difficile capire come Lagrange abbia costruito la sua *Démonstration d'un théorème d'arithmétique* ottenuta in effetti attraverso lunghi calcoli e *a priori* poco intuitiva. Tuttavia è possibile notare dei legami tra alcuni passaggi di questa breve Memoria e una serie di studi precedenti degli stessi Eulero e Lagrange. Alcuni sono appositamente evidenziati da Lagrange, mentre altri sembrano riflettere abituali pratiche matematiche. In questa sezione, ci concentreremo solo su alcune di questi legami.

3.1 Eulero e il teorema dei due quadrati: "*Ho finalmente trovato una dimostrazione definitiva*" [22]

Come abbiamo detto in precedenza, la corrispondenza tra Eulero e Goldbach è una ricca fonte per comprendere l'evoluzione della ricerca di Eulero in Teoria dei numeri. Veniamo così a sapere [23] che Eulero è stato in grado di mostrare nel 1742 che i numeri della forma a^2+b^2, dove a e b sono primi tra loro, non ammettono divisori della forma $4n$-1. Diverse lettere destinate a Goldbach contengono altre riflessioni di Eulero sulle somme di due quadrati. A partire dal 1747, cresce invece il numero dei riferimenti alle somme di tre o quattro quadrati. Nel 1748, Eulero dimostrò l'identità fondamentale prima citata: il prodotto tra due somme di quattro quadrati di numeri interi è una somma di quattro quadrati di numeri interi.
Il 12 aprile 1749, Eulero scrisse a Goldbach per annunciare che aveva ottenuto una dimostrazione del teorema dei due quadrati ed è sempre in questa lettera che gli presenta la dimostrazione di una versione debole del teorema dei quattro quadrati: ogni numero è somma di almeno quattro quadrati di numeri razionali. Nel caso della somma di due quadrati, la successione dei passaggi della dimostrazione adottata da Eulero ricorda quella che verrà utilizzato da La-

grange per la somma di quattro quadrati. Il matematico svizzero dimostra dapprima che il prodotto tra due somme di due quadrati è ancora somma di due quadrati, poi che i divisori delle somme di due quadrati primi tra loro sono a loro volta somme di due quadrati per dedurre, infine, il teorema dei due quadrati: tutti i numeri primi della forma $4n+1$ sono somma di due quadrati.

Si possono notare, anche in questa occasione, due caratteristiche ricorrenti nei lavori aritmetici di Eulero: la ricerca è illustrata a partire da esempi numerici e la prima Memoria di Eulero sul teorema dei due quadrati, presentata il 20 marzo 1749 all'Accademia di Berlino, non contiene altro che un *Tentamen demonstrationis* completato in una seconda Memoria presentata [24] il 15 ottobre 1750. In questi due testi troviamo metodi e strumenti simili a quelli utilizzati da Lagrange: anche Eulero si basa sul metodo della discesa infinita per dimostrare che i divisori delle somme di due quadrati, primi tra loro, sono somme di due quadrati; assume che esista una somma di due quadrati divisibile per un numero p che non è una somma di due quadrati e costruisce una successione decrescente di somme di due quadrati che ammettono un divisore che non è somma di quadrati e questo è impossibile (in quanto porta necessariamente a una somma di due quadrati che è un numero primo o è l'unità).

Per dimostrare il teorema dei due quadrati, Eulero ricorre in seguito al piccolo teorema di Fermat: il numero $4n+1$ divide la differenza $a^{4n}-b^{4n}$ se è primo con a e b e quindi divide uno dei due fattori $a^{2n}-b^{2n}$ e $a^{2n}+b^{2n}$. È dunque sufficiente provare che esistono due numeri a e b, primi con $4n+1$ tali che $4n+1$ non divida la differenza $a^{2n}-b^{2n}$: questo è l'oggetto della seconda Memoria di Eulero basata sul metodo delle differenze finite. Egli considera la successione di numeri $1, 2^{2n}, 3^{2n}, \ldots, (4n)^{2n}$ e suppone che tutte le differenze prime $2^{2n}-1, 3^{2n}-2^{2n}, \ldots, (4n)^{2n}-(4n-1)^{2n}$ siano divisibili per $4n+1$. Le differenze seconde, terze,..., di ordine $2n$ sono quindi divisibili per $4n+1$. Tuttavia, la differenza di ordine $2n$ è pari a $(2n)!$ e non può essere divisibile per $4n+1$ che è un numero primo. Allora, almeno una differenza prima non è divisibile per $4n+1$ e ci sono pertanto due numeri a e b tali che $a^{2n}-b^{2n}$ non è divisibile per $4n+1$.

La dimostrazione del teorema dei due quadrati coinvolge dunque diversi risultati e strumenti che saranno poi ripresi da Lagrange: è il caso per esempio del piccolo teorema di Fermat, del metodo di discesa infinita o delle differenze finite. Tuttavia, questi ultimi due metodi non saranno utilizzati da Lagrange nello stesso modo.

3.2 Una versione debole del teorema dei quattro quadrati di Eulero: l'elaborazione della teoria dei residui

In una Memoria presentata all'Accademia di Berlino nel 1751, Eulero tratta in modo completamente differente le somme di quadrati. Gran parte del testo è dedicata a ciò che Eulero chiama *residui* che sono, in questa Memoria, i resti dei quadrati dopo le divisioni per un numero p, primo o composto [25]. Eulero introduce anche la nozione di *complemento del residuo*, che è la differenza tra il residuo ottenuto e il divisore p, ottenendo numerose proprietà sui residui e i loro complementi. A partire dal teorema 14, Eulero trova il legame tra i residui e le somme di quadrati. Così, basandosi sulle considerazioni sui residui (distingue i casi in cui -1 è o meno un residuo), dimostra che per ogni numero primo p possiamo sempre trovare una somma di tre quadrati (o meno) divisibili per p (che corrisponde alla prima fase della dimostrazione di Lagrange prima ricordata). Deduce quindi la versione debole del teorema dei quattro quadrati attraverso un ragionamento per assurdo.

Nelle dimostrazioni di questi due teoremi, troviamo gli strumenti utilizzati successivamente da Lagrange: il piccolo teorema di Fermat, le differenze finite e in generale lo schema della dimostrazione; le considerazioni sui resti di divisioni euclidee appaiono poi progressivamente, fino allo sviluppo dei risultati sui residui quadratici nel contesto delle somme di quattro quadrati. Il metodo delle differenze finite non appare altrove all'interno della dimostrazione del teorema dei quattro quadrati data da Eulero e questo va nella direzione di quanto Eulero aveva esplicitamente affermato di voler fare in (Eulero 1760): cercare una dimostrazione diretta sulle somme di due quadrati, vale a dire basandosi su strumenti di calcolo ed evitando l'uso di risultati "estranei" alla Teoria dei numeri.

3.3 Lagrange e i problemi indeterminati di secondo grado (1768-1773)

Come abbiamo precisato nell'introduzione, Lagrange ha pubblicato parecchie Memorie sui problemi indeterminati di secondo grado. Il primo lavoro, presentato nel settembre del 1768 presso l'Accademia di Berlino, riguarda le soluzioni intere dell'equazione (detta di Pell-Fermat) $x^2-Ay^2=1$ dove A non è un quadrato. Lagrange fu il primo a dimostrare la sistematica esistenza di una soluzione particolare. In seguito ha proposto, come in precedenza Eulero, un metodo per determinare tutte le soluzioni, che sono infinite, partendo da una soluzione particolare. Tra il 1769 e il 1773, pubblicò altre tre Memorie riguardanti i problemi indeterminati di secondo grado che vedono le frazioni continue al cuore del metodo che Lagrange. ????????

Ci soffermiamo in particolare sulla risoluzione dell'equazione $A=u^2-Bt^2$ in numeri interi, presentata da Lagrange in *Sur la solution des problèmes indéterminés du second degré*. Il metodo risolutivo viene esposto in una cinquantina di pagine. Per collegarci con la sua dimostrazione del teorema dei quattro quadrati, noi ci concentreremo sull'utilizzazione da parte di Lagrange dei metodi della discesa infinita e delle differenze finite.

Lagrange riduce il problema al caso $A=p^2-Bq^2$, dove p e q e A e B sono due coppie di numeri primi tra loro, e dimostra che è necessario determinare dei numeri interi α, A_1, p_1 e q_1 tali che $AA_1=\alpha^2-B$ e $A_1=p_1^2-Bq_1^2$. Questo permette di ottenere la nuova equazione $A_1 = p_1^2 - Bq_1^2$ con $A_1 < A$. L'equazione iniziale è dunque risolvibile con soluzioni intere se l'equazione $A_1 = p_1^2 - Bq_1^2$ ha soluzioni intere e se le espressioni p in funzione di α, p_1, q_1, A e B sono intere. Si ottengono quindi due sistemi di equazioni tali che le A_i e α_i formano una successione decrescente di numeri positivi:

$$\begin{cases} AA_1 = \alpha^2 - B, \quad \alpha < \dfrac{A}{2} \\ A_1A_2 = \alpha_1^2 - B, \quad \alpha_1 = \mu_1 A_1 \pm \alpha < \dfrac{A_1}{2} \\ A_2A_3 = \alpha_2^2 - B, \quad \alpha_2 = \mu_2 A_2 \pm \alpha_1 < \dfrac{A_2}{2} \\ \ldots\ldots\ldots\ldots\ldots, \end{cases}$$

$$\begin{cases} A = p^2 - Bq^2, \\ A_1 = p_1^2 - Bq_1^2, \\ A_2 = p_2^2 - Bq_2^2, \\ A_3 = p_3^2 - Bq_3^2, \\ \ldots\ldots\ldots\ldots\ldots \end{cases}$$

Lagrange dimostra poi che, se un'equazione $A_n = p_n^2 - Bq_n^2$ è risolvibile mediante numeri interi, allora l'equazione originale è risolvibile con numeri interi se e solo se i numeri p_n, q_n, p_{n-1} e q_{n-1} sono interi. È qui che utilizza il metodo della discesa infinita al fine di ottenere, passo dopo passo, un'equazione più semplice da risolvere che gli permetta di dedurre il metodo risolutivo per tutte le equazioni precedentemente ottenute.
Un paragrafo del lavoro è dedicato alla determinazione del numero α tale che $\alpha^2 - B$ sia divisibile per A, quando A è un numero primo. Tutto questo si riduce a determinare se B è un residuo quadratico modulo A. Tuttavia, Lagrange presenta sistematicamente queste questioni in termini di divisibilità. Dimostra anche che $\alpha^2 - B$ è divisibile per A se e solo se anche

$$B^{\frac{A-1}{2}} - 1$$

è divisibile per A. Per questo pone:

$$P = \alpha^{2(m-1)} + \alpha^{2(m-2)}B + \alpha^{2(m-3)}B^2 + \ldots + B^{m-1},$$

dove:

$$m = \tfrac{A-1}{2}$$

e ottiene:

$$(\alpha^2 - B)P = \alpha^{2m} - B^m = \alpha^{A-1} - B^m = \alpha^{A-1} - 1 - (B^m - 1).$$

La somiglianza con le espressioni usate da Lagrange nel caso del teorema dei quattro quadrati è impressionante: applica anche il piccolo teorema di Fermat e le differenze finite per dimostrare che, se $B^m - 1$ è divisibile per A, allora esiste un numero α tale che A divide $\alpha^2 - B$. In effetti, grazie al piccolo teorema di Fermat, $\alpha^{A-1} - 1$ è divisibile per A (se α e A sono primi tra loro) e questo implica che anche $(\alpha^2 - B)P$ sia divisibile per A. Non rimane che dedurre che esiste un numero α tale che P non è divisibile per A: in ultima analisi, Lagrange applica il metodo delle differenze in maniera simile a come farà per il teorema dei quattro quadrati.

3.4 Lagrange, Eulero e il teorema dei quattro quadrati

Quanto considerato finora ci ha consentito di presentare un insieme di metodi e strumenti utilizzati dai due studiosi in molte loro opere, tutti poi sfruttati da Lagrange nella dimostrazione del teorema dei quattro quadrati.
Come precisato in precedenza, la reazione di Eulero alla dimostrazione del teorema dei quattro quadrati da parte di Lagrange non tardò ad arrivare. Mentre tutti si complimentavano con Lagrange per aver ottenuto la dimostrazione completa, Eulero mise in luce la lunghezza e gli aspetti troppo laboriosi e tecnici del testo, proponendo una dimostrazione più breve e semplice.
Il matematico svizzero parte dalle dimostrazioni sulle somme di due quadrati, tutte costruite in base alla stessa traccia, simile a quella utilizzata in precedenti lavori (e ripresa da Lagrange). Fornisce in tal modo un modello unificato di dimostrazione per questi risultati riuscendo a sottolineare la coerenza di questo insieme di risultati aritmetici [26].
Per quanto riguarda la dimostrazione del teorema di quattro quadrati, Eulero riprende la traccia sopra citata. Per ottenere il passo (II) della dimostrazione, si richiama nuovamente al metodo della discesa infinita: per dimostrare che un numero N (che divide una somma di quadrati, ma non è un divisore di ciascun quadrato) è una somma di quattro quadrati, Eulero costruisce una successione decrescente di interi positivi n, n', n''… tali che Nn, Nn', Nn''… siano delle somme di quadrati. È quindi necessario arrivare a ottenere che N·1 sia una somma di quattro quadrati. Eulero riprende dunque il metodo della discesa infinita "alla Lagrange". Tuttavia i calcoli necessari per la sua dimostrazione, attraverso delle sostituzioni algebriche, sono molto più brevi di quelli di Lagrange. Eulero dimostrò in un secondo tempo anche il passo (I) provando che, per ogni numero primo N, esiste un'infinità di somme di tre quadrati divisibili per N. Propose poi una dimostrazione del teorema basata sulla teoria dei residui.
L'analisi mostra le reciproche influenze tra Eulero e Lagrange: i due scienziati si basarono sulla stessa traccia di dimostrazione e sui vari metodi e strumenti che già si trovano nei loro testi (metodo della discesa infinita, metodo delle differenze finite, manipolazioni mediante identità algebriche, piccolo teorema di Fermat, considerazioni sulla divisibilità). Tuttavia, nell'applicazione degli stessi strumenti, si trovano anche delle differenze: è il caso del me-

Il metodo delle differenze finite non appare nella ricerca di Eulero sui quattro quadrati ma impiega una serie di risultati sui residui quadratici che gli permettono di produrre una dimostrazione puramente aritmetica. Lagrange, a sua volta, fornisce delle nuove prove dei risultati precedentemente dimostrati da Eulero a partire dai residui, utilizzando una varietà di strumenti analitici, algebrici e aritmetici.

todo della discesa infinita, il cui uso si sviluppa in maniera diversa nei rispettivi testi; il metodo delle differenze finite viene utilizzato da Eulero nella sua Memoria sul teorema dei due quadrati mentre Lagrange lo sfrutta nelle ricerche sui problemi indeterminati e, partendo da questi, prova il teorema dei quattro quadrati.

Emergono dunque delle pratiche proprie a ciascuno dei due matematici. Nel caso del passo (I) della dimostrazione del teorema dei quattro quadrati, Eulero e Lagrange propongono regolarmente le proprie dimostrazioni costruite su strumenti specifici. Il metodo delle differenze finite non appare nella ricerca di Eulero sui quattro quadrati ma impiega una serie di risultati sui residui quadratici che gli permettono di produrre una dimostrazione puramente aritmetica. Lagrange, a sua volta, fornisce delle nuove prove dei risultati precedentemente dimostrati da Eulero a partire dai residui, utilizzando una varietà di strumenti analitici, algebrici e aritmetici.

4. Lagrange e la teoria dei numeri: una prospettiva

Partendo dal teorema dei quattro quadrati, abbiamo potuto sottolineare diversi aspetti della pratica aritmetica di Lagrange e la circolazione di metodi e strumenti nei differenti testi considerati nella nostra analisi. Gli argomenti presi in considerazione potrebbero essere tuttavia estesi per cogliere anche altri aspetti delle pratiche in uso nella Teoria dei numeri nel seconda metà del Settecento. Considerando altri lavori di Lagrange, rimangono comunque dei punti in comune: ad esempio, nella Memoria sulla risoluzione numerica delle equazioni del 1769, Lagrange ricorre ancora alla teoria delle differenze finite.

In questo articolo ci siamo concentrati esclusivamente sui lavori di Eulero e Lagrange ma, se considerassimo anche l'opera di altri autori e tradizioni, potremmo ottenere valide informazioni sulla progressiva creazione di una autonoma Teoria dei numeri. Non a caso abbiamo citato i lavori di Lambert e i suoi sforzi per rendere popolare la Teoria dei numeri. Bullynck (in Bullynck 2009) mostra come la diffusione dei problemi medievali sui resti abbia portato a diverse tradizioni. Alcuni problemi, di origine cinese e indiana, vengono infatti tramandati nel XV e XVII secolo nei testi di Algebra italiani mentre nei volumi di calcolo francesi e tedeschi risultano molto studiati nel XVII secolo, soprattutto nei libri di Matematica ricreativa. Un esempio significativo è fornito dalla raccolta *Problèmes plaisants et délectables qui se font par les nombres* che Bachet pubblicò per la prima volta nel 1612 e poi riedità nel 1624. Il suo lavoro fu diffuso, nei secoli XVII e XVIII, in Francia e in Inghilterra principalmente attraverso i testi di Algebra. Poi, progressivamente, i riferimenti si ridussero all'*Aritmetica* di Diofanto e alla teoria delle equazioni mentre i problemi sui resti quasi scomparvero. La tradizione diofantea e i problemi sui resti rimasero invece separati nella letteratura matematica tedesca del XVII secolo e per buona parte del XVIII secolo. I problemi dei resti trovarono posto nei manuali di Aritmetica (*Rechenbücher*) e di Matematica ricreativa mentre quelli diofantei e le questioni sulla teoria delle equazioni si fecero sempre più rari trovando spazio solo sulle riviste accademiche. Nella seconda metà del Settecento, la soluzione generale per problemi dei resti (lineari) è inserita solo nei manuali di Eulero e di Abraham Kästner. Secondo la nostra analisi, queste due alternative – incentrate rispettivamente sulle equazioni indeterminate e sui resti – si ritrovano in parte in Lagrange e in Eulero.

Seguendo le loro dimostrazioni del teorema dei quattro quadrati, i due grandi matematici fornirono la dimostrazione del teorema di Wilson finendo nuovamente in competizione tra loro. Lagrange offrì due dimostrazioni basate su diversi strumenti – algebrici e aritmetici (con il piccolo teorema di Fermat) e analitici (tramite le differenze finite) – mentre Eulero propose una dimostrazione basata sulla teoria dei residui. Nei suoi successivi lavori sull'argomento, Lagrange non inserì la teoria dei residui e continuò a sviluppare i metodi non aritmetici. Così, per la risoluzione dell'equazione $z^2 = 2x^4 - y^4$, si basò sui risultati del Calcolo differenziale. Da parte sua, Eulero scrisse altre Memorie sui residui e preparò un progetto di trattato di Teoria dei numeri centrato proprio su questa teoria (Eulero 1849): da strumenti di ricerca, i residui diventarono progressivamente per Eulero un oggetto di studio. La Teoria dei numeri non è limita più all'analisi diofantea, come ancora in Lagrange, e in qualche misura annuncia le *Disquisitiones Arithmeticae* di Gauss [27].

Dopo il 1777 Lagrange non continuò più le ricerche in Teoria dei numeri. La sua posizione ambigua nei confronti di questo settore di ricerca si riflette nella lettera che inviò al giovane Gauss per congratularsi con lui per la pubblicazione delle *Disquisitiones Arithmeticae*: "*Vos Disquisitiones vous ont mis tout de suite au rang des premiers géomètres et je regarde la dernière section comme contenant la plus belle découverte analytique qui ait été faite depuis longtemps. Votre travail sur les planètes aura de plus le mérite de l'importance de son objet*" [28].

Il teorema dei quattro quadrati

[*Le vostre Disquisitiones vi elevano al rango dei migliori geometri e io considero l'ultima sezione come la più bella scoperta analitica che sia stata fatta da molto tempo a questa parte. Il vostro lavoro sui pianeti avrà merito maggiore dell'importanza dell'oggetto*]. Eulero e Lagrange testimoniano in una certa misura quindi due pratiche aritmetiche alternative: Eulero, con una Teoria dei numeri che vuole rendere sempre più autonoma e con prove basate su argomentazioni aritmetiche; Lagrange con un'Aritmetica fondata sulle equazioni indeterminate,

Note

[1] Grazie a questo teorema, tutti i numeri interi si possono scrivere come somma di quattro quadrati. La dimostrazione del teorema viene riportata raramente nella storiografia matematica. La nostra analisi si basa sui lavori di (Buraux-Bourgeois 1990; Buraux-Bourgeois 1993; Boucard 2011). Le ricerche di Eulero su questo argomento sono trattate, per esempio, in (Pieper 1993).

[2] L'affermazione è stata ampiamente dimostrata. I lavori di Teoria dei numeri di Lagrange e Legendre sono presentati come appartenenti a un periodo di transizione in (Weil 1984).

[3] Ci affidiamo in questo caso all'analisi di (Goldstein 1989) e riprendiamo alcuni brani tratti dalla corrispondenza.

[4] Questi nomi non comprendono ovviamente tutti gli amanti dei numeri. Infatti, come ricorda C. Goldstein: "*Questi nomi famosi ci consentono di valutare l'evolversi dei metodi. E se Goldbach richiama in una lettera ad Eulero, ripetutamente, le ipotesi di Fermat, ciò avviene perché nel corso dei secoli XVII e XVIII continuano a sopravvivere amanti dei numeri che trasmettono questo patrimonio e impediscono che si perda completamente nell'oblio*".

[5] Gli scritti di Aritmetica di Eulero occupano però "soltanto" 4 dei 70 tomi che compongono la sua *opera omnia*.

[6] La vita di Lagrange si svolge principalmente in tre città: Torino (1736-1766), Berlino (1766-1787) e Parigi (1787-1813).

[7] Si veda (Bullynck 2010).

[8] Sui problemi indeterminati di secondo grado: [Lagrange1773a, 1769b, 1770, 1773c]; sulle forme quadratiche: [Lagrange1775, 1777]. Per questa panoramica sul lavoro in Teoria dei numeri di Lagrange, ci affidiamo a varie sintesi e analisi delle opere aritmetiche del matematico torinese: (Weil 1984, cap. IV) e (Buraux 1990).

[9] Se n è un intero positivo, non necessariamente un quadrato, l'equazione $nx^2 + 1 = y^2$ ammette sempre delle soluzioni intere.

[10] Questo è particolarmente vero nelle sue *Additions* agli *Éléments d'algèbre* di Eulero, entrate a far parte della traduzione francese del lavoro di Eulero.

[11] Si vedano per esempio (Aubry 1909) e (Weyl 1984).

[12] Si veda (Lagrange1772a).

[13] L'enunciato del teorema di Wilson (come lo si può trovare in Lagrange) afferma che, se n è un numero primo qualunque, il numero $1\cdot2\cdot3\cdot4\cdot5\ldots(n\text{-}1)+1$ è sempre divisibile per n.
Si veda (Lagrange1773b).

[14] Si veda (Lagrange1779).

[15] Fermat si riferisce al risultato, ora noto come ultimo teorema di Fermat, che è annotato in una sua osservazione: "*Non è possibile dividere un cubo in altri due cubi o un biquadrato in altri due biquadrati o, in generale, una potenza superiore al quadrato in due potenze dello stesso grado*". Il teorema è stato dimostrato da Andrew Wiles nel 1994.

[16] Per i riferimenti storici sull'uso di questo metodo, facciamo riferimento a (Goldstein 1993) e (Bussotti 2006).

[17] Si vedano per esempio (Goldstein 1993) e (Goldstein 2004).

[18] Secondo il teorema di due quadrati, tutti i numeri primi della forma $4n+1$ possono essere scritti come somma di due quadrati.

[19] Eulero dimostra in (Eulero 1738) che il quinto numero di Fermat, $2^{32}+1$, è scomponibile e dunque la congettura è falsa.

[20] Si veda (Euler1760).

[21] Le questioni relative alle somme di quattro quadrati furono di grande attualità fino al XIX secolo. Per una panoramica sui principali contributi su questo tema, si veda (Dickson 1919, t. II, cap. VIII).

[22] Si scambiarono almeno cinque lettere dal dicembre 1769 al dicembre 1770.

[23] Supponiamo che esistano dei numeri primi che non si possono scrivere come somma di quattro quadrati: sia p il più piccolo di questi numeri. Allora esistono dei numeri interi a, b e c tali che $a^2+b^2+c^2=np$ dove $np < p$. Dunque, i fattori primi di n sono più piccoli di p e scomponibili come somme di quattro quadrati; n, e quindi p, è somma di quattro quadrati, il che contraddice l'ipotesi di partenza.

[24] La teoria delle differenze finite, già conosciuta da Leibniz, viene esposta da Eulero nel primo volume delle sue *Institutiones calculi differentialis cum eius usu in analysi finitorum ac doctrina serierum* (1755). Egli considera una funzione f, un incremento fisso ω e lavora sulla successione $x, x+\omega, x+2\omega,\ldots$ e $f(x), f(x+\omega), f(x+2\omega),\ldots$(usando la notazione $y, y^{I}, y^{II}, \ldots$). Definisce allora la successione di differenze prime: $\Delta f(x) = f(x+\omega) - f(x)$, $\Delta f(x+\omega)= f(x+2\omega) - f(x+\omega)$ e così via. Poi considera le differenze seconde $\Delta^2 f(x)= \Delta f(x+\omega) - \Delta f(x)$, $\Delta^2 f(x+\omega) = \Delta f(x+2\omega) - \Delta f(x+\omega)$ e mostra che:

$$\Delta^n f(x) = \sum_{j=0}^{n}(-1)^{n-j}\binom{n}{j}f(x+j\omega).$$

Prosegue quindi calcolando le differenze per alcune funzioni semplici. Per $f(x)=x^n$: $\Delta f(x) = (x+\omega)^n - x^n$ è un polinomio di grado $n-1$ avente come termine di grado massimo $\omega n x^{n-1}$; $\Delta^2 f(x)$ è un polinomio di grado $n-2$ avente come termine di grado massimo $\omega^2 n(n-1)x^{n-2}$; …; $\Delta^n f(x)$ è un polinomio costante uguale a $\omega^n n(n-1)(n-2)\ldots2\cdot1$. Le differenze di ordine superiore a n sono nulle.

[25] La citazione è tratta da una lettera che Eulero scrisse a Goldbach il 12 aprile 1749: "*Nunmehr habe ich einen endlich bündigen Beweis gefunden*".

[26] Ci affidiamo qui all'analisi di (Weil 1984, pp. 177-179).

[27] Si noti che questi lavori sono stati pubblicati rispettivamente nel 1758 e 1760 dando l'idea dei lunghi tempi che intercorrevano in quel periodo fra l'annuncio di un risultato e la relativa pubblicazione.

[28] In altre Memorie, Eulero usa il termine *residua* per designare per esempio i resti delle potenze successive dello stesso numero.

[29] Prima di esaminare il teorema dei quattro quadrati, Eulero aveva ottenuto dei risultati sulla somma dei quadrati della forma $x^2 + y^2$, $x^2 + 2y^2$, e $x^2 + 3y^2$.

[30] Tuttavia, Eulero pubblica un'altra Memoria di Aritmetica, non incentrata su residui, che coinvolge vari metodi.

[31] L'ultima sezione del libro Gauss si occupa della risoluzione delle equazioni binomie, che è quindi una questione algebrica.

[32] Ci riferiamo a (Boucard 2011).

trascurando l'uso dei residui. Al contrario, Eulero sottolinea l'interesse per il loro uso e studio, perché permettono di sviluppare i problemi legati alla divisibilità, e apre la strada a nuovi metodi e concetti nella Teoria della numeri. Lagrange riuscì a dimostrare gli stessi risultati senza ricorrere ai residui, sviluppando al contempo altre direzioni di ricerca. Sono indicazioni diverse che ritroviamo nei successivi lavori di Legendre e Gauss [29] e che risultano essenziali per capire i lavori aritmetici dei matematici francesi del primo Ottocento. ■

Bibliografia

Andoyer H. e Pierre H., "Les mathématiques pures de Descartes à Cauchy" in *Histoire de la nation française* (ed. Gabriel Hanotaux), T. XIV, Paris, Plon, 1924, pp. 23-80.

Aubry A., "Sur les travaux arithmétiques de Lagrange, de Legendre et de Gauss" in *L'enseignement mathématique* 11(1909), pp. 430-450.

Boucard J., "Un "rapprochement curieux de l'algèbre et de la théorie des nombres": études sur l'utilisation des congruences de 1801 à 1850", tesi di dottorato, Paris, Université Paris 6, 2011.

Bullynck M., "Modular Arithmetic before C.F. Gauss: Systematizations and Discussions on Remainder Problems in 18th-Century Germany" in *Historia Mathematica* 36 (2009), pp. 48-72.

Bullynck M., "A History of Factor Tables with Notes on the Birth of Number theory 1668-1817" in *Revue d'histoire des mathématiques* 16.2 (2010), pp. 133-216.

Buraux-Bourgeois B., "La théorie des nombres dans l'oeuvre de Lagrange", tesi di dottorato, Paris, Université de Paris-Nord, 1990.

Buraux-Bourgeois B., "L'analyse diophantienne chez Lagrange" in *Cahier du séminaire d'histoire des mathématiques* 3 (1993), pp. 13-23.

Bussotti P., *From Fermat to Gauss: Indefinite Descent and Methods of Reduction in Number Theory*, Augsburg, Erwin Rauner Verlag, 2006.

Dahan Dalmedico A., "La méthode critique du «mathématicien-philosophe»" in *L'École normale de l'an III. Leçons de mathématiques. Édition annotée des cours de Laplace, Lagrange et Monge avec introductions et annexes* (Bruno Belhoste et al. ed.) Paris, Dunod, 1992, pp. 170-192.

Dickson L.E., *History of the Theory of Numbers,* 1919. Ristampato Mineola: Dover Publications, Washington, Carnegie Institute of Washington, 2005.

Euler L., "Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus" in *Commentarii academiae scientiarum Petropolitanae* 6 (1738), pp. 103-107.

Euler L., "Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum" in *Novi Commentarii academiae scientiarum Petropolitanae* 5 (1760), pp. 13-58.

Goldstein C., "Le métier des nombres aux XVIIe et XIXe siècles" in *Éléments d'histoire des sciences* (Michel Serres ed.), Paris, Bordas, 1989, pp. 274-295.

Goldstein C., "Descente infinie et analyse diophantienne : programmes de travail et mises en oeuvre chez Fermat, Levi, Mordell et Weil" in *Cahiers du séminaire d'histoire des mathématiques*. 2e sér. 3 (1993), pp. 25-49. Disponibile on-line: *https://eudml.org/doc/91037*.

Goldstein C., "L'arithmétique de Pierre Fermat dans le contexte de la correspondance de Mersenne: une approche microsociale" in *Sciences et techniques en perspective* II 8.1 (2004), pp. 14-47.

Lagrange J.-L., "Solution d'un problème d'arithmétique" in *Miscellanea Taurinensia*, t. 4, *pour 1766-1769* (1773). Ristampato in *Œuvres de Lagrange* (J.-A. Serret ed.), t. 1, Paris, Gauthier-Villars, 1867, pp. 671-731.

Lagrange J.-L., "Sur la résolution des équations numériques" in *Mémoires de l'Académie royale des Sciences et Belles-lettres de Berlin, Année 1767* (1769). Ristampato in *Œuvres de Lagrange* (J.-A. Serret ed.), t. 2, Paris, Gauthier-Villars, 1868, pp. 539-578.

Lagrange J.-L., "Sur la solution des problèmes indéterminés du second degré" in *Mémoires de l'Académie royale des Sciences et Belles-lettres de Berlin, Année 1767* (1769). Ristampato in *Œuvres de Lagrange* (J.-A. Serret ed.), t. 2, Paris, Gauthier-Villars, 1868, pp. 377-535.

Lagrange J.-L., "Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers" in *Mémoires de l'Académie royale des Sciences et Belles-lettres de Berlin, Année 1768* (1770). Ristampato in *Œuvres de Lagrange* (J.-A. Serret ed.), t. 2, Paris, Gauthier-Villars, 1868, pp. 655-726.

Lagrange J.-L., "Démonstration d'un théorème d'arithmétique" in *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, Année 1770* (1772). Ristampato in *OEuvres de Lagrange* (J.-A. Serret ed.), t. 3, Paris, Gauthier-Villars, 1869, pp. 189-201.

Lagrange J.-L., "Démonstration d'un théorème nouveau concernant les nombres premiers" in *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, Année 1771*. Ristampato in *OEuvres de Lagrange* (J.-A. Serret ed.), t. 3, Paris, Gauthier-Villars, 1869, pp. 425-438.

Lagrange J.-L., "Additions. de l'analyse indéterminée" in *Élémens d'Algèbre d'Euler, traduits de l'allemand, avec des notes et des additions*, v. 2, Paris-Lyon, 1773. Ristampato in *OEuvres de Lagrange* (J.-A. Serret ed.), t. 7, Paris, Gauthier-Villars, 1869, pp. 5-180.

Lagrange J.-L., "Recherches d'arithmétique" in *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, Année 1773* (1775). Ristampato in *OEuvres de Lagrange* (J.-A. Serret ed.), t. 3, Paris, Gauthier-Villars, 1869, pp. 695-758.

Lagrange J.-L., "Suite des recherches d'arithmétique imprimées dans le volume de l'année 1773" in *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, Année 1775* (1777). Ristampato in *OEuvres de Lagrange* (J.-A. Serret ed.), t. 3, Paris, Gauthier-Villars, 1869, pp. 759-795.

Lagrange J.-L., "Sur quelques problèmes de l'analyse de Diophante " in *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, Année 1777* (1779). Ristampato in *OEuvres de Lagrange* (J.-A. Serret ed.), t. 4, Paris, Gauthier-Villars, 1869, pp. 377-398.

Pieper H., "On Euler's Contributions to the Four-Squares Theorem" in *Historia Mathematica* 20 (1993), pp. 12-18.

Scharlau W. e Opolka H., *From Fermat to Minkowski: lectures on the theory of numbers and its historical development*, New York, Springer, 1985.

Weil A., *Number Theory: An Approach through History from Hammurabi to Legendre*, Boston, Birkhäuser, 1984.