UNIVERSITÀ DEGLI STUDI DI BOLOGNA
Dipartimento di Matematica

Corso di Laurea in Matematica indirizzo Didattico

Il carteggio fra Sophie Germain e Carl Friedrich Gauss

Candidato: Cecilia Rossi

Relatore: Prof. Sandro Graffi

Anno Accademico 2016/2017

Indice

"*Non sono mai riuscita a giungere all'infinito, anche se ho spinto i limiti piuttosto in là...*"

Introduzione

* Quando nel 1889 fu inaugurata la Tour Eiffel, tra i nomi di tutti coloro che, con i loro studi sull'elasticità, avevano consentito la realizzazione dell'opera e che erano stati riportati sulla nuova costruzione, uno mancava. Quello di Sophie Germain. Trattandosi di una donna la cosa non stupisce, sebbene le fosse stato assegnato un premio di 3000 franchi, bandito da Napoleone, per la sua tesi *Recherches sur la théorie des surfaces élastiques* (1821), riguardante studi sull'elasticità. Premio che non andò a ritirare a causa di un comportamento ostile da parte di alcuni membri della commissione, fra cui Poisson.
Ma Sophie non si occupò solo di studiare le membrane elastiche, nonostante per molto tempo si sia creduto il contrario; uno dei suoi principali campi di ricerca e studio fu la teoria dei numeri. Studi recenti hanno portato alla luce la sua corrispondenza con Carl Friedrich Gauss, iniziata nel 1804, sospesa per un lungo periodo a causa degli impegni di quest'ultimo, nominato direttore dell'osservatorio astronomico di Gottinga, e ripresa nel 1819, in concomitanza dell'organizzazione da parte dell'Accademia di Parigi di un concorso volto a provare l'Ultimo Teorema di Fermat. Nel 1831, su proposta di Gauss, l'Università di Gottinga decise di conferirle il titolo di dottore onorario, ma Sophie, dopo due anni di malattia, colpita da un cancro alla mammella, si spense il 27 giugno 1831, prima che le potesse essere consegnata l'onorificenza. Sul certificato rilasciato alla sua morte figura come "redditiera" e non, più correttamente, come "matematica".
La tesi sarà strutturata in tre capitoli. Il primo tratterà della vita di Sophie Germain, delle sue amicizie, dei principali campi di interesse e dei progetti editoriali che si sono susseguiti al fine di portare alla luce la completa corrispondenza fra lei e Gauss, mentre il secondo ed il terzo saranno incentrati sulla corrispondenza sopracitata analizzando due lettere ed alcuni manoscritti, quelli ritenuti più significativi nel campo della Teoria dei Numeri.

*Per l'Introduzione seguiamo i testi [8] [15] [16]

Capitolo 1

Sophie Germain

1.1 Un inizio difficile

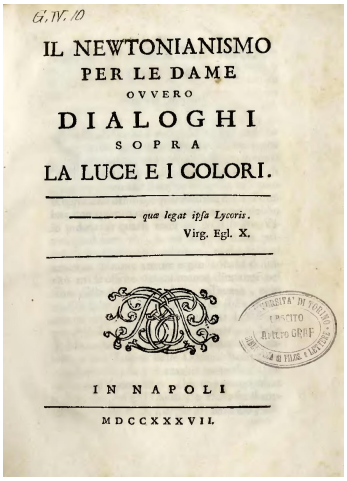
Sophie GERMAIN (portrait dit), à l'âge de 51 ans.

*Marie-Sophie Germain nacque a Parigi il 1 aprile 1776, poco prima della Rivoluzione Francese, secondogenita di Ambroise-Francois e Marie-Madeleine Gruguelu. La famiglia di Sophie apparteneva alla borghesia liberale e colta, il padre era un ricco mercante di seta che fu eletto come deputato dell'Assemblea Nazionale nel 1789 e, tre anni dopo, divenne membro dell'Assemblea Costituzionale.
I Germain, sebbene non aristocratici, erano mercanti da generazioni e disponevano di notevoli mezzi finanziari. C'è da meravigliarsi poiché era un azzardo per una giovane dell'estrazione sociale di Sophie provare un qualche interesse per la matematica (che andasse oltre quello puramente necessario

*Per il primo capitolo seguiamo i testi [1] [2] [3] [7] [15]

ai fini della conversazione nei salotti mondani). Un'opera di quell'epoca era *Newtonianismo per le dame* (1737), di Francesco Algarotti, impostata come dialogo fra una marchesa e un suo interlocutore, all'interno della quale si trovano paragoni azzardati fra la Legge di Gravitazione Universale e rapporti amorosi (Algarotti 1737, pp. 250):

> *"Non posso fare a meno di pensare che questa proporzionalità si osservi anche nell'amore: quindi dopo otto giorni di assenza l'amore diventa sessantaquattro volte più debole del primo giorno."*


G. IV. 10

IL NEWTONIANISMO
PER LE DAME
OVVERO
DIALOGHI
SOPRA
LA LUCE E I COLORI.

——— *quæ legat ipsa Lycoris.*
Virg. Egl. X.

IN NAPOLI
MDCCXXXVII.

Figura 1.1: Copertina di "Newtonianismo per le Dame"

Durante gli anni della Rivoluzione Sophie era una ragazzina e, costretta a rimanere in casa quando il periodo del Terrore iniziò nel 1793, trovò un diversivo nella lettura. Nella rifornita biblioteca paterna trovò *Histoire des Mathematiques* (1758) di Jean Etienne Montucla e lo lesse con grande interesse. In particolare, rimasta affascinata dal racconto della morte di Archimede, ucciso da un soldato romano poichè troppo assorto in una dimostrazione per prestargli ascolto. Decise così di dedicarsi completamente allo studio della matematica.
Studiò con grande passione e una volontà ferrea, in forte opposizione ai suoi genitori che trovavano questo desiderio estraneo al genere femminile ed alla classe sociale alla quale appartenevano. Il matematico italiano conte Guglielmo Libri, con cui Sophie ebbe una lunga e frequente corrispondenza, scrive che i genitori, per impedirle di dedicarsi pienamente a questa sua "malsana" passione, le togliessero al calar della sera tutte le candele ed i vestiti dalla

camera, ma di come ella riuscisse comunque a studiare coperta da un lenzuolo striminzito e usando solo qualche moccolo. La perseveranza di Sophie la portò a vincere infine le resistenze dei suoi che, sebbene non comprendessero né lei né la materia, non la ostacolarono più e, anzi, la sostennero per tutto il resto della sua vita.

1.2 Auguste Le Blanc

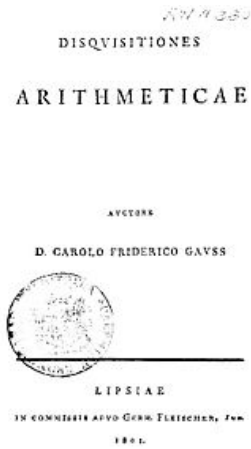
Sophie iniziò ad apprendere le prime nozioni di Matematica studiando *Cours des mathémati-ques* (1798) di Etienne Bézout e, successivamente, *Calcul differentiel et calcul integral* (1777) di Joseph Cousin. Imparò anche il Latino da autodidatta in modo da leggere autonomamente le opere di Isaac Newton e Leonhard Euler. Purtroppo per Sophie i tempi in cui visse erano tutto fuorché felici per una signorina dedita a studi matematici; così la sua preparazione fu frammentaria e disorganizzata. Non solo gli istitutori trovavano stravagante che si dedicasse con tanta frenesia ad una disciplina quale la matematica, ma era oltremodo difficile, se non addirittura impossibile, trovare insegnanti per signorine a livello di Sophie. Forse fu proprio questo uno dei motivi che la spinsero a voler frequentare le lezioni dell'École Centrale des Travaux Publiques (piu tardi confluita École Polytechnique), che aveva aperto i battenti nel 1794. Ovviamente l'accesso all'istituto, e di conseguenza la frequentazione delle lezioni, era aperto solo agli uomini perciò Sophie dovette inventarsi uno stratagemma: prese l'identità di Antoine-Auguste Le Blanc, uno studente iscritto all'École che successivamente aveva abbandonato gli studi per dedicarsi ad altro. Riuscì così a farsi dare gli appunti delle lezioni di chimica, tenute da Antoine-Francois de Fourcroy, e a consegnare le esercitazioni di analisi lasciate per casa da, nientedimeno, Joseph-Louis Lagrange.
Gli studenti erano invitati a presentare ai professori osservazioni scritte riguardo gli argomenti del corso e Lagrange si meravigliò del fatto che uno studente, che non aveva mai mostrato alcuna attitudine per la materia, fornisse delle risposte così acute e fuori dal comune e gli chiese di poterlo incontrare. Sophie fu così costretta a smettere i panni di Leblanc e, contrariamente a quanto si sarebbe aspettata, fu accolta da un Lagrange, meravigliato e ammirato, che si complimentò per il suo talento e la invitò a proseguire gli studi. La presenza di una giovane donna di talento nel campo della Matematica era fonte di grande curiosità fra gli uomini di scienza. Molti erano bendisposti nel mettere la loro conoscenza al servizio di Mademoiselle Germain ma, nondimeno, non tutti gli incontri erano piacevoli ed incoraggianti. Talvolta si sentiva intellettualmente sminuita; fu questo il caso dell'astronomo Joseph Lalande che le propose di leggere la sua opera *Astronomie des dames* (1785)

Figura 1.2: Sede dell'École Polytechnique dal 1794 al 1972

e a cui Sophie, irritata, rispose che aveva già letto *Système du monde* (1796) di Pierre Simon Laplace.
Sophie Germain divenne nota nei circoli intellettuali parigini come una sorta di prodigio del quale essere meravigliati, piuttosto che come una studentessa alla quale insegnare. Ciò di cui aveva realmente bisogno, e a cui aspirava, era una vera e propria istruzione formale ma, a quei tempi, ottenere una formazione completa era possibile solo alle persone di sesso maschile. Questo non solo le impedì la carriera scientifica, ma influenzò fortemente la sua personalità.

1.3 Gauss

Nel 1798 Adrien-Marie Legendre pubblicò *Essai sur la théorie des nombres* e Sophie iniziò a dedicarsi alla teoria dei numeri con grande fervore; non è noto come sia venuta a conoscenza dell'opera *Disquisitiones Arithmeticae* di Johann Carl Friedrich Gauss che fu pubblicata nel 1801, ma sicuramente rimase affascinata dall'originalità di questo lavoro.
Nelle *Disquisitiones* trovò un nuovo stimolo nella direzione della teoria dei numeri. Per un paio di anni studiò il trattato di Gauss, risolvendo molti esercizi e cercando di fornire dimostrazioni personali ai teoremi contenuti al suo interno. In cerca di riconoscimenti ed incoraggiamenti Sophie, il 21 novembre 1804, scrisse la prima lettera a Gauss, sempre sotto lo pseudonimo di Monsieur LeBlanc, per evitare (Dahan 1992, pp.73):


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

Figura 1.3: Copertina di *Disquisitiones Arithmeticae*

> *"Il ridicolo inevitabilmente associato alla condizione di donna studiosa."*

Dopo aver tessuto le lodi delle *Disquisitiones*, che a lungo erano stato l'oggetto della sua ammirazione e del suo studio, Sophie Germain condivise alcune delle sue idee e dei suoi risultati (Dahan 1992, pp.73):

> *"Sfortunatamente, la profondità del mio intelletto non uguaglia la voracità del mio appetito, e mi sento un po' temerario a disturbare un uomo di genio quando non ho altri titoli per pretendere la Sua attenzione..."*

e Gauss, dopo un intervallo di sette mesi, rispose (Dahan 1992, pp. 73) :

> *"Mi compiaccio profondamente che l'aritmetica abbia trovato in voi un cultore così abile. La vostra nuova dimostrazione... è molto bella, sebbene sembri applicarsi a un caso isolato."*

Di fatto Gauss aveva già scritto precedentemente al suo amico H.W. Olbers il 7 Dicembre 1804 dicendo (Schilling 1990, pp.237) :

> *"Ho ricevuto con piacere una lettera da un giovane geometra di Parigi, Le Blanc, che ha studiato l'algebra superiore con grande entusiasmo e mi ha fornito prova di esser penetrato nei meandri più profondi delle mie Disquisitiones Arithmeticae."*

Sophie Germain, sotto lo pseudonimo di Le Blanc, scrisse tre lettere a Gauss, e Gauss annoverò Le Blanc fra i suoi corrispondenti. Nonostante i complimenti di Gauss fossero sinceri, come è chiaramente dimostrato da alcune lettere

che scrisse a Olbers, e a dispetto della sollecitudine di Sophie, raramente commentò il suo lavoro.
Nel febbraio del 1807, come conseguenza della guerra Franco-Prussiana, Napoleone aveva inviato parte delle sue truppe in Prussia, dove viveva Gauss, e Sophie fece ricorso ad uno dei suoi amici: il generale Joseph-Marie Pernety, affinchè gli fosse garantita sicurezza. Pernety le mandò un messaggio per informarla del fatto che Gauss stesse bene ma che non conosceva alcuna Sophie Germain e fu così che, nella sua lettera successiva, si vide costretta a rivelare la sua identità. Sempre contrariamente a quanto si aspettasse, Gauss ne rimase sorpreso e ammirato e non tardò a scriverle che (Viola 2015, pp.58):

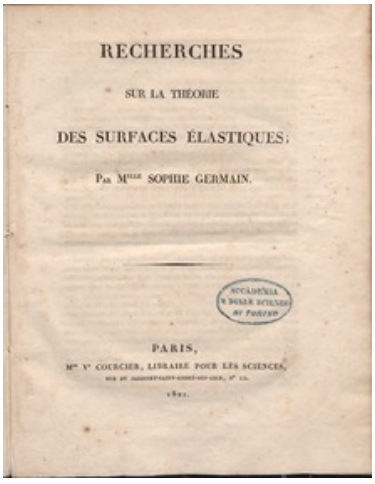
> *"Una donna, a causa del suo sesso e dei nostri pregiudizi, incontra molti più ostacoli di un uomo nel familiarizzarsi con problemi complessi. Tuttavia, quando supera queste barriere e penetra nelle profondità più recondite, rivela di possedere il coraggio più nobile, un talento straordinario e un genio superiore."*

.

1.4 Recherches sur la théorie des surfaces élastiques

Poco dopo l'invasione napoleonica Gauss fu nominato direttore dell'osservatorio astronomico di Gottinga e, dovendosi occupare di altro, interruppe la corrispondenza con Sophie. Le scrisse la sua ultima lettera nel gennaio 1808. In essa Gauss sembra dire che non avrà più tempo per continuare la corrispondenza. Sophie Germain gli scrisse altre tre lettere, alle quali, probabilmente, Gauss non rispose mai. Smise definitivamente di scrivergli nel 1809.
Priva del supporto matematico di Gauss, Sophie abbandonò la teoria dei numeri per dedicarsi ad altro. Nel 1808, dopo una serie di spettacolari esperimenti sull'intricato pattern vibrazionale di sottili lastre, eseguiti a Parigi dal fisico tedesco E.F. Chladni, l'Accademia delle Scienze di Parigi annunciò una competizione per la migliore tesi, supportata da prove sperimentali, sulla teoria matematica alla base dell'elasticità delle membrane. Sophie, messa da parte la sua amata teoria dei numeri, iniziò a studiare intensamente questo problema. Nel 1811, assistita da Legendre, presentò, come unica competitrice, il suo primo contributo all'Accademia. Purtroppo, la tesi da lei presentata, basata su una generalizzazione della teoria di Leonhard Euler sulle travi vibranti, era affetta da un errore significativo. Ad ogni modo la competizione

fu estesa per altri due anni e Sophie, aiutata dai due suoi mentori Lagrange e Legendre, inviò nel 1813 una versione rivista e corretta della sua prima tesi, ancora come unica competitrice. Questa volta, nonostante il modo in cui era giunta all'equazione fondamentale della tesi fosse ancora giudicato complessivamente sbagliato, le fu conferita una menzione d'onore per la parte riguardante il confronto fra la teoria ed i dati sperimentali.
La competizione fu estesa ulteriormente al 15 ottobre 1815. La terza memoria di Sophie, presentata ancora una volta come unica competitrice, differiva sotto molti aspetti dalle precedenti due. Uno di questi era l'aver cercato di estendere la sua teoria alle superfici curve, ma il suo lavoro, nonostante fosse interessante nell'intento, era ancora lacunoso. Ciononostante, la commissione, costituita da Poisson, Laplace, Legendre, Poinsot e Biot, decise di conferirle un premio con riserva. Nella motivazione, i membri del consiglio affermarono che l'equazione fondamentale della tesi (corretta), sebbene non fosse chiaramente dedotta dalle ipotesi, ma dal confronto fatto con i risultati osservati da Chaldni e con i nuovi esperimenti portati avanti al fine di verificare la teoria, era meritevole di vincere il premio.
Nel 1821 Sophie pubblicò a sue spese la memoria. Tuttavia non andò a ritirare il riconoscimento poichè in disaccordo con i comportamenti ostili di alcuni membri della commissione, fra cui Poisson.


RECHERCHES

SUR LA THÉORIE

DES SURFACES ÉLASTIQUES;

PAR Mlle SOPHIE GERMAIN.

PARIS,

Mme Ve COURCIER, LIBRAIRE POUR LES SCIENCES,

1821.

Figura 1.4: Copertina di *Recherches sur la théorie des surfaces élastiques*

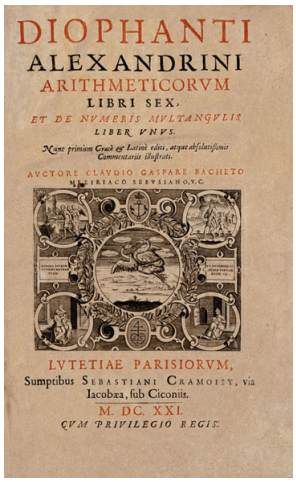


Figura 1.5: Copertina dell'Arithmetica di Diofanto

1.5 L'ultimo teorema di Fermat

Verso la fine del dicembre 1815, l'Accademia di Parigi aveva organizzato un nuovo concorso volto a provare l'Ultimo Teorema di Fermat.

$$x^n + y^n \neq z^n [n > 2, n \in \mathbb{N}]$$

> *"Dispongo di una meravigliosa dimostrazione di questo teorema, che non può essere contenuta nel margine troppo stretto della pagina".*

Con questa frase, lasciata a margine di una copia dell' *Arithmetica* (III, IV d.C.) di Diofanto, Pierre de Fermat lanciò nel 1637 quella che si rivelò la sfida matematica per eccellenza dei successivi tre secoli, trascorsi i quali riuscì a passare da semplice congettura a quello di teorema grazie alla dimostrazione del 1994 di Andrew Wiles. Mentre studiava il libro II dell'*Arithmetica*, probabilmente un'edizione latina del 1621 di Claude-Gaspard Bachet de Méziriac, Fermat fu colpito dalla varietà e dall'enorme quantità di terne pitagoriche e, dopo averne studiato la dettagliata esposizione, creò una equazione che, sebbene simile a quella di Pitagora, non aveva alcuna soluzione. Dal 1637 si erano succeduti vari tentativi di dimostrare che non potevano esistere x, y, z tali che $x^n + y^n = z^n$ per $n \leq 3$: Fermat aveva provato la congettura per n=4, Eulero per n=3 e Legendre per n=5.
La competizione dell'Accademia di Parigi fu estesa all'anno 1818 e infine ritirata nel 1820. Probabilmente, solo dopo la seconda chiamata Sophie Germain ritornò con forza a lavorare a questa sfida, sulla quale aveva già iniziato ad

interrogarsi nel 1804, anno della sua prima lettera a Gauss.
Non solo era convinta che la teoria delle congruenze e dei residui, sviluppata da Gauss nelle *Disquisitiones*, fosse lo strumento adatto per risolvere quell'antico problema, ma, nel 1818, la tesi di Louis Poinsot [†], *Sur l'application de l'algèbre à la théorie des nombres*, le diede un forte incoraggiamento nel proseguire in quella direzione. Nel maggio 1819, la visita di H.C. Schumacher, un amico di Gauss, le fornì il pretesto per scrivergli nuovamente. Il 12 maggio 1819 Sophie Germain scrisse una lettera, dalla sua casa parigina, a Gauss, che si trovava a Gottinga. Buona parte della lunga epistola è dedicata alla descrizione del suo lavoro sull'ultimo Teorema di Fermat e fornisce una finestra sulla loro interazione riguardo la teoria dei numeri, quindici anni dopo l'inizio della loro corrispondenza. Sophie, nella sua lettera, descrive inizialmente l'estensione di tanti anni di lavoro e, prosegue, entrando nei dettagli del suo progetto per provare l'ultimo Teorema di Fermat (Laubenbacher Pengelley (2010) pp.20):

> *"[...] Nonostante abbia lavorato per qualche tempo alla teoria delle superfici vibranti [...], Non ho mai smesso di pensare alla teoria dei numeri. Vi darò un'idea di quanto sono assorta in questa area di ricerca ammettendo che, anche senza speranza di successo, preferisco ancora concentrarmi su questo, rispetto ad altri lavori che mi potrebbero interessare, e, lavorando ai quali, potrei ottenere risultati sicuri.*
> *Prima che la nostra Accademia proponesse un premio per una dimostrazione dell'impossibilità dell'equazione di Fermat, questo tipo di sfida, che fu portata alle moderne teorie da un geometra che non possedeva le risorse che abbiamo noi oggi, mi tormentava spesso. Scorsi una vaga connessione fra la teoria dei residui e la famosa equazione; penso di avervene parlato molto tempo fa, perchè mi colpì appena lessi il vostro libro."*

Sophie continua la lettera spiegando a Gauss il suo sforzo nel provare l'Ultimo Teorema di Fermat, includendo il piano generale e un riassunto dei risultati ottenuti. Gli introduce il suo lavoro con le parole "Voici ce que j'ai trouvé:" (Laubenbacher Pengelley (2010) pp.22):

> *"Ecco cosa ho trovato: [...].*
> *L'ordine nel quale i residui (le potenze uguali agli esponenti) sono*

[†]Louis Poinsot (1777-1859) matematico e fisico francese, noto per i suoi studi di Meccanica Razionale e Geometria solida, gli fu conferita la Legione d'onore nel 1846 e fu eletto membro della Royal Society nel 1858.

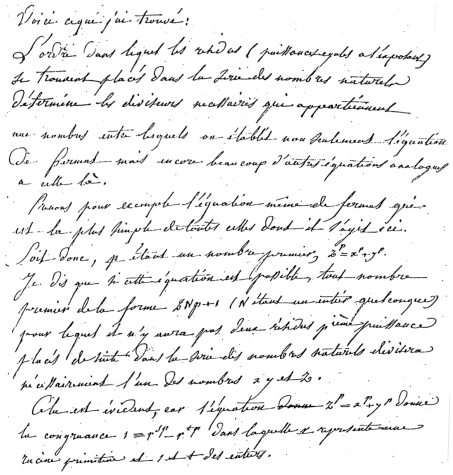


Figura 1.6: Estratto dalla lettera di Sophie Germain a Gauss del 1819

distribuiti nella sequenza dei numeri naturali, determina i divisori necessari che appartengono ai numeri fra i quali uno stabilisce, non solo l'equazione di Fermat, ma molte altre equazioni analoghe.
Prendiamo ora l'equazione di Fermat che è la più semplice di quelle che consideriamo qui. Abbiamo quindi $z^p = x^p + y^p$, *p numero primo. Sostengo che, se questa equazione è possibile, allora ogni numero primo della forma* $2Np + 1$ *(N intero), per il quale non ci sono due potenze residue p-esime nella sequenza dei numeri naturali, necessariamente divide uno dei numeri x, y, z.*
Questo è chiaro dal momento che l'equazione $z^p = x^p + y^p$ *soddisfa la congruenza* $1 \equiv r^{sp} - r^{tp}$ *dove r rappresenta una radice primitiva e s e t sono interi.[...]*
Segue che, se ci fossero infiniti numeri di questo tipo, l'equazione sarebbe impossibile.
Non sono mai riuscita a giungere all'infinito, anche se ho spinto i limiti piuttosto in là, mediante un metodo di prove troppo lungo per essere qui descritto. Ancora non mi azzardo ad asserire che, per ogni valore di p, non ci sia un limite oltre il quale tutti i numeri della forma $2Np + 1$ *abbiano due potenze redisue p-esime consecutive nella sequenza dei numeri naturali. Questo è il caso che concerne l'equazione di Fermat.*
Potete facilmente immaginare, Monsieur, che sono riuscita a dimostrare che questa equazione non sia possibile, fatta eccezione per i numeri la cui dimensione fa impallidire l'immaginazione;

> *perchè essa è anche soggetta a molte altre condizioni, che non ho il tempo di elencare a causa di tutti i dettagli necessari per stabilirne il successo. Ma tutto ciò non è sufficiente; abbiamo bisogno dell'infinito, non basta semplicemente il "molto grande"."*

Molte cose sono da sottolineare qui. Sorprendentemente, Sophie non accenna affatto all'unico risultato che le è stato accreditato in letteratura, quello che chiamiamo il Teorema di Sophie Germain [‡], bensì spiega un piano, semplice nella sua formulazione, per provare l'Ultimo teorema di Fermat. Questo piano richiede che, per un dato esponente primo p, uno stabilisca infiniti numeri primi, ognuno dei quali soddisfacente una condizione di non consecutività e, spiega a Gauss che, dal momento che ogni primo dovrà dividere uno fra x, y e z, l'esistenza di infiniti numeri primi di questo tipo renderà l'equazione di Fermat impossibile. Sophie scrive che ha lavorato a lungo e duramente a questo piano per sviluppare un metodo che verifichi le condizioni, facendo grandi progressi, ma non è stata in grado di portarlo a pieno compimento verificando le condizioni per infiniti numeri primi. Scrive anche che ha provato che una qualsiasi soluzione all'Equazione di Fermat farebbe impallidire l'immaginazione a causa delle sua grandezza.
Per un lungo periodo si è quindi pensato che l'unico contributo di Sophie all'Ultimo Teorema di Fermat fosse consistito in nel teorema attribuitole da Legendre in una nota a piè di pagina di un suo scritto. Solo recentemente, grazie allo studio di alcuni suoi manoscritti inediti (Del Centina 2008, Lauenbacher e Pengelley 2010), le sono stati riconosciuti risultati riguardanti l'Ultimo Teorema di Fermat che vanno ben oltre una semplice nota a piè di pagina.

1.6 L'amicizia con Guglielmo Libri

Nei primi anni del 1820, tramite il lavoro di Poisson, Fourier, Navier e Cauchy, emerse una nuova teoria delle superfici elastiche. Fu impossibile per Sophie prendere parte al suo sviluppo, non solo a causa delle sue lacune in analisi matematica, ma anche a causa dell'impossibilità ad accedere alle riunioni dell'Accademia, delle difficoltà incontrate nell'ottenere informazioni riguardo il lavoro degli altri e, purtroppo, del disinteresse con il quale veniva trattata. Non fu mai inclusa in serie discussioni scientifiche e tutto questo la pose in una posizione scomoda e disagevole.
Nel maggio 1825, durante uno dei ricevimenti del giovedì organizzati da Fran-

[‡]Teorema di Germain: Se p è un numero primo dispari tale che $2p+1$ è anch'esso primo e se x, y, z sono interi tali che nessuno di questi sia divisibile per p allora $x^p + y^p \neq z^p$

cois Arago all'Osservatorio, Sophie fece la conoscenza di Guglielmo Libri [§]. Sophie Germain e Guglielmo Libri condividevano molti interessi, in particolare una vera e propria passione per la Teoria dei Numeri e l'Ultimo Teorema di Fermat, e, nonostante Libri fosse più giovane di 26 anni, la loro divenne molto presto una solida amicizia. Si incontrarono diverse volte durante il soggiorno di Libri a Parigi. Nell'estate 1825 Libri tornò a Firenze dove iniziò la corrispondenza con Sophie.
Nel 1826 Sophie presentò all'Accademia una nuova memoria sull'elasticità, una versione che considerava assai migliore della precedente. Cauchy fu designato revisore della sua tesi. La incoraggiò a pubblicarla, probabilmente anche per sollevare l'Accademia dall'imbarazzo di dover avere a che fare con il suo lavoro, e il suo trattato apparì in *Annales de Chimie* nel 1828. Nel 1829, Sophie scrisse la sua ultima lettera a Gauss. L'occasione nacque dalla recente visita ricevuta da Mr. Bader, un allievo di Gauss, che le lasciò una copia dell'opera *Theoria residuorum biquadraticorum* scritta da Gauss e pubblicata nel 1828. Nel giugno 1830, Libri tornò a Parigi e andò a visitarla. A quanto riporta, fu durante la settimana di combattimenti della Rivoluzione di Luglio che Sophie scrisse il suo ultimo trattato sull'elasticità. In Dicembre Libri tornò a Firenze e nel febbraio 1831, Sophie gli comunicò per lettera che aveva trovato l'energia per scrivere una breve nota ad una questione che aveva sottoposto a Gauss nella sua prima lettera più di 25 anni prima.

1.7 Ultimi Anni

Nel 1831, su pressione di Gauss, l'Università di Gottinga si decise a conferirle il titolo di dottore onorario, ma Sophie, dopo due anni di malattia, colpita da un cancro alla mammella, si spense all'una del mattino del 17 giugno 1831, prima che le potesse essere consegnata l'onorificenza. Oltre al lavoro svolto in campo matematico, Sophie si dedicò a studi di Scienze Naturali e

[§]Guglielmo Libri, conte di Bagnano (1802-1869), nato a Firenze. Riceve un'ottima educazione e si iscrive all'Università di Pisa nel 1816. Si laurea in Matematica nel 1820 e lo stesso anno scrive *Memoria sulla teoria dei numeri* che spedisce a Legendre e Cauchy. Nel 1823 diventa professore di Fisica Matematica sempre all'Università di Pisa. Nell'inverno 1824, già noto come un talentuoso giovane matematico a Legendre e Cauchy grazie alla corrispondenza che tenevano, va a Parigi per presentare di persona i suoi scritti all'Accademia. Rimane a Parigi fino all'agosto 1825, quando ritorna a Firenze. Ritorna successivamente a Parigi nel 1830. Nel 1833 Libri ottiene la cittadinanza francese e, lo stesso anno, viene nominato membro dell'Accademia. Nel 1843 diventa anche professore della Sorbona. Nel 1848, accusato di essere coinvolto in vari furti di opere di biblioteche pubbliche francesi, si trasferisce a Londra dove continua il suo commercio di libri e manoscritti. Ritorna a Firenze nel dicembre 1868. Muore nel 1869 a Fiesole.

Filosofia. I suoi scritti filosofici *Considérations générales sur l'état des sciences et des lettres aux différentes époques de leur culture* e *Pensées diverses* furono pubblicati postumi. Il primo fu edito due anni dopo la sua scomparsa dal nipote Jacques-Amant Lherbette e molto apprezzato da Auguste Comte. Il secondo, che consiste in una lista di riflessioni sulla storia della Scienza e della Matematica, fu pubblicato, insieme ad alcune lettere, da Hyppolite Stupuy. Sul certificato rilasciato alla sua morte figura come "redditiera" e non, più correttamente, come "matematica". Quando nel 1889 fu eretta la Tour Eiffel, vi furono scritti i nomi di tutti coloro che con i loro studi sull'elasticità avevano contribuito alla realizzazione dell'opera, eccezion fatta per Sophie Germain. La sua tomba si trova al cimitero di Père-Lachaise con una modesta iscrizione:

> *"Ici repose Demoiselle Marie-Sophie Germain, née à Paris le 1er avril 1776, décédée en la dite ville, le 27 juin 1831"*

Figura 1.7: Lapide di Sophie Germain al cimitero Père-Lachaise

Sulla facciata della casa dove Sophie è morta, al numero 13 di rue de Savie, è stata posta una targa commemorativa. Sebbene Sophie Germain non abbia mai ricevuto alcun riconoscimento accademico, produsse certamente lavori degni e il suo avvicinamento al teorema fu uno dei passi più importanti fatti da un matematico dopo Eulero.

> *" Tutto considerato ella fu forse la donna intellettualmente più dotata che la Francia abbia mai prodotto. E tuttavia, per quanto possa sembrare strano, quando l'ufficiale di stato civile stilò il certificato di morte di questa illustre collega e collaboratrice dei più illustri membri dell'Accademia Francese delle Scienze, la qualificò come una donna che usufruiva di una rendita annuale e non come una matematica. E questo non è tutto. Quando fu eretta la Tour Eiffel, nella quale gli ingegneri furono costretti a dedicare particolare attenzione all'elasticità dei materiali impiegati, furono scritti*

in questa altissima struttura i nomi di settantadue scienziati. Ma nell'elenco non si trova il nome di Sophie Germain, quella figlia geniale, le cui ricerche contribuirono così tanto all'elaborazione della teoria dell'elasticità dei metalli. Venne esclusa dall'elenco per la stessa ragione per cui la Agnesi non fu eletta membro dell'Accademia di Francia, ossia in quanto donna? Sembrerebbe di sì. Se questa fu davvero la ragione, la vergogna è ancora maggiore per coloro che si resero responsabili di tale ingratitudine verso una donna che ha meritato così bene nella scienza e che con i suoi risultati si è guadagnata un posto invidiabile nella galleria delle celebrità."
H.J Mozans, 1913

Figura 1.8: Targa commemorativa sulla facciata della casa al numero 13 di rue de Savie

1.8 La Corrispondenza fra Gauss e Sophie Germain

La corrispondenza fra Gauss e Sophie Germain consiste di 14 lettere, 10 di Sophie e 4 di Gauss. Probabilmente, se alcune sono andate perse, è più probabile che siano di Gauss e non di Sophie perchè le lettere di quest'ultima vennero preservate con grande cura da Gauss che, alla sua morte, le lasciò in eredità all'Accademia di Gottinga. Le lettere di Sophie, invece, furono lasciate a Libri e, alcune di esse, vennero probabilmente confiscate dall'autorità francese.
Libri, nella sua breve biografia su Sophie Germain, fu il primo a menzionare uno scambio di lettere fra Sophie e Gauss. Successivamente Ernst Schering

[¶], uno degli editori delle opere di Gauss, durante il centenario dalla nascita di quest'ultimo, fece un discorso ufficiale all'Accademia delle Scienze di Gottinga. Questo fu pubblicato insieme ad alcune lettere provenienti dagli archivi di Gauss e, fra queste, c'era una lettera di Sophie Germain datata 20 febbraio 1807. A quanto sostiene Schering, la decisione di pubblicare questa lettera veniva dalla volontà di svelare la vera identità del Signor Le Blanc, citato da Gauss in una lettera a Olbers datata 3 settembre 1805. Nel 1879, Hippolyte Stupuy [‖] incluse nella sua rivalutazione del lavoro filosofico di Sophie Germain alcune lettere della sua corrispondenza. Fra queste c'erano tre lettere di Gauss e due, senza data, firmate "Le Blanc".
Sempre nel 1879, Baldassarre Boncompagni [**], pubblicò la riproduzione litografica della lettera di Gauss a Sophie del 30 aprile 1807. Questa lettera proveniva dagli archivi di Libri, che erano andati dispersi in una serie di aste pubbliche e private prima e dopo la sua morte (avvenuta nel 1869). Nell'ottobre 1879 Boncompagni inviò due copie della sua pubblicazione ad Angelo Genocchi [††], membro dell'Accademia delle Scienze di Torino, una per uso personale e l'altra per l'Accademia. Boncompagni chiese inoltre consiglio a Genocchi riguardo il contenuto matematico dello scambio epistolare. Nelle intenzioni di Boncompagni c'era il proposito di pubblicare un'opera riguardo le lettere di Gauss, che non vide mai la luce ma diede inizio ad uno scambio intenso fra Boncompagni e Genocchi, incentrato sulla corrispondenza Gauss-Germain.
Nel Novembre 1879 Ernst Schering presentò il lavoro di Boncompagni all'Accademia delle Scienze di Gottinga sottolinenando l'importanza di quella lettera, non solo perchè si trattava della prima scritta da Gauss alla Germain dopo essere stato informato della sua vera identità, ma principalmente perchè gli permise di datare gli studi di Gauss sui residui biquadratici. Michel Chasles [‡‡], presentando la pubblicazione di Boncompagni all'Accademia

[¶]Ernst Schering (1824-1897) si laureò alla Georg-August-Universitat di Gottinga, fu l'editore delle opere di Carl Friedrich Gauss.

[‖]Hippolyte Stupuy (1832-) giornalista. Ha collaborato a *l'Artiste* e *Républicain*.

[**]Baldassarre Boncompagni (1821-1894), principe di Piombino, è noto per le sue ricerche nell'ambito della Storia della Matematica. Fondò il *Bullettino di bibliografia e di storia delle Scienze matematiche e fisiche* anche conosciuto come *Bullettino* di Buoncompagni

[††]Angelo Genocchi (1817-1889), considerato uno dei più qualificati teorici dei numeri italiani del diciannovesimo secolo, fu uno dei primi matematici italiano ad imparare i nuovi metodi delle *Disquisitione Arithmeticae*. La sua opera *Sur la théorie des résidus quadratiques* gli diede fama internazionale.

[‡‡]Michel Chasles (1793-1880) dopo brillanti studi superiori entra all'Ecole Polytechnique nel 1812 sotto la guida di Simeon Denis Poisson. Nel 1814 viene chiamato alle armi da Napoleone in difesa di Parigi. Finita la guerra ritorna ai suoi studi di matematica e diventa professore nel 1841. Nel 1846 viene istituita per lui una cattedra di geometria

francese delle Scienze: rimarcò la rilevanza storica e scientifica della lettera ma invertendo l'ordine di importanza attribuitole da Schering (Del Centina, Fiocca 2012 pp.597):

> *" Questa lettera di grande interesse, non solo per le più alte questioni concernenti l'analisi dei residui cubici e biquadratici e per la menzione al lavoro sull'Astronomia al quale Gauss si è dedicato completamente nei precedenti cinque anni, ma, soprattutto, dal punto di vista storico per la corrispondenza avuta con uno studente dell'Ecole Polytechnique nell'arco di sei anni."*

Secondo questa nota, Chasles pensava, senza altre evidenze come supporto, che la corrispondenza fra i due fosse iniziata lo stesso anno della pubblicazione delle *Diquisitiones Arithmeticae*.
Il matematico belga Paul Mansion [§§] commentando la lettera di Gauss pubblicata da Boncompagni, mise l'enfasi su come:

- Sophie Germain aveva rivelato la sua identità a Gauss
- Gauss aveva trovato alcuni errori nei suoi teoremi
- Gauss aveva sviluppato abbastanza teoria sui residui cubici e biquadratici da poter riempire un volume ampio come le *Disquisitiones*.

Mansion concluse osservando che (Del Centina, Fiocca 2012 pp.597)

> *" L'ammirazione espressa da Gauss, alla fine come all'inizio della sua lettera, non dovrebbe sorprenderci. A parte per Sophie Germain, nessuno sembrava interessarsi alle Disquisitiones o dedicar loro l'attenzione che meritavano. E' naturale che il giovane geometra di Hannover, ancora non molto conosciuto a quei tempi, sentì ed espresse un forte piacere nell'avere trovato in Sophie Germain un lettore tanto scrupoloso e competente."*

Alla fine del 1879 solo sette lettere della corrispondenza Gauss-Germain erano note al pubblico e, in particolare, nessuno a quell'epoca sapeva dell'esistenza delle note matematiche incluse da Sophie nelle sue lettere, eccezion fatta per Schering che, il 3 marzo 1880, scrisse a Genocchi informandolo (Del Centina, Fiocca 2012 pp.598):

---

superiore alla Sorbona. Nel 1851 diventa membro dell'Accademia delle scienze francese. Diventa membro straniero della Royal Society il 15 giugno 1854 e i suoi lavori di geometria gli varranno la Medaglia Copley nel 1865.

[§§]Paul Mansion (1844-1919) studiò all'Ecole Normale des Sciences a Ghent, iniziò i suoi studi a diciotto anni nel 1862. Successivamente diventò Professore di Matematica all'Università di Ghent.

> *" Fra le lettere di Gauss ce ne sono 10 di Sophie Germain. Alle prime cinque sono allegate delle note matematiche che riempiono molti fogli. Sto valutando se pubblicare queste lettere come scritti scientifici dal momento che sono accurate."*

Contemporaneamente furono commissionate delle ricerche da parte di Boncompagni al fine di trovare altre lettere. Tre lettere di Gauss vennero riscoperte alla Bibliothèque Nationale di Parigi e, il 30 maggio 1880, Genocchi, mentre presentava il nuovo lavoro editoriale di Boncompagni all'Accademia delle Scienze di Torino, annunciò il suo sulla corrispondenza Germain-Gauss. Con questa opera, Genocchi, rivelò alla comunità di matematici e storici che la corrispondenza (nota) consisteva di dieci lettere della Germain e quattro di Gauss.

1.9 Il progetto editoriale di Boncompagni

Boncompagni richiese una copia di tutte le lettere e le note di Sophie, il 3 marzo 1880, Schering rispose (Del Centina, Fiocca 2012 pp.599):

> *" Avendo letto ora gli scritti di Sophie Germain, devo dirvi che, secondo la mia opinione, ciò che contengono di interesse puramente matematico è già stato pubblicato. Le altre cose mi sembrano meno interessanti dal punto di vista matematico e storico, in particolare alcune dimostrazioni contengono degli errori. Al fine di sottoporre queste considerazioni al vostro giudizio, ieri ho stilato una breve lista di lettere, note matematiche e del loro contenuto scientifico che includo qui. Vedrete che quello che è essenziale nella prima parte della nota nella prima lettera è già stato pubblicato nel Crelle's Journal VII, 1831. Per quanto riguarda la seconda parte della lettera che contiene un tentativo per provare un caso speciale dell'Ultimo teorema di Fermat, vi sto mandando una copia esatta, anche se non è corretto."*

Probabilmente Schering non lesse tutte le note matematiche di Sophie, o comunque, non le lesse prestando grande attenzione.
Lo stesso giorno in cui Schering scrisse a Genocchi, a proposito del suo piano di pubblicare tutte le lettere e note di Germain, cambiò idea. La ragione dietro una così rapida ritrattazione non è chiara.
Il 13 luglio, Boncompagni informò Genocchi di aver finalmente ricevuto una copia delle cinque lettere inedite e di tutte le note matematiche di Sophie. Nella sua lettera Boncompagnì dichiarò l'intenzione di voler pubblicare la

corrispondenza integrale, note matematiche incluse, nella forma di un piccolo libro intitolato *Carteggio fra Sophie Germain e Gauss*, e chiese a Genocchi cosa ne pensava a riguardo di questo progetto. In contrasto con Schering, Genocchi era convinto che le note fossero degne di essere pubblicate e appoggiò quindi l'idea di Boncompagni.
A metà novembre 1880 tutto era pronto. La bozza del libro era costituita da 69 pagine in tutto, 26 dedicate a Sophie, 7 a Gauss e le rimanenti 36 alle note matematiche. Boncompagni invitò Genocchi a cooperare alla correzione delle bozze e, specialmente, essendo ben consapevole delle sue lacune nella teoria dei numeri, lo invitò ad aiutarlo. La correzione della bozza durò un paio di mesi, durante i quali Genocchi fece visita a Boncompagni a Roma. L'esistenza di lettere e note matematiche inedite di Sophie Germain non era nota a tutti coloro che scrivevano a proposito della corrispondenza Germain-Gauss. Nella traduzione italiana dell'articolo di Siegmund Günther ¶¶ pubblicato nel *Bulletino*, l'editore (in una nota a piè di pagina firmata "B.B.") rettificava l'intervento di Günther (Del Centina, Fiocca 2012 pp.601):

> *" L'illustre Società Reale di Gottinga possiede dieci lettere di Sofia Germain, cinque delle quali sono qui menzionate dal sig. Günther, ed altre cinque finora inedite saranno da me in breve date alla luce. Unitamente a queste cinque lettere inedite pubblicherò cinque note matematiche di Sofia Germain, di ciascuna delle quali la medesima Società delle Scienze di Gottinga possiede un esemplare autografo. Tali note sono annesse alle prime cinque delle dieci suddette lettere di Sofia Germain."*

Boncompagni aveva lui stesso pianificato di scrivere un' introduzione al *Carteggio* ma, a causa degli impegni nella gestione del suo *Bullettino* e la stampa della *Regula Abaci* di Abelardo di Bath, che gli richiese più tempo di quanto si fosse aspettato, gli fu impossibile trovare il tempo per completarla. Da quello che appare in *Atti dell'Accademia Pontificia de' Nuovi Lincei 33* (1879-1880) si può dedurre che abbia presentato uno scritto intitolato *Intorno al carteggio tra Sofia Germain e Carlo Federico Gauss* all'Accademia Pontificia dei Nuovi Lincei. Questa era probabilmente una bozza dell'introduzione che aveva pianificato e la rimosse poco dopo, con l'intento di perfezionarla. Qualche anno dopo, Boncompagni pubblicò l'opera *Intorno ad una lettera di Carlo Federico Gauss al Dr. Enrico Guglielmo Mattia Olbers* (1884) all'interno della quale commentava ampiamente la lettera di Gauss ad Olbers del 3 settembre 1805.

¶¶Adam Wilhelm Siegmund Günther (1848-1923) è stato geografo e matematico tedesco. Il suo lavoro matematico comprendeva opere sul determinante, funzioni iperboliche, logaritmi e trigonometria.

Dal momento che nella lettera ad Olbers, Gauss menzionava ancora il suo corrispondente Monsieur Le Blanc con grandi apprezzamenti, Boncompagni ebbe l'opportunità di commentare le prime due lettere di Sophie e Gauss e le loro note. In particolar modo Boncompagni sottolineò il fatto che nella seconda nota Sophie forniva una nuova dimostrazione che 2 è un residuo quadratico per i primi della forma $8k + 1$ e $8k + 7$ e un "nonresiduo" per quelli della forma $8k + 3$ e $8k + 5$.
Genocchi, che aveva letto con grande attenzione ed interesse lo scambio epistolare fra Germain e Gauss, nel 1884 scrisse altre due note in materia. In esse accreditava Sophie di alcuni risultati contenuti nelle sue lettere. Purtroppo Boncompagni non portò mai a termine il suo progetto e, alcuni anni dopo l'iniziale interesse suscitato dalla prima edizione incompleta della corrispondenza, le lettere inedite di Germain e Gauss con note matematiche incluse, furono completamente dimenticate e, cosa è peggio, si pensò che fossero andate perse per sempre. Questo si rivelò non essere vero e sono stati, fortunatamente, preservati alla Niedersächsische Staats- und Universitätsbibliothek in Göttingen.

1.10 Lettere e manoscritti

La mia tesi è basata sull'analisi delle seguenti opere:

Lettera del 21 novembre 1804 di Sophie a Gauss trascritta in [2].

Lettera del 12 maggio 1819 di Sophie a Gauss Una lettera di otto pagine conservata alla Niedersächsische Staats-und Universitätsbibliothek Göttingen incentrata sul lavoro di Sophie sull'ultimo Teorema di Fermat trascritta in [2].

Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation $x^p + y^p = z^p$ Un manoscritto di 20 pagine conservato alla Bibliothèque Nationale trascritta in [3].

Démonstration de l'impossibilité de satisfaire en nombres entiers à l'equation $z^{2(8n\pm3)} = y^{2(8n\pm3)} + x^{2(8n\pm3)}$ Un manoscritto non datato conservato alla Bibliothèque Nationale.

Manoscritto non datato Manoscritto di tre pagine sulla dimostrazione del Teorema di Fermat per gli esponenti pari conservato alla Bibliothèque Nationale.

Capitolo 2

La prima lettera

2.1 Gauss e la Teoria dei Numeri

*Sophie Germain è sempre stata affascinata dalla Teoria dei Numeri nell'arco della sua vita. Principalmente autodidatta, dal momento che era esclusa dai livelli più alti di istruzione poichè donna, iniziò studiando *Théorie des Nombres*, pubblicato nel 1798, di Legendre e si dedicò successivamente alle *Disquisitiones Arithmeticae* (1801) di Gauss. Le *Disquisitiones* si distinguevano da tutte le opere precedenti poichè presentavano una organizzazione della teoria dei numeri come una vera e propria disciplina matematica col proprio corpo di metodi, tecniche e oggetti.

2.1.1 L'inizio della corrispondenza

Lo scambio di lettere fra Sophie e Gauss, intrapreso usando lo pseudonimo maschile "Le Blanc", iniziò nel 1804 e fu di grande stimolo per Sophie. Nella prima lettera del 1804 mandò a Gauss una parte del lavoro iniziale sull'ultimo Teorema di Fermat sottolineandogli di aver trovato una fonte di ispirazione proprio nelle *Disquisitiones*.
Gauss rimase molto colpito dal lavoro di Sophie al punto da essere egli stesso ispirato, come si evince in varie lettere inviate al suo collega Wilhelm Olbers †. Il 3 settembre 1805 Gauss scriveva (Laubenbacher, Pengelley 2010 pp.18):

> *"A causa di varie circostanze, in parte grazie a varie lettere da parte di LeBlanc, che ha studiato le mie Disq. Arith. con ve-*

*Per questo capitolo seguiamo [2] [3] [5] [12] [14]

†Heinrich Wilhelm Olbers (Arbergen, 11 ottobre 1758 – Brema, 2 marzo 1840) è stato un medico tedesco, molto conosciuto per l'attività di astronomo amatoriale, che gli permise di conseguire notevoli risultati.

> *ra passione riuscendo a padroneggiarle completamente e che mi ha inviato ripetutamente ragguardevoli messaggi a proposito, [...] sono stato tentato di riesumare le mie amate investigazioni aritmetiche."*

Dopo che gli fu rivelata la vera identità di LeBlanc scrisse ancora ad Olbers il 24 Marzo 1807 (Laubenbacher, Pengelley 2010 pp.19):

> *"Recentemente le mie Disq. Arith. sono state per me causa di grande sorpresa. Non vi ho scritto più volte a proposito del mio corrispondente LeBlanc da Parigi il quale mi ha fornito le prove di essere riuscito a padroneggiare completamente il mio lavoro? Questo LeBlanc si è recentemente rivelato a me più in profondità. LeBlanc è solo un nome fittizio utilizzato da una giovane donna di nome Sophie Germain e sono sicuro che questo fatto vi sorprenderà tanto quanto ha sorpreso me."*

Nella lettera di Guass ad Olbers del 21 Luglio dello stesso anno traspare come Sophie sia divenuta un membro di valore del suo circolo di corrispondenti (Laubenbacher, Pengelley 2010 pp. 19):

> *"Subito dopo il mio ritorno ho scoperto di aver ricevuto varie lettere da Parigi, da Bouvard, Lagrange e Sophie Germain. [...] Lagrange mostra ancora molto interesse nell'astronomia e nell'aritmetica superiore; i due teoremi (per i quali il numero primo 2 è un residuo o cubico o biquadratico), dei quali vi ho parlato qualche tempo fa, sono da lui considerati 'i più belli e difficili da dimostrare'. Ma Sophie Germain mi ha inviato le dimostrazioni; non sono ancora riuscito a guardarle con cura ma credo che siano buone; almeno si è avvicinata alla questione dal giusto punto di vista, sono solo più lunghe di quanto fosse necessario."*

I due teoremi sulle potenze dei residui erano parte di una lettera che Gauss aveva scritto a Sophie il 30 aprile 1807. Insieme a questi aveva incluso, ancora una volta senza dimostrazione, un ulteriore risultato noto come Lemma di Gauss [‡] , dal quale egli sostiene che si possano derivare dei casi speciali della Legge di Reciprocità Quadratica [§], uno dei primi risultati importanti scoperti e provati sui numeri primi. In una lettera datata 12 Maggio 1807 indirizzata ad Olbers, Gauss scrive (Laubenbacher, Pengelley 2010 pp. 19):

[‡]Lemma di Gauss: Per ogni primo dispari p, sia a un intero coprimo con p. Si considerino gli interi: $a, 2a, 3a, ..., \frac{p-1}{2}a$ e i loro residui modulo p ridotti nell'intervallo $[-\frac{p}{2}, \frac{p}{2}]$. Sia s il numero di questi residui che sono negativi. Allora: $\frac{a}{p} = (-1)^s$

[§]Legge di Reciprocità Quadratica: siano p e q due differenti numeri primi diversi da 2. Questo implica, in particolare, che p e q sono congrui a 1 oppure a 3 $(mod\ \ 4)$. Se

> *"Recentemente ho risposto ad una sua lettera e condiviso con lei un po' di Aritmetica e questo mi ha portato ad intraprendere ancora una ricerca; solo due giorni dopo ho fatto una scoperta molto piacevole. E' una dimostrazione nuova, breve e molto pulita del teorema fondamentale dell'art.131"*

La dimostrazione a cui Gauss fa riferimento, basata sul lemma sopracitato nella sua lettera a Sophie, è ora comunemente chiamata "terza" dimostrazione della Legge di Reciprocità Quadratica e fu pubblicata nel 1808 nel *Theorematis arithmetici demonstratio nova* dove scrisse di aver finalmente trovato (Laubenbacher, Pengelley 2010 pp. 19)

> *"la più semplice e naturale delle sue dimostrazioni"*

L'influenza di Gauss è evidente nei manoscritti di Sophie e permea tutto il suo lavoro; i suoi manoscritti e le sue lettere usano la nozione di congruenza ed un punto di vista "gaussiano", in contrasto con lo stile del suo mentore parigino Legendre di omettere i multipli del modulo nelle equazioni. Il lavoro di Sophie beneficia della scorrevolezza e del pensiero in termini di aritmetica modulo un numero primo delle *Disquisitiones* e Sophie sembra essere stata una delle prime, se non la prima, ad avere adottato ed assimilato nel suo lavoro di ricerca le idee contenute nelle *Disquisitiones*.

2.1.2 La prima lettera

Il 21 novembre 1804 Sophie scrisse la prima lettera a Gauss firmandosi Monsieur Le Blanc dal momento che temeva, usando le sue stesse parole (Dahan 1992, pp.73):

> *"Il ridicolo inevitabilmente associato alla condizione di donna studiosa."*

Sophie all'interno della lettera dopo aver tessuto le lodi delle *Disquisitiones*, che erano state a lungo oggetto di ammirazione e studio, condivise alcune delle sue idee e risultati.

---

almeno uni di essi è congruo a 1 $(mod\ \ 4)$, allora la congruenza $x^2 \equiv p(mod\ \ q)$ ha una soluzione x se e solo se la congruenza $y^2 \equiv q\ \ (mod\ \ p)$ ha una soluzione y (le due soluzioni in genere saranno differenti). Se invece entrambi i numeri prmi sono congrui a 3 $(mod\ \ 4)$ allora la congruenza $x^2 \equiv p\ \ (mod\ \ q)$ ha una soluzione x se e solo se la congruenza $y^2 \equiv q\ \ (mod\ \ p)$ non ha alcuna soluzione.

Nell'art. 357 di [5] Gauss dimostra che se n è un numero primo > 2 allora l'equazione

$$4\frac{x^n - 1}{x - 1} = Y^2 \pm nZ^2$$

dove Y e Z sono polinomi in x a coefficienti interi e il segno sulla destra è $+$ o $-$ a seconda che n sia della forma $4k + 3$ o $4k + 1$.
Nella prima parte dell'*addendum* Sophie estende questo risultato al caso dell'equazione più generica:

$$4\frac{x^{ns} - 1}{x - 1} = Y^2 \pm nZ^2$$

dove s è un intero positivo e Y e Z sono ancora polinomi in x a coefficienti interi. A questo fine utilizza, supposto $s = 2$ questo:

$$16\frac{x^{n2} - 1}{x - 1} = 16\frac{(x^n)^n - 1}{x - 1} = 4\frac{(x^n)^n - 1}{x^n - 1} \cdot 4\frac{x^n - 1}{x - 1}$$

da

$$4\frac{x^n - 1}{x - 1} = Y^2 \pm nZ^2$$

otteniamo:

$$16\frac{x^{n2} - 1}{x - 1} = (Y'^2 \pm nZ'^2)(Y^2 \pm nZ^2)$$

e dal momento che il secondo membro è uguale a $(YY' \pm nZZ')^2 \pm n(Y'Z \pm YZ')^2$ se poniamo $YY' \pm nZZ' = 2f$ e $Y'Z \pm YZ' = 2\phi$, considerando la divisibilità per 4, otteniamo:

$$4\frac{x^{n2} - 1}{x - 1} = f^2 \pm n\phi^2$$

Lo stesso ragionamento applicato all'ultima equazione ed a $4\frac{x^n-1}{x-1} = Y^2 \pm nZ^2$ ci fornisce il caso $s = 3$ etc. etc.
Sophie osserva che a causa dell'ambiguità dei segni ci sono 2^{s-1} polinomi differenti Y e 2^{s-1} polinomi differenti Z che soddisfano $4\frac{x^{ns}-1}{x-1} = Y^2 \pm nZ^2$.
Sia $m = (n-1)/2$ allora $z = x^m - ax^{m-1} + bx^{m-2} - etc. = 0$ è l'equazione le cui

soluzioni appartengono al periodo $(m, 1)$[¶]. Allora per l'art. 348 di [5] abbiamo $a = (m, 1)$ ed i coefficienti b, etc sono della forma$A + B(m, 1) + C(m, g)$, dove A, B, C sono interi.
Sia z' la trasformazione di z quando i periodi (m, g) e (m, g^2), sono sostituiti rispettivamente per $(m, 1)$ e (m, g) nei coefficienti di z, allora le radici di $z' = 0$ sono quelle contenute nel periodo (m, g) e segue che:

$$zz' = \frac{x^n - 1}{x - 1}$$

quindi per l'art. 357 di [5], z può essere ridotto alla forma $R + S(m, g) + T(m, 1)$, dove R, S, T sono polinomi a coefficienti interi e, conseguentemente, z' si riduce alla forma $z' = R + S(m, 1) + T(m, g)$. Da queste riduzioni è possibile determinare i coefficienti di Y e Z.
Gauss scrive (Del Centina, Fiocca 2012 pp.616):

> *"E' facile vedere che i due termini di grado massimo nella funzione Y saranno sempre $2x^m + x^{m-1}$ e quelli di grado massimo nella funzione Z saranno sempre x^{m-1}. Tutti i coefficienti rimanenti saranno interi che dipendono da n e dei quali non è possibile fornire una formula analitica generale."*

Nell' *addendum* Sophie, imitando il metodo di Gauss, rimpiazza $r = \cos\frac{kP}{n} + i\sin\frac{kP}{n}$ con $R = \cos\frac{kP}{n^s} + i\sin\frac{kP}{n^s}$ estendendo il risultato all'equazione $4\frac{x^{n^s}-1}{x-1} = Y^2 \pm nZ^2$. In altre parole mostra che, anche in questo caso, i coefficienti dei corrispondenti z e z', che sono ora polinomi di grado $(n^s - 1)/2$, possono essere espressi in termini dei periodi $(m, 1), (m, g)$. Questa proprietà si verifica anche per i polinomi Y e Z.
Il ragionamento seguito da Sophie le permette di determinare i coefficienti dei polinomi Y e Z per determinati valori di n ed s. Sophie sottolinea inoltre che (Del Centina, Fiocca 2012 pp. 616):

> *"Se $n = 4k + 1$, allora i coefficienti Y e Z sono uguali e di stesso segno, partendo da x^m come anche partendo da 1, cioè, se N è il coefficiente di x^{m-h} in Y o in z allora N è il coefficiente di x^h. Se $n = 4k + 3$, lo stesso si verifica per il segno opposto, cioè, se N è il coefficiente di x^{m-h} allora $-N$ è il coefficiente di x^h."*

Per dimostrare ciò procede in questo modo. Sia g ciò che denota la radice primitiva per il modulo n, e siano $[1], [g], ..., [g^{n-2}]$ gli elementi dell'insieme delle radici dell'equazione $zz' = X = 0$. Sophie nota che i coefficienti di Y e Z dipendono da quelli di z e z'. In base alla teoria dei periodi di Gauss, $z = 0$

[¶]questo argomento verrà analizzato più avanti nel capitolo

può essere messo nella forma $z = (x-[1])(x-[g^2])(x-[g^4])...(x-[g^{n-3}]) = 0$. Poichè $[1][g^2][g^4]...[g^{n-3}] = [1 + g^2 + g^4 + ... + g^{n-3}] = [0] = 1$, è possibile moltiplicare il secondo membro dell'equazione $z = (x - [1])(x - [g^2])(x - [g^4])...(x - [g^{n-3}]) = 0$ per $(1][g^2][g^4]...[g^{n-3}])^{m-1}$ senza modificare il primo e si possono moltiplicare in modo che ogni fattore sia moltiplicato per tutte le radici escluse quelle che appaiono nello stesso fattore. Questo procedimento permette di scrivere l'equazione nella forma:

$$z = ([-1] - 1)(x[-g^2] - 1)...(x[-g^{n-3}] - 1)$$

Quando $n = 4k + 1$, -1 è un residuo quadratico e l'equazione $z = ([-1] - 1)(x[-g^2] - 1)...(x[-g^{n-3}] - 1)$ si riduce alla forma $z = (x[1] - 1)(x[g^2] - 1)...(x[g^{n-3}] - 1)$ e, dal momento che il numero di fattori $m = 2k$ è pari, si possono cambiare tutti i segni, ottenendo $z = (1 - x[1])(1 - x[g^2])...(1 - x[g^{n-3}])$ che mostra come z sia una funzione omogenea di x ed 1 così come definita da Sophie.
Lo stesso ragionamento può essere applicato a z' e si ottiene $z' = (x-[g])(x-[g^3])(x-[g^5])...(x-[g^{n-2}]) = 0$. Da ciò segue che zz' è una funzione omogenea di x e 1.
Quando $n = 4k + 3$ si può procedere in un modo simile (ma ricordando che in questo caso -1 non è un residuo quadratico) per mostrare che zz' è una funzione omogenea di z e -1. A questo punto della lettera però Sophie asserisce che Y e Z sono funzioni omogenee di x e -1 senza aggiungere una spiegazione.
Ad ogni modo è possibile che questa proprietà effettivamente valga per Y. Legendre nella seconda edizione di *Théorie des nombres* del 1827 fornisce due metodi per ottenere i coefficienti di Y e Z per l'equazione $4\frac{x^n-1}{x-1} = Y^2 \pm nZ^2$. Il primo metodo è basato sulla teoria dei periodi e perciò è molto simile a quello usato da Sophie. Il secondo è basato su un "semplice" accorgimento.
Nello sviluppo di $(x - 1)^n$, tutti i coefficienti, eccetto il primo e l'ultimo, sono divisibili per n. Quindi si potrebbe scrivere $(x - 1)^n = x^n - 1 - nT$ con T un polinomio adeguato di grado $n - 1$. Ricordando l'equazione $4\frac{x^n-1}{x-1} = Y^2 \pm nZ^2$ si ha $4X(x - 1) = 4(x - 1)^n + 4nT = (x - 1)(Y^2 \pm nZ^2)$. Quindi, omettendo i multipli di n, si ottiene $4(x-1)^n = (x-1)Y^2$ e, di conseguenza, $Y = 2(x - 1)^m$. Per determinare i coefficienti di Y bisogna solamente ridurre (mod n) i coefficienti dello sviluppo di $2(x - 1)^m$.
Sophie tornò sull'equazione $4\frac{x^{ns}-1}{x-1} = Y^2 \pm nZ^2$ in una nota intitolata *Note sur la manière dont se composent les valeurs de y et z dans l'équation* $\frac{4(x^p-1)}{x-1} = y^2 \pm z^2$ *et celle de* Y' *et de* Z' *dans l'équation* $\frac{4(x^{p2}}{x-1} = Y'^2 \pm Z'^2$ pubblicata nel 1831, l'anno della sua scomparsa. In questa opera, usando il risultato

sopracitato di Legendre, al quale si riferisce come (Del Centina, Fiocca 2012 pp.617)

> *"utile per stabilire immediatamente che* Y *nell'equazione* $4\frac{x^n-1}{x-1} = Y^2 \pm nZ^2$ *è un polinomio omogeneo di* x *e 1"*

determina la forma della potenza di x nei polinomi Y' e Z' quando $s = 2$.
Quasi alla fine dell' *addendum*, Sophie fornisce, usando il metodo dell' art.345 di [5] una nuova dimostrazione del fatto che 2 sia un residuo primo della forma $8k + 1$ e $8k + 7$ ed un non-residuo per i primi della forma $8k + 3$ e$8k + 5$.
Questo è l'unico risultato che Gauss commentò nella sua risposta alla prima lettera di Sophie (Del Centina, Fiocca 2012 pp.617)

> *"La sua nuova dimostrazione per i primi per i quali 2 è un residuo o un non-residuo mi fa estremamente piacere. E' molto chiara, nonostante sembri insolita, e non applicabile ad altri numeri."*

Nell'ultimissima parte dell' *addendum* Sophie parla di quello che sembra essere il suo primo approccio all'ultimo Teorema di Fermat. Asserisce di aver provato il teorema per gli esponenti $p - 1$ quando p è un numero primo del tipo $8n + 7$.
Sia p un numero primo maggiore di 3 e poniamo $2p' := p - 1$. Se x, y, z è una soluzione primitiva dell'equazione $x^{p-1} + y^{p-1} = z^{p-1}$, allora $x^{p'}, y^{p'}, z^{p'}$ soddisfa $X^2 + Y^2 = Z^2$, in questo modo uno fra x o y deve essere pari e l'altro dispari. Sophie inizialmente prova questi due risultati:

1. (1) se x, y, z sono a due a due interi coprimi che soddisfano l'equazione di Fermat, allora p divide il pari fra x, y e z è dispari e non divisibile per p.

   Ponendo $y = 2phf$ prova allora che $x^{p'} = f^{2p'} - 2^{2p'-2}p^{2p'}h^{2p'}$ e da ciò ottiene

2. (2) se x, y, z sono come in (1) allora $x^{p'} = fx$ è un residuo quadratico modulo p.

Sia $x = f^2 + mp^{2p'}$ dove m non è divisibile per p. Sviluppando la p'-esima potenza di x, si ottiene $f^{2p'} - 2^{2p'-2}p^{2p'}h^{2p'} = f^{2p'} + p'f^{2p'-2}mp^{2p'} + ...+$ da cui Sophie asserisce che si ha $m = k^{2p'}$ e quindi $-2 \equiv f^2 \pmod{p}$. Segue che $x^{p-1} + y^{p-1} = z^{p-1}$ non ha soluzioni intere quando -2 non è un residuo quadratico (mod p), quindi per numeri primi della forma $8n+5$ e $8n+7$ ([5] art.113).
Nel primo caso $p-1$ è sempre divisibile per 4, e allora il risultato segue dall'impossibilità di $x^4+y^4 = z^4$ ma, nel secondo caso, $p-1$ non è mai divisibile

per 4 e non sempre è divisibile per 3. Quindi l'ultimo Teorema di Fermat sarebbe dimostrato per l'esponente $p-1$ quando $p = 8n+7$.
Purtroppo non si può asserire che m sia necessariamente una $2p'$-esima potenza e il ragionamento di Sophie contiene quindi un errore. Ad ogni modo è da sottolineare come il suo fosse uno dei primi tentativi di approciarsi alla teoria delle congruenze e dei residui per dimostrare l'ultimo Teorema di Fermat per alcuni esponenti. Sophie Germain probabilmente continuò a studiare l'ultimo Teorema di Fermat negli anni seguenti ma non tornò mai su questo argomento fino al 1819.

2.2 Congruenza

Entriamo ora nello specifico dei termini usati precedentemente.

Congruenza Due numeri interi a e b sono detti "congruenti modulo θ" (dove θ è un numero naturale chiamato modulo) se la loro differenza $a-b$ è un multiplo di θ; questo si vede facilmente se divisi per θ hanno lo stesso resto (**residuo**). Ovviamente i **residui** sono numeri compresi fra 0 e $\theta - 1$ inclusi).
Scriviamo allora $a \equiv b \pmod{\theta}$ e diciamo "a congruente a b modulo θ" (o in breve, solo " a è b modulo θ").

Proprietà della congruenza La congruenza è una relazione di equivalenza infatti:

- **Proprietà riflessiva**: ogni numero è congruo a sè stesso modulo θ, per ogni θ diverso da 0 fissato.
  $a \equiv a \pmod{\theta} \quad \forall a \in \mathbb{N}\ \forall \theta \in \mathbb{N}_0$

  Dimostrazione:
  si ha $a-a=0$. Ma ogni intero non nullo è divisore di 0. Quindi θ divide (a-a).

- **Proprietà simmetrica**: se a è congruo b modulo θ allora b è congruo ad a modulo θ.

  $$a \equiv b \pmod{\theta} \Rightarrow b \equiv a \pmod{\theta} \quad \forall a, b \in \mathbb{N}, \forall \theta \in \mathbb{N}_0$$

  Dimostrazione:
  se θ divide $(a-b)$, allora θ divide anche $(b-a) = -(a-b)$.

- **Proprietà transitiva**: se a è congruo a b modulo θ e b è congruo a c modulo θ allora anche a è congruo a c modulo θ.

  $$a \equiv b \pmod{\theta} \wedge b \equiv c \pmod{\theta} \Rightarrow a \equiv c \pmod{\theta} \quad \forall a, b, c, \in \mathbb{N}, \quad \forall \theta \in \mathbb{N}_0$$

  Dimostrazione:
  se θ divide $(a-b)$ e θ divide $(b-c)$ allora, per la proprietà distributiva della divisione rispetto alla somma, θ divide anche $[(a-b)+(b-c)] = [a-b+b-c] = (a-c)$.

Invarianza rispetto alle operazioni aritmetiche Una importante caratteristica della relazione di congruenza è il fatto di essere preservata dalle usuali operazioni aritmetiche tra interi:

- **Invarianza per addizione**: sommando o sottraendo la stessa quantità a due numeri congurenti modulo θ, i nuovi numeri ottenuti sono ancora congruenti tra loro modulo θ. Più sinteticamente:

  $$a \equiv b \pmod{\theta} \leftrightarrow (a+c) \equiv (b+c) \pmod{\theta} \quad \forall a, b, c \in \mathbb{N}, \forall \theta \in \mathbb{N}_0$$

  Dimostrazione:
  scriviamo $(a-b) = (a-b+c-c) = (a+c)-(b+c)$

- **Invarianza per moltiplicazione**: moltiplicando per una stessa quantità due numeri congruenti modulo θ, i nuovi numeri ottenuti sono ancora congruenti tra loro modulo θ.

  $$a \equiv b \pmod{\theta} \Rightarrow a \cdot c \equiv b \cdot c \pmod{\theta} \quad \forall a, b, c \in \mathbb{N}, \forall \theta \in \mathbb{N}_0$$

  Dimostrazione:
  Se θ divide $(a-b)$ allora θ divide $(a-b) \cdot c$ (questa proprietà si può invertire solo se MCD(θ, c)=1.)

- **Invarianza rispetto elevamento a potenza**: elevando due numeri congrui modulo θ alla stessa potenza k, i numeri ottenuti sono ancora congrui tra loro modulo θ.

  $$a \equiv b \pmod{\theta} \Rightarrow a^k \equiv b^k \pmod{\theta} \quad \forall a, b, k \in \mathbb{N}, \forall \theta \in \mathbb{N}_0$$

Dimostrazione:
Se $a \equiv b \equiv 0 \pmod{\theta}$ la proposizione è banale.
Se $a \equiv b \pmod{\theta}$ non sono nulli, supponiamo di sapere che $a^{k-1} \equiv b^{k-1} \pmod{\theta}$. Moltiplicando entrambi i termini per a grazie all'invarianza per moltiplicazione, avremo $a^k \equiv b^{k-1} \cdot a \pmod{\theta}$. Partiamo ora dalla congruenza $a \equiv b \pmod{\theta}$ e moltiplichiamo entrambi i membri per $b^{k-1} \pmod{\theta}$, sempre grazie all'invarianza per moltiplicazione.
Otteniamo: $a \cdot b^{k-1} \equiv b^k \pmod{\theta}$. Confrontando le due espressioni ed utilizzando le proprietà simmetrica e transitiva, si deduce che $a^k \equiv b^k \pmod{\theta}$. Poichè la proposizione è vera per $k = 1$ e il fatto che sia vera per $k - 1$ implica che essa è vera per k. Per il principio di induzione la proposizione allora è vera per ogni k. (Questa proprietà si può invertire solo se k è diverso da 0).

2.3 I risultati di Gauss

Sia p un numero primo, per comodità introduciamo la notazione

$$p^* = \begin{cases} +p & p = 1 \mod (4) \\ -p & p = 3 \mod (4) \end{cases}$$

Il teorema di Gauss dice che esistono polinomi Z e Y con coefficienti interi tali che:

$$4\frac{x^p - 1}{x - 1} = Y^2 - p^* Z^2,$$

Definiamo

$$\Phi_p(x) := \frac{x^p - 1}{x - 1},$$

Il risultato di Gauss si ottiene dal fatto che possiamo scrivere $\Phi_p(x) = z(x)\hat{z}(x)$ dove

$$\begin{aligned} \Phi_p(x) &= z(x)\hat{z}(x) \\ &\text{dove} \\ z(x) &= R(x) + S(x)R_1 + T(x)R_2 \\ \hat{z}(x) &= R(x) + S(x)R_2 + T(x)R_1 \end{aligned}$$

e R_1 e R_2 sono due numeri tali che:

$$R_1 + R_2 = -1, \quad R_1 - R_2 = \sqrt{p^*}.$$

Se diamo per scontata l'espressione $z(x)$ abbiamo:

$$z(x) = R(x) + S(x)(R_1 + R_2) - R_2(\, S(x) - T(x)\,)$$

ma anche:

$$z(x) = R(x) + R_1(S(x) - T(x)) + T(x)(R_2 + R_1)$$

sommandole entrambe otteniamo:

$$\begin{aligned} 2z(x) &= 2R(x) + (\, S(x) + T(x)\,)(R_1 + R_2) + (\, S(x) - T(x)\,)(\, R_1 - R_2\,) \\ &= 2R(x) - S(x) - T(x) + \sqrt{p^*}(\, S(x) - T(x)\,) \end{aligned}$$

la stessa manipolazione su $\hat{z}(x)$ produce:

$$2\hat{z}(x) = 2R(x) - S(x) - T(x) - \sqrt{p^*}(\, S(x) - T(x)\,)$$

e da queste due otteniamo:

$$4\hat{z}(x)z(x) = 4\Phi_p(x) = (\, 2R(x) - S(x) - T(x))^2 - p^*(\, S(x) - T(x)\,)^2.$$

2.4 Le equazioni Ciclotomiche

Sia p un numero primo, l'equazione

$$x^p - 1 = 0$$

ha la radice p:

$$\zeta_p^k, \quad 0 \leq k < p, \quad \text{dove} \quad \zeta_p = e^{\frac{i2\pi}{p}}$$

quindi il polinomio

$$\Phi_p(x) = \sum_{i=0}^{p-1} x^i = \frac{x^p - 1}{x - 1}$$

ammetterà le $p-1$ radici $\{\zeta_p^k, \quad 1 \leq k < p\}$.

Infatti:

$$\sum_{i=0}^{n-1} (\zeta_p^k)^i = \frac{\zeta_p^{nk} - 1}{\zeta_p^k - 1} = 0$$

perciò:

$$\sum_{i=1}^{n-1} (\zeta_p^k)^i = -1.$$

2.5 Le radici primitive

Teorema 2.5.1 (**Piccolo Teorema di Fermat**). *Sia p un numero primo, allora $a^p - a = pm$ per qualche $m \geq 0$.*

Dimostrazione. Assumiamo che esista un a tale che $a^p - a = pm$ per qualche $m \geq 0$, Allora:

$$\begin{aligned} (a+1)^p - (a+1) &= \sum_{j=0}^{p} \binom{p}{j} a^j - (a+1) \\ &= a^p - a + \sum_{j=1}^{p-1} \frac{p!\, a^j}{j!(p-j)!} \end{aligned}$$

La quantità

$$\frac{p!}{j!(p-j)!}$$

è chiaramente un numero intero, ma se p è primo, dobbiamo avere $j!(p-j)!$ che divida $(p-1)!$ quando $0 < j < p$. Per completare la dimostrazione osserviamo che: $1^p - 1 = 0$. □

Corollario 2.5.2. *Per $a < p$ abbiamo $a^{p-1} = 1 \mod (p)$.*

Definizione 2.1 (**Ordine di un elemento**)**.** L' ordine di a, $(a)|_p$, relativamente al primo p è il più piccolo intero j tale che $a^j = 1 \mod (p)$.

Definizione 2.2 (**Radice primitiva**)**.** Diciamo che g è una radice primitiva del primo p se $(g)|_p = p - 1$.

Teorema 2.5.3. *Ogni primo p ha almeno una radice primitiva.*

2.6 Periodi

Se p è primo e g una radice primitiva di p, chiaramente possiamo guardare a $g^k \mod (p)$ come ad una permutazione dei numeri $1, 2, \ldots, p-1$. Le $p-1$ radici di $\Phi_p(x)$ possono essere caratterizzate come

$$\{\zeta_p^{g^k}, \quad 1 \leq k \leq p-1\}.$$

Definizione 2.3 (**Periodo di Gauss**)**.** Sia g una radice primitiva di p, ed $ef = (p-1)$. Un Periodo di Gauss è la funzione:

$$P_{f,e}(z) = \sum_{j=0}^{f-1} z^{g^{je}}, \tag{2.1}$$

dove z può assumere i valori ζ^{g^k} per ogni k.

Definizione 2.4. Siano, g, p, e, f come nella definizione precedente. Con il simbolo $(f, g^k), \quad 0 \leq k < e$ denotiamo l'insieme di f radici

$$\{\zeta^{g^{je+k}}, \quad 0 \leq j < f\}$$

.

Successivamente sceglieremo $f = (p-1)/2$ ed $e = 2$.

Possiamo ora introdurre le funzioni $z(x)$ e $\hat{z}(x)$ e dimostrare le loro proprietà.

$$\begin{aligned} z(x) &= \prod_{j=0}^{f-1} \left(x - \zeta_p^{g^{2j}}\right) \\ \hat{z}(x) &= \prod_{j=0}^{f-1} \left(x - \zeta_p^{g^{2j+1}}\right) \end{aligned}$$

L'unica proprietà evidente è:

$$\Phi_p(x) = z(x)\hat{z}(x).$$

Vogliamo determinare i coefficienti a_n tali che:

$$z(x) = \sum_{n=0}^{f} a_{f-n}x^n.$$

Teorema 2.6.1. *La soluzione è data dall'equazione ricorsiva:*

$$(n+1)\, a_{n+1} \;=\; -\sum_{i=0}^{n} a_{n-i}S_{i+1} \tag{2.2}$$

dove:

$$S_i := \sum_{i=0}^{f-1} \left(\zeta_p^{2j+k}\right)^i$$

Per dimostrarlo abbiamo bisogno di un risultato preliminare. Introduciamo il simbolo:

$$f^{(n)}(x) := \frac{d^n f(x)}{dx^n}.$$

Teorema 2.6.2. *Sia $f(x) = e^{g(x)}$, allora:*

$$f^{(n)}(x) = \sum_{i=0}^{n-1} \left(\begin{array}{c} n-1 \\ i \end{array} \right) f^{(n-1-i)}(x)g^{(i+1)}(x)$$

Dimostrazione.

$$\begin{aligned}
f^{n+1}(x) &= \sum_{i=0}^{n-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right) f^{n-i}(x)g^{i+1}(x) + \sum_{i=0}^{n-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right) f^{n-1-i}(x)g^{i+2}(x) \\
&= \sum_{i=0}^{n-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right) f^{n-i}(x)g^{i+1}(x) + \sum_{i=1}^{n}\left(\begin{array}{c} n-1 \\ i-1 \end{array}\right) f^{n-i}(x)g^{i+1}(x) \\
&= f^n(x)g^1(x) \\
&+ \sum_{i=1}^{n-1}\left(\begin{array}{c} n-1 \\ i \end{array}\right) f^{n-i}(x)g^{i+1}(x) + \sum_{i=1}^{n-1}\left(\begin{array}{c} n-1 \\ i-1 \end{array}\right) f^{n-i}(x)g^{i+1}(x) + f(x)g^{n+1}(x) \\
&= f^n(x)g^1(x) \\
&+ \sum_{i=1}^{n-1}\left[\left(\begin{array}{c} n-1 \\ i \end{array}\right) + \left(\begin{array}{c} n-1 \\ i-1 \end{array}\right)\right] f^{n-i}(x)g^{i+1}(x) + f(x)g^{n+1}(x) \\
&= f^n(x)g^1(x) + \sum_{i=1}^{n-1}\left(\begin{array}{c} n \\ i \end{array}\right) f^{n-i}(x)g^{i+1}(x) + f(x)g^{n+1}(x) \\
&= \sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) f^{n-i}(x)g^{i+1}(x)
\end{aligned}$$

$$\begin{aligned}
f^{(n+1)}(x) &= \sum_{i=0}^{n}\left(\begin{array}{c} n \\ i \end{array}\right) f^{n-i}(x)g^{i+1}(x) \\
&= g^{n+1}(x) + \sum_{i=0}^{n-1}\left(\begin{array}{c} n \\ i \end{array}\right) f^{n-i}(x)g^{i+1}(x)
\end{aligned}$$

□

Tornando a 2.6.1,è ovvio che

$$V_k(t) := \prod_{j=0}^{f-1}\left(1 - t\zeta_p^{g^{2j+k}}\right) = \sum_{n=0}^{f} a_n t^n.$$

e chiaramente,

$$a_n = \frac{1}{n!}\frac{d^n V_k(t)}{dt^n}\bigg|_{t=0}$$

Definiamo

$$\varphi_k(t) := \log\left(V_k(t)\right) = \sum_{j=0}^{f-1}\log(1 - tr_j)$$

allora,

$$V_k(x) \;=\; e^{\varphi_k(x)}$$

e da

$$\frac{d^{n+1}V_k}{dt^{n+1}} = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) \frac{d^{n-i}V(t)}{dt^{n-i}} \frac{d^{i+1}\varphi_k(t)}{dt^{i+1}}$$

otteniamo l'equazione ricorsiva:

$$(n+1)!\; a_{n+1} \;=\; \sum_{i=0}^{n} (n-i)! \left(\begin{array}{c} n \\ i \end{array} \right) a_{n-i} \frac{d^{i+1}\varphi_k(t)}{dt^{i+1}}\bigg|_{t=0}$$

Tenendo presente che:

$$\frac{d^{i+1}\varphi_k(t)}{dt^{i+1}} \;=\; \sum_{j=0}^{f-1} \frac{d^{i+1}\log(1-tr_j)}{dt^{i+1}}\bigg|_{t=0} = \sum_{j=0}^{f-1} i!\;(r_j)^{i+1}$$

e infine:

$$\begin{aligned}(n+1)!\; a_{n+1} \;&=\; -\sum_{i=0}^{n} (n-i)! \left(\begin{array}{c} n \\ i \end{array} \right) a_{n-i} \sum_{j=0}^{f-1} i!\;(r_j)^{i+1} \\ &=\; -n! \sum_{i=0}^{n} a_{n-i} S_{i+1}, \quad \text{where} \quad S_i = \sum_{i=0}^{f-1} \left(\zeta_p^{2j+k}\right)^i\end{aligned}$$

dividendo entrambi i membri per $n!$ concludiamo:

$$(n+1)\; a_{n+1} = -\sum_{i=0}^{n} a_{n-i} S_{i+1}$$

con la condizione $a_0 = 1$.

Usando questo risultato troviamo i primi termini:

$$\begin{aligned} a_0 &= 1 \\ a_1 &= -a_0 S_1 \\ 2a_2 &= -[a_1 S_1 + a_0 S_2] \\ 3a_3 &= -[a_2 S_1 + a_1 S_2 + a_0 S_3] \\ 4a_4 &= -\ldots \end{aligned}$$

D'ora in avanti la discussione è la seguente: ogni S_i e prodotto di S_i può essere scritta come combinazione di

$$a_0 + a_1 R_1 + a_2 R_2$$

Segue che $z(x)$ può essere scritta nella forma desiderata, dopo aver dimostrato che R_1 e R_2 si "comportano" come detto.

Teorema 2.6.3.

$$\sum_{j=0}^{f-1} \zeta^{g^{je+k}} = \sum_{j=0}^{f-1} \zeta^{g^{(j+l)e+k}}$$

per ogni $l \in$.

Dimostrazione. Dal momento che

$$g^{fe+q} = g^{fe} g^q = g^{p-1} g^q = g^q,$$

senza perdere in generalità possiamo dimostrare il teorema nel caso $l < p$.

$$\begin{aligned}
\sum_{j=0}^{f-1} \zeta^{g^{je+k}} &= \sum_{j=0}^{l-1} \zeta^{g^{je+k}} + \sum_{j=l}^{f-1} \zeta^{g^{je+k}} \\
&= \sum_{j=f}^{f+l-1} \zeta^{g^{je+k}} + \sum_{j=l}^{f-1} \zeta^{g^{je+k}} \\
&= \sum_{j=l}^{f+l-1} \zeta^{g^{je+k}} = \sum_{j=0}^{f-1} \zeta^{g^{(j+l)e+k}}
\end{aligned}$$

□

Corollario 2.6.4. *Se f è pari, la quantità $P_{f,e}(z)$ è reale.*

Dimostrazione. Scegliamo $l = f/2$ nell'esercizio precedente. Con questa scelta il risultato precedente diventa [‖]

$$P_{f,e}(z) = P^{\dagger}_{f,e}(z).$$

□

Teorema 2.6.5.

$$\sum_{k=0}^{e-1} P_{f,e}(\zeta^{g^k}) = -1$$

Dimostrazione. Dal momento che $g^k, \quad 1 \leq k \leq p-1$ è una permutazione di $1, 2 \ldots, p-1$, chiaramente:

$$\sum_{k=0}^{e-1} P_{f,e}(\zeta^{g^k}) = \sum_{k=1}^{p-1} \zeta^k = -1$$

□

[‖]con la notazione † intendiamo complesso coniugato

Calcoliamo ora $P^2_{f,e}(\zeta^{g^k})$.

$$P^2_{f,e}(\zeta^{g^k}) = \sum_{j=0}^{f-1} \zeta^{je+k} \sum_{l=0}^{f-1} \zeta^{le+k}$$

Usando il risultato di (2.6.3) possiamo scrivere:

$$\begin{aligned} P^2_{f,e}(\zeta^{g^k}) &= \sum_{j=0}^{f-1} \zeta^{g^{je+k}} \sum_{l=0}^{f-1} \zeta^{g^{(j+l)e+k}} \\ &= \sum_{j,l=0}^{f-1} \zeta^{g^{je+k}+g^{(j+l)e+k}} \\ &= \sum_{j,l=0}^{f-1} \left(\zeta^{g^k}\right)^{g^{je}+g^{(j+l)e}} \\ &= \sum_{j,l=0}^{f-1} \left(\left(\zeta^{g^k}\right)^{1+g^{le}}\right)^{g^{je}} \\ &= \sum_{l=0}^{f-1} P_{f,e}\left(\left(\zeta^{g^k}\right)^{1+g^{le}}\right) \end{aligned}$$

$$\begin{aligned} P_{f,e}(\zeta^{g^k})P_{f,e}(\zeta^{g^h}) &= \sum_{j=0}^{f-1} \zeta^{g^{je+k}} \sum_{l=0}^{f-1} \zeta^{g^{le+h}} \\ &= \sum_{j,l=0}^{f-1} \zeta^{g^{je+k}+g^{(l+j)e+h}} \\ &= \sum_{j,l=0}^{f-1} \left(\zeta^{g^k+g^{le+h}}\right)^{je} \\ &= \sum_{l=0}^{f-1} P_{f,e}\left(\zeta^{g^k+g^{le+h}}\right) \end{aligned}$$

Calcoliamo

$$S_i := \sum_{j=0}^{f-1} \left(\zeta^{g^{je+k}}\right)^i$$

Formalmente

$$S_i = \sum_{k=0}^{e-1} m_{i,k} P_{f,e}\left(\zeta^{g^k}\right), \quad m_{i,k} \in \{0,1\}, \quad \sum_{k=0}^{e-1} m_{i,k} = 1$$

2.7 La matematica di Gauss

Servendoci di [14] ricostruiamo altri risultati.

Dal momento che:

$$\begin{aligned} F_{(p-1)/2}(\zeta) &= \sum_{j=0}^{(p-1)/2-1} (\zeta)^{g^{2j}} \\ F_{(p-1)/2}((\zeta)^g) &= \sum_{j=0}^{(p-1)/2-1} (\zeta)^{g^{2j+1}} \end{aligned}$$

Abbiamo:

$$\begin{aligned} F_{(p-1)/2}(\zeta) + F_{(p-1)/2}(\zeta^g) &= -1 \\ F_{(p-1)/2}(\zeta) F_{(p-1)/2}(\zeta^g) &= -\frac{p-1}{4} \end{aligned}$$

Quindi sono le due radici dell'equazione quadratica:

$$x^2 + x - (p-1)/4 = 0,$$

$$\text{quindi} \quad x_{1,2} = -\frac{1}{2} \pm \frac{\sqrt{p}}{2}$$

Segue che

$$F_{(p-1)/2}(\zeta) - F_{(p-1)/2}(\zeta^g) = \pm\sqrt{p}$$

2.7.1 I polinomi primitivi

Teorema 2.7.1. *Se $\gamma_p(f(x)) \neq 0\ \forall p$ e $\gamma_p(g(x)) \neq 0\ \forall p$ allora $\gamma_p(f(x)g(x)) \neq 0\ \forall p$.*

Dimostrazione. Siano Q_f e Q_g i razionali che rendono $f(x)$ e $g(x)$ primitivi. Allora:

$$Q_g g(x) Q_h h(x) = Q_f Q_p f(x)$$

Dal momento che $f(x)$ è intero, allora $Q_f Q_p$ devono essere interi, quindi $Q_f Q_p f(x)$ non può essere primitivo. □

2.8 Il contributo di Sophie all'ultimo Teorema di Fermat

Arriviamo alla parte finale dell' *addendum* della prima lettera a Gauss. Sophie, come già abbiamo detto precedentemente, voleva dimostrare l'ultimo Teorema di Fermat per gli esponenti $n = p - 1$, dove p è un numero primo della forma $8k + 7$.

Sia p un numero primo, $p > 3$ e poniamo $2p' = p - 1$. Se x, y e z costituiscono una soluzione primitiva dell'equazione $x^{p-1} + y^{p-1} = z^{p-1}$, allora $x^{p'}, y^{p'}$ e $z^{p'}$ soddisfano l'equazione $X^2 + Y^2 = Z^2$ e si può supporre che x sia dispari e y pari.

Teorema 2.8.1. *Sia x, y, z una tripletta pitagorica irriducibile, mostriamo che z deve essere dispari.*

Dimostrazione. Assumiamo che $z = 2q$, allora dobbiamo avere $x = 2n + 1$ e $y = 2m + 1$. Segue che:

$$4(n^2 + m^2 + n + m) + 2 = 4q^2$$

ma ciò è impossibile dal momento che:

$$\begin{aligned} 4(n^2 + m^2 + n + m) + 2 &= 2 \mod 4 \\ 4q^2 &= 0 \mod 4. \end{aligned}$$

□

Inoltre uno fra x e y deve essere un multiplo di p. Infatti se x, y, z e p sono coprimi, da $x^{p-1} - 1 + y^{p-1} - 1 = z^{p-1} - 2$ e dal piccolo teorema di Fermat si ottiene l'assurdo $-1 \equiv 0 \pmod{p}$; allo stesso modo se x, y e p sono coprimi e z è un multiplo di p, si ottiene l'assurdo $-2 \equiv 0 \pmod{p}$. Supponiamo che x sia un multiplo di p e poniamo $x = phf$ (si può supporre che f ed h siano entrambi dispari e h non sia divisibile per p), allora si ha

$$(phf)^{2p'} + y^{2p'} = z^{2p'}$$

e di conseguenza

$$z^{2p'} - y^{2p'} = (z^{p'} + y^{p'})(z^{p'} - y^{p'}) = (phf)^{2p'}$$

Dal momento che $z^{p'} + y^{p'}$ e $z^{p'} - y^{p'}$ non sono entrambi divisibili per p (altrimenti z e y sarebbero entrambi divisibili per p, in contraddizione col fatto che x, y, z siano coprimi), segue che:

$$y^{p'} \pm z^{p'} = (pf)^{2p'}, \quad y^{p'} - (\pm z^{p'}) = h^{2p'}, \quad 2y^{p'} = (pf)^{2p'} + h^{2p'}$$

Da queste equazioni, dal momento che per il piccolo Teorema di Fermat si ha che $h^{2p'} - 1 \equiv 0 \pmod{p}$, segue che $2y^{p'} - 1 \equiv 0 \pmod{p}$, quindi $4y^{2p'} \equiv 1 \pmod{p}$ e quindi, poichè $y^{2p'} - 1 \equiv 0$, $4 \equiv 1 \pmod{p}$ che implica che $p = 3$ contrariamente all'ipotesi. Riassumendo:

sia p un numero primo, $p > 3$. Se x, y, z sono numeri interi coprimi tali che $x^{p-1} + y^{p-1} = z^{p-1}$, allora p divide il numero pari fra x ed y e, in particolare, z è dispari e non divisibile per p.
Avendo supposto y pari, possiamo scrivere $y = 2phf$, dove al massimo uno fra h e f è divisibile per p, allora

$$(2phf)^{2p'} = z^{2p'} - x^{2p'} = (z^{p'} + x^{p'})(z^{p'} - x^{p'})$$

Come nel caso precedente $z^{p'} + x^{p'}$ e $z^{p'} - x^{p'}$ non possono essere entrambi divisibili per p. Se

$$z^{p'} \pm x^{p'} = 2p^{2p'} f^{2p'} - 2^{2p'-1} h^{2p'}$$

e dal momento che $(2h)^{2p'} \equiv 1 \pmod{p}$, si ottiene

$$4x^{p'} \equiv 2^{2p'} h^{2p'}, \quad 4x^{p'} \equiv 1 \equiv z^{2p'}, \quad 4 \equiv x^{p'}, \quad 16 \equiv x^{2p'} \equiv 1$$

o $15 \equiv 0 \pmod{p}$, quindi $p = 3$ in contraddizione con l'ipotesi, oppure $p = 5$, che è impossibile perchè l'equazione $X^4 + Y^4 = Z^4$ non ha soluzioni. Se

$$z^{p'} \pm x^{p'} = 2f^{2p'}, \quad z^{p'} - (\pm x^{p'}) = 2^{2p'-1} p^{2p'} h^{2p'}$$

nel caso in cui p non divida f si ha

$$2x^{p'} = 2f^{2p'} - 2^{2p'-1} p^{2p'} h^{2p'}$$

o

$$x^{p'} = f^{2p'} - 2^{2p'-2} p^{2p'} h^{2p'}$$

Allora $x^{p'} \equiv f^{2p'} \equiv 1 \pmod{p}$, in particolare $x \equiv f^2 \pmod{p}$ cioè x è un residuo quadratico. Riassumendo:
sia $p > 3$ un numero primo. Se x, y, z sono coprimi interi, e $x^{p-1} + y^{p-1} = z^{p-1}$ è soddisfatta, allora x è un residuo quadratico (mod p).
Sia $x = f^2 + mp^{2p'}$ con m non divisibile per p, allora si ha:

$$x^{p'} = f^{2p'} + 2^{2p'-2}p^{2p'}h^{2p'} = f^{2p'} + p'f^{2p'-2}mp^{2p'} + ...$$

e quindi

$$2^{2p'-2}p^{2p'}h^{2p'} = p'f^{2p'-2}mp^{2p'} + ...$$

o

$$p'f^{2p'-2}m + ... = 2^{2p'-2}h^{2p'}$$

Dal momento che tutti i termini successivi dello sviluppo di $f^2 + mp^{2p'}$ sono multipli di m, allora m divide $(2h)^{2p'}$. A questo punto Sophie asserisce che, dal momento che ogni fattore di $h^{2p'}$ è una $2p'$-esima potenza, si debba avere $m = k^{2p'}$. Quindi

$$p'f^{2p'-2}k^{2p'} + ... = 2^{2p'}h^{2p'}$$

o

$$4p'f^{2p'-2}k^{2p'} \equiv 2^{2p'}h^{2p'} \equiv 1 \pmod{p}$$

Quindi poichè $k^{2p'} \equiv 1 \pmod{p}$ si ha $4p'f^{2p'-2} \equiv 1 \equiv f^{2p'}$ e perciò $4p' \equiv f^2$ ma $4p' \equiv -2$ e quindi $-2 \equiv f^2 \pmod{p}$. Segue dunque che $x^{p-1} + y^{p-1} = z^{p-1}$ non è risolvibile se -2 non è un residuo quadratico mod p e ciò avviene per tutti i primi p delle forme $8n + 5$, $8n + 7$. Per tutti i primi della forma $8n + 5$, $p - 1$ è divisibile per 4. Dal momento che $X^4 + Y^4 = Z^4$ non ha soluzioni non banali, lo stesso avviene per la data equazione che è nota. Quando p è della forma $8n+7$, allora $p-1$ non è divisibile per 4 e poichè non è sempre divisibile per 3 Sophie pensò di aver dimostrato l'ultimo Teorema di Fermat per l'esponente $p-1$ quando p è come sopra. Purtroppo non possiamo affermare che $m = k^{2p'}$ quindi la sua dimostrazione non è completa.

Gauss rispose alla lettera di Sophie sei mesi dopo e scrisse (Del Centina 2007 pp.7):

> *"Ho letto con piacere le cose che mi avete gentilmente inviato. Sottolineo con molto dispiacere che gli altri impegni di cui mi sto occupando non mi permettano affatto di essere libero al momento e dedicarmi al mio amore per l'aritmetica."*

Non fece commenti o riferimenti alla dimostrazione che lei gli aveva mandato al fine di sottoporla al suo giudizio.

Capitolo 3

Voici ce que j'ai trouvé

3.1 Il teorema di Sophie Germain

* Studi recenti, fra cui quelli condotti da Laubenbacher e Pengelley, hanno portato alla luce che i risultati attribuiti da Legendre a Sophie, in una sua Memoria del 1823, sono solo la punta dell'iceberg di un lavoro ben più articolato ed approfondito. Sophie, infatti, portò avanti un vero e proprio piano di attacco per provare l'ultimo Teorema di Fermat per ogni $n \geq 3$. Il risultato attribuitole da Legendre, conosciuto oggi come Teorema di Sophie Germain, era semplicemente una piccola parte del suo piano, un pezzettino che poteva essere incapsulato ed applicato separatamente dal contesto come un teorema indipendente.

Teorema 3.1.1 (**Teorema di Sophie Germain**). *Per un esponente primo dispari p, se esiste un primo ausiliario θ tale che non ci siano due p-esime potenze consecutive modulo θ diverse da zero o che p non sia esso stesso una p-esima potenza modulo θ, allora in ogni soluzione all'equazione di Fermat $z^p = x^p + y^p$, uno fra x,y e z deve essere divisibile per p^2.*

Il Teorema di Sophie Germain può essere applicato a molti esponenti primi p, producendo un valido primo ausiliario, al fine di eliminare l'esistenza di soluzioni all'equazione di Fermat che coinvolgono numeri non divisibili per l'esponente p. Questa eliminazione è oggi chiamata Caso 1 dell'ultimo Teorema di Fermat.
Nell'enunciato del Teorema di Sophie Germain, quando si considera se due numeri siano "consecutivi modulo θ", non si intende che la loro differenza sia esattamente 1, ma piuttosto che essi siano congruenti ad 1 modulo θ; questo

*Per il Capitolo 2 seguiamo i testi [7] [2] [3]

si può determinare osservando i residui dei due numeri e valutando se siano consecutivi o meno [†].

3.1.1 Esempio

Scegliamo $p = 3$ e $\theta = 13$, entrambi primi e verifichiamo le due ipotesi del Teorema di Sophie Germain. Dobbiamo trovare tutti i residui diversi da zero della terza potenza modulo 13. Dobbiamo considerare solo i cubi dei possibili residui modulo 13, cioè i cubi dei numeri da 0 a 12 dal momento che tutti gli altri numeri ci fornirebbero solo delle ripetizioni cicliche e dal momento che vogliamo solo dei risultati modulo θ diversi da 0 possiamo ometterlo.

Residui	1	2	3	4	5	6	7	8	9	10	11	12
Cubi	1	8	27	64	125	216	343	512	729	1000	1331	1728
Residui cubici	1	8	1	12	8	8	5	5	1	12	5	12

I residui di $8^3 = 512 \pmod 3$ possono essere ottenuti dividendo 512 per 13 con resto 5 ma ci sono modi molto più veloci per ottenerli dal momento che utilizzando la congruenza ogni numero può essere facilmente rimpiazzato con qualsiasi numero congruente ad esso. Per esempio, possiamo facilmente calcolare che $8^3 = 64 \cdot 8 \equiv (-1) \cdot (-5) = 5 \pmod{13}$ [‡].
Osservando i nostri numeri, ci chiediamo ora quale delle due ipotesi del Teorema di Sophie Germain siano soddisfatte. Infatti nessuna coppia di residui cubici diversi da zero $1, 5, 8, 12$ modulo 13 sono consecutivi e nemmeno $p = 3$ si trova fra i residui.
Il Teorema di Sophie prova allora che ogni soluzione all'equazione di Fermat $z^3 = x^3 + y^3$ dovrebbe avere uno fra x, y o z divisibile per $p^2 = 9$.
Tornando al trattato di Legendre, subito dopo il teorema egli fornisce una tavola che verifica le ipotesi di quest'ultimo per $p < 100$. Da questa tavola si assume che Sophie abbia sviluppato lei stessa una tavola dei residui al fine di verificare ed applicare il suo teorema.
Legendre, nella sua memoria, prosegue sviluppando mezzi teorici al fine di verificare le ipotesi del Teorema di Sophie Germain e spinge l'analisi oltre al in modo da dimostrare che ogni soluzione dell'equazione di Fermat sarebbe costituita da numeri molto estesi.
Per più di due secoli si è pensato erroneamente che questo teorema e la sua

[†] I residui 0 e $\theta - 1$ dovrebbero essere considerati consecutivi nel modo in cui rappresentano i numeri attraverso la congruenza. Comunque, dal momento che siamo interessati unicamente ai numeri con residui diversi da 0, questa complicazione non sorge nel nostro caso.

[‡] $8^3 = 64 \cdot 8 \equiv 12 \cdot 8 \equiv -1 \cdot -5$

applicazione per esponenti minori di 100 costituissero l'intero contributo di Sophie al Teorema di Fermat.

3.2 La lettera del 1819

Il 12 Maggio 1819, Sophie scrisse una lettera dalla sua casa parigina a Gauss, che si trovava a Gottinga, all'interno della quale descriveva il suo lavoro sull'ultimo Teorema di Fermat. La lettera, come già abbiamo detto nel primo capitolo, ci offre una finestra sull'interazione fra Sophie e Gauss nel contesto della Teoria dei Numeri a distanza di quindici anni dall'inizio della loro corrispondenza. Ci mostra come Sophie ai tempi considerava il suo lavoro sull'ultimo Teorema di Fermat nel contesto più ampio della sua ricerca matematica e, nello specifico, all'interno della sua interazione con Gauss. La lettera inoltre ci fornisce i dettagli sui suoi progressi al fine di provare l'ultimo Teorema di Fermat e ci permette di confrontarlo con il teorema attribuitole da Legendre nel 1823.
Riprendiamo ora la lettera (Laubenbacher, Pengelley 2010 pp. 22):

> *"Ecco cosa ho trovato: [...].*
> *L'ordine nel quale i residui (le potenze uguali agli esponenti) sono distribuiti nella sequenza dei numeri naturali, determina i divisori necessari che appartengono ai numeri fra i quali uno stabilisce, non solo l'equazione di Fermat, ma molte altre equazioni analoghe.*
> *Prendiamo ora l'equazione di Fermat, che è la più semplice di quelle che consideriamo qui. Abbiamo quindi* $z^p = x^p + y^p$*, p numero primo. Sostengo che, se questa equazione è possibile, allora ogni numero primo della forma* $2Np + 1$ *(N intero), per il quale non ci sono due potenze residue p-esime nella sequenza dei numeri naturali, necessariamente divide uno dei numeri x, y, z."*

Sophie qui considera la congruenza modulo un primo ausiliario della forma $\theta = 2Np+1$ che non ha potenze residue p-esime diverse da zero. Nonostante la forma di θ non sia necessaria per il ragionamento successivo Sophie sa che solo i moduli primi della forma $\theta = 2Np + 1$ possono avere potenze residue p-esime non consecutive diverse da zero e che, implicitamente, anche Gauss ne è a conoscenza. Quindi si restringe, senza menzionarlo, a considerare solo i primi di questa forma.

> *"Questo è chiaro dal momento che l'equazione* $z^p = x^p + y^p$ *soddisfa la congruenza* $1 \equiv r^{sp} - r^{tp}$ *dove r rappresenta una radice*

primitiva e s e t sono interi.[...]
Segue che, se ci fossero infiniti numeri di questo tipo, l'equazione sarebbe impossibile.
Non sono mai riuscita a giungere all'infinito, anche se ho spinto i limiti piuttosto in là, mediante un metodo di prove troppo lungo per essere qui descritto. Ancora non mi azzardo ad asserire che, per ogni valore di p, non ci sia un limite oltre il quale tutti i numeri della forma $2Np + 1$ abbiano due potenze residue p-esime consecutive nella sequenza dei numeri naturali. Questo è il caso che concerne l'equazione di Fermat.
Potete facilmente immaginare, Monsieur, che sono riuscita a dimostrare che questa equazione non sia possibile, fatta eccezione per i numeri la cui dimensione fa impallidire l'immaginazione; perchè essa è anche soggetta a molte altre condizioni, che non ho il tempo di elencare a causa di tutti i dettagli necessari per stabilirne il successo. Ma tutto ciò non è sufficiente; abbiamo bisogno dell'infinito, non basta semplicemente il "molto grande"."

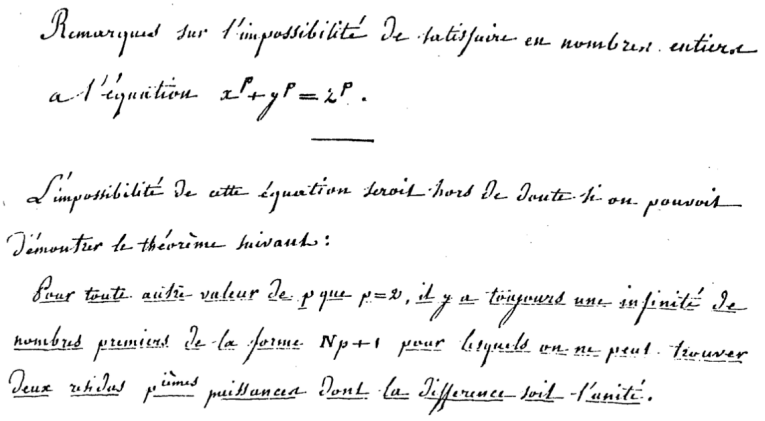
Qui Sophie usa due fatti riguardanti i residui modulo primo θ:

- Quando il modulo è primo si può dividere, in aritmetica modulare, per ogni numero con residui diversi da zero. Quindi se nessuno fra x, y, z fosse divisibile per θ, allora la divisione modulare dell'equazione di Fermat per x^p o y^p produrrebbe due potenze residue p-esime consecutive diverse da zero.
- Per un modulo primo c'è sempre un numero, chiamato radice primitiva del modulo, tale che ogni numero con residui diversi da zero è congruente ad una potenza della radice primitiva.

3.3 Il grande piano

3.3.1 Il piano di Sophie per dimostrare l'ultimo Teorema di Fermat

Abbiamo avuto modo di vedere, analizzando la lettera precedente, che il grande piano di Sophie per dimostrare l'ultimo Teorema di Fermat per un esponente p si basa sullo sviluppo di metodi al fine di corroborare la seguente condizione per infiniti primi ausiliari della forma $\theta = 2Np + 1$


Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation $x^p+y^p=z^p$.

L'impossibilité de cette équation seroit hors de doute si on pouvoit démontrer le théorème suivant:

Pour toute autre valeur de p que $p=2$, il y a toujours une infinité de nombres premiers de la forme $Np+1$ pour lesquels on ne peut trouver deux nombres pûmes puissances dont la difference soit l'unité.

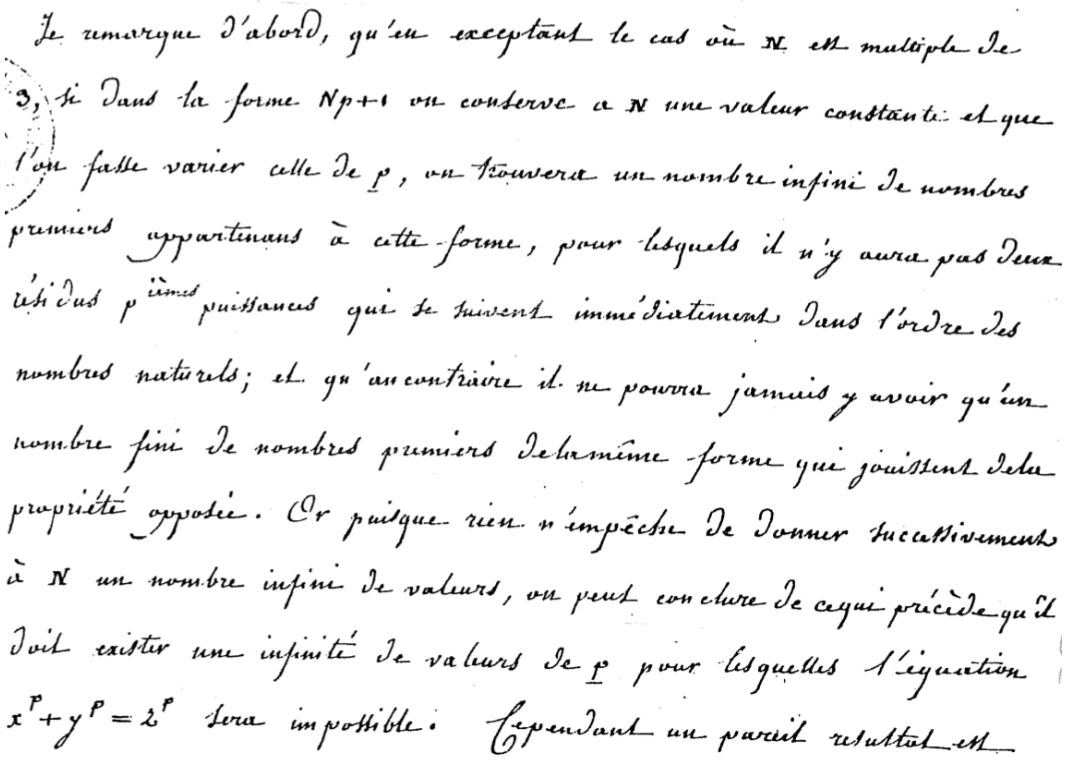
Figura 3.1: Manoscritto non datato di Sophie intitolato: *"Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation* $x^p + y^p = z^p$*"*

Condizione N-C (Non-Consecutività) Non esistono due potenze residue p-esime consecutive diverse da zero modulo θ.

Nel manoscritto *Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation* $x^p + y^p = z^p$ Sophie sostiene che per ogni N fissato (eccetto quando N è un multiplo di 3, per il quale mostra che la condizione N-C non si verifica mai) esisteranno solo un numero finito di numeri p per i quali l'ausiliare $\theta = 2Np + 1$ non soddisfi la condizione N-C. La maggior parte del manoscritto di Sophie è dedicata a supportare questa tesi; nonostante non sia stata in grado di portarla a compimento, il suo lavoro è stato provato molti anni dopo, nel 1894, da Ernst Wendt [§] in *Arithmetische Studien über den letzten Fermatschen Satz, welcher aussagt daß die Gleichung* $a^n = b^n + c^n$ *für* $n > 2$ *in ganzen Zahlen nicht aufslösbar ist (Studi aritmetici sull'ultimo Teorema di Fermat, che afferma che l'equazione* $a^n = b^n + c^n$ *non è risolubile nei numeri interi per* $n > 2$*)* (anche se non abbiamo indizi che egli fosse a conoscenza del lavoro di Sophie).
C'è una grande differenza nell'analizzare la condizione N-C per un fissato N rispetto ad analizzarla per un fissato p. Per dimostrare il Teorema di Fermat per un p fissato, è necessario verificare la condizione N-C per infiniti N mentre l'approccio di Sophie consiste nel fissare N e verificare la condizione N-C per un numero finito di p.

[§]Adolf Ernst Wendt (1872–1946), matematico ed esperto di nautica tedesco

Esempio Consideriamo ora il caso $N = 1$, cioè, quando $\theta = 2p + 1$ è anche esso un numero primo (oggi chiamato primo di Germain). Sophie era a conoscenza del fatto che ci sono sempre esattamente $2N$ potenze residue p-esime diverse da zero modulo un ausiliario primo della forma $\theta = 2Np + 1$ e, in questo caso, i numeri 1 e $2p = \theta - 1 \equiv -1$ sono le sole potenze residue p-esime diverse da zero e la condizione N-C è automaticamente verificata. Per $N > 1$ con più potenze residue p-esime diventerebbe più difficile andarle ad analizzare. Ricordiamo inoltre che la la condizione del Teorema di Sophie, che p non sia esso stesso una potenza p-esima modulo θ, è ovviamente verificata in questo caso. Il Teorema di Sophie Germain verifica automaticamente questo caso ogni volta che $2p + 1$ è primo. Questo probabilmente ci chiarisce come mai alcuni autori abbiano pensato che il Teorema di Sophie Germain si occupi solo di primi di Germain come ausiliari.



Je remarque d'abord, qu'en exceptant le cas où N est multiple de 3, si dans la forme Np+1 on conserve a N une valeur constante et que l'on fasse varier celle de p, on trouvera un nombre infini de nombres premiers appartenans à cette forme, pour lesquels il n'y aura pas deux résidus $p^{\text{ièmes}}$ puissances qui se suivent immédiatement dans l'ordre des nombres naturels; et qu'au contraire il ne pourra jamais y avoir qu'un nombre fini de nombres premiers de la même forme qui jouissent de la propriété opposée. Or puisque rien n'empêche de donner successivement à N un nombre infini de valeurs, on peut conclure de ce qui précède qu'il doit exister une infinité de valeurs de p pour lesquelles l'équation $x^p + y^p = z^p$ sera impossible. Cependant un pareil resultat est

Figura 3.2: Introduzione *Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation* $x^p + y^p = z^p$[11]

3.3.2 Stabilire la Condizione di Non Consecutività per ogni N

Al fine di stabilire la condizione N-C per vari N e p, Germain si lancia in una analisi estesa sulle consequenze delle potenze residue p-esime consecutive diverse da zero modulo un primo $\theta = 2Np+1$ (con N che non può mai essere un multiplo di 3).
La sua analisi comprende tutti i numeri naturali per p, non solo i numeri primi e ciò e fondamentale in relazione alla forma di θ dal momento che Sophie intende applicare l'induzione matematica su N e, infine, spiegare nel dettaglio la sua idea su come dovrebbe svolgersi una dimostrazione per induzione.
In ogni parte del suo scritto impiega la nozione e la notazione di congruenza introdotta da Gauss e utilizza scrupolosamente la comprensione del fatto che le $2Np$ unità moltiplicative modulo θ sono cicliche [¶], generate da una radice primitiva $2Np$-esima dell'unità, e le permettono di intraprendere una analisi dettagliata della posizione relativa delle potenze p-esime diverse da zero (cioè le $2N$-esime radici di 1) fra i residui.
Sophie è inoltre consapevole che i sottogruppi del gruppo delle unità sono ciclici (esprimiamo questo concetto utilizzando termini moderni), conosce le relazioni che intercorrono fra essi e le utilizza dettagliatamente. Nel corso della sua analisi deduce che in molti casi l'esistenza di una p-esima potenza residua consecutiva diversa da zero porterebbe 2 ad essere una p-esima potenza modulo θ e, di conseguenza, conclude che la Condizione N-C è valida sotto la seguente ipotesi:

Condizione 2-N-p Il numero 2 non è una p-esima potenza residua modulo θ.

Questa ipotesi è sempre una condizione necessaria affinchè sia valida la Condizione N-C, perchè se 2 è una potenza p-esima, allora 1 e 2 sono potenze p-esime consecutive diverse da zero. Fare questa assunzione non è quindi una restrizione e Sophie valuta se la Condizione 2-N-p sia sufficiente ad assicurare la condizione N-C.
Sempre assumendo questa ipotesi e la condizione sempre necessaria che N non sia un multiplo di 3, l'analisi di Sophie mostra inizialmente che se esistono due potenze residue p-esime consecutive diverse da zero allora invertendole, sottraendo loro -1 o iterando combinazioni di queste due trasformazioni, può ottenere più coppie di potenze residue p-esime diverse da zero.

[¶]Un gruppo G è **ciclico** se esiste un elemento g del gruppo (detto generatore) tale che G è l'insieme delle potenze di g ad esponente intero, in simboli $G = \{g^n : \quad n \in \mathbb{Z}$

Sophie dimostra che, sotto l'assunzione costante che 2 non è un potenza p-esima residua modulo θ, questo processo di trasformazione produce almeno sei coppie totalmente disgiunte e, dal momento che ci sono precisamente $2N$ potenze residue p-esime diverse da zero modulo θ, dimostra immediatamente la Condizione N-C per tutti i primi ausiliari θ con $N = 1, 2, 4, 5$ (fintanto che p soddisfa la Condizione 2-N-p).
Sophie continua con una analisi ancora più dettagliata di queste coppie permutate di potenze residue p-esime consecutive (sempre assumendo la condizione 2-N-p) per verificare la Condizione N-C per $N = 7$ (escludendo ovviamente $p = 2$) e $N = 8$.
A questo punto Sophie spiega il suo piano generale per continuare il metodo di analisi per N maggiori e di come userebbe l'induzione su N per ogni p simultaneamente. Sophie discute che l'esistenza di potenze residue p-esime consecutive diverse da zero porterebbe ad una coppia di potenze residue p-esime consecutive, x, $x+1$ per le quali x è congruente ad una potenza dispari (necessariamente inferiore a $2N$) di $x+1$, sostiene che si dovrebbero analizzare i casi dell'espansione binomiale della potenza di $x+1$, al variare di N, per arrivare alla contraddizione desiderata e porta avanti un calcolo completo e dettagliato per $N = 10$ come esempio specifico del suo metodo di induzione.

3.3.3 La verifica della condizione 2-N-p

Sophie sottolinea che se 2 fosse un p-esima potenza modulo $\theta = 2Np + 1$ ciò significherebbe che $2^2N \equiv 1 \pmod{\theta}$ (dal momento che la struttura moltiplicativa è ciclica). Chiaramente per N fissato, questo succede solo per un numero finito di p e Sophie determina facilmente queste eccezioni per $N = 10$ calcolando e fattorizzando manualmente ciascun $2^{2N} - 1$ e osservando se uno fra questi fattori primi è della forma $2Np + 1$.

Esempio $N = 7$

$$2^{14} - 1 = 3 \cdot 43 \cdot 127 = 3 \cdot (14 \cdot 3 + 1) \cdot (14 \cdot 9 + 1)$$

E' evidente che per $p = 3, 9$ la Condizione 2-N-p, per ogni N, non è verificata. Sophie presenta poi una tavola riassuntiva di tutti i suoi risultati che verificano la Condizione N-C per primi ausiliari θ per valori di $N \leq 10$ e primi $2 < p < 100$ e scrive che può facilmente essere estesa oltre. Tolto il caso $\theta = 43 = 14 \cdot 3 + 1$, gli unici altri primi ausiliari nella sua tabella che devono essere omessi sono $\theta = 31 = 10 \cdot 3 + 1$, che non verifica la condizione 2-N-p e $\theta = 61 = 20 \cdot 3 + 1$ che è una eccezione nella sua analisi della Condizione N-C per $N = 10$. Ciascuno N della sua tabella possiede almeno 5 primi p

con $2 < p < 100$ per i quali $\theta = 2Np + 1$ è anche esso primo e soddisfa la Condizione N-C.
Nonostante il numero di p che devono essere esclusi dalla Condizione 2-N-p possa apparire limitato per ogni N, non abbiamo modo di verificarlo. Sophie in particolare non discute questo problema per la Condizione 2-N-p e, senza una limitazione, non è chiaro se questo metodo possa veramente dimostrare il Teorema di Fermat.

3.3.4 I ruoli di N e p

Dimostrare la Condizione N-C per ogni N, ciascuno per un numero finito di p, non risolve immediatamente il problema di Fermat.
Ciò di cui abbiamo bisogno, per ogni primo p fissato, è che la Condizione N-C sia verificata per infiniti N, non il viceversa. Infatti $p = 3$ dovrebbe essere escluso dalla verifica della Condizione N-C per tutti gli N sufficientemente grandi, in tal caso il metodo di Sophie non proverebbe l'ultimo Teorema di Fermat per $p = 3$. Sophie è consapevole di questa complicazione, del fatto che i suoi risultati non risolvano completamente il problema e di non aver dimostrato la congettura di Fermat per ciascun esponente predeterminato ma, allo stesso tempo, è convinta che i suoi prerequisiti reggano e i suoi risultati per $N \leq 10$ supportano questa idea. Finora infatti l'unico primo dispari escluso è $p = 3$ per $N = 10$.
Il commento finale di Sophie è che, quando si raggiungono valori di N ancora più grandi, c'è sempre una quantità non trascurabile di valori di p per i quali la Condizione N-C non vale. Se questa quantità di numeri fosse limitata da un certo K per ogni N, che è effettivamente ciò che lei sostiene, allora si potrebbe concludere che il suo metodo arrivi a provare l'ultimo Teorema di Fermat per tutti i K valori di p nonostante non si sappia di preciso di quali valori stiamo parlando. Lei stessa sostiene che ciò proverebbe il teorema per infiniti p anche se non per un valore di p predeterminato.

3.4 Il fallimento del grande piano

Sophie era a conoscenza del fatto che il suo piano non funzionasse?
Per rispondere a questa domanda possiamo esaminare la sua corrispondenza con Gauss ed una lettera che scrisse a Legendre.
Una indicazione del fatto che il metodo di Sophie, al fine di dimostrare l'ultimo Teorema di Fermat, non funzionasse, anche se non viene fatto il suo nome, si trova nel lavoro di Guglielmo Libri.
E' piuttosto complicato tenere traccia dei lavori di Libri e della loro sequenza

cronologica. In parte perchè Libri presentò o pubblicò vari lavori tutti con lo stesso titolo e in parte perchè alcuni di questi furono pubblicati più e più volte. Nel 1829 Libri pubblicò una memoria intitolata *Mémoire sur la théorie des nombres*, ripubblicata successivamente parola per parola come tre distinte opere nel *Crelle's Journal* [‖]. La memoria termina con uno studio di Libri sul numero di soluzioni delle varie congruenze riguardanti l'ultimo Teorema di Fermat. Fra le altre cose Libri mostra che per gli esponenti 3 e 4 ci può essere al massimo un numero finito di primi ausiliari soddisfacenti la Condizione N-C. Libri inoltre sostiene che il suo metodo proverà lo stesso per esponenti più grandi e sottolinea esplicitamente come il suo approccio dimostri come i tentativi altrui di dimostrare l'ultimo Teorema di Fermat trovando infiniti ausiliari di questo tipo fossero vani. Libri scrive inoltre che tutti i risultati da lui ottenuti erano già presenti in due memorie precedenti del 1823 e del 1825 pubblicate dall'Accademia delle Scienze di Parigi. L'opera di libri del 1825 fu pubblicata anche nel 1822/1828 con lo stesso titolo di quella del 1829 rendendo il tutto più difficile da distinguere.

3.4.1 Gauss, Legendre e Libri

Sophie ha mai saputo da Libri, o in altro modo, che il suo grande piano per dimostrare l'ultimo Teorema di Fermat avrebbe potuto non funzionare?
Nel 1819 risultava entusiasta nella sua lettera a Gauss riguardante il suo metodo per dimostrare l'ultimo teorema di Fermat basato sul lavoro estensivo esemplificato dal manoscritto *Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation* $x^p + y^p = z^p$. Sappiamo inoltre che nel 1823 Legendre aveva scritto la sua memoria citando il Teorema di Germain ma non menzionando affatto il metodo per trovare infiniti ausiliari primi su cui Sophie si era assai concentrata. E' probabile pensare che Sophie venne a conoscenza del fatto che Libri padroneggiasse il suo metodo poichè si erano conosciuti ed avevano instaurato un solido legame di amicizia a partire dal 1825 così come una frequente corrispondenza. Sembra probabile che fra il 1819 e il 1825 Sophie abbia realizzato, leggendo il lavoro di Libri, che il suo grande piano non fosse destinato a funzionare.

[‖]Il *Journal für die reine und angewandte Mathematik (Rivista di matematica pura e applicata)*, meglio noto come *Crelle's Journal*, è una rivista di matematica tedesca, la più antica tuttora esistente. Fu fondata a Berlino nel 1826 dal matematico e ingegnere tedesco August Leopold Crelle, che la diresse per i primi 52 volumi, fino al 1855. In seguito ne sono stati direttori, tra gli altri, Karl Weierstrass e Leopold Kronecker. Ha pubblicato molti articoli teorici di famosi matematici, tra cui i lavori di Abel e di Eisenstein. È stampata in tre lingue: tedesco, inglese e francese.

3.4.2 La dimostrazione di Legendre

Dalla lettera di Sophie a Gauss del 1819 si evince come lei credesse che per ogni primo $p > 2$ ci fossero infiniti primi ausiliari soddisfacenti la condizione N-C mentre da una lettera (non datata) a Legendre Sophie dimostra il contrario per $p = 3$.
Sophie inizia la sua lettera di tre pagine ringraziando Legendre per averle detto il giorno precedente che si può dimostrare che tutti i numeri della forma $6a + 1$ maggiori di 13 hanno una coppia di residui cubici consecutivi diversi da zero. Questo significa dire che per $p = 3$ non ci sono primi ausiliari della forma $\theta = 2Np + 1$ che soddisfino la condizione N-C oltre $N = 1, 2$. Questa affermazione sembra contraddire il successo di Sophie nel manoscritto *Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation* $x^p + y^p = z^p$ nel provare la condizione N-C per tutti i numeri primi p dispari con $N = 1, 2, 4, 5, 7, 8, 10$ ma, leggendo più attentamente, si vede che questo funziona solo per $N = 1, 2$ e, una volta considerate queste eccezioni, cioè quando θ non è un numero primo o la Condizione 2-N-p non vale o quando si esclude $p = 3$ per $N = 10$, allora l'affermazione di Legendre è vera. Sophie provvedette subito a scrivere una dimostrazione per Legendre.

Il grande piano non funziona per p=3 Per ogni primo θ della forma $6a+1$, con $\theta > 13$, esistono residui cubici consecutivi diversi da zero. In altre parole la condizione N-C non vale per $\theta = 2Np + 1$ con $p = 3$ e $N > 2$,così i soli ausiliari primi validi per $p = 3$ per la condizione N-C sono $\theta = 7$ e 13.

Dimostrazione Consideriamo solo i residui diversi da zero $1, ..., 6a$. Supponiamo che la Condizione N-C sia verificata (cioè non ci siano coppie consecutive di residui cubici fra queste) e supponiamo non ci siano coppie di residui cubici la cui differenza è 2 **. Ci sono $2a$ residui cubici distribuiti fra i $6a$ residui e, al fine di separare adeguatamente i $2a$ residui cubici, devono esserci $2a-1$ intervalli contenenti i $4a$ residui non cubici diversi da zero. Ogni intervallo contentente almeno 2 residui non cubici. Dal momento che ognuno di questi $2a - 1$ intervalli ha almeno 2 residui non cubici, utilizzando $4a - 2$ residui non cubici, c'è flessibilità nell'allocare i 2 rimanenti dei $4a$ residui non cubici. Ciò significa che tutti gli intervalli devono contenere esattamente 2 residui non cubici fatta eccezione per un singolo intervallo con 4 residui non cubici o due intervalli con 3 residui non cubici ciascuno.
Siamo già a conoscenza degli specifici residui cubici 1 e 8 ($\theta = 6a+1 > 13$) e

** qui parliamo letteralmente di residui e non di classi di congruenza. Con questa assunzione 1 e -1, che sono classi di congruenza cubica la cui differenza è 2 ma non sono residui ed i loro residui non hanno differenza 2, non violano la nostra assunzione

sappiamo che 2 e 3 non possono essere residui cubici per le nostre assunzioni precedenti. Se 4 fosse un residuo cubico allora lo sarebbe anche $8/4 = 2$ (alternativamente $8 - 4 = 4$ violerebbe la condizione N-C). Sophie scrive che la sequenza di residui cubici $1, 5, 8, 1, ..., 6a-10, 6a-7, 6a-4, 6a$ deve essere necessariamente questa dal momento che i residui cubici sono disposti simmetricamente modulo $\theta = 6a + 1$ e si conoscono le ampiezze degli intervalli. E' da sottolineare che i due intervalli eccezionali devono essere di tre numeri mancanti ciascuno all'inizio e alla fine della sequenza.
Per verificare che ciò è assurdo consideriamo inizialmente per $\theta \leq 6{\cdot}5{+}1 = 31$, il residuo cubico $3^3 = 27$. Notiamo che contraddice la sequenza precedente dal momento che è più piccolo di $6a \leq 30$ ma non è congruente a 2 modulo 3 come avviene per tutti i residui inferiori della lista fatta eccezione per 1. L'unico altro primo $\theta > 13$ è 19 per il quale $4^3 = 64$ ha residuo 7 che non è nella lista.
Perciò una delle due assunzioni iniziali deve essere falsa. Se N-C non è vera allora abbiamo terminato. Consideriamo quindi il fallimento dell'altra condizione (che non esistono due coppie di residui cubici la cui differenza è 2). Siano r ed r' residui cubici con $r - r' = 2$. Sia x una radice primitiva dell'unità modulo θ (cioè un generatore del gruppo ciclico delle unità moltiplicative rappresentate dai residui primi diversi da zero). Dobbiamo allora avere $2 \equiv x^{3f\pm1}$, cioè la potenza di x che rappresenta 2 che non può essere divisibile per 3 dal momento che 2 non è un residuo cubico.
Ora consideriamo $r + r'$. Affermiamo che $r + r' \not\equiv 0$ dal momento che se avessimo $r + r' \equiv 0$ allora $2 = r - r' \equiv r - (-r) = 2r$ e quindi $r \equiv 1$ e, di conseguenza, $r = 1$ andrebbe a violare $r - r' = 2$. Qui è importante sottolineare che stiamo lavorando con residui r ed r' entrambi non negativi e più piccoli di $6a + 1$ e quindi le richieste che $r \equiv 1$ ed $r - r' = 2$ sono incompatibili dal momento che non ci sono $0 < r,r' < 6a + 1$ per i quali si possano avere $r \equiv 1$ e $r - r' = 2$; questo è collegato all'osservazione iniziale che le classi 1 e -1 non violino la nostra condizione iniziale.
Dal momento che $r + r' \not\equiv 0$ è una unità e quindi congruente ad una potenza x^m. Se m fosse divisibile per 3 allora la congruenza $r + r' \equiv x^m$ sarebbe una differenza di residui cubici e quindi un altro residuo cubico, andando così a violare la Condizione N-C. Abbiamo così $r + r' \equiv x^{3g\pm1}$. Il segno di $3f \pm 1$ deve essere concorde con quello di $3g \pm 1$ perchè, se così non fosse, $r + r' \equiv x^{3g\mp1}$ e $r^2 - r'^2 = (r - r')(r + r') \equiv 2x^{3g\mp1} \equiv x^{3f\pm1}x^{3g\mp1} = x^{3(f+g)}$ che dà ancora una volta un residuo cubico uguale ad un altro residuo cubico e cioè una contraddizione.
Infine combiniamo $r - r' \equiv x^{3f\pm1}$ con $r + r' \equiv x^{3g\pm1}$ per ottenere $2r \equiv x^{3f\pm1} + x^{3g\pm1}$ e, di conseguenza, $x^{3f\pm1}r \equiv x^{3f\pm1} + x^{3g\pm1}$ risultando in $r \equiv 1 + x^{3(g-f)}$ ancora una volta contraddicendo la Condizione N-C. Quindi l'assunzione ini-

ziale della Condizione N-C deve essere falsa.
c.v.d.

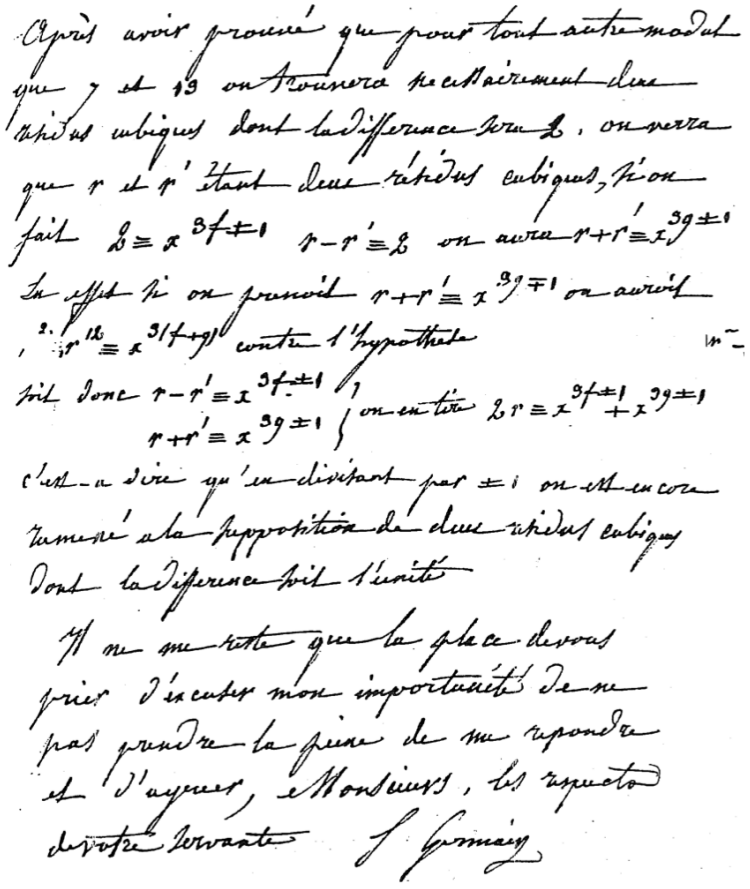


Figura 3.3: Lettera non datata a Legendre sulla dimostrazione che il grande piano non funziona per $p = 3$

3.4.3 Il metodo di Legendre per stabilire la Condizione N-C

Analizziamo ora il metodo di Legendre per stabilire la Condizione N-C. Sebbene egli ottenga delle conclusioni molto simili a quelle di Sophie l'approccio è molto diverso come anche la sua notazione. Legendre usa n per indicare l'esponente primo (mentre Sophie utilizzava p) (Laubenbacher, Pengelley 2010 pp.38-39):

> *"Si può anche dimostrare che quando si ha* $\theta = 4n + 1$ *queste due condizioni sono soddisfatte. In questo caso ci sono 4 residui* r *che si ricavano dall'equazione* $r^4 - 1 = 0$*, che si spezza in altre due* $r^2 - 1 = 0$*,* $r^2 + 1 = 0$*. La seconda, dalla quale si ricava il numero* μ[††] *è facile da risolvere; perchè si sa che, nel caso in questione,* θ*, che può essere scritto nella forma* $a^2 + b^2$*, è sufficiente a determinare* μ *usando la condizione che* $a + b\mu$ *è divisibile per* θ*; così omettendo multipli di* θ *si può porre* $\mu^2 = -1$ *ed i quattro valori di* r *diventano* $r = \pm(1, \mu)$*. Da ciò si vede che la condizione* $r' = r + 1$ *può essere soddisfatta solo nel caso* $\mu = 2$ *dal quale si hanno* $\theta = 5$ *ed* $n = 1...$*"*

Legendre non usa l'idea o la notazione di congruenza utilizzata da Sophie e, a sua volta, adottata da Gauss. Focalizza la sua attenzione sulle radici dell'unità dall'equazione che le definisce e non fa uso della Condizione 2-N-p ma è interessato alle conseguenze della forma lineare $4n + 1$.
Nel caso successivo, per $N = 4$ e $\theta = 8n + 1$, si concentra ancora una volta sulle radici dell'"equazione unità" e sostiene che in questo caso il primo $8n+1$ deve avere la forma quadratica $a^2 + 2b^2$ entrando in una discussione relativa alle radici dell'"equazione unità".
Legendre, a differenza di Sophie, che aveva lavorato sui casi $N = 1, 2, 4, 5$ in un colpo solo, costruisce la sua analisi sulle radici $2N$-esime dell'unità un valore alla volta a partire da $N = 1$.

3.5 La grande dimensione delle soluzioni

Nonostante Sophie credesse che il suo grande piano fosse in grado di dimostrare l'Ultimo Teorema di Fermat per infiniti esponenti primi, riconosceva il fatto di non averlo applicato ancora ad un singolo esponente. Scrisse quindi che sperava almeno di poter dimostrare per un specifico esponente che ogni soluzione possibile dell'equazione di Fermat sarebbe dovuta essere estremamente grande.
Nelle ultime quattro pagine di *Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation* $x^p + y^p = z^p$ Sophie stabilisce, prova ed applica un teorema inteso a dimostrare ciò. Di fatto parla di questo teorema due volte, la prima all'inizio del manoscritto dove ricorda che ogni ausiliario primo soddisfacente la Condizione N-C dovrà per forza dividere uno dei numeri x, y, z dell'equazione di Fermat ma osserva che per avere una limitazione in-

[††] μ nella lettera è la radice primitiva quarta dell'unità che genera le quattro potenze n-esime

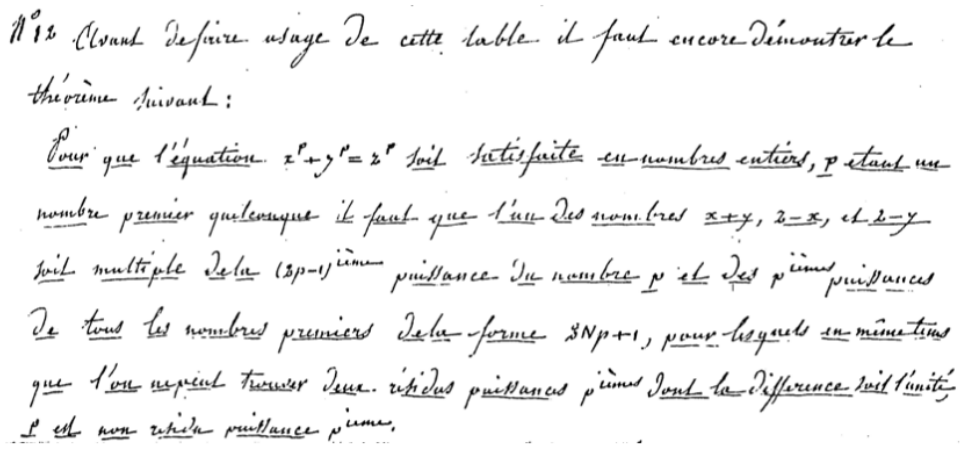


Figura 3.4: Parte finale del manoscritto *Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation* $x^p + y^p = z^p$

feriore significativa sulle soluzioni, si dovrebbe impiegare un ausiliario primo molto grande. Poi scrive (Laubenbacher, Pengelley 2010 pp.42):

> *"Fortunatamente si può evitare questo impedimento utilizzando il seguente teorema"*

Teorema 3.5.1 (**La grande dimensione delle soluzioni**). *Affinchè l'equazione* $x^p + y^p = z^p$ *sia soddisfatta da numeri naturali, essendo* p *un qualsiasi numeri primo, è necessario che uno fra* $x + y$, $z - y$ *e* $z - x$ *sia un multiplo di una* $(2p-1)$*-esima potenza del numero* p *e della* p*-esima potenza di tutti i numeri primi della forma* $[\theta =]Np + 1$ *per il quale non si possono trovare contemporaneamente due potenze* p*-esime residue [mod* θ*]* *la cui differenza sia uno e* p *non sia una potenza* p*-esima residua [mod* θ*]* [‡‡].

Probabilmente è questo il teorema al quale Sophie si stava riferendo quando scrisse a Gauss che ogni possibile soluzione sarebbe stata data da numeri "*la cui dimensione spaventa l'immaginazione*". Precedentemente in questo manoscritto Sophie scrive che applicherà il teorema per diversi valori di p usando la sua tabella. Menziona anche che già solo per $p = 5$ i possibili ausiliari primi $\theta = 11, 41, 71, 101$ mostrano che ogni soluzione dell'equazione di Fermat dovrebbe avere almeno 39 cifre.

[‡‡] il teorema richiede implicitamente che esista almeno un θ di questo tipo

3.5.1 La dimostrazione di Sophie del Teorema sulla dimensione delle soluzioni

Le prime due ipotesi del Teorema sulla dimensione delle soluzioni sono: la Condizione N-C, da lei già studiata precedentemente per il suo Grande Piano, e la

Condizione p-N-p (p non è una potenza p-esima)
p non è una potenza p-esima residua modulo θ.

Questa precisamente è la seconda ipotesi del Teorema di Sophie Germain.

L'equazione di Barlow-Abel

La dimostrazione inizia implicitamente con il fatto che la Condizione N-C implica che uno fra x, y, z debba essere divisibile per θ. Riprendendo le parole di Sophie (Laubenbacher, Pengelley (2010) pp.43):

> *"Assumendo l'esistenza di un singolo numero soggetto a questa doppia condizione, dimostrerò che il numero x, y, z dell'equazione $x^p + y^p = z^p$ che è un multiplo di θ deve essere necessariamente un multiplo di p^2.*
> *Infatti se i numeri x, y, z sono coprimi, allora i numeri*
> *$x + y$ e $x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 +$ etc*
> *$z - y$ e $z^{p-1} - z^{p-2}y + z^{p-3}y^2 - z^{p-4}y^3 +$ etc*
> *$z - x$ e $z^{p-1} - z^{p-2}x + z^{p-3}x^2 - z^{p-4}x^3 +$ etc*
> *non possono avere altri divisori comuni fatta eccezione per p."*

Per la prima coppia questa ultima affermazione può essere vista denotando l'espressione a destra sulla prima riga con $\phi(x, y)$. Se un qualche primo q diverso da p divide entrambi i numeri allora $y = -x \pmod{q}$, dal quale abbiamo $\phi(x, y) \equiv px^{p-1} \pmod{q}$. Allora x e $x+y$ sono entrambi divisibili per q, in contraddizione con l'ipotesi che x e y siano coprimi. Questo esclude tutti i primi eccetto p come potenziali comuni divisori di $x + y$ e $\phi(x, y)$.

> *"Quindi se tre numeri x, y e z sono coprimi con p, allora si avrebbe, con $z = lr \quad x = hn \quad y = vm$:*

$$x + y = l^p \quad x^{p-1} - x^{p-2} + x^{p-3}y^2 - x^{p-4}y^3 + etc = r^p$$

$$z - y = h^p \quad z^{p-1} + z^{p-2} + z^{p-3}y^2 - +z^{p-4}y^3 + etc = n^p$$

$$z - x = v^p \quad z^{p-1} + z^{p-2} + z^{p-3}x^2 + z^{p-4}x^3 + etc = m^p$$

"

Queste equazioni furono date da Barlow [§§] attorno al 1810 e stabilite indipendentemente da Abel nel 1823.
Si possono ottenere in questo modo; l'ipotesi che x, y, z e p siano coprimi e l'equazione di Fermat "forzano" $x + y$ e $\phi(x, y)$ ad essere coprimi. Dal momento che il prodotto di $x + y$ e $\phi(x, y)$ è uguale a z^p, ognuno di essi deve essere una potenza p-esima. Similmente si ottengono le altre.

3.5.2 Divisibilità per p

In questa parte della dimostrazione di Sophie troveremo una forma "debole" del Teorema di Sophie Germain per cui uno fra x, y, z deve essere divisibile per p (Laubenbacher, Pengelley 2010 pp.45)

> *"Senza perdere in generalità assumo che il numero z che è un multiplo del numero primo [θ] della forma $2Np + 1$ esista. Si ha quindi che $l^p + h^p + v^p \equiv 1 \pmod{2Np+1}$. E dal momento che, per ipotesi, non può essere, per questo modulo, che due potenze p-esime abbiano differenza 1, sarà necessario che sia l e non r, ad avere questo modulo come fattore. Dal momento che $x + y \equiv 0 \pmod{2Np+1}$ si conclude che $px^{p-1} \equiv r^p \pmod{2Np+1}$ che significa che, poichè x è una potenza residua p-esima, anche p sarà una potenza residua p-esima, contrariamente all'ipotesi; quindi il numero z deve essere un multiplo di p. "*

La condizione N-C e la congruenza $l^p + h^p + v^p \equiv 0 \pmod{\theta = 2Np + 1}$ implicano che uno fra l, h o v è divisibile per θ. Se lo fosse uno fra h o v, allora x o y sarebbero divisibili per θ, in contraddizione con la tesi che x,y e z siano coprimi. Questo implica che l sia il numero divisibile per θ e quindi

[§§]Peter Barlow (Norwich, 1776 – Woolwich, 1862). Matematico e fisico inglese, studiò i fenomeni elettromagnetici. Fu professore di matematica alla Royal Military Academy di Woolwich. Oltre a numerosi trattati di matematica si interessò di astronomia e migliorò la costruzione di obiettivi acromatici per telescopi, inventando la lente di Barlow. Compì importanti studi sul magnetismo e determinò il modo per compensare l'azione delle masse metalliche delle navi sulle bussole. Propose la ruota che reca il suo nome, un semplicissimo motore elettrico. Si occupò inoltre di problemi relativi all'ingegneria ferroviaria.

$y \equiv -x \pmod{\theta}$. Sostituendo troviamo $\phi(x,y) \equiv px^{p-1} \equiv r^p \pmod{\theta}$. Inoltre dal momento che $z \equiv 0 \pmod{\theta}$ concludiamo da $z - x = v^p$ che x è una potenza p-esima modulo θ. Quindi p è anche una potenza p-esima modulo θ in contraddizione con l'altra ipotesi del teorema.
Siamo riusciti a derivare una contraddizione dall'assunzione che x, y, z e p fossero coprimi (che li costringe ad essere multipli di p). Sophie, al fine di proseguire con la sua dimostrazione, cambia implicitamente l'ipotesi su z che esso sia il numero noto per essere divisibile per p ma non necessariamente per θ e, come riflesso della sua modifica, cambia la prima coppia di equazioni con un'altra.

3.5.3 Il teorema di Sophie come ricaduta

Sophie continua la sua dimostrazione per provare la forma "forte" del Teorema di Sophie Germain (Laubenbacher, Pengelley 2010 pp 46):

> *"Ponendo $z = lrp$, l'unica ipotesi ammissibile è che*
>
> $$x + y = l^p p^{p-1} \quad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + etc = pr^p$$
>
> *perchè se, contrariamente, assumessimo che*
>
> $$x + y = l^p p \quad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + etc = p^{p-1}r^p$$
>
> *allora*
>
> $$(x+y)^{p-1} - x^{p-1} - x^{p-2}y + x^{p-3}y^2 + etc$$
>
> *sarebbe divisibile per p^{p-1}. Osserviamo che nell'equazione $2z - x - y = h^p + v^p$ la forma del secondo membro lo forza ad essere divisibile per p o p^2. Di conseguenza si vede che con le presenti ipotesi z debba essere multiplo di p^2."*

Vediamo come Sophie arriva alla sua affermazione.
Dal momento che $z^p = x^p + y^p$ deve essere divisibile per p, dobbiamo solo mostrare che $\phi(x,y)$ è divisibile esattamente per la potenza prima di p. Se poniamo $x + y = s$, allora

$$\phi(x,y) = \frac{(s-x)^p + x^p}{s} = s^{p-1} - \binom{p}{1} s^{p-2}x + \ldots - \binom{p}{p-2} sx^{p-2} + \binom{p}{p-1} x^{p-1}.$$

Osserviamo ora che tutti gli addendi a secondo membro sono divisibili per p^2 dal momento che p divide $s = x + y \equiv x^p + y^p = z^p \pmod{p}$ per il

piccolo Teorema di Fermat, mentre l'ultimo è divisibile esattamente per p dal momento che x e p sono coprimi.
Infine per dimostrare che questo forza z ad essere divisibile per p^2, osserviamo che l'equazione $2z - x - y = h^p v^p$ ci assicura che p divida $h^p + v^p$. Inoltre p divide $h+v$ per il Piccolo Teorema di Fermat applicato ad h e v. Ora notiamo che, dal momento che $h \equiv -v \pmod{p}$, segue che $h^p \equiv -v^p \pmod{p^2}$. Quindi p^2 divide z perchè p^2 divide $x + y$ per la nuova coppia di equazioni di Sophie.
Questa parte di dimostrazione costituisce una dimostrazione valida per il Teorema di Sophie Germain.

3.5.4 Un errore nella dimostrazione

Sophie continua la sua dimostrazione dimostrando la divisibilità per θ (Laubenbacher Pengelley 2010 pp.48):

> *"L'ultima cosa che rimane da dimostrare è che tutti i numeri primi della forma $\theta = 2Np + 1$, che sono soggetti alle stesse condizioni dei numeri la cui esistenza è stata assunta, sono necessariamente multipli di z.*
> *Al fine di ottenere questo supponiamo che sia y, per esempio, e non z, ad avere uno dei numeri in questione come fattore. Allora per questo modulo avremo $h^p - l^p \equiv v^p$ e conseguentemente $v \equiv 0, \quad z \equiv x, \quad pz^{p-1} \equiv m^p$ che significa che p è la potenza residua p-esima contrariamente all'ipotesi."*

Qui Sophie, invece di usare l'equazione $x+y = l^p p^{p-1} \quad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + etc = pr^p$ risultante dalla p-divisibilità di z, usa erroneamente l'equazione originale $x + y = l^p \quad x^{p-1} - x^{p-2} + x^{p-3}y^2 - x^{p-4}y^3 + etc = r^p$ che necessita dell'ipotesi che x, y, z e p siano coprimi. Sottraendo

$$x + y = l^p \quad x^{p-1} - x^{p-2} + x^{p-3}y^2 - x^{p-4}y^3 + etc = r^p$$

e

$$z - y = h^p \quad z^{p-1} + z^{p-2} + z^{p-3}y^2 - +z^{p-4}y^3 + etc = n^p$$

e paragonando i risultati con

$$z - x = v^p \quad z^{p-1} + z^{p-2} + z^{p-3}x^2 + z^{p-4}x^3 + etc = m^p$$

ottiene la congruenza $h^p - l^p \equiv v^p \pmod{\theta}$ perchè $y \equiv 0 \pmod{\theta}$.
Dal momento che né h né l possono essere divisibili per θ (dal momento che né x né z lo sono) la Condizione N-C implica che $v \equiv 0 \pmod{\theta}$ quindi

$z \equiv x$.
Il fatto che $pz^{p-1} \equiv m^p$ segue dal secondo membro di $z - x = v^p, \quad z^{p-1} + z^{p-2} + z^{p-3}x^2 + z^{p-4}x^3 + etc = m^p$.
$z \equiv h^p$ segue da $z - y = h^p, \quad z^{p-1} + z^{p-2} + z^{p-3}y^2 - +z^{p-4}y^3 + etc = n^p$, dal momento che $y \equiv 0$ e, infine, questo permette di esprimere p come residuo di una potenza p-esima che contraddice la Condizione p-N-p.
Fatta eccezione per l'errore notato, la dimostrazione del Teorema di Sophie è completa. Se fosse stata usata l'equazione corretta $x + y = l^p p^{p-1}, \quad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + etc = pr^p$, allora, al posto della Condizione N-C, la dimostrazione avrebbe avuto bisogno di una condizione analoga ma differente per la congruenza $h^p - l^p p^{p-1} \equiv v^p$ che si ottiene sottraendo $x + y = l^p p^{p-1}, \quad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + etc = pr^p$ da $z - y = h^p, \quad z^{p-1} + z^{p-2} + z^{p-3}y^2 - +z^{p-4}y^3 + etc = n^p$. Potremmo aver bisogno della seguente ipotesi aggiuntiva:

Condizione N-p^{-1} Non ci sono due potenze residue p-esime che differiscano per p^{-1} (equivalentemente $-2N$) modulo θ.

Aggiungendo questa condizione come ipotesi aggiuntiva si ottiene una dimostrazione valida del teorema.

3.5.5 Un tentativo di rimediare?

Sophie ha mai realizzato che ci fosse un errore fondamentale nella sua dimostrazione? Laubenbacher e Pengelley in [7] notano come all'inizio di uno dei paragrafi del manoscritto *Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation* $x^p + y^p = z^p$ ci siano scritte due parole "voyez errata" o "voyez erratu". Non molto più avanti, sempre nello stesso manoscritto, ci sono due pagine intitolate "errata" all'interno delle quali si trovano le considerazioni di prima. Sophie scrive le tre equazioni, questa volta usando l'equazione giusta

$$x + y = l^p p^{p-1}, \quad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + etc = pr^p$$

e nota come si arrivi ad una congruenza della forma "alterata"

$$l^p p^{2p-1} + h^p + v^p \equiv 0$$

che dovrebbe portare ad una contraddizione. Sophie successivamente osserva

come il caso $p = 5$ ed $N = 1$ non verifichi la condizione N-p^{-1} ¶¶ e si imbarca nella missione di dimostrare la sua tesi con altri mezzi. Laubenbacher e Pengelley in [7] sottolineano come sia difficile interpretare questi commenti marginali ma di come Sophie si dimostri versatile nell'utilizzare forme quadratiche e reciprocità quadratica per provare a risolvere questo problema

3.6 Esponenti della forma $2(8n \pm 3)$

Considererò ora il manoscritto intitolato *Démonstration de l'impossibilité de satisfaire en nombres entiers à l'équation* $z^{2(8n\pm3)} + x^{2(8n\pm3)}$ conservato alla Bibliothèque Nationale de France di Parigi di cui ad oggi non si trova una versione online e che non è ancora stato parte di alcun progetto editoriale. Per fare ciò mi servirò delle riflessioni di Laubenbacher e Pengelley in [7] ***. All'interno di *Démonstration de l'impossibilité de satisfaire en nombres entiers à l'équation* $z^{2(8n\pm3)} + x^{2(8n\pm3)}$ Sophie enuncia e dimostra tre teoremi e termina la sua opera con una discussione finale che si ricollega al titolo del manoscritto. Nonostante Sophie non parli apertamente del quadro generale, lasciando al lettore il compito di ricomporre tutti i pezzi del puzzle, è chiaro che stia procedendo a dimostrare l'ultimo Teorema di Fermat eliminando le soluzioni per le quali gli esponenti primi $p = 8n \pm 3$ dividono o non dividono uno fra x^2, y^2, z^2 nell'equazione di Fermat $(x^2)^p + (y^2)^p = (z^2)^p$.

3.6.1 Caso 1 e Teorema di Sophie Germain

Sophie inizia eliminando le soluzioni per le quali nessuno numero è divisibile per p e lo afferma per tutti gli esponenti dispari (Laubenbacher Pengelley 2010 pp.55):

> *"Primo teorema. Per ogni primo [dispari] p nell'equazione* $z^p = x^p + y^p$*, uno fra* x, y, z *dovrà essere multiplo di* p^2*."*

Attualmente il fatto che le soluzioni debbano essere p-divisibili (Sophie afferma qualcosa di più, che siano p^2 divisibili) viene chiamato Caso 1 dell'ultimo

¶¶ 1 e -1 sono entrambi potenze quinte e differiscono di $2N = 2$. Di fatto la Condizione N-p^{-1} si verifica piuttosto di rado se paragonata alla Condizione N-C e quindi assumerla come ipotesi verifica una dimostrazione ma probabilmente non è molto utile

*** Nonostante non abbia accesso alla fonte originale e non possa verificare le affermazioni di Laubenbacher e Pengelley trovo doveroso dover parlare anche di questa categoria di numeri che soddisfano il Teorema di Fermat al fine di fornire un quadro generale ed esauriente del lavoro di Sophie

Teorema di Fermat. Da sottolineare come non ci siano ipotesi dal momento che Sophie desidera dimostrare come il Caso 1 sia vero in generale anche se riconosce come, per provare ciò, abbia bisogno di altro (Laubenbacher Pengelley 2010 pp.55):

> *"Per dimostrare questo teorema basta supporre che esista almeno un numero primo θ della forma $2Np+1$ per il quale sia impossibile trovare allo stesso tempo due potenze residue p-esime [mod θ] la cui differenza sia 1 e p non sia un potenza residua p-esima [mod θ]."*

Oggigiorno questa affermazione viene riconosciuta come ipotesi del Teorema di Sophie Germain anche se per lei questa non era solo una ipotesi ma qualcosa che pensava fosse vera e dimostrabile con i suoi metodi poichè prosegue scrivendo (Laubenbacher Pengelley 2010 pp.55):

> *"Non solo esiste sempre un numero θ che soddisfi queste due condizioni ma i calcoli indicano che debba esserci un numero infinito di essi. Per esempio se $p = 5$ allora $\theta = 2 \cdot 5 + 1 = 11$, $2 \cdot 4 \cdot 5 + 1 = 41$, $2 \cdot 7 \cdot 5 + 1 = 71$, $2 \cdot 10 \cdot 5 + 1 = 101$ etc."*

La dimostrazione del Primo Teorema è molto simile alla parte iniziale del Teorema sulla dimensione delle soluzioni che inizia ad andare storto solo dopo aver provato la p^2-divisibilità. In questa dimostrazione, come nell'altra, dimostra senza problemi la divisibilità per p^2 e, all'interno dei vari manoscritti di Sophie, è ciò che si avvicina maggiormente alla dimostrazione di quello che oggi viene chiamato Teorema di Sophie Germain.

3.6.2 Caso 2 per p che divide z

Il resto del manoscritto si occupa del caso 2 dell'ultimo Teorema di Fermat che è caratterizzato dalle equazioni

$$x + y = l^p \quad x^{p-1} - x^{p-2} + x^{p-3}y^2 - x^{p-4}y^3 + etc = pr^p$$

$$z - y = h^p \quad z^{p-1} + z^{p-2} + z^{p-3}y^2 - +z^{p-4}y^3 + etc = n^p$$

$$z - x = v^p \quad z^{p-1} + z^{p-2} + z^{p-3}x^2 + z^{p-4}x^3 + etc = m^p$$

Per completezza Laubenbacher e Pengelley menzionano il fatto che il Teorema 2 contenga un risultato tecnico non rilevante per la dimostrazione portata avanti da Sophie. Forse scrisse il teorema e la sua dimostrazione in quel punto perchè era un suo risultato del Caso 2 che è il principale argomento del resto del manoscritto [†††].

Continuando con il Caso 2 si nota che, avendo a che fare con quadrati, l'equazione $(x^2)^p + (y^2)^p = (z^2)^p$ ha una assimmetria che forza la separazione delle considerazioni su z da quelle su x o y nel dimostrare l'ultimo Teorema di Fermat. Sophie parla della p-divisibilità di z nel Teorema 3 che asserisce che z non può essere un multiplo di p se p ha la forma $8n+3$, $8n+5$ o $8n+7$. Dimostra il Teorema 3 per assurdo ipotizzando che z sia divisibile per p. La sua dimostrazione inizia con alcune equazioni che hanno bisogno di derivate avanzate. Usando il fatto che i numeri di ciascuna coppia delle equazioni

$$x + y = l^p \quad x^{p-1} - x^{p-2} + x^{p-3}y^2 - x^{p-4}y^3 + etc = pr^p$$

$$z - y = h^p \quad z^{p-1} + z^{p-2} + z^{p-3}y^2 - +z^{p-4}y^3 + etc = n^p$$

$$z - x = v^p \quad z^{p-1} + z^{p-2} + z^{p-3}x^2 + z^{p-4}x^3 + etc = m^p$$

siano coprimi per ciascuna soluzione coprima costituita prendendo a due a due x^2, y^2, z^2 (una volta inserita la p^2-divisibilità), il secondo membro di queste equazioni diventa:

$$x^2 + y^2 = p^{4p-1}l^{2p}$$

[†††] Il Teorema 2 asserisce che nelle equazioni

$$x + y = l^p \quad x^{p-1} - x^{p-2} + x^{p-3}y^2 - x^{p-4}y^3 + etc = pr^p$$

$$z - y = h^p \quad z^{p-1} + z^{p-2} + z^{p-3}y^2 - +z^{p-4}y^3 + etc = n^p$$

$$z - x = v^p \quad z^{p-1} + z^{p-2} + z^{p-3}x^2 + z^{p-4}x^3 + etc = m^p$$

i numeri r, m,n possono avere divisori primi solo della forma $2Np + 1$ e in particolare che i divisori primi di r devono essere della forma $2Np^2 + 1$.

$$z^2 - y^2 = h^{2p}$$

$$z^2 - x^2 = v^{2p}$$

Sophie dimostra il Teorema 3 per $p = 8n+3$ e $8n+7$ usando il fatto, noto già ai tempi di Fermat, che una somma di quadrati non possa contenere divisori primi di questi due tipi. Per $p = 8n + 5$ la discussione è diversa poichè presi $z - y$ e $z + y$ coprimi, si ha $z + y = (h')^{2p}$ e $z + x = (v')^{2p}$, dai quali $y^2 \equiv (h')^{4p} \pmod{p}$ e $x^2 \equiv (v')^{4p} \pmod{p}$ e quindi $(h')^{4p} + (v')^{4p} \equiv 0 \pmod{p}$ perchè $x^2 + y^2$ è divisibile per p. Questa è una contraddizione dal momento che -1 non è un residuo biquadratico modulo $8n + 5$.
L'errore in questa dimostrazione non è ovvio. Le espressioni elevate alla $2p$ per $z + y$ e $z + x$ si basano sul fatto che $z - y$ e $z + y$ siano coprimi. Questo sarebbe vero per una coppia di coprimi di x, y, z se i numeri di ogni differenza fossero uno pari ed uno dispari ma, altrimenti, la loro somma e differenza ha precisamente 2 come massimo comune divisore. Scrivendo $(x^p)^2 + (y^p)^2 = (z^p)^2$ si vede che la parità diversa non si verifica né per $z - y$ né per $z - x$. Prendiamo $z - y$ allora o $z - y$ o $z + x$ ha un solo 2 come fattore (dal momento che y e z sono coprimi),e quindi non può essere una potenza $2p$-esima. Si può includere il fattore 2 e riprendere l'analisi di Sophie da capo ma ci si troverebbe a dover verificare se -4 sia un residuo biquadratico modulo $8n + 5$ il che è vero. In conclusione la dimostrazione di Sophie è fatalmente errata per il caso $p = 8n + 5$.

3.7 Esponenti pari

In un altro manoscritto di tre pagine non datato conservato sempre alla Bibliothèque Nationale [‡‡‡] si trovano due teoremi. Il primo afferma che l'equazione "quasi-Fermat" $2z^m = y^m + x^m$ non ha soluzioni naturali non banali (cioè oltre $x = y = z$) per ogni esponente pari $m = 2n$ con $n > 1$. Di fatto Sophie asserisce che la sua dimostrazione si applica ad una intera famiglia di equazioni simili nelle quali gli esponenti non sono sempre gli stessi per tutte le variabili. La sua dimostrazione inizia con una caratterizzazione parametrica delle soluzioni intere dell'equazione "quasi-Pitagorica" $2c^2 = b^2 + a^2$ (

[‡‡‡]Anche di questo manoscritto non è reperibile una trascrizione perciò mi baso completamente sulle analisi di Laubenbacher e Pengelley in [7]

tramite $c = z^n, b = y^n, a = x^n$) simile alla ben nota caratterizzazione parametrica delle triplette Pitagoriche usata da Eulero nella sua dimostrazione dell'ultimo Teorema di Fermat per l'esponente 4.

3.7.1 La dimostrazione di Eulero dell'ultimo Teorema di Fermat per n=4

[§§§]Eulero, analizzando le note di Fermat, trovò una dimostrazione abbozzata del caso $n = 4$ che Fermat stesso aveva inserito all'interno di una dimostrazione riguardante il fatto che un triangolo rettangolo non possa essere equiesteso ad un quadrato.

Teorema 3.7.1. *Siano x, y, z tre numeri interi positivi tali che*

$$x^2 + y^2 = z^2 \tag{3.1}$$

allora esistono p e q coprimi, di opposta parità e $p > q$ tali che:

$$\begin{cases} x = 2pq \\ y = p^2 - q^2 \\ z = p^2 + q^2 \end{cases} \tag{3.2}$$

Dimostrazione. Consideriamo x, y, z tali che $x^2 + y^2 = z^2$, supponiamo che x, y, z siano primi fra loro. Se due di essi avessero un fattore comune, allora per 3.7.1 sarebbe comune anche al terzo e se tutti e tre avessero un fattore comune d tale per cui

$$\begin{cases} x = x'd \\ y = y'd \\ z = z'd \end{cases} \tag{3.3}$$

sostituendo $d^2(x'^2 + y'^2) = d^2z'^2$ e semplificando d^2 otterremmo che gli interi $x' = \frac{x}{d}$, $y' = \frac{y}{d}$, $z' = \frac{z}{d}$ formerebbero una nuova terna pitagorica detta primitiva. Ogni terna può essere quindi ridotta ad una primitiva dividendo per il massimo comune divisore.
Possiamo aggiungere che x, y, z non possono essere dispari (e nemmeno tutti e tre pari perchè li abbiamo presi coprimi) poichè se lo fossero da 3.7.1 avremmo al primo membro la somma di due numeri dispari che ci fornirebbe un numero pari. Al tempo stesso z non potrà essere pari perchè se lo fosse

[§§§]per la dimostrazione seguiamo il testo [6]

risulterebbe $z = 2n$ che al quadrato è un multiplo di 4 e tale numero dovrebbe essere uguale alla somma di due numeri dispari elevati al quadrato ma ciò è impossibile. Quindi z deve essere dispari e x e y avranno parità opposta. Supponiamo x pari e y dispari. Da 3.7.1:

$$x^2 = z^2 - y^2 = (z - y)(z + y)$$

otteniamo che $x, z+y, z-y$ sono pari, in quanto somma di due numeri dispari e abbiamo u, v, w tali che

$$x = 2u$$

$$z + y = 2v$$

$$z - y = 2w$$

quindi da 3.7.1

$$(2u)^2 = (2v)(2w)$$

$$u^2 = vw \tag{3.4}$$

con v e w coprimi dal momento che qualsiasi loro fattore comune dividerebbe anche z e y poichè $v + w = z$ e $v - w = y$ ma z, y sono coprimi.
La 3.7.1 ha senso solo se v e w sono dei quadrati, quindi esistono p e q tali che

$$v = p^2$$

$$w = q^2$$

con p e q coprimi.
Sostituendo avremo

$$z = v + w = p^2 + q^2$$

$$y = v - w = p^2 - q^2$$

dove $p > q$ (poichè y è un intero positivo), inoltre hanno opposta parità perchè z, y sono dispari. Se esprimiamo x in funzione di p e q otteniamo:

$$x^2 = z^2 - y^2 = (z - y)(z + y) = 2w2v = 4p^2q^2$$

da questa ricaviamo che

$$x = 2pq$$

Di conseguenza qualunque siano p, q tali che per $p > q$ siano coprimi e abbiano opposta parità, otteniamo delle terne pitagoriche date da:

$$\begin{cases} x = 2pq \\ y = p^2 - q^2 \\ z = p^2 + q^2 \end{cases} \tag{3.5}$$

Lemma 3.7.2 (**La discesa infinita**)**.** *Non esiste una proprietà che, se soddisfatta da un intero positivo, possa essere soddisfatta da un intero positivo più piccolo*

Teorema 3.7.3. *L'equazione*

$$x^4 + y^4 = z^4 \tag{3.6}$$

non ammette soluzioni intere positive quando $xyz \neq 0$.

Dimostrazione. Per dimostrare questo teorema consideriamo il caso in cui $x^4 + y^4 = z^2$ poichè la 3.7.3 può essere scritta così $x^4 + y^4 = (z^2)^2$.
Per le stesse ragioni del Teorema 3.7.1 avremo che x, y, z sono coprimi e quindi lo sono anche x^2, y^2, z^2, inoltre, essendo terne pitagoriche, dalla 3.7.1 possiamo scrivere:

$$\begin{cases} x = 2pq \\ y = p^2 - q^2 \\ z = p^2 + q^2 \end{cases} \tag{3.7}$$

dove p e q sono coprimi, di parità opposta e $p > q > 0$ (come nella dimostrazione di 3.7.1).
Dalla seconda delle precedenti equazioni possiamo scrivere

$$y^2 + q^2 = p^2$$

nuovamente avremo che y, p, q sono delle terne pitagoriche, dove p è dispari (vedi 3.7.1), quindi q sarà pari poichè hanno opposta parità, possiamo scrivere:

$$\begin{cases} x = 2pq \\ y = a^2 - b^2 \\ z = a^2 + b^2 \end{cases} \tag{3.8}$$

dove a, b sono coprimi, di parità opposta e $a > b > 0$.
Scriviamo x in funzione di a e b:

$$x^2 = 2pq = 2(a^2 + b^2)(2ab) = 4ab(a^2 + b^2)$$

dove $ab(a^2+b^2)$ è un quadrato. Inoltre, ab e (a^2+b^2) sono coprimi, infatti, se $P|ab$, allora dovrebbe dividere a oppure b ma non entrambi in quanto coprimi quindi non può dividere (a^2+b^2). Poichè ab e (a^2+b^2) sono quadrati, allora, essendo ab un quadrato e a e b coprimi, anche a e b sono dei quadrati. Poniamo $a = X^2$ e $b = Y^2$, così:

$$X^4 + Y^4 = a^2 + b^2 = p < p^2 + q^2 = z^2 < z^4 = x^4 + y^4$$

Iterando il procedimento si troveranno delle nuove soluzioni $X' < X$ e $Y' < Y$ tali che

$$(X')^4 + (Y')^4 < z^4$$

procedendo così all'infinito.
Si è così arrivati ad una discesa infinita di interi positivi, che come abbiamo visto nel Lemma 3.7.2 è impossibile. Il teorema dimostra che se la somma di due potenze quarte non può essere un quadrato, a maggior ragione non potrà essere una potenza quarta.
Da questo teorema, segue che, l'equazione $x^{4m} + y^{4m} = z^{4m}$ non ammette soluzioni quando m è un intero positivo, infatti, posto $X = x^m$, $Y = y^m$ e $Z = z^m$ otterrei l'equazione $X^4 + Y^4 = Z^4$ che come visto dal teorema 3.7.3 non ammette soluzioni intere positive; quindi quando n divide 4 l'equazione $x^n + y^n = z^n$ non ammette soluzioni. Un esponente $n > 2$ che non è divisibile per 4 e non è potenza di 2, deve essere diviso da qualche primo $p \neq 2$, poniamo $n = pm$; per provare che $x^n + y^n = z^n$ è impossibile, è sufficiente provare che $x^p + y^p = z^p$ è impossibile.

Nel 1997 Henri Darmon e Loic Merel dimostrarono che l'equazione "quasi-Fermat" per $m > 2$ aveva soluzioni non banali. Molto prima Eulero aveva dimostrato la sua impossibilità per $m = 4$ e poi per $m = 3$.
L'affermazione di Sophie si è così verificata essere vera.
La seconda affermazione che si trova nel manoscritto riguarda la dimostrazione dell'ultimo Teorema di Fermat per tutti gli esponenti pari maggiori di 2, cioè per $z^{2n} = y^{2n} + x^{2n}$ con $n > 1$ e la sua dimostrazione si affida alla non dimostrata coprimarietà delle due espressioni.

3.8 L'approccio di Sophie all'ultimo Teorema di Fermat

Riassumiamo i passi fatti da Sophie nel corso degli anni e nei vari manoscritti verso la dimostrazione dell'ultimo Teorema di Fermat.

3.8.1 Il grande piano

Nel manoscritto *Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation* $x^p + y^p = z^p$ Sophie mette a punto un grande piano per dimostrare l'ultimo Teorema di Fermat per ogni esponente primo $p > 2$ basato sulla soddisfazione di una condizione di non consecutività (Condizione N-C) per infiniti primi ausiliari. Sviluppa un algoritmo che dimostri la condizione entro certi limiti e delinea una dimostrazione per induzione da applicare ai primi ausiliari. Le sue tecniche per la verifica della Condizione N-C sono completamente differenti, seppur altrettanto dettagliate, da quelle di Legendre.
Sophie probabilmente non impiegò ulteriori energie nel suo grande piano dopo che Legendre le scrisse che il piano sarebbe fallito per $p = 3$ e lei gli inviò una dimostrazione (nella quale mostra che ci sia solo un numero finito di ausiliari N-C validi) che confermava questa supposizione. Diversamente da Legendre Sophie adotta il linguaggio di Gauss e le sue riflessioni delle *Disquisitiones*. L'approccio di Sophie per verificare la Condizione N-C fu scoperto indipendentemente da L.E. Dickson nel ventesimo secolo. In anni più recenti altri ricercatori si sono avvicinati alla Condizione N-C per induzione, come fece Sophie.

3.8.2 La grande dimensione delle soluzioni

Sempre nel manoscritto *Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation* $x^p + y^p = z^p$ Sophie scrive un teorema e delle applicazioni basate sul soddisfacimento delle Condizioni N-C ed p-N-p per suffragare la sua idea che le soluzioni dell'equazione di Fermat debbano avere dimensioni estremamente grandi. Successivamente trova un errore nei suoi calcoli e tenta di porvi rimedio usando la sua conoscenza sui residui quadratici. La parte valida della dimostrazione contiene al suo interno quello che oggi chiamiamo Teorema di Sophie Germain che permette la dimostrazione del Caso 1 se si soddisfano entrambe le condizioni. Gli sforzi di Sophie volti a soddisfare la Condizione p-N-p si basano sui suoi risultati teorici che mostrano come spesso questa segua dalla Condizione 2-N-p, già studiata per la Condizione

N-C. Questi risultati furono scoperti indipendentemente molto più avanti da Ernst Wendt, Leonard Eugene Dickson e Harry Schultz Vandiver.

3.8.3 Esponenti $2(8n\pm3)$ e il Teorema di Sophie Germain

Nel manoscritto *Démonstration de l'impossibilité de satisfaire en nombres entiers à l'équation* $z^{2(8n\pm3)} + x^{2(8n\pm3)}$ Sophie fa un tentativo di dimostrare l'ultimo Teorema di Fermat per tutti gli esponenti $2p$ dove $p = 8n \pm 3$ è primo. Inizia con una dimostrazione di quello che oggi è chiamato Teorema di Sophie Germain, questo manoscritto infatti è la migliore fonte originale del teorema per cui è famosa. Si potrebbe pensare che questo manoscritto stia ad indicare uno sforzo per sistemare l'errore nel Teorema delle grandi dimensioni delle soluzioni nel manoscritto *Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation* $x^p + y^p = z^p$ ma i dettagli della dimostrazione ci suggeriscono diversamente poichè tradiscono lo stesso errore del manoscritto precedente.

3.8.4 Esponenti pari

Nell'ultimo manoscritto analizzato Sophie scrive due teoremi e le loro dimostrazioni al fine di dimostrare l'ultimo Teorema di Fermat per tutti gli esponenti pari con metodi completamente differenti da quelli visti negli altri manoscritti. Sophie pianifica di dimostrare l'ultimo Teorema di Fermat mostrando inizialmente che una famiglia di equazioni Diofantee leggermente differenti non ha soluzione così inizia scrivendo che le equazioni "quasi-Fermat" $2z^{2n} = y^{2n} + x^{2n}$ non hanno soluzioni non banali positive per $n > 1$. Questa affermazione è stata dimostrata solo recentemente. La dimostrazione di Sophie soffriva dello stesso tipo di errore riscontrato precedentemente.

3.8.5 Rivalutazione del suo lavoro

Analizzando i vari documenti si evince che Sophie decise di concentrarsi sulla dimostrazione di teoremi generali che potessero essere applicati ad inifiniti esponenti primi nell'equazione di Fermat piuttosto che eliminare i casi per singoli esponenti come avevano già fatto altri. A questo scopo sviluppò diverse tecniche multisfaccettate sia negli scopi che nei metodi cercando di non concentrarsi troppo su esempi o soluzioni ad hoc. Un mezzo che le venne in soccorso fu il punto di vista moderno sulla teoria dei numeri esposto da Gauss nelle *Disquisitiones*. L'importanza delle tecniche di Sophie per verificare le Condizioni N-C e p-N-p è sottolineata dalla tarda riscoperta di esse da parte di altri ricercatori e inoltre il suo approccio fu più sistematico e teorico di

quello di Legendre o dei matematici pre-Gaussiani. Per oltre duecento anni l'articolato piano di Sophie per attaccare l'ultimo Teorema di Fermat è rimasto nascosto nei suoi manoscritti inediti e nessuno sapeva che tutti i risultati, volti a verificare le Condizioni N-C e p-N-p, pubblicati da Legendre e citati ed usati ampiamente da altri, erano merito di Sophie.
L'impressione che se ne ricava è che Sophie sarebbe riuscita a raggiungere molti altri risultati se le fosse stato permesso di avere un normale accesso all'istruzione, alle istituzioni professionali e alle pubblicazioni dell'epoca. L'evidenza dei manoscritti di Sophie e il paragone con il lavoro di Legendre mostrano un lavoro indipendente e sofisticato sull'ultimo Teorema di Fermat, molto più esteso del singolo risultato attribuitole. Questo corrobora l'idea dell'isolamento nel quale vivesse e suggerisce come buona parte di questo impressionante lavoro, probabilmente, fosse noto solo ad una cerchia ristretta di amici fidati. Sophie fu una stratega, una donna coraggiosa e soprattuto una teorica dei numeri molto più impressionante di quanto si fosse mai pensato.

Appendice

In Appendice trascriviamo le lettere trattate nei capitoli precedenti, scambiate fra Sophie Germain e Gauss, riprese dai testi di Stupuy (1879, pp. 302-307, 318-320) e Boncompagni (1879), e il manoscritto intitolato *Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation* $x^p + y^p = z^p$ ripreso da Del Centina (2007) .

I

Paris, ce 21 novembre 1804 Monsieur Vos Disquisitiones Arithmeticae font depuis longtems l'objet de mon admiration et de mes études. Le dernier chapitre de ce livre renferme, entr'autres choses remar- quables, le beau théorème contenu dans l'équation

$$\frac{4(x^n - 1)}{x - 1} = Y^2 \pm nZ^2;$$

je crois qu'il peut etre généralisé ainsi,

$$\frac{4(x^{n^s} - 1)}{x - 1} = Y^2 \pm nZ^2$$

n étant toujours un nombre premier et s un nombre quelconque. Je joins à ma let- tre deux démonstrations de cette généralisation.
Après avoir trouvé la première j'ai cherché comment la méthode que vous avez employé art. 357, pouvait etre appliqué au cas que j'avais à considérer; j'ai fait ce travail avec d'autant plus de plaisir, qu'il m'a fourni l'occasion de me familiariser avec cette méthode, qui, je n'en doute pas, sera dans vos mains l'instrument de nouvelles decouvertes.
J'ai ajouté à cet art. quelques autres considérations. La derniere est relative à la cèlèbre équation de Fermat $x^n + y^n = z^n$, dont l'impossibilité en nombres entiers n'a encore été démontrée que pour $n = 3$ et $n = 4$: je crois etre parvenu à prouver cette impossibilité pour $n = p - 1$, p étant un nombre premier de la forme $8k + 7$. Je prens la liberté de sousmettre ces essais à

votre jugement persuadé que vous ne dedaignerez pas d'éclairer de vos avis un amateur enthousiaste de la science que vous cultivez avec de si brillants succès.
Rien n'égale l'impatience avec laquelle j'attens la suite du livre que j'ai entre les mains, je me suis fait informer que vous y travailliez en ce moment et je ne négli- gerai rien pour me la procurer aussi tot qu' elle paraitra. Malheuresement l'étendue de mon esprit ne répond pas à la vivacité de mes gouts, et je sens q'il y a une sorte de témérité à importuner un homme de génie lorsqu'on a d'autre titre à son attention qu'une admiration nécessairement partagée par tous ses lecteurs.
En relisant la mémoire de M. de La Grange (Berlin 1775) j'ai vu avec étonnement qu'il n'a pas su réduire la quantité

$$s^{10} - 11(s^8 - 4s^6r^2 + 7s^4r^4 - 5s^2r^6 + r^8)r^2$$

à la forme $4t^2 - 11u^2$, car

$$s^{10} - 11(s^8 - 4s^6r^2 + 7s^4r^4 - 5s^2r^6 + r^8)r^2$$

$$= s^{10} - 2 \cdot 11 \cdot s^6r^4 + 11(5+6)r^8s^2 - 11(s^8 - 6s^6r^2 + 7s^4r^4 + 6s^2r^6 + r^8)r^2$$

$$= s^{10} - 2 \cdot 11s^6r^4 + 112r^8s^2 - 11(s^8 - 6s^6r^2 + 9s^4r^4 - 2s^4r^4 + 6s^2r^6 + r^8)r^2$$

$$= (s^5 - 11sr^4)^2 - 11(s^4 - 3s^2r^2 - r^4)^2$$

cette remarque est une nouvelle preuve de l'avantage de votre méthode qui s'ap- pliquant à toutes les valeurs de n, donne pour chaque cas des valeurs de Y et Z indépendantes du talonnement.
Si, connaissant les valeurs de Y et Z dans l'équation

$$\frac{4(x^n - 1)}{x - 1} = Y^2 \pm nZ^2$$

on voulait avoir celles de Y' et Z' dans l'équation

$$\frac{4(x^{n^s} - 1)}{x - 1} = Y'^2 \pm nZ'^2$$

il est clair qu'il suffirait de changer les signes de tous les termes de Y et Z qui cont- iennent des puissances de x dont l'exposant est impair.
Je n'ai pas voulu fatiguer votre attention en multipliant les remarques dont votre livre a été pour moi l'occasion: si je puis espérer que vous acceuilliez favorablement celles que j'ai l'honneur de vous communiquer et que vous ne les trouviez pas entière- ment indignes de répondre veuilliez l'adresser A' Monsieur Sylvestre de Sacy ¶¶¶ membre de l'Institut national, Rue Sante Famille A' Paris, qui me la remettra.
Croyez, Monsieur au prix que j'attacherais à un mot d'avis de votre part et recevez l'assurance du profond respect de
votre très humble serviteur
et très assidu lecteur
Le Blanc

Addendum

On peut toujours satisfaire à l'équation $\frac{4(x^{n^s}-1)}{x-1} = Y^2 \pm nZ^2$, n étant un nombre premier et s un nombre quelconque. Car la proposition étant démontrée pour le cas ou $s = 1$ il en résulte qu'elle a lieu aussi pour $s = 2$. En effet soit $\frac{4((x^n)^n-1)}{x^n-1} = \frac{4(x^{n^2}-1)}{x^n-1} = Y'^2 \pm nZ'^2$, il est clair que Y' et Z' sont composées des x^n comme Y et Z le sont de x dans l'équation $4(x^n - 1) = Y^2 \pm nZ^2$, on a donc $\frac{16(x^{n^2}-1)}{x-1} = \frac{4[(x^n)^n-1]}{x^n-1} \cdot \frac{4(x^n-1)}{x-1} = (Y'^2 \pm nZ'^2) \cdot (Y^2 \pm nZ^2) = (YY' \pm nZZ'^2) \cdot n(Y'Z \mp YZ'^2)$.
A' cause de $Y'^2 \pm nZ'^2$ et $Y^2 \pm nZ^2$ multiples de 4, il faut que Y' et Z' soient pairs ou impairs en meme temps et que Y et Z satisfassent aux memes conditions, d'où nous concluons $YY' \pm nZZ' = 2f : x, Y'Z \mp YZ' = 2\phi : x$ et par conséquent $\frac{4(x^{n^2}-1)}{x-1} = (f : x)^2 \pm n(\phi : x)^2$.
On trouve de meme

$$\frac{4((x^{n^2})^n - 1)}{x^{n^2} - 1} x = Y''2 \pm nZ''^2;$$

$$\frac{16(x^{n^3} - 1)}{x - 1} = \frac{4[(x^{n^2})^n - 1]}{x^{n^2} - 1} \cdot \frac{4(x^{n^2} - 1)}{x - 1}$$

¶¶¶Antoine-Isaac Silvestre de Sacy (1758-1838) professore di Arabo alla Ecole des Langues orientales, e, dal 1806, anche professore di Persiano al College de France

$$= (Y''^2 \pm nZ''^2) \cdot ((f:x)^2 \pm (\phi:x)^2)$$

$$= (Y''f : x \pm nZ''\phi : x)^2 \pm n(Y''\phi : x \mp Z''f : x)^2$$

d'où nous concluons

$$Y''f : x \pm nZ''\phi : x = 2f' : x$$

$$Y''\phi : x \mp Z''f : x = 2\phi' : x$$

$$\frac{4(x^{n^3}-1)}{x-1} = (f' : x)^2 \pm n(\phi' : x)^2$$

et ainsi de suite.

Exemples

$$\frac{4(x^9-1)}{x-1} = (2x^4 + x^3 + x + 2)^2 + 3(x^3 - x)^2$$

$$\frac{4(x^{27}-1)}{x-1} = (2x^{13} + x^{12} + x^{10} + 2x^9 + x^4 + 2x^3 - x + 1)^2$$

$$+3(x^{12} - x^{10} - x^4 - x - 1)^2$$

$$\frac{4(x^{25}-1)}{x-1} = (2x^{12} + x^{11} + 2x^{10} + x^7 + 3x^6 + x^5 + 2x^2 + x + 2)^2$$
$$-5(x^{11} + x^7 + x^6 + x^5 + x)^2$$

Nous observons qu'il y a toujours au moins 2^{s-1} valeurs différentes de Y et

Z dans l'équation $\frac{4(x^{n^s}-1)}{x-1} = Y^2 \pm nZ^2$; car, l'ambiguité des signes dans les quantités $YY' \pm nZZ'$, $Y'Z \pm YZ'$ fournit deux valeurs différentes pour les quantités $f : x$, $: x$ qui répondent à $s = 2$: ces deux valeurs pouvant etre mises dans les quantités $Y''f : x \pm nZ''\phi : x$,$Y''\phi : x \mp Z''f : x$ donnent, à cause de la nouvelle ambiguitée des signes, 4 valeurs pour $f'' : x$, $\phi'' : x$ qui répondent a $s = 3$; de sorte qu'en continuant le meme raisonnement, on trouve que s augmentant d'une unité, le nombre des valeurs de Y et Z qui satisfont pour la précedente valeur doit etre multiplié par 2. D'où il rsulte 2^{s-1} pour l'expression générale de ce nombre.
En suivant la démonstration du théorème exprimé par l'équation $4zz' = 4\frac{x^n-1}{x-1} = Y^2 \pm nZ^2$ on voit qu'elle est fondee sur la forme de $z = R + S(m,1) + T(m,g)$ et que cette forme elle meme résulte de ce que les coefficients $a = q = (m,1)$, $b = \frac{aq-q'}{2} = \frac{(m,1)^2-(m,2)}{2}$, etc. de l'équation du m-ième degré $z = x^m - ax^{m-1} + bx^{m-2} - etc. = 0$, ne sont composés que des quantités 1, $(m,1)$, (m,g) prises un nombre de fois détérminé par la valeur de m. Pour étendre ce théorème au cas ou l'exposant de x est une puissance quelcon- que d'un nombre premier c'est-à-dire, pour démontrer l'équation $4zz' = 4\frac{x^{n^s}-1}{x-1} = Y^2 \pm nZ^2$, il suffit donc d'établir que les coefficients de l'équation du $\frac{n^s-1}{x-1}$) -ième= $(mn^{s1}+mn^{s2}+...+mn+m)$-ième $[m = (n1)/2]$degré

$$z = x^{mn^{s-1}+mn^{s-2}+...+m} - Ax^{mn^{s-1}+mn^{s-2}+...+m-1} + Bx^{mn^{s-1}+mn^{s-2}+...+m-2} - ... \pm$$

$$Vx^{mn^{s-1}+...+mn} \mp A'x^{mn^{s-1}+...+mn-1} \pm B'x^{mn^{s-1}+...+mn-2} \mp ...$$

$$+V'x^{mn^{s-1}+...+m(n-1)} - A'x^{mn^{s-1}+...+m(n-1)-1} + B'x^{mn^{s-1}+...+m(n-1)-2} - ...$$

$$+V^n x^{mn^{s-1}} + ... + mn^2 - A^{n+1}x^{mn^{s-1}+...+mn^2-1} + B^{n+1}x^{mn^{s-1}+...+mn^2} - 2 - ...$$

$$^{n+1}x^{mn^{s-1}+...+m(n^2-1)} \mp A^{n+2}x^{mn^{s-1}+\Delta\Delta\Delta+m(n^2-1)-1}$$

$$\mp B^{n+2}x^{mn^{s-1}+...+m(n^2-1)-2} \mp ...$$

$$...(\pm ou+)V^{n^{s-1}+n^{s-2}+...+n-1}x^m(\mp ou-)A^{n^{s-1}+n^{s-2}+...+n}x^{m-1}(\pm ou+)$$

$$B^{n^{s-1}} + n^{s-2} + ... + nx^{m-2}(\pm ou - ...)$$

$$(+ou\pm)V^{n^{s-1}+n^{s-2}+...+n} = 0$$

ne contiennent que les quantités 1, (m, 1), (m, g) prises un nombre de fois déterminé par la valeur de n et par celle de s. ($N.^{ote}$ Les signes + et - devant etre alternatifs dans cette équation on voit que les signes supérieurs se rapportant au cas ou m est pair et les inférieurs à celui où m est impair; on voit en outre que suivant que l'indice de V est pair ou impair les termes de la ligne à laquelle il appartient, ont ou n'ont pas, de doubles signes).
Ainsi il s'agit de choisir $m + mn + mn^2 + ... + mn^{s-2} + mn^{s-1}$ racines parmi les $n^s - 1$ racines de l'équation $\frac{x^{n^s}-1}{x-1} = 0$, de manière que $A, A', ..., B, B', ...$ satisfassent aux conditions indiquées.
Pour cela il faut que la somme de ces racines, celle de leurs quarrés, et en général celle de leurs puissances quelconques, ne soient fonctions que des quantités $(m, 1), (m, g)$ et de l'unité.
Al'imitation de ce qui a été pratiqué pour l'équation $\frac{x^n-1}{x-1} = 0$ prenons pour racines de l'équations $\frac{x^{n^s}-1}{x-1} = 0$, toutes les puissances de R moindres que n^s, c'est-a dire, $R, R^2, ..., R^n, R^{n+1}, ..., R^{n^s-1}$ en observant qu'au lieu de $r = cos\frac{kP}{n} + isin\frac{kP}{n}$ on a ici $R = cos\frac{kP}{n^s} + isin\frac{kP}{n^s}$.
Parmi ces racines nous prenons pour l'équation $z = 0$, d'abord les m puissances de R exprimées par les résidus quadratiques (mod n) multipliés par n^{s-1}, par exemple si on a $g^4 \equiv a$ (mod n) [alors] $R^{(an)n^{s-1}}$ sera une de ces racines; leur somme sera (m, 1); car (m,1)est la somme de toutes les puissances de $r = cos\frac{kP}{n} + isin\frac{kP}{n}$ exprimées par les résidus quadratiques (mod n) et il est clair que $R^{n^{s-1}} = (cos\frac{kP}{n^s} + isin\frac{kP}{n^s})^{n^{s-1}} = cos\frac{kP}{n} + isin\frac{kP}{n}$.
Nous prenons ensuite les mn puissances de R exprimées par les résidus quadra-tiques (mod n) augmentés du nombre n, multiplié par 0, 1, 2,..., n-1 et multi-pliés par n^{s2}, par exemple si on a $g^4 \equiv a$(mod n) [alors] $R^{(a+hn)n^{s-2}}$ sera une de ces racines, n étant un quelconque des nombres 0,1,2,...,n-1. Si on fait $r' = cos\frac{kP}{n^2} + isin\frac{kP}{n^2}$ et que l'on prenne (m,1/n) pour la somme des puissances de r' exprimées par les résidus quadratiques (mod n) on aura pour la somme des mn racines, $(m, 1/n)(1 + r'^n + r'^{2n} + r'^{3n} + ... + r'^{(n-1)n})$ et réservant r, pour exprimer les racines del'équation $x^n - 1 = 0$, cette quantité deviendra $(m, 1)(1 + r + r^2 + r^3 + ... + r^{n-1})$ qui est visiblement égale à zéro,

puisqu'elle est multipliée par la somme des racines de l'équation $x^n - 1 = 0$. La somme de ces racines peut encore etre consideree comme celle des puissances de r' exprimées par les résidus quadratiques (mod n^2), car ces résidus ne peuvent différer de ceux (mod n) que de la quantite n prise un nombre de fois moindre que n, et sous ce point de vue, elle peut etre mise sous la forme $[1] + [g^2] + [g^4] + ... + [g^{n(n-1)-2}] = (mn, 1)$.
Nous prenons de meme les mn^2 puissances de R exprimées par les residus quadratiques (mod n^2) augmentés du nombre n^2, multiplié par $0, 1, ..., n1$ et multipliées par n^{s-3}, par exemple, si on a $y^4 \equiv a + hn \pmod{n^2}$ [alors] $R^{(a+hn+h'n^2)n^{s-3}}$ sera une de ces racines. Si on fait $r'' = cos\frac{kP}{n^3} + isin\frac{kP}{n^3}$, et que l'on prenne (mn,1) pour la somme i-ième puissances de r'' exprimées par les résidus quadratiques $(mod \quad n^2)$, on aura pour la somme des mn^2 racines $(mn, \frac{1}{n})(1 + r''^{n^2} + r''^{2n^2} + ... + r''^{(n-1)n^2}) = (mn, \frac{1}{n})(1 + r + ... + r^{n-1}) = 0$.
La somme des ces racines peut encore etre considerée comme celle des puissances de r'' exprimées par les résidus quadratiques $(mod \quad n^3)$, car ces résidus ne peuvent differir de ceux $(modn^2)$ que de la quantité n^2 prise un nombre de fois moindre que n, et sous ce point de vue elle peut etre mise sous la forme $[1] + [g^2] + [g^4] + ... + [g^{n^2(n-1)-2}] = (mn^2, 1)$.
On trouvera de meme que la somme des mn^3 racines doit etre exprimée par $(mn^3, 1)$ et qu'ayant aussi $1 + r + r^2 + ... + r^{n-1}$ pour facteur elle est égale a zéro; il en est de meme des mn^4 racines et de $mn^5, mn^6, ..., mn^{s1}$ racines. Aussi la somme des $m + mn + mn^2 + ... + mn^{s1}$ racines de l'équation $z = 0$ sera $(m, 1) + (mn, 1) + (mn^2, 1) + ... + (mn^{s1}, 1)$, et elle se réduira, a cause de $(mn, 1) = 0, (mn^2, 1) = 0, ..., (mn^{s1}, 1) = 0$, a $(m, 1)$.
Il est visible par la nature des périodes $(mn, 1), (mn^2, 1), ..., (mn^{s-1}, 1)$ qu'elles seroient encore équal a zéro, si on élevait tous leur térmes à une puissansce quelconque q (q etant premier à n) car elle resteront toujours multipliées par la quantité $1+r+r^2+...+r^{n-1}$, d'où il résulte que $(mn, g), (mn^2, g), ..., (mn^{s-1}, g)$ seront également nulles, c'est-a dire que la somme des racines de l'équation $z' = 0$, se reduit à (m, g). Il en résulte encore que la somme des puissances q iémes des racines c' est-a dire $(m, q) + (mn, q) + ... + (mn^{s-1}, q)$ se réduit à (m,q); car $(mn, q), (mn^2, q), ..., (mn^{s-1}, q)$ sont $= 0$.
Si on élevait tous les termes des périodes $(mn, 1), (mn, g)$ à la puissance n on aurait $(mn, n) = n(m, 1), (mn, ng) = n(m, g)$, puis à la puissance n^2 on aurait $(mn, n^2) = n(m, n) = n, (mn, n^2g) = n(m, gn) = n$, les périodes $(mn^2, n), ..., (mn^2, ng)$ sont nulles mais $(mn^2, n^2) = n^2(m, 1), (mn^2, g^2n^2) = n^2(m, g)$ en poursuivant les memes calculs on voit que les coefficients des équations $z = 0$, $z' = 0$ satisfont aux conditions exigées.

Exemples

Soit $n = 3, s = 2$,
$z = x^{3+1} - Vx^3 + V'x^2 - V''x + V''' = 0.$

On trouve en employant pour calculer les coefficients $V, V', ...$ la méthode de l'art. 349:
$V = (1,1), V' = 0, V'' = (1,1), V''' = (1,2),$

$z = x^4 - (1,1)x^3 - (1,1)[x] + (1,2),$

$R = x^4, S = -x^3 - x, T = 1, Y = 2R - S - T = 2x^4 + x^3 + x - 1,$

$Z = T - S = x^3 + x + 1$

Soit
$n = 3, s = 3,$

$z = x^{9+3+1} - Vx^{9+3} + V'x^{9+2} - V''x^{9+1} + V'''x^9 - V''''x^8 + V^v x^7 - V^{vi}x^6$
$+V^{vii}x^5 - V^{viii}x^4 + V^{ix}x^3 - V^x x^2 + V^{xi}x - V^{xii} = 0.$

On trouve
$V = (1,1), \quad V' = 0, \quad V'' = (1,1), \quad V''' = (1,2), \quad V''' = 0, \quad V^v = 0, \quad V^{vi} = 0,$
$V^{vii} = 0, V^{viii} = (1,1), V^{ix} = (1,2), V^x = 0, V^{xi} = (1,2), V^{xii} = 1 :$

$z = x^{13} - (1,1)x^{12} - (1,1)x^{10} + (1,2)x^9 - (1,1)x^4 + (1,2)x^3 + (1,2)x - 1 = 0,$
$R = x^{13} - 1, \quad S = -x^{12} - x^{10} - x^4, \quad T = x^9 + x^3 + x,$
$Y = 2x^{13} + x^{12} + x^{10} - x^9 + x^4 - x^3 - x - 2, \quad Z = x^{12} + x^{10} + x^9 + x^4 + x^3 + x.$

Soit
$n = 5, s = 2;$

$z = x^{2\cdot5+2} - Ax^{2\cdot5+1} + Vx^{2\cdot5} - A'x^{2(51)} + V'x^{2(5-1)-1} - A''x^{2(5-1)-1} + V''x^{2(5-2)}$
$-A'''x^{2(5-2)-1} + V'''x^{2(5-2)} A'''x^{2(5-2)-s} + V'''x^2 - A^v x + V^v = 0.$

On trouve
$A = (2,1), \quad A' = 0, \quad A'' = (2,1), \quad A''' = (2,1), \quad A''' = 0,$
$A^v = (2,1), \quad V = 1, \quad V' = 0, \quad V'' = 2 + (2,2), \quad V''' = 0, \quad V'''' = 1, \quad V^v = 1$

$z = x^{12} - (2,1)x^{11} + x^{10} - (2,1)x^7 + [(2,2)+2]x^6 - (2,1)x^5 + x^2 - (2,1)x + 1 = 0.$
$R = x^{12} + x^{10} + 2x^6 + x^2 + 1, \quad S = -x^{11} - x^7 - x^5 - x, \quad T = x^6,$
$Y = 2x^{12} + x^{11} + 2x^{10} + [x^7] + 3x^6 + x^5 + 2x^2 + x + 2, \quad Z = x^1 1 + x^7 + x^6 + x^5 + x.$

En examinant la maniére dont se forment les coefficien[t]s de l'équation $z = 0$, nous avons remarqué que les $m + mn + mn^2 + ... + mn^{s-2}$ premiers coefficien[t]s de l'équation du $(m + mn + mn^2 + ... + mn^{s-1})^{ime}$ degré sont égaux à ceux de l'équation du$(m + mn + mn^2 + ... + mn^{s-2})^{ime}$ degré, que les $m + mn + mn^2 + ... + mn^{s-2}$ suivants sont égaux à zéro, et que le $(2m + 2mn + 2mn^2 + ... + 2mn^{s-2})^{ime}$ est $(m, 1)$ de sorte que si on connait les coefficients de l'équation $z = 0$ du $(\frac{n^{s-1}-1}{2})^{ime}$ degré on a sans calcul les $2m + 2mn + 2mn^2 + ... + 2mn^{s-2} + 1 = n^{s-1}$ premiers, de l'équation $z = 0$ du $\frac{ns-1}{2})^{ime}$ degré.
On trouve aussi par cette méthode qu'il y a au moins 2^{s-1} valeurs différentes de Y et Z:car,en reprenant la somme $(m, 1) + (mn, 1) + (mn^2, 1) + ... + (mn^{s-1}, 1)$ des racines de l'équation $z = 0$, on voit que l'ont peut changer $(mn, 1)$ en (mn, g) sans que les précédentes conclusions soient [soyent] altérées, et comme il y a $s-1$ quantités $(mn, 1), (mn^2, 1) + ... + (mn^{s-1}, 1)$ et que les memes changements peuvent etre faits 1 a 1, 2 a 2, etc. on a en ajoutant 1 pour le cas où il n'y a aucun changement $1 + s - 1 + \frac{(s-1)(s-2)}{2} + \frac{(s-1)(s-2)(s-3)}{2 \cdot 3} + etc. = 2^{s-1}$ pour le nombre des différentes formes de cette somme. Ces changements n'influissent à la verité que sur les puissances n, n^2, etc. des racines à cause de $(mn, n) = n(m, 1), (mn^2, n^2) = n^2 = n^2(m, 1)$, etc. mais cela suffit à y donner des valeurs differentes pour R, T et S et par conséquent aussi pour Y et Z.

Nous avons remarqué que les coeficients des termes de Y et Z art. 357 sont, pour $n = 4k + 1$ les memes et de memes signes à partir de x^m qu'a partir de 1; c'est-a-dire, que si on a N pour coefficient de x^{m-h} dans Y ou Z, N sera aussi coefficient de x^h dans la meme quantité. Pour $n = 4k + 3$ les memes coefficients sont de signes contraires; c'est-à-dire, que si on a N pour coefficient de x^{m-h} dans Y ou Z, N sera coefficient des x^h dans la meme quantité. Pour démontrer cette règle nous observerons que les coefficients de Y et Z dépendent de ceux des différents termes de $z = 0$ et $z' = 0$; or l'équation $z = 0$, peut etre mise sous cette forme $z = (x - [1])(x - [g^2])(x - [g^4])...(x - [g^{n-3}]) = 0$, et a cause de $[1][g^2][g^4]...[g^{n-3}] = [1 + g^2 + g^4 + ... + g^{n-3}] = [0] = 1$. On peut donc multiplier le second nombre par $([1][g^2][g^4]...[g^{n-3}])^{m-1}$ sans que le premier recoive aucun changement.
Effectuant donc cette multiplication de maniére que chaque facteur se trouve multiplié par le produit de toutes les racines $[1], [g^2]$,etc. moins celle qui en-

tre dans ce facteur, et réduisant l'équation devient $z = (x[-1]-1)(x[-g^2]-1)(x[-g^4]-1)...(x[-g^{n-3}]-1)$
Lorsque $n = 4k+1, -1$ étant résidu quadratique, l'équation se transforme ainsi: $z = (x[1]-1)(x[g^2]-1)(x[g^4]-1)...(x[g^{n-3}]-1)$ et comme le nombre $m = 2k$ des facteurs est pair on peut changer tous les signes ce qui donne $z = (1-x[1])(1-x[g^2])(1-x[g^4])...(1-x[g^{n-3}])$.
Cette forme compareée à la première montre que z est fonction homogéne de x et de 1.
Lorsque $n = 4k+3, -1$ est non résidu, ainsi la valeur de z doit etre mise sous la forme $z = (x[g]-1)(x[g^3]-1)(x[g^5]-1)...(x[g^{n-2}]-1)$: qui étant comparée à celle de z', savoir $z' = (x-[g])(x-[g^3])(x-[g^5])...(x-[g^{n-2}])$ montre que zz'' et par conséquent aussi Y et Z sont fonctions homogènes de x et -1.

La méthode de l'art. 345 donne après les réductions convenables. Pour n = 4k + 1 $q^2 = m+(m,2)+2(m,1+g^2)+(m,1+g^4)+(m,1+g^6)...+(m,1+g^{m-2})$.
Et on tire de la considération des deux équations $(p-q)^2 = n, (p+q)^2 = 1$ cette autre valeur de $q^2, q^2 = k+1+p$: donc si $k+1$ est pair, il faut que $(m,2) = p = (m,g)$,c'est-à-dire que 2 soit non résidu: au contraire si $k+1$ est impair il faut que $(m,2) = (m,1)$ car $1-(m,1) = -2(m,1)-(m,g) = -2(m,1)-p$, c'est-à-dire que 2 soit résidu.
Ainsi 2 est résidu des nombres premiers de la forme $8k'+1$ et non résidu de ceux de la forme $8k'+5$.
La comparaison des deux valeurs de q^2 relatives a $n = 4k+3$ donne de meme $-k+p = (m,2)+2(m,1+g^2)+(m,1+g^4)+...+(m,1+g^{m-1})$ et par conséquent $p = (m,2)$ lorsque k est pair et $q = (m,2)$ lorsque k est impair c'est-à- dire 2 non résidu pour les nombres de la forme $8k'+3$ et résidu pour ceux de la forme $8k'+7$.
Les précédents théorèmes sont démontrés dans plusieurs endroits du livre, par des méthodes qui diffèrent toutes de celle-ci.

On peut démontrer l'impossibilité de satisfaire en nombres entiers à l'équation $x^{p-1}+y^{p-1} = z^{p-1}$, p étant un nombre premier de la forme $8n+7$.
En effet, si on veut satisfaire à l'équation $x^{p-1}+y^{p-1} = z^{p-1}$, p étant un nombre premier quelconque, il faut prendre pour x ou y un multiple de p. Car faisant d'abord x, y et z premiers à p et mettant la proposée sous la forme $x^{p-1}-1+y^{p-1}-1 = z^{p-1}-2$, il en résultera, à cause de $z^{p-1}-1 \equiv 0$ (mod p), $\equiv 0$, et faisant ensuite x et y premiers à p et z multiples de ce nombre on sera mené à conclure $2 \equiv 0$.
Soit donc x impair et multiple de p, en mettant $2p'$ au lieu de $p-1$ et phf à la place de x la proposée devient $(phf)^{2p'}+y^{2p'} = z^{2p'}$, ou $z^{2p'}-y^{2p'} = (phf)^{2p'}$

d'où on tire $y^{p'} \pm z^{p'} = (pf)^{2p'}$, $y^{p'} \mp z^{p'} = h^{2p'}$, $2y^{p'} = (pf)^{2p'} + h^{2p'}$, h étant premierà p, $h^{2p'} - 1 \equiv 0(modp)$ donc aussi $2y^{p'} - 1 \equiv 0(modp)$, et a cause de $y^{2p'} - 1 \equiv 0$, $y^{p'} \equiv 2$, $y^{2p'} \equiv 4 \equiv 1$ d'où résulte $p = 3$.
Supposons donc $y = 2pfh$, la proposée deviendra $(2pfh)^{2p'} = x^{2p'} - z^{2p'}$. Examinons d'abord le cas ou $x^{p'} \pm z^{p'} = 2p^{2p'} f^{2p'}$, $x^{p'} \mp z^{p'} = 2^{2p'-1} h^{2p'}$ d'où on tire $2x^{p'} = 2p^{2p'} f^{2p'} + 2^{2p'-1} h^{2p'}$ et $(2h)^{2p'} \equiv 1(\text{mod p})$, $4x^{p'} \equiv 2^{2p'} h^{2p'}$, $4x^{p'} \equiv 1 \equiv x^{2p'}$, $4 \equiv x^{p'}$, $16 \equiv x^{2p'} \equiv 1$ c'est-à-dire $15 \equiv 0$ et par conséquent $p = 3$ ou $p = 5$.
Supposons enfin $x^{p'} \pm z^{p'} = 2f^{2p'}$, $x^{p'} \mp z^{p'} = 2^{2p'-1} p^{2p'} h^{2p'}$, d'où on tire $2x^{p'} = 2f^{2p'} + 2^{2p'-1} p^{2p'} h$ ou $x^{p'} = f^{2p'} + 2^{2p'-2} p^{2p'} h^{2p'}$ soit $x = f^2 + mp^{2p'}$ le dévelopement donne $f^{2p'} + p' f^{2p'-2}(mp^{2p'}) + ... \equiv f^{2p'} + 2^{2p'-2} p^{2p'} h^{2p'}$, $p' f^{2p'-2}(mp^{2p'}) + ... = 2^{2p'-2} p^{2p'} h^{2p'}$ ou $p' f^{2p'-2}(m) + ... = 2^{2p'-2} h^{2p'}$ comme tous les termes suivants du dévelopement de $f^2 + mp^{2p'}$ sont multiples de m, il faut que $h^{2p'}$ soit divisible par ce nombre et comme tous les facteurs de $h^{2p'}$ sont élevés à la puissance $2p'$ on doit faire $m = k^{2p'}$. L'équation devient $p' f^{2p'-2} k^{2p'} + ... = 2^{2p'-2} h^{2p'}$ ou $4p' f^{2p'-2} k^{2p'} \equiv 2^{2p'} h^{2p'} \equiv 1(\text{mod p})$ et à cause de $k^{2p'} \equiv 1$, $4p' f^{2p'-2} \equiv 1 \equiv f^{2p'}$ d'où on tire $4p' \equiv f^2$ mais à cause de $2p' + 1 = p$, $4p' \equiv -2$ d'ou resulte $-2 \equiv f^2$.
Ainsi l'équation $x^{p-1} + y^{p-1} = z^{p-1}$ est impossible lorsque -2 est non résidu quadratique: c'est ce qui a lieu pour les nombres premiers des formes $8n + 5$, $8n+7$. Mais nous avons vu plus haut que le cas $p = 5$ échape à notre méthode et d'aillieurs l'impossibilité de l'équation $x^4 + y^4 = z^4$ a eté démontrée ainsi elle est uniquement appliquable aux nombres $8k + 7$.

La risposta di Gauss

Brunswick 16 juin 1805
Monsieur, il me faut vous demander mille fois pardon d'avoir laissé six mois sans réponse l'obligeante lettre dont vous m'avez honoré. Certainement je me serais empressé de vous témoigner tout de suite combien m'est cher l'intérét que vous prenez aux recherches auxquelles j'ai dévoué la plus belle partie de ma jeunesse, qui ont été la source de mes jouissances les plus délicieuses et qui me seront toujours plus chères qu'aucune autre science. Mais je me flattais de temps en temps de pouvoir gagner assez de loisir pour mettre en ordre et vous communiquer pour écrit l'une ou l'autre de mes autres recherches arithmétiques, pour vous rendre en quelque sorte le plaisir que vous m'avez fait par vos communications. Mon espérance a été vaine. Ce sont surtout mes occupations astronomiques qui à présent absorbent presque tout mon temps. Je me réserve pourtant de m'entretenir avec vous des mystères de mon arithmétique chérie, aussitot que je serai assez heureux d'y pouvoir retourner.
J'ai lu avec plaisir les choses que vous m'avez bien voulez communiquer ; je

me félicite que l'arithmétique acquiert en vous un ami assez habile. Surtout votre nouvelle démonstration pour les nombres premiers, dont 2 est résidu ou non résidu, m'à extrémement plu ; elle est très fine, quoiqu'elle semble etre isolée et ne pouvoir s'appliquer à d'autre nombres. J'ai très souvent considéré avec admiration l'enchainement singulier des vérités arithmetiques. Par exemple, le théorème que je nommé fondamental (art. 131) et les théorèmes particuliers concernant les résidus 1 ± 2, s'entrelacent à une foule d'autres vérités où l'on les aurait jamais cherché! Outre les deux démonstrations que j'ai données dans mon ouvrage, je suis en possession de deux ou trois autre, qui du moins ne le cèdent pas à celle-là en question d'élégance.
Je remarque avec beaucoup de regret que les autres occupations ou je suis engagé ne me permettent point du tout de me livrer à présent à mon amour pour l'arithmétique. Ce ne sera peut-etre qu'après plusieurs années que je pourrai penser à la publication de la suite de mes recherches qui rempliront aisément un ou deux volumes semblables ou premier. Mais je croirais n'avoir pas assez vécu, si je mourrais sans avoir achevé toutes les recherches intéressantes auxquelles je me suis une fois livré. Au reste, chez nous en Allemagne, la publication d'un tel ouvrage a ses difficultés : quoiqu'on en dise, le gout pour les mathématiques pures, si l'on cherche de la profondeur, n'est pas trop général. Nos libraires ne se mélent guère de ces sortes de livres, et je ne suis pas assez riche pour faire à mes frais l'impression et me soumettre à la malhonnéteté des libraires étrangers, comme il m'est arrivé à l'occasion du premier volume. Un M.***, par exemple libraire à Paris, a recu de moi, il y a presque trois ans, des exemplaires pour la valeur de six cent quatre-vingt francs ; mais jamais je n'ai recu un sou de lui, et il ne s'est meme pas donné la peine de répondre à mes lettres.
Peut-etre vous pourriez me donner des renseignements par quel moyen, on pourrait engager cet homme à faire son devoir.
Agréez, Monsieur, l'expression de ma haute considération.

Ch.Fr. Gauss.

IX

Paris (Rue de Braque n.4) ce 12 mai 1819
Monsieur,
Je regrette infiniment que vous n'ayez pas accompagné Monsieur votre ami; j'aurais eu le plus grand plaisir a vous entendre parler des belles théories

qui sont l'objet de vos études favorites et pour lequelles j'ai moi meme une véritable passion.
Les démonstrations nouvelles que contient votre mémoire m'ont enchan-tée. Vous paraissez préférer la dernière à cause de la liason qu'elle établit entre des vérités qui au premier coup d'oeil semblent etre independants. J'ai sans doute été fort sensible à ce genre de surprise que déjà plusieurs endroits des disquisitiones m'avoient fait éprouver. Cependant je vous avourez que l'énoncé du théorème nr. 2 m'a plu encore d'avantage. Cette phrase qui le termine: *Tunc tres numeri n, N, 1/4(m- 1)(N - 1), vel omnes simul pares erunt, vel unus par duoque reliqui impares* m'a frappé d'un genre d'admiration en quelque sorte contraire a celui dont je viens de parler car on y sent la démonstration toute entière et par cette raison elle me semble avoir atteint le plus haut degre d'elegance que l'on puisse immaginer.
C'est toujours avec un nouvel intéret que l'on considère des points de vue différents d'une meme verité: l'applications entièrement neuve que vous faites du théorème foundamental à la detérmination de la question de résidu ou non résidu présent un autre genre de jouissance: c'est une véritable acquisition qui peut etre d'un grand usage.
Je regrette que vous différiez depuis si longtem[p]s de nous donner vos recherches sur les résidus cubiques et biquarrés en traitant ces questions il est probable que vous auriez le moyen d'aller encore plus loin, je veux dire d'étendre la théorie aux résidus puissance quelconque.
Je n'ai pas encore eu le tem[p]s de lire le mémoire sur les attractions , je me propose de l'étudier car cet objet m'est beaucoup moins familier que la théorie des résidus. J'ai voulu me réserver avant le départ de Monsieur votre ami, le tem[p]s de vous faire les remerciements que je vous dois et aussi de vous communiquer les recherches que m'ont occupées depuis l'époque à laquelle j'ai eu l'honneur de vous écrire.
Quoique j'ai travaillé pendans quelque tem[p]s à la théorie des surfaces vibrantes (à laquelle j'aurais beaucoup de choses à ajouter si j'avais la raison de faire les expériences que j'ai imaginés concernants les surfaces cylindriques) je n'ai jamais cessé de penser à la théorie des nombres. Je vous donnerai une idée de ma préoccupation pour ce genre de recherces en vous avouant que meme sans aucune expérance de succès je la préfère à un travail qui me donnerait nécessairement un résultat et qui pourtant m'intéresse...quand j'y pense.
Longtem[p]s avant que notre académie ait proposé pour sujet de prix la dé-

Il testo in questione è quello di Gauss del 1819 *Theorematis fundamentalis in doctrina de residuis quadraticis, demonstrationes et ampliationes novae*

L'opera di cui si parla è probabilmente *Theoria attractionis corporum sphaerodicorum ellipticorum homogeneorum methodo nova tractata*

monstration de l'impossiblité de l'équation de Fermat, cet[te] espèce de défi porté aux théories modernes par un géomètre qui fuit privé des res[s]ources que nous possédons aujourd'hui, me tourmentait souvent. J'entre-voyais vaguement une liaison entre la théorie des résidus et la fameuse équation, je crois meme vous avez parlé anciennement de cette idée car elle m'a frappée aussitot que j'ai connu votre livre.
Voici ce que j'ai trouve:
L'ordre dans lequel les résidus (puissances égales à l'éxposant) se trouvent placés dans la série des nombres naturels détermine les diviseurs nécessaires qui appartiennent aux nombres entre lequels on établit non seulement l'équation de Fermat mais encore beaucoup d'autres équations analogues a celle-là. Prenons pour exemple l'équation meme de Fermat qui est la plus simple de toutes celles dont il s'agit ici.
Soit donc, p étant un nombre premier, $z^p = x^p + y^p$.
Je dis que si cette équation est possible, tout nombre premier de la forme 2 N p + 1 (N étant un entier quelconque) pour lequel il n'y aura pas deux résidus p-ième puissance placés de suite dans la série des nombres naturels divisera nécessairement l'un des nombres x, y et z.
Cela est évident, car l'équation $z^p = x^p + y^p$ donne la congruance [congruence] $1 \equiv r^{sp} - r^{tp}$ dans la quelle r représente une racine primitive et s et t des entiers.
On sait que l'équation a une infinité de solutions lorsque p = 2. Et en effet tous les nombres, exceptés 3 et 5 ont au moins deux résidus quarrés dont la difference est l'unité. Aussi dans ce cas la forme connue savoir $h^2 + f^2$, $2fh$, $h^2 - f^2$ des nombres z [x], y et z montre-t-elle que l'un de ces nombres est multiple de 3 et aussi que l'un des memes nombres est multiple de 5.
Il est aisé de voir que si un nombre quelconque k est résidu puissance p-ième mod 2N p + 1 et qu'il y ait deux résidus puissance p-ieme meme mod. dont la différence soit l'unité, il y aura aussi deux résidus puissances p-ième dont la différence sera k.
Mais il peut arriver qu'on ait deux résidus p-ième dont la différence soit k, sans que k soit résidu p-ième.
Cela posé voici l'équation générale dont la solution me semble dépendre comme celle de Fermat de l'ordre des résidus:

$$kz^n = x^p \pm y^p$$

car d'après ce que vient d'etre dit on voit que tous nombre premier de la forme 2N p+1 pour lequel deux résidus p-ièmes n'ont pas le nombre k pour différence divise le nombre z [l'un des nombres x, y, z]. Il suit delà que s'il y

avait un nombre infini de tels nombres l'équation serait impossible.
Je n'ai jamais pu [pu] arriver à l'infini quoique j'ai reculé bien loin les limites par un méthode de tatonnement trop longue pour qu'il me soit possible de l'exposer ici. Je n'oserais meme pas affirmer que pour chaque valeur de p il n'existe pas une limite au-delà de laquelle tous les nombres de la forme 2 N p + 1 auraient deux résidus p-ièmes placés de suite dans la série des nombres naturels. C'est le cas qui intéresse l'équation de Fermat.
Vous concevrez aisément, Monsieur, que j'ai du parvenir à prouver que cette équation ne serait possible qu'en nombres dont la grandeur effraye l'imagination; car elle est encore assujettie à bien d'autres conditions que je n'ai pas le tem[p]s d'examiner à cause des détails nécessaires pour [en] établir la réalité. Mais tout ce la n'est encore rien, il faut l'infini et non pas le très grand.
Chemin fesant [faisant] je me suis aidée d'un systéme de six congruances [congruences] dont une quelconque redonne les cinq autres. Lorsque pour un nombre de la forme 2N p + 1, 2 est non résidu puissance p-ième et qu'en meme tem[p]s N est premier à 3 les six congruances [congruences] ne sont pas réductibles à un moindre nombre. On peut etre sur alors (n étant un nombre entier différent pour chaque valeur de 2N p + 1) qu'il y a toujours $6n$ résidus p-ièmes (mod 2N p + 1) placés deux à deux près l'un de l'autre dans la série des nombres naturels. J'ai fait beaucoup d'efforts pour trouver les cas dans laquelles n = 0. La méthode que j'ai emploié [employée] montre que le nombre des conditions à remplir pour que n ne soit pas zéro dépend de la valeur de N dans le nombre 2Np + 1 que l'on prend pour modul[e]: elle est parfaitement indépendante de celle de p (par conséquent [dans] tout [ce] qui suit p ne répresente plus exclusi[ve]ment les nombres premiers mais des entiers quelconques c'est ce qui est évident par les exemples que je citerai dans la suite) en sorte que toute les fois que je calculais des valeur de N pour lesquelles 2N +1 ou 4N +1 étaient premiers je trouvais toujours moyen de remplir les conditions exigées. Cela doit etre en effet puisqu'il y a toujours deux résidus puissance placés de suite dans la série des nombres naturels et qu'excepté pour 3 et pour 5 il y a toujours aussi deux résidus quarrés placé de suite.
Lorsque N n'est pas trop grand on n'a qu'un petit nombre de conditions à essayer et si on ne trouve aucun nombre qui y satisfasse on peut etre sur que quelque soit p on n'a jamais deux résidus p-ièmes (mod 2N p + 1) placés de suite dans la série des nombres naturels.
La méthode donne toutes les valeurs de p pour lesquelles il y a deux résidus qui se suivent, elle donne aussi pour chaque valeur de p la totalité des cas où un résidu p-ième est suivi d'un semblable residu. Elle donne avec un égale facilité les cas où l'intervalle qui sépare deux résidus p-ièmes est k mais si k est > 1 le système des six congruences n'a plus lieu. Cette méthode n'a

d'autre inconvénient que la longueur lorsque N est un peu grand. A la vérité certains artifices de calcul qui se présentens naturellement peuvent l'abréger un peu. Au reste les calculs qu'elle exige sont extremement simples et faciles. Voici quelques exemples extraites d'une note déjà ancienne que je n'ai pas le tem[p]s de vérifier:
En excluant p = 1 et p = 2 on trouve qu'aucun nombre premier des formes 4 p + 1, 8p + 1 ne peuvent avoir deux résidus p-ièmes dont la difference soit l'unité: que le seul nombre premier de la forme 10 p + 1 qui ait deux résidus de suite est $10 \cdot 3 + 1$: Que les seuls nombres de la forme 14 p + 1 qui ayent [ayant] deux résidus de suite sont $14 \cdot 3 + 1$ et $14 \cdot 9 + 1$: que le seul nombre de la forme 16p + 1 qui ait deux résidus de suite est $16 \cdot 16 + 1$: que le seul nombre de la forme 20 p + 1 qui ait deux résidus de suite est $20 \cdot 16 + 1$.
Je suppose que vous avez sous les yeux le mémoire ou plutot le projet de mémoire de Mr. Poinsot car il faut faire soi-meme le travail que l'auteur s'est épargné. Quoi- qu'il en est soit son idée m'a parue fort heureuse. J'ai admiré comment étant partis de principes si différen[t]s, il m'avait fourni en quelque sorte la méthaphisique de ma méthode. En effet en fesant [faisant] usage de la remarque de cet auteur on voit comment j'ai du arriver aux résultats que je viens d'exposer car il s'agit ici de traiter les racines de l'équation binome du degré 2N, et quoique les quantités résultantes de la combinaison de ces racines (ou ce qui revient au meme, et est plus conforme à la méthode que j'ai employée de la combinaison de leurs puissances) ne puisse devenir réeles que pour certaines valeurs de 2N p + 1 et par conséquent aussi de p, leurs rapports entr'elles [entre-elles] sont indépendants des valeurs de p.
J'ai cherché aussi à appliquer les idées de Mr. Poinsot aux nombres de la forme $2^s p + 1$ qui donnent à résoudre une équation binome de l'ordre 2^s .
J'aurais voulu établir un rapport entre les valeurs des racines de cette équation et celle de l'équation du degré $2^{s'}$ qui donne les résidus p-ièmes puissances (mod $2^{s'}p + 1$). Si on pouvait trouver dans quels cas le nombre $2^s p + 1$ se trouve parmi les racines de l'équation de l'ordre $2^{s'}$ et vice-versa dans quels cas $2^{s'}p + 1$se trouve parmi les racines del'équation del'ordre $2^{s'}$ cela serait fort jolie et tout à fait analogue au théorème fondamental, mais je n'y suis pas.
La notation de Mr. Poinsot m'a encore fourni une nouvelle manière de prouver que 2 est résidu quarré des nombres de la forme 8n + 1 e non résidu quarré de ceux de la forme 8n + 5: je ne sais pourquoi cette vérité se montre sous tant de faces différentes. Voici ce que c'est: $2\sqrt{-1} = (1 + \sqrt{-1})^2$ parconséquent $2\sqrt{-1}$ est résidu quarré: si le modul[e] est $8n+1$, $\sqrt{-1}$ est résidu quarré: si le modul est $8n + 5$, $\sqrt{-1}$ est non résidu quarré donc etc.
On voit aussi au moyen de cette notation que si 2 est résidu p-ième (mod 2Np+1), p étant toute fois un nombre impair, on aura trois résidus p-ièmes

qui se suivront dans la série des nombre naturels. Ces trois résidus seront $\sqrt{-1}-1$,$\sqrt{-1}$, $\sqrt{-1}+1$. En effet si 2 est rèsidus p-ième $\pm 2\sqrt{-1}$ et par conséquent aussi $(\sqrt{-1}\pm 1)^2$ et $\sqrt{-1\pm 1}$ seront également résidus p-ième donc etc.

Je réclame votre indulgence pour le peu de soin avec lequel est rédigée cette longue lettre. Je n'ai pas eu le tem[p]s nécessaire pour mettre plus d'ordre dans mes idées. J'ai ecrit d'abondance et de souvenir et par conséquent trop lachement. Je n'ai pas voulu manquer l'occasion de vous consulter sur l'importance qu'il est permis d'attacher aux idées que j'ai l'honneur de vous communiquer. Je serais surtout curieuse de savoir ce que vous pensez du parti que l'on peut tirer de l'ordre dans lequel les residus p-iémes se trouvent placés dans la série des nombres naturels. Je crois que cette considération est particulière et j'ai trop peu de confiance dans mon jugement pour oser décider si elle mérite d'etre suivie.

Je puis vous assurer, Monsieur, que c'est l'étude de votre livre qui a changé en passion le gout que j'avais déjà pour l'analyse indéterminée. Ce n'est pas ici le lieu de revenir sur les belles choses qu'il contient; elles ont été trop bien appréciées par tous ceux qui l'ont étudié pour qu'il me reste quelque chose de nouveau à en dire. Qu'il me soit permis cependant de vous tèmoigner à quel point la simple substitution des congruances [congruences] representèes par le signe $\equiv$ m'a paru importante. La notion d'égalité indiquée autrefois par le signe $=$ e me semblait toujour en contradiction avec la marche de l'analyse et je ne puis exprimer combien de netteté et par conséquent de facilité j'ai trouvé dans cette branche de calcul, avec le secours de votre notation. Il faut avoir manié le calcul pour sentir ces choses-là. A la verité avec ce secours je n'ai pas encore été bien loin.

Je vous aurais [aurez] la plus grande obligation si vous etes assez bon pour prendre la peine de me dire ce que vous pensez de la marche que j'ai suivie. Quelque soit votre avis je le recevrez [recevrais] avec respect et reconnaissance.

Agréez, Monsieur, l'assurance de la sincère admiration avec laquelle j'ai l'honneur d' etre

votre très humble servante
Sophie Germain

REMARQUE SUR L'MPOSSIBILITE DE SATISFAIRE EN NOMBRES ENTIERS A L' EQUATION $x^p + y^p = z^p$

L'impossibilité de cette équation serait hors de doute si on pouvait démontrer le théorème suivant:
Pour toute autre valeur de p que $p = 2$, il y a toujours une infinité de nombres premiers de la forme $N_{p+1} + 1$ pour lesquels on ne peut trouver deux résidus p^{ime} puissances dont la différence soit l'unité.
Après avoir établi qu'il résulterait en effet de ce théorème que dans l'équation $x^p + y^p = z^p$, les nombres x, y et z ne pourraient etre qu'infinis; je passe à l'examen de quelques propositions particulières qui au défaut d'une démonstration absolue, servent à établir au moins, la nécessité que les meme nombres x, y e z soient des nombres fort grands.
Je remarque d'abord, qu'en exceptant le cas où N est multiple de 3, si dans la forme $Np+1$ on conserve à N une valeur constante et que l'on fasse varier celle de p, on trouvera un nombre infini de nombres premiers appartenant à cette forme, pour lesquels il n'y aura pas deux résidus pièmes puissances qui se suivent immédiatement dans l'ordre des nombres naturels, et qu'au contraire il ne pourra jamais y avoir qu'un nombre fini de nombres premiers de la meme forme qui jouissent de la propriété opposée. Or puisque rient n'empeche de donner successivement à N un nombre infini de valeurs, on peut conclure de ce qui précède qu'il doit exister une infinité de valeurs de p pour lesquelles l'équation $x^p + y^p = z^p$ sera impossible. Cependant un pareil résultat est trop vague pour s'appliquer à la démonstration de l'impossibilité de la meme équation dans le cas d'une valeur déterminée de p. En effet si on dénote par a cette valeur, on pourra toujours craindre que les nombres $Na + 1$, $N'a + 1$ etc. se trouvent parmi les nombres premiers des formes plus générales $Np+1$, $N'p+1$ etc. pour lesquels il peut exister deux résidus pièmes puissances dont la différence soit l'unité; et, malgré le peu de probabilité que cette objection soit justifiée par l'examen, je n'ai pu réussir à la détruire.
Dans la vue de démontrer au moins qu'en supposant que l'équation $x^p + y^p = z^p$ soit satisfaite, les nombres x, y et z ne pouvant etre que des nombres fort grands, j'ai dressé une table des nombres premiers des formes $2p + 1, 4p + 1, 8p + 1, 10p + 1, 14p + 1, 16p + 1$ et $20p + 1$ pour lesquels il ne peut exister deux résidus puis- sances pièmes dont la différence soit l'unité en la bornant aux cas dans lesquels p est un nombre premier moindre que 100. Le théorème dont j'ai parlé comprend également à la vérité le cas où p est un nombre premier et ceux dans lesquels p est un nombre composé; mais puisque dans le cas de $p = 4$, l'impossibilité de l'èquations dont il s'agit, est démontrée d'une manière absolue (v. Théorie des Nombres de Mr. Le Gendre p. 203) on peut se contenter, dans les recherches sui- vantes, du cas où p est

un nombre premier. Il est aisé de voir au reste, que rien n'aurait e empeché de continuer cette table en donnant à p des valeurs plus grandes que 100.
Si pour prouver que x, y et z doivent etre des nombres fort grands on se bornait à la considération de l'impossibilité de trouver pour plusieurs des nombres premiers de la forme $Np + 1$, deux résidus puissances pièmes dont la différence soit l'unité, on serait obligé d'employer d'assez grands nombres de cette classe: heureusement on peut éviter un pareil embarras au moyen du théorème suivant: *Pour que l'équation* $x^p + y^p = z^p$ *soit satisfaite en nombres entiers, p étant un nombre premier quelconque, il faut que l'un des nombres* $x + y, z - y$ *et* $z - x$ *soit multiple de la* $(2p - 1)^{imes}$ *puissance du nombre p et des pièmes puissances de tous les nombres premiers de la forme* $Np + 1$*, pour lesquels, en meme tem[p]s que l'on ne peut trouver deux résidus pièmes dont la différence soit l'unité, p est non résidu puissance pième.*
Après avoir démontré ce théorème, je l'applique, à l'aide des nombres contenus dans la table dont j'ai parlé, à différentes valeurs de p. Le cas $p = 3$ ayant été démontré d'une manière absolue (v. Théorie des Nombres page 207) j'ai choisi pour premier exemple le cas $p = 5$, et j'ai trouvé, en employant seulement la considération des quatre nombres 31, 41, 71 et 101 que si l'équation $x^5 + y^5 = z^5$ est possible, les valeurs des x, y et z ne pourront jamais etre exprimées avec moins de 39 figures de chiffres.
Le valeurs suivantes de p, donnent, comme on le verra des résultats encore plus satisfaisants.
n.1. Il est aisé de voir qu'une condition indispensable à remplir pour que l'équation $x^p + y^p = z^p$ soit possible, est qu'un quelconque des nombres x, y et z soit multiple de chacun des nombres premiers de la forme $Np + 1$ pour lesquels il ne se trouve pas deux résidus pièmes [puissance] qui se suivent immédiatement dans la série des nombres naturels.
En effet, lorsque x, y et z sont premiers au nombre $Np+1$ si on dénote par r la puissance p^{ime} d'une des racines primitives (mod. $Np+1$) on a toujours, s, t et v étant des nombres entiers quelconques, $r^s \equiv x^p$, $r^t \equiv y^p$,$r^v \equiv z^p$ en sorte que l'équation à la quelle il faut satisfaire donne la congruence $r^s + r^t \equiv r^v$, et par conséquent celle-ci $r^{s-t} + 1 \equiv r^{v-t}$. Si l'un des nombres $s - t$ ou $v - t$ est négatif, on mettra à sa place $N + s - t$ ou $N + v - t$ ce qui, à cause de $r^N \equiv 1$, ne changera rien à la congruence. On sera donc toujours mené à conclure la nécessitè que deux rèsidus pièmes puissances (mod. $Np + 1$) ayant l'unité pour différence.
n.2. Dans le cas où $p = 2$, on peut toujours trouver, pour tout autre module que les nombres 3 et 5, deux résidus pièmes puissance, c'est à dire deux résidus quarrés dont la différence soit l'unitè. Pour le prouver je considérerai à part les nombres premiers de la forme $4k + 3$ et ceux de la forme $4k + 1$. A l'égard des nombres de la forme $4k + 3$, -1 est non résidu quarré, en sorte

que la série des nombres $1, 2, ..., 4k+2$, commence par un résidu et finit par un non résidu: ainsi, il faut pour que deux résidus ne s'y trouvent pas placés à coté l'un de l'autre, que chacun d'eux soit séparè du suivant par un non résidu, c'est à dire qu'il faut que tous les nombres pairs soient non résidus mais le quarré 4 se trouve nécessairement parmi ces nombres lorsque l'on donne à k toute autre valeur que zéro. Le nombre 3 est donc le seul nombre premier de la forme $4k+3$ pour lequel on ne puisse pas trouver deux résidus quarres dont la différence soit l'unité.

Lorsqu'il s'agit des nombres premiers de la forme $4k+1$, -1 est résidu ainsi la série des nombres naturels plus petits que $4k+1$, commence et finit par un résidu; deux non résidus doivent par conséquent s'y trouver placès à la suite l'un de l'autre; mais pour que deux des résidus ne jouissent pas de la meme propriété il faut qu'il n'y ait que deux seulement des non résidus qui ayent [ayant] l'unité pour différence. En général à cause de -1 résidu, si n et $n+1$ sont non résidus $4k-n$ et $4k-n+1$, seront aussi non résidus. On est donc mené, dans la supposition présente à la condition $4k-n=n$, $2k=n$. Il en résulte, comme dans le cas précédent, que tous les nombres pairs compris dans la série $1, 2, ..., 2k$, devront etre non résidus, et que le quarré 4 étant compris parmi ces nombres pour toute autre valeur de k que $k=1,5$ est le seul nombre premier de la forme $4k+1$, pour lequel on ne puisse pas trouver deux résidus quarrés dont la difference soit l'unité.

La forme connue de valeurs de x, y et z dans l'équation $x^2+y^2=z^2$ savoir $x=p^2-q^2$, $y=2pq$, $z=p^2+q^2$ montre en effet que l'un des nombres x, y et z est toujours multiple de 3 et que de meme aussi l'un de ces nombres est multiple de 5.

n. 3. Pour toute autre valeur de p que $p=2$, non seulement il n'est pas vrai que, les deux moindres des nombres premiers des formes $Np+1$ exceptés, on ait toujours deux résidus pièmes puissances dont la différence soit l'unité; mais au contraire il me parait certain qu'il y a toujours, alors, une infinité de nombres premiers des formes $Np+1$ *pour les quels il ne peut exister deux résidus* p^{imes} *puissances qui ayent [ayant] l'unité pour différence.*

Si ce théorème était démontré, l'impossibilité de satisfaire en nombres entiers à l'èquation $x^p+y^p=z^p$, pour toute autre valeur de p que $p=2$, en serait une conséquence immédiate; car un quelconque des nombres x, y et z devant alors etre multiple de chacun des nombres auxquels s'appliqueraient le théorème, ils seraient eux memes infinis.

Au défaut d'une démonstration absolue que j'ai inutilement cherchée, je me bornerai à indiquer une méthode propre à faire connaitre, pour quelque valeur de p que ce puisse etre, seux des nombres premiers des formes $Np+1$ qui pourront avoir deux résidus p^{imes} puissances dont la diffèrence soit l'unité.

n. 4. Tant que l'on veut comprendre dans une expression générale le cas $p=2$

et ceux qui se rapportent aux autres valeurs de p, on est obligé d'écrire $Np+1$ au lieu de $2Np+1$: car il est visible que cette dernière forme ne renfermerait que les nombres $4N+1$. Mais si on écarte cette valeur de p qui a été examinée à part, on verra aisément qu'en donnant à p les valeurs convenables, les nombres premiers seront tous renfermés dans la forme $2Np+1$.
Cette forme montre que, quelque soit p, -1 résidu puissance p^{ime}; par conséquent, excepté le cas où 2 serait résidu piéme puissance, il ne pourra exister qu'un nombre pair de résidus pièmes [puissance] qui augmentés de l'unité, donnent de nou- veaux résidus pièmes [puissance]. En effet si les nombres R est $R+1$ sont l'un et l'autre rèsidus pièmes, les nombres $2Np+1-R$ et $2Np-R$ le seront également; mais lorsque l'on aura $2Np-R=R$, $Np=R$ c'est à dire lorsque 2 sera résidu p^{imes} les deux couples de résidus p^{imes} [puissance] se réduiront à un seul.
Lorsque N est multiple de 3, c'est à dire lorsqu'il s'agit des nombres premiers de la forme $6N'p+1$, on peut toujours trouver deux résidus pièmes puissances qui, augmentés de l'unité, donnent de nouveaux residus piemes. En effet on peut toujours satisfaire alors à la congruence $x^3 \equiv 1$, et par conséquent à celle-ci $x^2-x+1 \equiv 0$ de laquelle il résulte que x et $x-1$ sont à la fois résidus puissances p^{imes}.
n. 5. Toutes les fois que 2 sera non résidu puissance pième, et que le nombre N sera premier à 3, on peut etre sur que s'il existe deux résidus pièmes (mod. $2Np+1$) dont la différence soit l'unité, il y aura en meme tem[p]s 5 autres couples de résidus puissances p^{imes} qui jouiront de la meme propriété.
En effet si, en dénotant comme je l'ai déjà fait $n1$, par r la puissance p^{ime} d'une des racines primitives (mod. $2Np+1$) et par s et t des nombres entiers quelconques, on suppose la congruence $1+r^t \equiv r$ s il en résultera les 5 suivantes:

$$1+r^{2N-t} \equiv r^{s-t}$$
$$1+r^{N-s} \equiv r^{t-s}$$
$$1+r^{N+s} \equiv r^{N+t}$$
$$1+r^{N+s-t} \equiv r^{N-t}$$
$$1+r^{N+t-s} \equiv r^{2N-s}$$

Pour saisir la loi suivant laquelle les 5 dernières congruences sont déduites de la première, il suffit d'observer qu'un terme conserve sa place lorsque son exposant est augmenté de la quantité $2N$, et qu'au contraire le meme terme passe de l'autre coté du signe $\equiv$ lorsque son exposant est augmenté de la

quantité N. Par la meme raison on voit qu'il est inutile de discuter les grandeurs relatives des nombres N , s et t ; car le nombre négatif quelconque $-v$ peut etre remplacé par le nombre positif $2N - v$, sans qu'il en résulte aucun changement.
n.6. Je vais examiner à présent quels sont le cas dans lesquels les six congruences données dans le n précédent peuvent etre réduites à un moindre nombre.
Je supposerai d'abord que la première de ces congruences se confonde avec la seconde. On aura alors $t \equiv 2N - t$,$s \equiv s - t$ (mod. $2N$), $t \equiv 0$ (mod. $2N$), les six congruences seront donc reduites aux trois suivante

$$1 + 1 \equiv r^s$$
$$1 + r^{N-s} \equiv r^{2N-s}$$
$$1 + r^{N+s} \equiv r^N$$

Si on veut à présent que la meme première congruence se confonde avec la quatrième,on aura $t \equiv N + s$,$s \equiv N + t$ (mod.$2N$) et les six congruences seront réduites aux trois suivante:

$$1 + r^t \equiv r^{N+t}$$
$$1 + r^{2N-t} \equiv r^N$$
$$1 + 1 \equiv r^{2N-s10}$$

Si l'on suppose ensuite que la première congruence se confonde avec la sixième, on aura $N + t - s \equiv t$, $2N - s \equiv s$(mod. $2N$) et les six congruences seront réduites aux trois suivantes:

$$1 + r^t \equiv r^N$$
$$1 + r^{2N-t} \equiv r^{N-t}$$
$$1 + 1 \equiv r^{N+t}$$

Il est visible que les trios suppositions précédentes se rapportent au cas où 2 est résidu puissance p^{ime}.
On peut encore supposer que la première des six congruences se confonde avec la troisième. On a alors $N - s \equiv t$, $t - s \equiv s$ (mod. $2N$), $t \equiv 2s$,

$N \equiv s + t \equiv 3s$ et les six congruences se réduisent aux deux suivantes

$$1 + r^{2s} \equiv r^s$$
$$1 + r^{N+s} \equiv r^{N+2s}$$

Dans ce dernier cas les premiere troisième et cinquième congruences se confondent: ainsi il ne reste plus aucune supposition à examiner, il est donc vrai, comme je l'ai avancé $n5$, que lorsque 2 est non résidu p^{ime} puissance et que N est premier à 3, les six congruences qui résultent de la supposition d'une seule d'entre elles, ne peuvent etre réduites à un moindre nombre.
n.7. Il est bon d'examiner encore le cas dans lequel, en meme tem[p]s que pour un module quelconque il n'y aurait que six couples de résidus puissances pième qui ayent [ayant] l'unité pour différence, trois ou un plus grand nombre des memes résidus se trouveraient placés à coté les uns des autres dans la série des nombres naturels. Dans cette supposition, il faudra qu'un ou plusieurs des puissances de r qui entrent dans les six congruences

$$1 + r^t \equiv r^s \quad 1 + r^{N+s} \equiv r^{N+t}$$
$$1 + r^{2N-t} \equiv r^{s-t} \quad 1 + r^{N+s-t} \equiv r^{N-t}$$
$$1 + r^{N-s} \equiv r^{t-s} \equiv 1 + r^{N+t-s} \equiv r^{2N-s}$$

appartiennent en meme tems à plusieurs d'entre elles.
On aura donc $s \equiv 2N - t$, $s \equiv N - s$, $s \equiv N + s$,$s \equiv N + s - t$ où $s \equiv N + t - s \pmod{2N}$. Si on fait $s \equiv N - s$ on trouvera $1 + 2r^t + r^{2t} \equiv r^{2s}r^N \equiv -1, 2(1 + rt) \equiv -r^{2t}$ ou $2r^s \equiv -r^{2t}$, cette supposition ne peut donc convenir qu'au cas où 2 serait résidu pième; ainsi elle doit etre écartée. A l'égard des deux suppositions $s \equiv N+s$ et $s \equiv N+s-t$, elles sont entièrement inadmissible; car la première veut que $N \equiv 0 \pmod{2N}$, et la seconde donne, à cause de $N \equiv t$, $1 + r^N \equiv 0 \equiv r^s$. Il ne reste donc plus à examiner que les deux suppositions $s \equiv 2N - t$et $s \equiv N + t - s$ qui, on va le voir, donnent des résultats équivalents.
En effet soit $2N - t \equiv s$ on aura

$$1 + r^{2N-s} \equiv r^s$$
$$1 + r^s \equiv r^{2s}$$
$$1 + r^{N-s} \equiv r^{2N-2s}$$
$$1 + r^{N+s} \equiv r^{N-s}$$

$$1 + r^{N+2s} \equiv r^{N+s}$$
$$1 + r^{N-2s} \equiv r^{2N-s}$$

par conséquent les quatre résidus des puissances r^{N+2s}, r^{N+s}, r^{N-s} et r^{2N-2s} se trouveront placés de suite dans la série des nombres naturels.
Soit ensuite $s \equiv N + t - s$ on aura

$$1 + r^{N+2s} \equiv r^{s}$$

$$1 + r^{N-2s} \equiv r^{N-s}$$

$$1 + r^{N-s} \equiv r^{N+s}$$

$$1 + r^{N+s} \equiv r^{2s}$$

$$1 + r^{2N-s} \equiv r^{2N-2s}$$

$$1 + r^{s} \equiv r^{2N-s}$$

par conséquent les quatre résidus des puissances r^{N+2s}, r^{s}, r^{2N-s} et r^{2N-2s} se trouvent placés de suite dans la série des nombres naturels. En prenant

$$x \equiv r^{N+2s}$$

ou

$$x \equiv r^{N+2s}$$

$$1 + x \equiv r^{N+s}$$
$$1 + x \equiv r^{s}$$

$$2 + x \equiv r^{N-s}$$
$$2 + x \equiv r^{2N-s}$$

$$3 + x \equiv r^{2N-2s}$$
$$3 + x \equiv r^{2N-2s}$$

il en résultera la condition $(x+1)(x+2) \equiv 1$, d'où on tire celle-ci $(2x+3)^2 \equiv 5$. On voit donc que lorsque, pour un module quelconque, il n'y aura que six couples de résidus puissances p^{ismes} dont la différence soit l'unité, et qu'il se trouvera plus de deux de ces résidus placés de suite dans la série des nombres naturels, il y aura nécessairement quatre des meme résidus qui jouiront de cette propriété; mais qu'elle ne pourra convenir qu'aux seuls nombres pour lesquels 5 sera résidu quarré.
La congruence $(x+1)(x+2) \equiv 1$ mise sous la forme $x(x+1) \equiv -(2x+1)$ montre que, lorsqu'elle est satisfaite, $2x+1$ est aussi résidu pième puissance; en sorte qu'on a alors au moins six résidus puissances pièmes du meme signe savoir, $1, x, x+1, x+2, x+3$ et $2x+1$.En effet si on supposait $x \equiv 2x+1, x+1 \equiv 2x+1, x+2 \equiv 2x+1$ ou $x+3 \equiv 2x+1$ il en résulterait $x+1 \equiv 0, x \equiv 0, x1 \equiv 0$ ou $x2 \equiv 0$; si on faisait $-x \equiv 2x+1$, $-(x+1) \equiv 2x+1$, ou $-(x+2) \equiv 2x+1$ on aurait à cause de $x^2 - 3x + 1$; $x^2 \equiv 0$, $x^2 - 1 \equiv 0$ ou $x^2 - 2 \equiv 0$. Enfin si on prenait $-(x+3) \equiv 2x+1, 3x+4 \equiv 0$ on trouverait $x^2 + 6x + 9 \equiv 4$ et par conséquent, à cause de $x+3$ résidu pieme puissance, 2 serait aussi résidu pième puissance.
n.8. Il résulte des remarques précédentes que exceptant toujours le cas où 2 serait résidu puissance pième, quelque soit le nombre p dans les nombres premiers des formes $2p+1, 4p+1, 8p+1$ et $10p+1$,on ne pourra jamais trouver deux résidus puissances pièmes dont la différence soit l'unité.
Il en résulte aussi que pour toute autre valeur que $p = 2$, on ne pourra pas trouver non plus deux résidus pièmes puissances mod.$14p+1$ qui ayent [ayant] l'unité pour différence. On voit en effet qu'en supposant que le six congruences $n5$ ayent [ayant] lieu, il y aura toujours alors une d'entre elles entre deux résidus puissances $(2p)^{imes}$. Soient donc s et t de nombres pairs, on devra avoir à la fois

$$1 + r^t \equiv r^s$$

e

$$1 + r^t + r^s + r^{2N-s} + r^{2N-t} + r^{s-t} + r^{2N-(s-t)} \equiv 0$$

par conséquent (en multipliant par r^{s+t})

$$r^{s+t} + r^{2t+s} + r^{2s+t} + r^t + r^s + r^{2s} + r^{2t} \equiv$$

$$(1 + r^t)(r^s + r^{2s}) + r^t + r^{2t} + r^{2t+s} \equiv$$

$$(1 + r^t)r^s(1 + r^s + r^t) \equiv 2r^s r^s r^s \equiv 0.$$

Il reste à examiner le cas dans lequel la congruence $(x + 1)(x + 2) \equiv 1$ serait satisfaite. Si on veut que $x+1$ et $x+2$ soient résidus quarrés on fera $x+1 = x'$ on aura donc

$$x'^6 + x'^5 + x'^4 + x'^3 + x'^2 + x' + 1 \equiv 0$$

et a cause de $x'2 + x' \equiv 1$ on trouvera

$$2x'^4 + x'^3 + x'2 + x' + 1 \equiv 0$$

$$-x'^3 + 3x'^2 + x' + 1equiv0$$

$$x'^3 + x'^2 - x' \equiv 0$$

$$4x'^2 + 1 \equiv 0.$$

Si on suppose au contraire que $x + 1$ et $x + 2$ soient non résidus quarrés, on

pourra prendre $x+2=x''$; on aura alors

$$x''^6 - x''^5 + x''^4 - x''^3 + x''^2 - x'' + 1 \equiv 0$$

et à cause de $x''^2 - x'' \equiv 1$ on trouvera

$$2x''^4 - x''^3 + x''^2 - x'' + 1 \equiv 0$$

$$x''^3 + 3x''^2 - x'' + 1 \equiv 0$$

$$x''^3 - x''^2 - x'' \equiv 0$$

$$4x''^2 + 1 \equiv 0$$

Ainsi, soit que $x+1$ soit résidu ou non résidu quarré, il faudra que 2 étant toujours non résidu puissance pième 4 soit au contraire résidu puissance p^{ime} c'est à dire que le nombre p ne pourra etre different de 2. On peut donc etre sur que tant que 2 est non résidu puissance p^{ime} le nombre 29 dont les 7 résidus 2^{imes} puissances de meme signe sont $1, x, x+1, x+2, x+3, 2x+1, 3x+1$, ou $1, 4, 5, 6, 7, 9, 13$, est le seul nombre premier de la forme $14p+1$ pour lequel on puisse satisfaire à la congruence $1+r^t \equiv r^s$.
Les memes remarques peuvent encore servir à prouver que quelque soit le nombre p dans les nombres premiers de la forme $16p+1$, on ne pourra jamais trouver deux résidus puissances p^{imes} dont la différence soit l'unité.
En effet on sait déjà que l'on ne peut trouver deux semblables résidus pour les nombres premiers de la forme $8p+1$, par conséquent il ne pourra se trouver deux nombres pairs s et t qui remplissent pour les nombres de la forme $16p+1$ la condition $1+r^t \equiv r^s$, et puisqu'une quelconque des 6 congruences $n5$ redonne les cinq autres, on peut toujours supposer au contraire que s et t représentent deux nombres impairs.
Tant que la condition $(x+1)(x+2) \equiv 1$ ne serait pas remplie, on aurait donc neuf puissances impaires savoir $1, r^t, r^s, r^{2N-t}, r^{N-s}, r^{N+s}, r^{N+t}, r^{N-t}$et r^{2N-s} qui donnerait autant de résidus puissances p^{imes} essentiellement différents, tandis que pour la présente valeur de N qui est 8 il ne peut exister plus de 8 pareils résidus.
En admettant au contraire la condition $(x+1)(x+2) \equiv 1$ on en tire d'abord $(x+1)2 \equiv -x, \pm 1 \equiv x^4$,on a donc encore deux cas à examiner. Si on

prend le signe supérieur dans la congruence $\pm 1 \equiv x^{2[4]}$ on aura $x^4 - 1 \equiv 0$ en meme tem[p]s que $x^2 \equiv -(3x+1)$,$x^4 \equiv 9x^2 + 6x + 1$ aussi on trouvera $9x^2 + 6x, 3x + 2 \equiv 0$,$x^2 \equiv 1$,par conséquent $x + 1 \equiv 0$ ou $x - 1 \equiv 0$. En adoptant le signe inférieur, on aura $x^4 + 1 \equiv 0$ en meme tems que $x^4 \equiv 9x^2 + 6x + 1$, on trouvera donc $9x^2 + 6x + 2 \equiv 7x^2 \equiv 0$.
Il est clair que ces différents résultas sont également inadmissibles et que l'on peut regarder comme hors de doute que lorsque 2 est non résidu puissance pième il est toujours impossible de satisfaire à la condition $1 + r^t \equiv r^s$ pour quelques nombres de la forme $16p + 1$ que ce puisse etre.
n.9. Pour les nombres premiers $2Np + 1$ dans lesquels N est plus grand que 8, on est forcé de faire à part l'analyse des différents cas qui se rapportent à chacune des valeurs du nombre N. La méthode que j'ai employée consiste à supposer qu'il existe en effet deux rèsidus pièmes puissances tels que x et $x + 1$, et à faire successivement x congruent à chacune des puissances impairs de $x + 1$ dont les exposants sont $<$ [moindres] que $2Np$. Il résulte de ces divers essais un certain nombre de conditions. Lorsqu-aucune d'elles ne peuvent etre remplies on est sur que quelque soit p, il ne peut jamais y avoir pour aucun nombre premier de la forme $2Np + 1$ deux résidus puissances pièmes dont la différence soit l'unité.
Lorsqu'au contraire quelques-unes des meme conditions peuvent etre satisfaites, elles ne peuvent pourtant jamais l'etre que par un petit nombre des nombres premiers de la forme $2Np + 1$ et ces nombres sont les seuls de la meme forme pour lesquels il existe 2 résidus puissances p^{imes} dont la différence soit l'unité.
Pour se convaincre que cette methode est applicable à toutes les valeurs de N , il faut d'abord observer que si N est un nombre premier, une des six congruences $n5$ sera nécessairement entre deux non résidus quarrés, et qu'aucune des puissances impaires de $x + 1$ ne sera congruente à une autre des meme puissances. On verra ensuite que lorsque N sera un nombre composé nn' les cas où on pourra avoir $1 + r^{n't} \equiv r^{n's}$ étant déjà connus par l'examen des nombres de la forme $2Np + 1$, on pourra toujours supposer $x + 1$ résidu p^{ime} puissance non résidu n'^{ime} puissance, en sorte que les puissances impaires de $x + 1$ seront encore incongruentes entr'elles [entre-elle] et que par conséquent, tant que n' sera un nombre impair, le nombre x se trouvera nécessairement parmi leurs résidus. Enfin on verra qu'à cause de la liaison qui existe entre les six congruences données $n5$, si n' est un nombre pair, on pourra toujours trouver des valeurs de $x + 1$ et x telles que x soit aussi non résidu puissance n'^{ime} .
Je prendrai pour exemple les cas où $N = 10$. On sait d'avance, tant que 2 est non résidu p^{ime} puissance, que pour les nombres premiers de la forme $10p + 1$ il ne peut exister deux résidus p^{imes} puissances dont la différence soit l'unité.

Il est donc permis de supposer l'un et l'autre nombres x et $x+1$ non résidus quarrés module $20p+1$ et de faire successivement:

$$x \equiv (x+1)^3, x^3+3x^2+2x+1 \equiv 0$$

d'où il résulte

$$x^4 \equiv (x+1)^{12} \equiv -(x+1)^2$$

$$x^4+x^2+2x+1 \equiv 0$$

$$x^4-x^3-2x^2 \equiv 0, x^2-1 \equiv x+1$$

$$x, x-1 \equiv 1, x \equiv 2.$$

$$x \equiv (x+1)^5, x^5+5x^4+10x^3+10x^2+4x+1 \equiv 0$$

d'où il résulte

$$x^2 \equiv (x+1)^{10} \equiv -1, x^2+1 \equiv 0$$

et par conséquent

$$5x^4+9x^3+10x^2+4x+1 \equiv 0$$

$$9x^3+5x^2+4x+1 \equiv 0$$

$$5x^3+4x^2 \equiv 0, 5x \equiv -4, 25x^2 \equiv -25 \equiv 16, 41 \equiv 0, p=2.$$

$$x \equiv (x+1)^7$$

d'où il résulte

$$x(x+1)^2 \equiv -1, x^3 + 2x^2 + x + 1 \equiv 0$$

et encore

$$x^3 \equiv (x+1)^{21} \equiv x + 1, x^3 - x - 1 \equiv 0$$

$$2x^2 + 2x + 2 \equiv 0, x^3 \equiv 1$$

qui ne peut etre [?] N multiple de 3.

$$x \equiv (x+1)^9$$

d'où il résulte

$$x(x+1) \equiv -1, x^2 + x + 1 \equiv 0$$

condition impossible à remplir lorsque N est premier à 3

$$x \equiv (x+1)^{11} \equiv -x - 1, 2x + 1 \equiv 0$$

c'est à dire 2 résidu puissance p^{ime}.

$$x \equiv (x+1)^{13} \equiv -(x+1)^3, x^3 + 3x^2 + 4x + 1 \equiv 0$$

d'où il résulte

$$x^4 \equiv (x+1)^{12} \equiv -(x+1)^2$$

$$x^4 + 3x^3 + 4x^2 + x \equiv 0, x^4 + x^2 + 2x + 1 \equiv 0$$

$$3x^3 + 3x^2 \equiv x + 1$$

$$3x^2 \equiv 1$$

$$3x^2 \equiv 1$$

donne

$$249x^{10} \equiv -249 \equiv 1, 244 = 4\Delta 61 \equiv 0p = 3.$$

$$x \equiv (x+1)^{15} \equiv -(x+1)^5,$$

$$x^5 + 5x^4 + 10x^3 + 10x^2 + 6x + 1 \equiv 0$$

d'où il résulte

$$x^2 \equiv (x+1)^{10} \equiv -1$$

et par conséquent

$$5x^4 + 9x^3 + 10x^2 + 6x + 1 \equiv 0$$

$$9x^3 + 5x^2 + 6x + 1 \equiv 0$$

$$3x^3 + 4x^2 \equiv 0, \quad 3x \equiv -4, \quad 9x^2 \equiv -9 \equiv 16, \quad 25 \equiv 0.$$

$$x \equiv (x+1)^{17} \equiv -(x+1)^7$$

d'où il résulte

$$x(x+1)^3 \equiv 1, x^4 + 3x^3 + 3x^2 + x + 1 \equiv 0$$

et encore

$$x^3 \equiv -(x+1), x^3 + x + 1 \equiv 0$$

par conséquent $x^4 + 4x^3 + 3x^2 + 2x \equiv 0$ donne

$$x^3 + 4x^2 + 3x + 2 \equiv 0$$

$$x^3 + 4x^2 + 9x + 2 - x3 - x - 1 \equiv 0, ...4x^2 + 2x + 1 \equiv 0$$

$$x^3 + x + 1 - (4x^2 + 2x + 1) \equiv 0, ...x^3 - 4x^2 - x \equiv 0, x^2 - 4x - 1 \equiv 0$$

$$4x^2 + 2x + 1 + (x^2 - 4x - 1) \equiv 0, ...5x^2 - 2x \equiv 0, 5x \equiv 2, 4x^2 - 16x - 4 \equiv 0$$

$$4x^2 - 16x - 4 - (4x^2 + 2x + 1) \equiv 0, ...18x - 5 \equiv 0, 18 \cdot 5x + 25 \equiv 0$$

$$36 + 25 \equiv 61 \equiv 0, p = 3.$$

$$x \equiv (x+1)^{19}$$

d'où il résulte

$$x^5 \equiv (x+1)^{95} \equiv -(x+1)^5$$

$$2x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1 \equiv 0$$

et encore $x(x+1) \equiv 1$

$$3x^4 + 12x^3 + 10x^2 + 5x + 1 \equiv 0$$

par conséquent

$$9x^3 + 13x^2 + 5x + 1 \equiv 0$$

$$4x^2 + 14x + 1 \equiv 0$$

$$10x + 5 \equiv 0$$

$$2x + 1 \equiv 0.$$

On voit donc qu'en exceptant toujours le cas où 2 serait résidu puissance p^{ime}, les seules valeurs de p qui remplissent les conditions nécessaires pour que deux résidus puissances p^{imes} module $20p + 1$ ayent [ayant] l'unité pour différence, sont $p = 2$ et $p = 3$.
On ne rencontrerait pas plus de difficulté dans l'examen des valeurs suivantes de N , et on trouverait toujours que parmi le nombre infini des nombres premiers des formes $2Np + 1$ il n'y en a jamais qu'un très petit nombre pour lesquels deux résidus pièmes puissances ayent [ayant] l'unité pour différence. J'ai déjà observé que cette remarque suffit bien pour établir d'une manière générale qu'il y a une infinité de cas dans lesquels il y est impossible de satisfaire en nombres entiers a l'équation $x^p + y^p = z^p$ mais qu'elle est insuffisant pour démontrer la meme impossibilité dans le cas d'une valeur déterminée de p.
n. 10. En se bornant à l'examen des nombres premiers des formes $2p+1, 4p+1, 8p+1, 10p+1, 14p+1, 16p+1$ et $20p+1$ il faut encore déterminer quels sont ceux d'entre ces nombres pour lesquels 2 est résidu p^{ime} puissance.
Il est aisé de voir qu'en général si 2 est résidu pième puissance (mod. $2Np+1$) on aura la congruence $2^{2N} \equiv 1$ par conséquent

$$N \equiv 1 donner a 2^2 \equiv 1, 3 \cdot 1 = 2 + 1 \equiv 0$$

$$N \equiv 2 \ldots\ldots\ldots\ldots 2^4 \equiv 1, 1 \cdot 3 \cdot 5 = 3 \cdot [4 + 1] \equiv 0$$

$$N \equiv 4.....2^8 \equiv 1, 1 \cdot 3 \cdot 5 \cdot 17 = 3 \cdot 5 \cdot [16 + 1] \equiv 0$$

$$N \equiv 5.....2^{10} \equiv 1, 3 \cdot 11 \cdot 31 = 3 \cdot [10 + 1] \cdot [10 \cdot 3 + 1] \equiv 0$$

$$N \equiv 7.....2^{14} \equiv 1, 3 \cdot 43 \cdot 127 = 3 \cdot [14 \cdot 3 + 1] \cdot [14 \cdot 9 + 1] \equiv 0$$

$$N \equiv 8.....2^{16} \equiv 1, 1 \cdot 3 \cdot 5 \cdot 17 \cdot 257 = 3 \cdot 5 \cdot 17 \cdot 16 \cdot 16 + 1 \equiv 0$$

$$N \equiv 10.....2^{20} \equiv 1, 3 \cdot 11 \cdot 31 \cdot 25 \cdot 41 = 3 \cdot 5 \cdot 5 \cdot 11 \cdot 31 \cdot 20 \cdot 2 + 1[\equiv 0]$$

Le cas où $p = 1$ satisfait nécessairement à la condition que deux résidus pièmes puissances se trouvèrent placés de suite dans la série des nombres naturels; il en est de meme du cas où $p = 2$, puisque, comme je l'ai démontré $n2$, pour toute autre valeur de N que $N = 1$ on peut toujours trouver deux résidus quarrés module $2N \cdot 2 + 1$ dont la différence soit l'unité. Ces deux cas sont à la vérité entièrement étrangers aux considérations suivantes, mais il était bon d'observer que les nombres qui s'y rapportent se présentent toujours, car leur existence connue d'ailleurs peut servir à justifier la méthode qui les reproduit.

n.11. En réunissant les résultats obtenus $n8, 9$ et 10 et écartant les deux cas $p = 1$, $p = 2$ on peut donc établir que quelque soit p il ne peut jamais exister pour aucun nombre premier des formes $2p + 1, 4p + 1$ et $8p + 1$ deux résidus puissances pièmes dont la différence soit l'unité; que pour le nombres premiers de la forme $10p + 1$ il n'y a qu'une seule valeur de p savoir $p = 3$ qui satisfasse à cette condition que pour les nombres de la forme $14p + 1$ les seules valeurs de p qui remplissent la meme condition sont $p = 3$ et $p = 9$; que pour les nombres premiers de la forme $16p + 1$ la seule valeur de p qui s'accorde avec la condition dont il s'agit est $p = 16$; qu'enfin pour les nombres premiers de la forme $20p + 1$ on n'a encore qu'une seule valeur de p qui convienne savoir $p = 16[20]$.

Je vais placer ici la table de ceux des nombres premiers de ces différentes formes pour lesquels on ne peut pas trouver deux residus puissances p^{imes} dont la différence soit l'unité et quoiqu'il soit facile de la pousser plus loin je

la bornerai au cas où p est un nombre premier moindre que 100.

$$2p + 1 = 2 \cdot 3 + 1 = 7$$

$$2 \cdot 5 + 1 = 11$$

$$2 \cdot 11 + 1 = 23$$

$$2 \cdot 23 + 1 = 47$$

$$2 \cdot 29 + 1 = 59$$

$$2 \cdot 41 + 1 = 83$$

$$2 \cdot 53 + 1 = 107$$

$$2 \cdot 83 + 1 = 167$$

$$2 \cdot 87 + 1 = 179$$

$$4p + 1 = 4 \cdot 3 + 1 = 13$$

$$4 \cdot 7 + 1 = 29$$

$$4 \cdot 13 + 1 = 53$$

$$4 \cdot 37 + 1 = 149$$

$$4 \cdot 43 + 1 = 173$$

$$4 \cdot 67 + 1 = 269$$

$$4 \cdot 73 + 1 = 293$$

$$4 \cdot 79 + 1 = 317$$

$$4 \cdot 97 + 1 = 389$$

$$8p + 1 = 8 \cdot 5 + 1 = 41$$

$$8 \cdot 11 + 1 = 89$$

$$8 \cdot 17 + 1 = 137$$

$$8 \cdot 29 + 1 = 233$$

$$8 \cdot 71 + 1 = 569$$

$$10p + 1 = 10 \cdot 7 + 1 = 71$$

$$10 \cdot 13 + 1 = 131$$

$$10 \cdot 19 + 1 = 191$$

$$10 \cdot 31 + 1 = 311$$

$$10 \cdot 43 + 1 = 421$$

$$10 \cdot 97 + 1 = 971$$

$$14p + 1 = 14 \cdot 3 + 1 = 43$$

$$14 \cdot 5 + 1 = 71$$

$$14 \cdot 17 + 1 = 239$$

$$14 \cdot 47 + 1 = 659$$

$$14 \cdot 53 + 1 = 743$$

$$14 \cdot 59 + 1 = 827$$

$$14 \cdot 83 + 1 = 1169$$

$$16p + 1 = 16 \cdot 7 + 1 = 113$$

$$16 \cdot 37 + 1 = 593$$

$$16 \cdot 61 + 1 = 977$$

$$16 \cdot 97 + 1 = 1553$$

$$20p + 1 = 20 \cdot 5 + 1 = 101$$

$$20 \cdot 23 + 1 = 461$$

$$20 \cdot 41 + 1 = 821$$

$$20 \cdot 47 + 1 = 941$$

$$20 \cdot 53 + 1 = 1061$$

$$20 \cdot 59 + 1 = 1181$$

n 12. Avant de faire usage de cette table il faut encore démontrer le théorème suivant:
Pour que l'équation $x^p + y^p = z^p$ soit satisfaite en nombres entiers, p étant un nombre premier quelconque, il faut que l'un des nombres $x + y, z - xetz - y$ soit multiple de la $(2p-1)^{ime}$ puissance du nombre p et des pième puissances

de tous les nombres premiers de la forme $2Np+1$, pour lesquels en meme tem[p]s que l'on ne peut trouver deux résidus puissances p^{ime} dont la différence soit l'unité, p est non résidu puissance p^{ime}.
Démonstration.
En supposant l'existence d'un seul des nombres assujettis à cette double condition, je prouverai d'abord que celui des nombres x, y et z qui dans l'equation $x^p + y^p = z^p$ sera supposé multiple du nombre supposé devra nécessairement en meme tem[p]s [etre] multiple du nombre p^2.
En effet lorsque x, y et z sont premiers entr'eux [entre-eux] les nombres
$x + y$ et $x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + ...$,
$z - y$ et $z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 + ...$,
$z - x$ et $z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 + ...$,
ne peuvent avoir d'autres diviseurs communs que le nombre p. Si on voulait donc que les trois nombres x, y et z fussent tous premiers à p on aurait, en fesant [faisant] $z = lr, y = hn, x = vm$

$$x + y = l^p, x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + ... = r^p$$

$$z - y = h^p, z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 + ... = n^p$$

$$z - x = v^p, z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 + ... = mp.$$

Pour fixer les idées je supposerai que c'est le nombre z qui est multiple de nombre premier de la forme $2Np+1$ dont on a supposé l'existence, on aura alors $l^p + h^p + v^p \equiv 0 \pmod{2Np+1}$; et puisque par hypothèse il ne peut y avoir pour ce module deux résidus puissances pièmes dont la différence soit l'unité il faudra que ce soit l et non pas r qui ait le meme module pour facteur. De $x + y \equiv 0 \pmod{2Np+1}$ on conclut $px^{p-1} \equiv r^p \pmod{2Np+1}$ c'est à dire, à cause de x résidu puissance p^{ime}, p aussi résidu pième puissance ce qui est contraire à l'hypothèse; il faut donc que z soit multiple de p. En prenant actuellement $z = lrp$, la seule supposition admissible est

$$x + y = l^p p^{p-1}, x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + ... = pr^p$$

car si on faisait au contraire

$$x + y = l^p p, x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + ... = p^{p-1}r^p$$

alors

$$(x+y)^{p-1} - x^{p-1} - x^{p-2}y + ...$$

serait divisible par p^{p-1}. Par conséquent si on observe que dans l'équation $2z - x - y = h^p + v^p$ la forme du second membre veut qu'il soit premier à p ou multiple de p^2 on verra que dans le suppositions présentes z aussi doit etre multiple de p^2.
Le seule chose qui reste à prouver est que tous les nombres premiers de la forme $2Np+1$ qui sont assujettis aux memes conditions que celui de la meme forme dont on a supposé l'existence sont nécessairement multiples de z.
Pour y parvenir supposons pour un instant que ce soit y par exemple et non pas z, qui ait un des nombres dont il s'agit pour facteur, nous aurons pour ce module $h^p - l^p \equiv v^p$, par conséquent $v \equiv 0, z \equiv x, pz^{p-1} \equiv m^p$ c'est à dire p résidu puissance p^{ime} contre l'hypothèse.
Il est visible que le raisonnement serait absolument le meme si au lieu de prendre z multiple du nombre premier de la forme $2Np+1$ dont on a supposé l'existence on voulait que ce fut y ou x qui fut multiple du meme nombre: seulement au lieu d'avoir pour résultat l dans l'équation $x + y = p^{p1}l^p$ multiple de p et de tous les nombres premiers de la forme $2Np+1$ pour lesquels en meme tem[p]s que l'on ne peut trouver deux résidus puissances p^{imes} dont la différence soit l'unité on aurait v dans l'équation $z - x = p^{p-1}v^p$, ou h dans l'équation $z - y = p^{p-1}h^p$, multiple des memes nombres.
On voit que cette démonstration suppose que parmi les nombres de la forme $2Np+1$ pour lesquels on ne peut trouver deux résidus puissances p^{imes} dont la différence soit l'unité il y en ait au moins un pour lequel p soit non résidu puissance p^{ime}, et qu'elle fournira des résultats d'autant plus satisfaisants que l'on connaitra un plus grand nombre de telles valeurs de $2Np+1$.
Pour les obtenir il suffira d'essayer la division du nombre $(2N)^{2N} - 1 = (2N)^N + 1(2N)^N - 1$ par les nombres de la forme $2Np+1$ qui rempliront la première condition, car il est évident que p sera non résidu puissance p^{ime} de tous ceux de ces nombres qui ne seront pas facteurs de $(2N)^{2N} - 1$. En effet à cause de -1 résidu puissance pième, les nombres p et $2N$ seront en meme tem[p]s résidus ou non résidus puissances p^{imes} module $2Np+1$.
Mais lorsque N est de la forme $2^a p^b, a$+1et $b+1$ étant des nombres entiers quelconques premiers à p il est inutile d'essayer la division dont on vient de parler car alors p sera nécessairement non résidu p^{ime} puissance toutes les fois que 2 sera non résidu pième puissance.
Les formes générales $2p+1$,$4p+1, 8p+1$ et $16p+1$ appartiennent à ce cas,

aussi bien que le nombre $2(2 \cdot 5)5 + 1$, qui est compris dans la table.
A l'égard du cas où $N = 5$ on a

$$(2N)^N + 1(2N)^N - 1 = 100001 \cdot 99999 = 11 \cdot 41 \cdot 271 \cdot 9 \cdot 9091$$

$$= 11 \cdot 910 \cdot 4 + 110 \cdot 27 + 110 \cdot 909 + 1$$

par conséquent p est non résidu pième puissance de tous les nombres premiers de la forme $10p + 1$ dans lesquels p n'est ni 4, ni 27, ni 909.
Lorsque $N = 7$ [on a]

$$(2N)^N + 1(2N)^N - 1 = 3 \cdot 5 \cdot 13 \cdot 8108731 \cdot 7027567$$

par conséquent p est non résidu p^{ime} puissance de tous les nombres premiers de la forme $14p + 1$ qui ne divisent ni 8108731, ni 7027567 je me suis assurée tous ceux qui se trouvent dans la table sont dans ce cas.
Enfin lorsque N = 10 [on a]

$$(2N)^N + 1(2N)^N - 1 = (20)^{10} + 1(20)^5 + 1(20)^5 - 1$$

$$= 401 \cdot 3 \cdot 8490719867 \cdot 3 \cdot 7 \cdot 152381 \cdot 19 \cdot 11 \cdot 61 \cdot 251$$

$$[3 \cdot 7 \cdot 11 \cdot 19 \cdot 41 \cdot 61 \cdot 251 \cdot 401 \cdot 152381 \cdot 222361 \cdot 2801]$$

et je me suis assuré aussi qu'aucun des nombres contenus dans la table ne divisent le nombre 8490719867.
n 13. L'impossibilité de l'équation $x^3 + y^3 = z^3$ étant démontrée, le premier cas qui se présente à examiner dans l'équation $x^p + y^p = z^p$ est celui où $p = 5$. En vertu du thèorème précédent l'un des nombres $x+y, z-y$et $z-x$ doit etre multiple de la neuvième puissance de 5 et des cinquièmes puissances des quatre nombres 11, 41, 71 et 101 contenus dans la table donnée $n11$, or le nombre

$$59 \cdot 115 \cdot 415 \cdot 715 \cdot 1015 = (161706055)^5 \cdot 625$$

ne pouvant etre écrit avec moins de trente neuf figures de chiffres; lors meme

que l'on supposerait qu'il est facteur du nombre $x + y$, et ce nombre est impair, suppositions qui comme on le voit sont moins favorables; on trouverait toujours que les deux nombres x et y ou au moins un d'eux et à plus forte raison le nombre z ne pourraient pas etre écrits avec un moindre nombre de chiffres.

A l'aide de la meme table on trouvera, en n'employant meme $p = 7$ l'un des nombres $x+y$, $z-y$ et $z-x$ sera multiple de qu'un seul des nombres de chaque forme qu'elle fournit lors que p est $>$ que 17 que l'un des nombres $x+y$, $z-y$ et $z-x$ doit etre multiple d'un nombre $>$ que $5^9 \cdot 11^5 \cdot 41^5 7^{13} \cdot 29^7 \cdot 71^7 \cdot 113^7$ et ce nombre est visiblement plus grand que $5^9 \cdot 11^5 \cdot 41^5 \cdot 71^5 \cdot 101^5$.

Et encore en observant que pour les nombres plus grands que 17 je n'ai pris qu'un des chiffres fournis par la table.

Lorsque

$p = 11$ l'un des memes nombres sera multiple de $1129 \cdot 2311 \cdot 8911$
$p = 13$.....$1325 \cdot 5313 \cdot 13113$
$p = 17$.....$1733 \cdot 13717 \cdot 23917$
$p = 19$.....$1937 \cdot 19117 \cdot 13113$
$p = 23$.....$2345 \cdot 4723$
$p = 29$.....$2957 \cdot 5920$
$p = 31$.....$3161 \cdot 31131$
$p = 37$.....$3773 \cdot 14937$
$p = 41$.....$4181 \cdot 8341$
$p = 43$.....$4385 \cdot 17343$
$p = 47$.....$4793 \cdot 94147$
$p = 53$.....$53105 \cdot 10753$
$p = 59$.....$59117 \cdot 82759$
$p = 61$.....$61121 \cdot 97761$
$p = 67$.....$67133 \cdot 26967$
$p = 71$.....$71141 \cdot 56971$
$p = 73$.....$73145 \cdot 29373$
$p = 79$.....$79158 \cdot 31779$
$p = 83$.....$83175 \cdot 16783$
$p = 89$.....$89178 \cdot 17989$
$p = 97$.....$97193 \cdot 38997$

Bibliografia

[1] Dahan Dalmedico Amy (1992), *Sophie Germain*, "Le Scienze", 282, pp. 70-75.

[2] Del Centina Andrea e Fiocca Alessandra (2012), *The correspondence between Sophie Germain and Carl Friedrich Gauss* , "Archive for History of Exact Sciences", Vol. 66, fasc. 6, pp. 585-700.

[3] Del Centina Andrea (2008), *Unpublished manuscripts of Sophie Germain and a revaluation of her work on Fermat's Last Theorem*, "Archive for History of Exact Sciences", Vol. 62, fasc. 4, pp. 349-392.

[4] Id. (2005), *Letters of Sophie Germain preserved in Florence, Historia mathematica*, Vol. 32, p. 60-75,
(consultato il 23/11/16), (`http://dm.unife.it/geometria/storia/Letteregermain_en.pdf`).

[5] Gauss Carl Friedrich (1801), *Disquisitiones Arithmeticae*, Lipsia, Fleischer.

[6] Harlod M. Edwards (1977), *Fermat's Last Theorem*, New York, Springer.

[7] Laubenbacher Reinhard e Pengelley David (2010), *"Voici ce que j'ai trouvé:" Sophie Germain's grand plan to prove Fermat's Last Theorem*, (consultato il 23/11/2016), (`https://www.math.nmsu.edu/~davidp/germain06-ed.pdf`).

[8] Navarro Joaquìn (2013), *Donne nella matematica* (2011), Villatuerta (Navarra), Rodesa.

[9] O'Connor J. J. e Robertson E. F. (1996), *Sophie Germain*, (consultato il 23/11/2016), (`http://www-history.mcs.st-andrews.ac.uk/Biographies/Germain.html`).

[10] Id. (1996), *Fermat's last theorem*, (consultato il 23/11/2016), (`http://www-history.mcs.st-andrews.ac.uk/HistTopics/Fermat's_last_theorem.html#40`).

[11] Id. (2012), *Paul Mansion*, (consultato il 26/03/2017),(`http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Mansion.html`).

[12] Ribenboim Paulo (1999), *Fermat's Last Theorem for Amateurs*, New York, Springer.

[13] Sampson J.H. (1990), *Sophie Germain and the theory of numbers*, "Archive for history of Exact Sciences", Vol. 41, pp. 157-161.

[14] Savitt David *The mathematics of Gauss*, (consultato il 9/05/2017), (`http://www.math.cornell.edu/~web401/steve.gauss17gon.pdf`).

[15] Singh Simon (2004), *L'ultimo teorema di Fermat* (1997), Bergamo, BUR.

[16] Viola Clara (2015),*Donne matematiche*, Ariccia (RM), Aracne.

"*Ma tutto ciò non è sufficiente; abbiamo bisogno dell'infinito, non basta semplicemente il "molto grande"...*"