

“Voici ce que j’ai trouvé.”* Sophie Germain’s grand plan to prove Fermat’s Last Theorem†

Reinhard Laubenbacher
Virginia Bioinformatics Institute
Virginia Polytechnic Institute and State University
Blacksburg, VA 24061, USA

David Pengelley‡
Mathematical Sciences
New Mexico State University
Las Cruces, NM 88003, USA

Copyright © 2007 Reinhard Laubenbacher & David Pengelley

July 4, 2007

Abstract

A study of Sophie Germain’s extensive manuscripts on Fermat’s Last Theorem calls for a reassessment of her work in number theory. There is much in these manuscripts beyond the single theorem for Case 1 for which she is known from a published footnote by Legendre. Germain had a fully-fledged, highly developed, sophisticated plan of attack on Fermat’s Last Theorem. The supporting algorithms she invented for this plan are based on theoretical concepts, ideas and

* “Here is what I have found:”

† We owe heartfelt thanks to many people who have helped us tremendously with this project over a long fifteen years: Hélène Barcelo, Louis Bucciarelli, Keith Dennis, Mai Gehrke, Tiziana Giorgi, Catherine Goldstein, Maria Christina Mariani, Pat Penfield, Donato Pineider, and Ed Sandifer, along with Marta Gori of the Biblioteca Moreniana, as well as the Bibliothèque Nationale, New York Public Library, Niedersächsische Staats- und Universitätsbibliothek Göttingen, and the Interlibrary Loan staff of New Mexico State University.

‡ Dedicated to the memory of my parents, Daphne and Ted Pengelley, for inspiring my interest in history, and to Pat Penfield, for her talented, dedicated, and invaluable editorial help, love and enthusiasm, and support for this project.

results discovered independently only much later by others, and her methods are quite different from any of Legendre's. In addition to her program for proving Fermat's Last Theorem in its entirety, Germain also made major efforts at proofs for particular families of exponents. The isolation Germain worked in, due in substantial part to her difficult position as a woman, was perhaps sufficient that much of this extensive and impressive work may never have been studied and understood by anyone.

Une étude approfondie des manuscrits de Sophie Germain sur le dernier théorème de Fermat, révèle que l'on doit réévaluer ses travaux en théorie des nombres. En effet, on trouve dans ses manuscrits beaucoup plus que le simple théorème du premier cas que Legendre lui avait attribué dans une note au bas d'une page et pour lequel elle est reconnue. Mme Germain avait un plan très élaboré et sophistiqué pour prouver entièrement ce dernier théorème de Fermat. Les algorithmes qu'elle a inventés sont basés sur des concepts théoriques qui ne furent indépendamment découverts que beaucoup plus tard. Ses méthodes sont également assez différentes de celles de Legendre. En plus, Mme Germain avait fait de remarquables progrès dans sa recherche concernant certaines familles d'exposants. L'isolement dans lequel Sophie Germain se trouvait, en grande partie dû au fait qu'elle était une femme, fut peut-être suffisant, que ses impressionnants travaux auraient pu passer complètement inaperçus et demeurer incompris.

Das Studium von Sophie Germain's extensiven Manuskripten über den Fermat Satz legt eine Neuauslegung ihrer zahlentheoretischen Arbeiten nahe. Diese Manuskripte enthalten viel mehr als nur das einzige Theorem über Fall I für das sie aufgrund einer veröffentlichten Fussnote von Legendre bekannt ist. Germain hatte einen umfassenden, ausgereiften und tiefgehenden Angriffsplan für das Fermat Problem. Die zugrundeliegenden Algorithmen die sie dafür erfand basieren auf theoretischen Konzepten, Ideen und Resultaten die erst viel später von anderen unabhängig wiederentdeckt wurden, und ihre Methoden unterscheiden sich deutlich von denen Legendres. Über ihr Programm das Fermatsche Problem komplett zu lösen hinaus hat Germain auch grosse Anstrengungen gemacht Beweise für einzelne Familien von Exponenten zu finden. Die Isolation in der Germain arbeitete war vielleicht genug dass vieles dieses ausgreifenden und beeindruckenden Werkes der Nachwelt verloren hätte gehen koennen.

Contents

| | |
|--|----------|
| 1 Introduction | 4 |
| 1.1 Gauss and Germain on number theory | 6 |

| | | |
|----------|--|-----------|
| 1.2 | Sophie Germain's explication to Gauss of her grand plan . . . | 8 |
| 1.3 | Our manuscript sources | 10 |
| 1.4 | The major divisions of Germain's work | 12 |
| 1.5 | Reevaluation | 13 |
| 2 | Sophie Germain's grand plan | 13 |
| 2.1 | Germain's plan for proving Fermat's Last Theorem | 14 |
| 2.2 | Did Germain ever know her grand plan cannot succeed? . . . | 18 |
| 2.3 | Comparing Germain's grand plan with Legendre, Dickson, and recent results on Case 1 | 23 |
| 2.4 | Comparing Manuscripts A and D: Polishing for the prize com- petition? | 26 |
| 3 | Large size of solutions | 27 |
| 3.1 | Germain's approach to large size solutions | 28 |
| 3.2 | Comparing Germain on Condition p - N - p and Large Size with Legendre, Wendt, Dickson, Vandiver | 36 |
| 4 | Fermat's Last Theorem for exponents of form $2(8n \pm 3)$ | 39 |
| 4.1 | Case 1 and Sophie Germain's Theorem | 40 |
| 4.2 | Case 2 for p dividing z | 42 |
| 4.3 | Case 2 for p dividing x or y | 43 |
| 4.4 | Manuscript B as source for Legendre? | 43 |
| 5 | Fermat's Last Theorem for even exponents | 44 |
| 6 | Germain's approaches to Fermat's Last Theorem: précis and connections | 45 |
| 6.1 | The grand plan to prove Fermat's Last Theorem | 45 |
| 6.2 | Large size of solutions and Sophie Germain's Theorem | 45 |
| 6.3 | Exponents $2(8n \pm 3)$ and Sophie Germain's Theorem | 46 |
| 6.4 | Even exponents | 46 |
| 7 | Reevaluation of Germain's work in number theory | 47 |
| 7.1 | Germain as strategist: theories and techniques | 47 |
| 7.2 | Interpreting the errors in Germain's manuscripts | 48 |
| 7.3 | Review by others versus isolation | 49 |
| 8 | Conclusion | 52 |

1 Introduction

Sophie Germain was the first woman known for important original research in mathematics.¹ While Germain is perhaps best known for her work in mathematical physics, her number theoretic research on Fermat's Last Theorem has been considered by many to be her best mathematics. We will make a substantial reevaluation of her work on the Fermat problem, based on translation and detailed mathematical interpretation of numerous documents in her own hand, heretofore perhaps never seriously analyzed, and will argue that her accomplishments are much broader, deeper, and more significant than has ever been realized.

On the twelfth of May, 1819, Sophie Germain penned a letter from her Parisian home to Carl Friedrich Gauss in Göttingen [Ge1]. Most of this lengthy letter describes in some detail her work on substantiating Pierre de Fermat's claim that the equation $z^p = x^p + y^p$ has no solutions in positive natural numbers for exponents $p > 2$. The challenge of proving this famous assertion of Fermat has had a tumultuous history, culminating in Andrew Wiles' success at the end of the twentieth century [Ri].

Shortly we shall see what astonishing words Germain wrote to Gauss in her letter of 1819, but first let us briefly recap, for both context and contrast, exactly what she has been known for from the number theory literature.

Once Fermat's claim had been proven by Euler for exponent 4 in the eighteenth century, it could be fully confirmed by substantiating it just for odd prime exponents. But when Germain began working on the problem at the turn of the nineteenth century, the only prime exponent that had a proof was 3 [Ed, Ri]. In 1823 Adrien-Marie Legendre wrote a treatise on Fermat's Last Theorem, ending with his own ad hoc proof for exponent 5. What interests us, though, is the first part of Legendre's treatise, since Germain's work on the Fermat problem has long been understood to be entirely described by a single footnote there [Di, Ed, Le, Ri]. Here Legendre presents a general analysis of the Fermat equation, whose main theoretical highlight is a theorem encompassing all odd prime exponents. In modern terminology:

Sophie Germain's Theorem. *For an odd prime exponent p , if there exists an auxiliary prime θ such that there are no two nonzero consecutive p -th powers modulo θ , nor is p itself a p -th power modulo θ , then in any solution*

¹A good biography of Germain, with concentration on her work in elasticity theory, discussion of her personal and professional life, and references to the historical literature about her, is the book by Louis Bucciarelli and Nancy Dworsky [BD].

to the Fermat equation $z^p = x^p + y^p$, one of x , y , or z must be divisible by p^2 .

Legendre supplies a table verifying the hypotheses of the theorem for $p < 100$ by brute force display of all the p -th power residues modulo a single auxiliary prime θ chosen for each value of p . Legendre then credits Sophie Germain with both the theorem, which is the first general result about arbitrary exponents for Fermat's Last Theorem, and its successful application for $p < 100$. One assumes from Legendre that Germain developed the brute force table of residues as her means of verification and application of her theorem. Legendre continues on to develop more theoretical means of verifying the hypotheses of Sophie Germain's Theorem, and he also pushes the analysis further to demonstrate that any solutions to certain Fermat equations would have to be extremely large.

For almost two centuries, it has been assumed that this theorem and its brute force tabular application to exponents less than 100 constitute Germain's entire work in this area, the basis of her reputation [Ed, Ri]. However, we will find that this presumption is dramatically off the mark as we study Germain's manuscripts. It is not easy to decipher Germain's handwriting, translate, fill in gaps, and understand both the grammar and the mathematics of the extant archive material in Germain's hand. But the reward is a wealth of new material, a vast expansion over the very limited information known just from Legendre's footnote. We will explore the much enlarged scope and extent of Germain's work that is revealed, and its ambitiousness and importance. Together these will prompt a major reevaluation, and recommend a substantial elevation of her reputation.

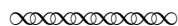
Before going directly to Germain's own writing, we note that even the historical record based solely on Legendre's footnote has been unjustly portrayed. Even the limited results that Legendre clearly attributed to Germain have been badly understated and misattributed in much of the vast secondary literature. Some writers state only weaker forms of Sophie Germain's Theorem, such as merely for $p = 5$, or only for auxiliary primes of the form $2p + 1$ (known as "Germain primes", which happen always to satisfy the two required hypotheses). Others only conclude divisibility by the first power of p , and some writers have even attributed the fuller p^2 -divisibility, or the determination of qualifying auxiliaries for $p < 100$, to Legendre rather than to Germain. A few have even confused the results Legendre credited to Germain with a completely different claim she had made in her first letter to Gauss, in 1804 [St]. Fortunately a few books have correctly stated Legendre's attribution to Germain [Di, Ed, Ri]. We will not elaborate in detail on

the huge related mathematical literature except for specific relevant comparisons of mathematical content with Germain’s own work. Ribenboim’s most recent book [Ri] gives a good overall history of related developments, including windows into the large intervening mathematical literature.

In spite of the failures of much of the literature to report accurately the credit Legendre gave her, Sophie Germain’s Theorem can clearly be used, by producing a valid auxiliary, to eliminate the existence of solutions to the Fermat equation involving numbers not divisible by the exponent p . This elimination is today called “Case 1” of Fermat’s Last Theorem. Work on Case 1 has continued to the present, and major results, including for instance its recent establishment for infinitely many prime exponents p [AH, Fo], have been proven by building on the very theorem that Germain introduced.

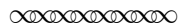
1.1 Gauss and Germain on number theory

Let us compare the meager published historical record, responsible for her reputation, with Germain’s own words to Gauss. Her 1819 letter was written after an eleven year hiatus in their correspondence, so she had much to catch up on. The letter describes the broad scope of Germain’s many years of work, in addition to much detail on her program for proving Fermat’s Last Theorem:



[...] Although I have worked for some time on the theory of vibrating surfaces [...], I have never ceased thinking about the theory of numbers. I will give you a sense of my absorption with this area of research by admitting to you that even without any hope of success, I still prefer it to other work which might interest me while I think about it, and which is sure to yield results.

Long before our Academy proposed a prize for a proof of the impossibility of the Fermat equation, this type of challenge, which was brought to modern theories by a geometer who was deprived of the resources we possess today, tormented me often. I glimpsed vaguely a connection between the theory of residues and the famous equation; I believe I spoke to you of this idea a long time ago, because it struck me as soon as I read your book.²



²“Quoique j’ai travaillé pendant quelque tem[p]s a là théorie des surfaces vibrantes [...], je n’ai jamais cessé de penser a la théorie des nombres. Je vous donnerai une idée de ma préoccupation pour ce genre de recherches en vous avouant que même sans aucune esperance de succès je la prefere a un travail qui me donnerais necessairement en resultat et qui pourtant m’interesse ... quand j’y pense.

Clearly number theory held a very special fascination for Germain throughout much of her life. Largely self-taught, due to her exclusion as a woman from higher education and normal subsequent academic life, she first studied Legendre's *Théorie des Nombres*, published in 1789, and then devoured Gauss' *Disquisitiones Arithmeticae* when it appeared in 1801. Gauss' work was a complete departure from everything that came before, and established number theory as a mathematical subject in its own right, with its own body of methods and techniques, such as the theory of congruences. Germain initiated a correspondence with Gauss, initially under the male pseudonym LeBlanc, which continued for a number of years and gave tremendous impetus to her work. In this early exchange of letters lasting from 1804 to 1808, she sent Gauss some of her work on Fermat's Last Theorem stemming from inspiration she had received from his *Disquisitiones*. Excerpts can be found in Chapter 3 of [BD] and in [St].

Gauss was greatly impressed by Germain's work, and was even stimulated thereby in some of his own, as evidenced by his remarks in a number of letters to his colleague Wilhelm Olbers. On September 3, 1805 Gauss wrote [Sc, p. 268]: "Through various circumstances — partly through several letters from LeBlanc in Paris, who has studied my *Disq. Arith.* with a true passion, has completely mastered them, and has sent me occasional very respectable communications about them, [...] I have been tempted into resuming my beloved arithmetic investigations." After LeBlanc's true identity was revealed to him, he writes again to Olbers, on March 24, 1807 [Sc, p. 331]: "Recently my *Disq. Arith.* caused me a great surprise. Have I not written to you several times already about a correspondent LeBlanc from Paris, who has given me evidence that he has mastered completely all investigations in this work? This LeBlanc has recently revealed himself to me more closely. That LeBlanc is only a fictitious name of a young lady Sophie Germain surely amazes you as much as it does me."

Gauss' letter of July 21 of the same year shows that Germain was a valued member of his circle of correspondents [Sc, pp. 376–377]: "Upon my return I have found here several letters from Paris, by Bouvard, Lagrange, and Sophie Germain. [...] Lagrange still shows much interest in astronomy and higher arithmetic; the two sample theorems (for which prime numbers

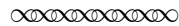
"Longtems [sic] avant que notre academie ais proposé pour sujet de prix la démonstration de l'impossibilité de l'équation de Fermat ces espece de défi—porté aux théories modernes par un géometre — qui fus privé des ressources que nous possedons aujourd'hui me tourmentoiois souvent. Y'entrevois *vaguement* une liaison entre la théorie des residues et la fameuse équation, je crois même vous avoir parlé anciennement de cette ideé car elle m'a frappé aussitôt que j'ai connu votre livre."

is two a cubic or biquadratic residue), which I also told you about some time ago, he considers ‘that which is most beautiful and difficult to prove.’ But Sophie Germain has sent me the proofs for them; I have not yet been able to look through them, but I believe they are good; at least she has approached the matter from the right point of view, only they are a little more long-winded than will be necessary.”

The two theorems on power residues were part of a letter Gauss wrote to Germain on April 30, 1807 [Ga1, vol. 10, pp. 70–74]. Together with these theorems he also included, again without proof, another result now known as Gauss’ Lemma, from which he says one can derive special cases of the Quadratic Reciprocity Theorem. In a May 12, 1807 letter to Olbers, Gauss says “Recently I replied to a letter of hers and shared some Arithmetic with her, and this led me to undertake an inquiry again; only two days later I made a very pleasant discovery. It is a new, very neat, and short proof of the fundamental theorem of art. 131.” [Ga1, vol. 10, p. 566] The proof Gauss is referring to, based on the above lemma in his letter to Germain, is now commonly called his “third” proof of the Quadratic Reciprocity Theorem, and was published in 1808 [Ga2], where he says he has finally found “the simplest and most natural way to its proof” (see also [LP1, LP2]).

1.2 Sophie Germain’s explication to Gauss of her grand plan

Germain continues the letter of 1819 to Gauss by explaining her major effort to prove Fermat’s Last Theorem:



Here is what I have found: [...]

The order in which the residues (powers equal to the exponent) are distributed in the sequence of natural numbers determines the necessary divisors which belong to the numbers among which one establishes not only the equation of Fermat, but also many other analogous equations.

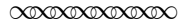
Let us take for example the very equation of Fermat, which is the simplest of those we consider here. Therefore we have $z^p = x^p + y^p$, p a prime number. I claim that if this equation is possible, then every prime number of the form $2Np + 1$ (N being any integer), for which there are no two consecutive p -th power residues in the sequence of natural numbers, necessarily divides one of the numbers x , y , and z .

This is clear, since [if not] the equation $z^p = x^p + y^p$ yields the congruence $1 \equiv r^{sp} - r^{tp}$ in which r represents a primitive root and s and t are integers.³ [...]

It follows that if there were infinitely many such numbers, the equation would be impossible.

I have never been able to arrive at the infinity, although I have pushed back the limits quite far by a method of trials too long to describe here. I still dare not assert that for each value of p there is no limit beyond which all numbers of the form $2Np + 1$ have two consecutive p -th power residues in the sequence of natural numbers. This is the case which concerns the equation of Fermat.

You can easily imagine, Monsieur, that I have been able to succeed at proving that this equation is not possible except with numbers whose size frightens the imagination; because it is also subject to many other conditions which I do not have the time to list because of the details necessary for establishing ?? ?????. But all that is still not enough; it takes the infinite and not merely the very large.⁴



³Germain is considering congruence modulo the auxiliary prime $\theta = 2Np + 1$. She is observing that if none of x, y, z were divisible by θ , then division of the Fermat equation by x^p or y^p would produce two nonzero consecutive p -th power residues. Her claim follows.

⁴“Voici ce que j’ai trouvé:

“L’ordre dans lequel les residus (puissances egales a l’exposant) se trouvent placés dans la serie des nombres naturels détermine les diviseurs necessaires qui appartiennent aux nombres entre lesquels on établis non seulement l’équation de Fermat mais encore beaucoup d’autres équations analogues a celle là.

“Prenons pour exemple l’équation même 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, tous [sic] nombre premier de la forme $2Np + 1$ (N étant un entier quelconque) pour lequel il n’y aura pas deux résidus $p^{\text{ième}}$ puissance placés de suite dans la serie 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 congruence $1 \equiv r^{sp} - r^{tp}$ dans laquelle r represente une racine primitive et s et t des entiers.

“... Il suis delà que s’il y avois un nombre infini de tels nombres l’équation serois impossible.

“Je n’ai jamais pû arriver a l’infini quoique j’ai reculé bien loin les limites par une methode de tatonnement trop longue pour qu’il me sois possible de l’exposer ici. Je n’oserois même pas affirmer que pour chaque valeur de p il n’existe pas une limite audela delaquelle tous les nombres de la forme $2Np + 1$ auroient deux résidus $p^{\text{ièmes}}$ placés de suite dans la serie des nombres naturels. C’est le cas qui interesse l’équation de Fermat.

“Vous concevrez aisement, Monsieur, que j’ai dû parvenir a prouver que cette équation ne serois possible qu’en nombres dont la grandeur effraye l’imagination; Car elle est encore assujettée a bien d’autres conditions que je n’ai pas le tems [sic] d’énumérer a cause des details necessaire pour en établir ?lu? ?reassité?. Mais tout cela n’est encore rien, il faut l’infini et non pas le très grand.”

Several things are remarkable here. Most surprisingly, Germain does not mention to Gauss anything even hinting at the only result she is actually known for in the literature, what we call Sophie Germain’s Theorem. Why not? Where is it? Instead, Germain explains a plan, simple in its conception, for proving Fermat’s Last Theorem outright. It requires that, for a given prime exponent p , one establish infinitely many auxiliary primes each satisfying a non-consecutivity condition on its p -th power residues (note that this condition is the very same as one of the two hypotheses required in Sophie Germain’s Theorem for proving Case 1, but there one only requires a single auxiliary prime, not infinitely many). She writes that she has worked long and hard at this plan by developing a method for verifying the condition, made great progress, but has not been able to bring it fully to fruition (even for a single p) by verifying the condition for infinitely many auxiliary primes. She also writes that she has proven that any solutions to a Fermat equation would have to frighten the imagination with their size. And she explains in broad outline all her work on the problem. Clearly we should now be very curious about her work in these two directions, perhaps completely distinct from the theorem for which Legendre cites her.

1.3 Our manuscript sources

Fortunately, the Germain biography [BD], which led us to her letter to Gauss, also tells us that many of Germain’s manuscripts lie in the archives of the Bibliothèque Nationale in Paris. Many others are also held in the Biblioteca Moreniana, in Firenze (Florence), Italy [Ce, Ce1]. The story of how Germain’s manuscripts ended up in these two collections is an extraordinary and fascinating one, a consequence of the amazing career of Guglielmo (Guillaume) Libri, mathematician, historian, bibliophile, thief, and friend of Sophie Germain [Ce, RM]. In particular, it appears that many of Germain’s manuscripts in the Bibliothèque Nationale were probably among those confiscated by the police from Libri’s apartment at the Sorbonne when he fled to London in 1848 to escape the charge of thefts from French public libraries [Ce, p. 146]. The Germain manuscripts in the Biblioteca Moreniana were among those shipped with Libri’s still remaining vast collection of books and manuscripts before he set out to return from London to Florence in 1868. The Germain materials are among those fortunate to have survived intact despite a tragic string of events following Libri’s death in 1869 [Ce, Ce1]⁵.

⁵See also [Ce2, Ce3, Ce4] for the fascinating story of Abel manuscripts discovered in the same Libri collections.

How Libri obtained Germain’s manuscripts remains unknown, but it would be entirely in character for him to have managed this, since by hook or by crook he built a gargantuan private library of important books, manuscripts, and letters [Ce].⁶ We should probably thank Libri, the efforts of many others after his death, and much good fortune, for saving Germain’s amazing manuscripts. Otherwise they might well simply have drifted into oblivion.

There are hundreds of sheets of Germain’s handwritten papers in the Bibliothèque Nationale, many of them number theory. They are almost all undated, relatively unorganized, almost all unnumbered except by the archive. And they range all the way from scratch paper to some beautifully polished finished pieces, in handwriting that is sometimes extremely difficult to decipher. It appears that their mathematical content has received little attention in the nearly two centuries since Germain wrote them. We cannot possibly provide a definitive evaluation here of this treasure trove of Germain’s manuscripts in the Bibliothèque Nationale, as well as those in the Biblioteca Moreniana. Rather, we will focus our attention in these manuscripts on the major claims she made in her 1819 letter to Gauss, their potential relationship to Sophie Germain’s Theorem, and her other work on Fermat’s Last Theorem.

We will explain some of Germain’s most important mathematical approaches to Fermat’s Last Theorem, provide a sense for the results she successfully obtained, compare them with the impression of her work left by Legendre’s treatise, and in particular discuss possible overlap between Germain’s work and Legendre’s. We will also find connections between Germain’s work on Fermat’s Last Theorem and that of mathematicians of the later nineteenth and twentieth centuries. Finally, we will discuss claims in Germain’s manuscripts to have actually fully proven Fermat’s Last Theorem for certain exponents.

The assessment presented here is based principally on study of her two undated manuscripts entitled *Remarques sur l’impossibilité de satisfaire en nombres entiers a l’équation $x^p + y^p = z^p$* [Ge2, pp. 198 (right)–208 (left)] (hereafter called Manuscript A, 20 sheets numbered in her hand, but attached two to one to the archive numbering), and *Démonstration de l’impossibilité de satisfaire en nombres entiers à l’équation $z^{2(8n\pm 3)} = y^{2(8n\pm 3)} + x^{2(8n\pm 3)}$*

⁶After his expulsion from Tuscany for his role in the plot to persuade the Grand-Duke to promulgate a constitution, Libri traveled for many months, not reaching Paris until fully six months after Germain died, making it all the more extraordinary that it seems he ended up with almost all her papers. [Ce, p. 142f]

[Ge2, pp. 92 (right)–94 (left)] (Manuscript B, 4 sheets)⁷, along with a polished set of three pages [Ge3, p. 348 (right)–349 (right)] (Manuscript C) stating and claiming a proof of Fermat’s Last Theorem for all even exponents. These three manuscripts are found in the Bibliothèque Nationale. We will also compare Manuscript A with another very similar manuscript of the same title, held in the Biblioteca Moreniana (Manuscript D, 25 pages, the 19th blank; see our discussion) [Ge5, cass. 11, ins. 266][Ce, p. 234]. Together these appear to be her primary pieces of polished work in these archives on Fermat’s Last Theorem. Nevertheless, our assessment is based on only part of her approximately 150–200 pages of number theory manuscripts in the Bibliothèque, and other researchers may ultimately have more success than we at deciphering, understanding, and interpreting them. Also, there are numerous additional Germain papers in the Biblioteca Moreniana that may yield further insight [Ce, Ce1]. Finally, even as our analysis and evaluation answers many questions, it will also raise numerous new ones, so there is fertile ground for much more study of her manuscripts by others. In particular, questions of the chronology of much of her work, and of her interaction with others, still contain enticing perplexities.

1.4 The major divisions of Germain’s work

In section 2 we will elucidate from Manuscripts A and D the methods Germain developed in her “grand plan” for proving Fermat’s Last Theorem outright, the progress she made, and its difficulties. We will compare Germain’s methods with her explanation to Gauss and Legendre’s work. Moreover, the non-consecutivity condition on p -th power residues, which is key to both Germain’s grand plan and to utilizing her theorem to prove Case 1, has been pursued by later mathematicians all the way to the present day, and we will compare her approach to later ones. We will also explore whether Germain at some point realized that her grand plan could not be carried through, using the published historical record and a single relevant letter from Germain to Legendre.

In section 3 we will explore Germain’s effort at proving and applying a theorem which we shall call “Large size of solutions”, whose intent is to convince that any solutions which might exist to a Fermat equation would have to be astronomically large, the second point she mentioned to Gauss. Her effort is challenging to evaluate, since her proof as given in the primary manuscript is flawed, but she later recognized this and attempted to

⁷Part of this manuscript, essentially the content of Sophie Germain’s Theorem, was translated and discussed in [LP].

compensate. Moreover Legendre published similar results and applications, which we will contrast with Germain's. We will discover that the theorem which has been known in the literature as Sophie Germain's Theorem is simply minor fallout from her "Large size of solutions" analysis, and we compare some of the methods used by later workers to apply her theorem with her own methods.

Germain's mathematical aims, namely her grand plan, large size of solutions, and p^2 -divisibility (which includes Case 1), are all intertwined in her manuscripts, largely because the hypotheses needing verification overlap. We have separated our exposition of them, however, in order to facilitate direct comparison with Legendre's treatise, which had a different focus but much apparent overlap with Germain's, and to enable easier comparison with the later work of others.

In section 4 we will analyze Manuscript B, which claims proof of Fermat's Last Theorem for a large family of exponents, by building on an essentially self-contained statement of Sophie Germain's Theorem. And in section 5 we consider a very different approach (Manuscript C) claiming to prove Fermat's Last Theorem for all even exponents, based on the impossibility of another Diophantine equation.

1.5 Reevaluation

Our paper will end with an assessment of Germain's full-fledged attack on Fermat's Last Theorem, her analysis leading to claims of astronomical size for any possible solutions to the Fermat equation, the fact that Sophie Germain's Theorem is in the end a small piece of something much more ambitious, our assessment of how independent her work actually was from her mentor Legendre's, of the methods she invented for verifying various conditions, and the paths unknowingly taken in her footsteps by later researchers. We propose that a substantial reevaluation is in order. The results Sophie Germain obtained and the methods she developed place her at the forefront of number-theoretic research in the early nineteenth century.

2 Sophie Germain's grand plan

In her letter to Gauss [Ge1] in 1819, Germain summarized her plan for proving Fermat's Last Theorem. Our aim is to show its promise, thoroughness and sophistication.

Manuscript A contains, among other things, the details of this program for producing, for each odd prime exponent p , an infinite sequence of quali-

ying auxiliary primes, which, as she explained to Gauss, would prove Fermat’s Last Theorem. This occupies more than 16 pages of the manuscript, in very fine, detailed, polished writing. We analyze Germain’s plan in this section, ending with a comparison between Manuscripts A and D and what it suggests.

2.1 Germain’s plan for proving Fermat’s Last Theorem

Let us call Germain’s condition on auxiliary primes $\theta = 2Np + 1$

Condition N-C (Non-Consecutivity). *There are **no** two nonzero consecutive p^{th} power residues, modulo θ .*

Early on in Manuscript A, Germain states that for each fixed N (except when N is a multiple of 3, for which she shows that Condition N-C always fails⁸), there will only be finitely many exceptional numbers p for which the auxiliary $\theta = 2Np + 1$ will fail to satisfy Condition N-C (only primes of the form $\theta = 2Np + 1$ can possibly satisfy the N-C condition⁹). Much of her manuscript is devoted to supporting this claim; while not carried to fruition, Germain’s insight was vindicated much later when proven by E. Wendt in 1894 [Di, Ri, We].¹⁰

Establishing Condition N-C for each N , and an induction on N

In order to establish Condition N-C for various N and p , Germain engages in extensive analysis over many pages of the general consequences of nonzero consecutive p -th power residues modulo a prime $\theta = 2Np + 1$ (N never a multiple of 3). Her analysis actually encompasses all natural numbers for p , not just primes. This is important in relation to the form of θ , since she intends to carry out a mathematical induction on N , and eventually explains in detail her ideas about how the induction should go. She employs throughout the notion and notation of congruences introduced by Gauss, and utilizes to great effect a keen understanding that the $2Np$ multiplicative units mod θ are cyclic, generated by a primitive $2Np$ -th root of unity, enabling her to engage in detailed analyses of the relative placement of the nonzero p -th powers (i.e., the $2N$ -th roots of 1) amongst the residues. She is acutely

⁸See [Ri, p. 127].

⁹See [Ri, p. 124].

¹⁰Germain’s aim follows immediately from Wendt’s recasting of the condition in terms of a circulant determinant depending on N . Condition N-C fails to hold for θ only if p divides the determinant, which is nonzero for all N not divisible by 3. There is no indication that Wendt was aware of Germain’s work.

aware that subgroups of the group of units are also cyclic, and of their orders and interrelationships, and uses this in a detailed way. Throughout her analyses she deduces that in many instances the existence of nonzero consecutive p -th power residues would ultimately force 2 to be a p -th power mod θ , and she therefore repeatedly concludes that Condition N-C holds under the hypothesis that we will call

Condition 2-N- p (2 is Not a p -th power). *The number 2 is not a p -th power residue, modulo θ .*

Notice that this hypothesis is always a necessary condition for Condition N-C to hold, since if 2 is a p -th power, then obviously 1 and 2 are nonzero consecutive p -th powers; so making this assumption is no restriction, and Germain is simply exploring whether 2-N- p is also sufficient to ensure N-C.

Always assuming this hypothesis, which we shall discuss later, and also the always necessary condition that $3 \nmid N$, Germain's analysis initially shows that if there exist two nonzero consecutive p -th power residues, then by inverting them, or subtracting them from -1 , or iterating combinations of these transformations, she can obtain more pairs of nonzero consecutive p -th power residues.¹¹

Germain proves that, under her constant assumption that 2 is not a p -th power residue modulo θ , this transformation process will produce at least 6 completely disjoint such pairs, i.e., involving at least 12 actual p -th power residues. Therefore since there are precisely $2N$ nonzero p -th power residues modulo θ , she instantly proves Condition N-C for all auxiliary primes θ with $N = 1, 2, 4, 5$ as long as p satisfies Condition 2-N- p . Germain continues with more detailed analysis of these permuted pairs of consecutive p -th power residues (still assuming Condition 2-N- p) to verify Condition N-C for $N = 7$ (excluding $p = 2$) and $N = 8$ (here she begins to use inductive information for earlier values of N).

At this point Germain explains her general plan to continue the method of analysis to higher N , and how she would use induction on N for all p simultaneously. In a nutshell, she argues that the existence of nonzero consecutive p -th power residues would have to result in a pair of such, x ,

¹¹In fact these transformations are permuting the pairs of consecutive residues according to an underlying group with six elements, which we shall discuss later. Germain even notes, when explaining the situation in her letter to Gauss [Ge1], that from any one of the six pairs, her transformations will reproduce the five others. This approaches the existence of inverses in a group, and Germain's phenomenon, if it had become known, could have served as one of several important examples in the early nineteenth century that stimulated the development of the group concept.

$x + 1$, for which x is (congruent to) an odd power (necessarily less than $2N$) of $x + 1$. She claims that one must then analyze cases of expansions of the binomial, depending on the value of N , to arrive at the desired contradiction, and she carries out a complete detailed calculation for $N = 10$ (excluding $p = 2, 3$) as a specific “example” of how she says the induction will work in general.

We have found it quite difficult to understand fully this part of the manuscript. Germain’s claims may in fact hold, but we have not managed to verify them completely from what she says. We have difficulty with an aspect of her argument for $N = 7$, with her explanation of exactly how her mathematical induction will proceed, and with an aspect of her explanation of how in general a pair $x, x + 1$ with the property claimed above is ensured. Finally, Germain’s example calculation for $N = 10$ is much more ad hoc than one would like as an illustration of how things would go in a mathematical induction on N . Nonetheless, her instincts here were correct, as proven by Wendt.

The interplay between N and p

But lest the reader think that proving N-C for all N , each with finitely many excepted p , would immediately solve the Fermat problem, note that what is actually needed, for each fixed prime p , is that Condition N-C holds for infinitely many N , not the other way around. For instance, perhaps $p = 3$ must be excluded from the validation of Condition N-C for all sufficiently large N , in which case Germain’s method would not prove Fermat’s Last Theorem for $p = 3$. Germain makes it clear early in the manuscript that she recognizes this issue, that her results do not completely resolve it, and that she has not proved Fermat’s claim for a single predetermined exponent. But she also states that she strongly believes that the needed requirements do in fact hold, and that her results for $N \leq 10$ strongly support this. Indeed, note that so far the only odd prime excluded in any verifications was $p = 3$ for $N = 10$ (recall, though, that we have not yet examined Condition 2-N- p , which must also hold in all her arguments, and which will also exclude certain combinations of N and p when it fails).

Germain’s final comment on this issue states first that as one proceeds to ever higher values of N , there is always no more than a “very small number” of values of p for which Condition N-C fails. If indeed this, the very crux of the whole approach, were the case, in particular if the number of such excluded p were bounded uniformly, say by K , for all N , which is what she in effect claims, then a little reflection reveals that indeed her

method would have proven Fermat's Last Theorem for all but K values of p , although one would not necessarily know which values. She herself states that this would prove the theorem for infinitely many p , even though not for a single predetermined value of p . It is in this sense that Germain believed her method could prove infinitely many instances of Fermat's Last Theorem.

Verifying Condition 2-N- p

We conclude our exposition of Germain's grand plan in Manuscript A with her analysis of Condition 2-N- p , which was required throughout all her arguments above. She points out that for 2 to be a p -th power mod $\theta = 2Np + 1$ means that $2^{2N} \equiv 1 \pmod{\theta}$ (since the multiplicative structure is cyclic). Clearly for fixed N this can only occur for finitely many p , and she easily determines these exceptional cases through $N = 10$, simply by calculating and factoring each $2^{2N} - 1$ by hand, and observing whether any of the prime factors are of the form $2Np + 1$ for any natural number p . To illustrate, for $N = 7$ she writes that

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

so that $p = 3, 9$ are the only values for which Condition 2-N- p fails for this N .

Germain then presents a summary table of all her results verifying Condition N-C for auxiliary primes θ using relevant values of $N \leq 10$ and primes $2 < p < 100$, and says that it can easily be extended further.¹² The results in the table are impressive. Aside from the case of $\theta = 43 = 14 \cdot 3 + 1$ just illustrated, the only other auxiliary primes in the range of her table which must be omitted are $\theta = 31 = 10 \cdot 3 + 1$, which she determines fails Condition 2-N- p , and $\theta = 61 = 20 \cdot 3 + 1$, which was an exception in her N-C analysis for $N = 10$. In fact each N in her table ends up having at least five primes p with $2 < p < 100$ for which $\theta = 2Np + 1$ is also prime and satisfies the N-C condition.

While the number of p requiring exclusion for Condition 2-N- p may appear "small" for each N , there seems no obvious reason why it should necessarily be uniformly bounded for all N ; Germain does not discuss this issue specifically for Condition 2-N- p . As indicated above, without such a bound it

¹²The table is slightly flawed in that she includes $\theta = 43 = 14 \cdot 3 + 1$ for $N = 7$ despite the excluding calculation we just illustrated, which Germain herself had just written out; it thus seems that the manuscript may have simple errors, suggesting it may sadly never have received good criticism from another mathematician.

is not clear that this method could actually prove any instances of Fermat's theorem.

Results of the grand plan

To summarize, Germain had a sophisticated and highly developed grand plan for proving Fermat's Last Theorem for infinitely many exponents. It relied heavily on expertise with the multiplicative structure in a cyclic prime field and a set (group) of transformations of consecutive p -th powers, and it involved many clever ideas which we have not laid out here in detail. She carried her program out in an impressive range of values for the necessary auxiliary primes, believed that the evidence indicated one could push it further using mathematical induction by her methods, and she was optimistic that by doing so it would prove Fermat's Last Theorem for infinitely many prime exponents. In hindsight we know that, promising as it may have seemed at the time, the program can never be carried to completion.

2.2 Did Germain ever know her grand plan cannot succeed?

To answer this question we examine the published record, correspondence with Gauss, and a letter from Germain to Legendre.

Libri claims that such a plan cannot work

Published indication that Germain's method can not succeed in proving Fermat's Last Theorem came in work of Guglielmo (Guillaume) Libri, a rising mathematical star in the 1820s. It is a bit hard to track and compare the content of his relevant works and their dates, partly because Libri presented or published several different works all with the same title, but some of these were also multiply published. Our interest is in the content of just two different works. In 1829 Libri published a set of his own memoirs [Li1]. One of these is titled *Mémoire sur la théorie des nombres*, republished later word for word as three papers in Crelle's Journal [Li]. The memoir published in 1829 ends by applying Libri's study of the number of solutions of various congruence equations to the situation of Fermat's Last Theorem. Among other things, Libri shows that for exponents 3 and 4, there can be at most finitely many auxiliary primes satisfying the N-C condition. And he claims that his methods will clearly show the same for all higher exponents. Libri explicitly notes that his result proves that the attempts of others to prove Fermat's Last Theorem by finding infinitely many such auxiliaries are in vain.

Libri also writes in his 1829 memoir that all the results he obtains were already presented in two earlier memoirs of 1823 and 1825 to the Academy of Sciences in Paris. Libri's 1825 presentation to the Academy was also published, in 1833/1838 [Li3], confusingly with the same title as the 1829 memoir. This presumably earlier document¹³ is quite similar to the publication of 1829, in that it develops methods for determining the number of solutions to quite general congruence equations, including that of the N-C condition, but it does not explicitly work out the details for the N-C condition applying to Fermat's Last Theorem, as did the 1829 memoir. Thus it seems that close followers of the Academy should have been aware by 1825 that Libri's work would doom the auxiliary prime approach to Fermat's Last Theorem, but it is hard to pin down exact dates. Much later, P. Pepin [Pe1, pp. 318–319][Pe2] and A.-E. Pellet [Pe, p. 93] (see [Di][Ri, pp. 292–293]) confirmed all of Libri's claims, and L. E. Dickson [Di1, Di2] gave specific bounds. For completeness, we mention that Libri also published a memoir on number theory in 1820, his very first publication, with the title *Memoira Sopra La Teoria Dei Numeri* [Li2], but it was much shorter and does not contain the same type of study or results on the number of solutions to congruence equations.

What Germain knew and when: Gauss, Legendre, and Libri

So did Germain ever know from Libri or otherwise that her grand plan to prove Fermat's Last Theorem could not work, and if so, when?

We know that in 1819 she was enthusiastic in her letter to Gauss about her method for proving Fermat's Last Theorem, based on extensive work exemplified by Manuscript A.¹⁴ In it Germain details several specific examples of her results on the N-C condition that match perfectly with Manuscript A, and which she explicitly explains have been extracted from an already much older note (“d'une note déjà ancienne”) that she has not had the time

¹³One can wonder when the document first published in 1833, but based on Libri's 1825 Academy presentation, was really written or finalized. Remarks he makes in it suggest, though, that it was essentially his 1825 presentation.

¹⁴Near the end she even expresses to Gauss how a brand new work by L. Poincot [Po] will help her further her efforts to confirm the N-C condition by giving a new way of working with the p -th powers mod $\theta = 2Np + 1$. She interprets them as the solutions of the binomial equation of degree $2N$, i.e., of $x^{2N} - 1 = 0$. Poincot's memoir takes the point of view that the mod θ solutions of this equation can be obtained by first considering the equation over the complex numbers, where much was already known about the complex $2N$ -th roots of unity, and then considering these roots as mod p integers by replacing the complex number $\sqrt{-1}$ by an integer whose square yields $-1 \pmod{p}$.

to recheck. In fact everything in the extensive letter to Gauss matches the details of Manuscript A. This suggests that Manuscript A is likely the older note in question, and considerably predates her 1819 letter to Gauss. Thus 1819 is our lower bound for the answer to our question. We also know that by 1823 Legendre had written his memoir crediting Germain with her theorem, but without even mentioning the method of finding infinitely many auxiliary primes that Germain had pioneered to try to prove Fermat’s Last Theorem. We know, too, that Germain wrote notes in 1822 on Libri’s 1820 memoir,¹⁵ but this first memoir did not study modular equations, hence was not relevant for the N-C condition. It seems likely that she came to know of Libri’s claims dooming her method, based either on his presentations to the Academy in 1823/25 or the later memoir published in 1829, particularly because Germain and Libri had met and were personal friends from 1825, as well as frequent correspondents. It thus seems probable that sometime between 1819 and 1823 or 1825 Germain would have come to realize that her grand plan could not work.

Germain proves to Legendre that the plan fails for $p = 3$

In fact, though, we do not need to speculate about Germain’s knowledge of Libri’s work in order to answer our primary question, since we have found separate evidence of Germain’s realization that her method of proving Fermat’s Last Theorem cannot succeed, at least not in all cases. While Manuscript A and her letter of 1819 to Gauss evince her belief that for every prime $p > 2$, there will be infinitely many auxiliary primes satisfying the N-C condition, there is an undated letter to Legendre in which Germain actually proves the opposite for $p = 3$ [Ge4]. Although we have found nothing else in the way of correspondence between Legendre and Germain on Fermat’s Last Theorem, we are fortunate to know of this one critical letter, held in the Samuel Ward papers of the New York Public Library.¹⁶

Sophie Germain began her three page letter by thanking Legendre for “telling” her “yesterday” that one can prove that all numbers of the form $6a+1$ larger than 13 have a pair of consecutive (nonzero) cubic residues. This amounts to saying that for $p = 3$, no auxiliary primes of the form $\theta = 2Np+1$

¹⁵Germain’s three pages of notes [Ge5, cass. 7, ins. 56][Ce, p. 233], while not directly about Fermat’s Last Theorem, do indicate an interest in modular solutions of roots of unity equations, which is what encompasses the distribution of p -th powers modulo θ . Compare this with what she wrote to Gauss about Poincot’s work, discussed in the previous footnote.

¹⁶The Samuel Ward papers include “letters by famous mathematicians and scientists acquired by Ward with his purchase of the library of mathematician A. M. Legendre.” We thank Louis Bucciarelli for providing us with this lead.

satisfy the N-C condition beyond $N = 1, 2$. At first sight this claim is perplexing, since it seems to contradict Germain's success in Manuscript A at proving Condition N-C for almost all odd primes p whenever $N = 1, 2, 4, 5, 7, 8, 10$. However, the reader may check that for $p = 3$ her results in Manuscript A actually only apply for $N = 1$ and 2 , once one takes into account the exceptions, i.e., when either θ is not prime, or Condition 2-N- p fails, or when she specifically excluded $p = 3$ for $N = 10$. So the claim in Germain's letter to Legendre is actually conceivably true, that there are only two valid auxiliary primes for $p = 3$. Germain immediately writes a proof for him. We will elucidate her proof here in our own words, in order to show the mathematical flavor and level of her thinking, but we will expand substantially on her highly condensed explanation in the letter, since it is hard to follow otherwise.

Germain's Letter to Legendre. *For any prime θ of the form $6a+1$, with $\theta > 13$, there are (nonzero) consecutive cubic residues. In other words, the N-C condition fails for $\theta = 2Np + 1$ when $p = 3$ and $N > 2$, so the only valid auxiliary primes for $p = 3$ for the N-C condition are $\theta = 7$ and 13 .*

Proof. We consider only the nonzero residues $1, \dots, 6a$. Suppose that N-C is true, i.e., there are no consecutive pairs of cubic residues (c.r.) amongst these, and suppose further that there are also no pairs of c.r. whose difference is 2. (Note something important here. We mean literally residues, not congruence classes, with this assumption, since obviously 1 and -1 are cubic congruence classes whose difference is 2. But they are not both actual residues, and their residues don't have difference 2. So they don't violate our assumption.) There are $2a$ c.r. distributed somehow amongst the $6a$ residues, and without any differences of 1 or 2 allowed, according to what we have assumed. Therefore to separate adequately these $2a$ residues from each other there must be $2a - 1$ gaps containing the $4a$ nonzero non-cubic residues (n.c.r.), each gap containing at least 2 n.c.r. Since each of these $2a - 1$ gaps has at least 2 n.c.r., utilizing $4a - 2$ n.c.r., this leaves flexibility for allocating only 2 remaining of the $4a$ n.c.r. This means that all the gaps must contain exactly 2 n.c.r. except for either a single gap with 4 n.c.r., or two gaps with 3 n.c.r. in each.

We already know of the specific c.r. 1 and 8 (recall $\theta = 6a+1 > 13$). and we know that 2 and 3 cannot be c.r. by our two assumptions. If 4 were a c.r., then so would $8/4 = 2$ (alternatively, $8 - 4 = 4$ would violate N-C), so 4 is also not a c.r. Now Germain writes down a pattern for the sequence of c.r. that we do not understand, and claims it is obviously absurd for $\theta > 13$.¹⁷

¹⁷Germain writes that the list is (presumably omitting those at the ends) $1 + 4, 5 + 3,$

We can easily arrive at a pattern and an absurdity ourselves. From what Germain already has above, the c.r. sequence must clearly be the list 1, 5, 8, 11, \dots , $6a - 10$, $6a - 7$, $6a - 4$, $6a$, since the c.r. are symmetrically placed via negation modulo $\theta = 6a + 1$, and we know the gap sizes. Notice that the two exceptional gaps must be of 3 each, located at the beginning and end. To see this is absurd, for $\theta \geq 6 \cdot 5 + 1 = 31$, consider the c.r. $3^3 = 27$. Notice it contradicts the pattern listed above, since it is less than $6a \geq 30$, but is not congruent to 2 modulo 3, as are all the lesser residues in the list except 1. Finally, the only other prime $\theta > 13$ is 19, for which $4^3 = 64$ has residue 7, which is not in the list.

So one of the two initial assumptions must be false. If N-C fails, we are done. So consider the failure of the other assumption, that there are no pairs of c.r. whose difference is 2. Let then r and r' be c.r. with $r - r' = 2$. Let x by a primitive root of unity modulo θ , i.e., a generator of the cyclic group of multiplicative units represented by the nonzero prime residues. We must have $2 \equiv x^{3f \pm 1}$, i.e., the power of x representing 2 cannot be divisible by 3, since 2 is not a c.r. Now consider $r + r'$. (We claim that $r + r' \not\equiv 0$, since if it were, then $2 = r - r' \equiv r - (-r) = 2r$, yielding $r \equiv 1$, and hence $r = 1$, which violates $r - r' = 2$. Here it is critical to recall that we are dealing with actual residues r and r' , both nonnegative numbers less than $6a + 1$, i.e., the requirements $r \equiv 1$ and $r - r' = 2$ are incompatible, since there are no $0 < r, r' < 6a + 1$ for which $r \equiv 1$ and $r - r' = 2$; this is related to the observation at the beginning that the congruence classes 1 and -1 are not violating our initial assumption.)

Since $r + r' \not\equiv 0$, it is a unit, and thus must be congruent to some power x^m . If m were divisible by 3, then the congruence $r + r' \equiv x^m$ would provide a difference of c.r. yielding another c.r., which violates N-C after division by the latter. So we have $r + r' \equiv x^{3g \pm 1}$. Now the sign in $3f \pm 1$ must agree with that in $3g \pm 1$, since if not, say $r + r' \equiv x^{3g \mp 1}$, then $r^2 - r'^2 = (r - r')(r + r') \equiv 2x^{3g \mp 1} \equiv x^{3f \pm 1} x^{3g \mp 1} = x^{3(f+g)}$, again producing a difference of c.r. equal to another c.r., a contradiction. Finally, we combine $r - r' \equiv x^{3f \pm 1}$ with $r + r' \equiv x^{3g \pm 1}$ to obtain $2r \equiv x^{3f \pm 1} + x^{3g \pm 1}$, and thus $x^{3f \pm 1} r \equiv x^{3f \pm 1} + x^{3g \pm 1}$, becoming $r \equiv 1 + x^{3(g-f)}$, again contradicting N-C. Thus the original assumption of Condition N-C must have been false. Q.E.D.

Notice that Germain's proof displays a rather advanced group-theoretic view at the end. Indeed it is an impressive proof for one she tells Legendre she developed overnight.

$8 + 3, 11 + 3, 14 + 3, \dots, 6a - 17, 6a - 4$ [sic], $6a - 11, 6a - 8, 6a - 5$.

Probably these dramatic failures of Condition N-C for $p = 3$ greatly sobered Germain's previous enthusiasm for pursuing her grand plan any further for other exponents. We mention in passing that, optimistic as Germain was at one point about finding infinitely many auxiliary primes for each p , not only is that hope dashed by Germain's letter to Legendre, and by Libri's results, but even today it is not known whether, for an arbitrary prime p , there is even one auxiliary prime θ satisfying Condition N-C [Ri, p. 301].

2.3 Comparing Germain's grand plan with Legendre, Dickson, and recent results on Case 1

We know of no concrete evidence that anyone else ever pursued a grand plan similar to Sophie Germain's for proving Fermat's Last Theorem, despite the fact that Libri wrote of several (unnamed) mathematicians who attempted this method. Germain's extensive work on this approach appears to be entirely, independently, and solely hers, despite the fact that others were interested in establishing Condition N-C for different purposes.

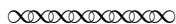
Legendre's methods for establishing Condition N-C

Why did Legendre not mention Germain's full scale attack on Fermat's Last Theorem in his treatise of 1823? Whether because he was by that point unconfident that it could work (as the letter from Germain suggests) or whether he might have known even more certainly from Libri's upcoming work that it was unfeasible, we do not know. On the other hand, it certainly seems unlikely that he could have been unaware of Germain's extensive work on it, given her letter to him about Condition N-C for cubic residues. Thus in the end we cannot discern with any certainty why Legendre was silent in print about Germain's plan for proving Fermat's Last Theorem.

Nonetheless, Legendre had two other reasons for wanting to establish Condition N-C himself, and he develops N-C results in roughly the same range for N and p as did Germain, albeit not mentioning hers. One of his reasons was to verify Case 1 of Fermat's Last Theorem for many prime exponents, since, recall, Condition N-C for a single auxiliary prime is also one of the hypotheses of Sophie Germain's Theorem. Indeed, Legendre develops results for N-C, and for the second hypothesis of her theorem, that enable him to find a qualifying auxiliary prime for each odd exponent $p \leq 197$, which extends the scope of the table he implicitly attributed to Germain. Legendre goes on to use his N-C results for a second purpose as well, namely

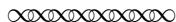
to show for a few small exponents that any solutions to the Fermat equation would have to be very large indeed. We will discuss this additional use of N-C in the next section.

Having said that Legendre obtained roughly similar N-C conclusions as Germain, why do we claim that her approach to N-C verification itself is entirely independent? This is because Germain's method of analyzing and proving the N-C condition, explained in brief above, is utterly unlike Legendre's. We illustrate this by quoting Legendre's explanation [Le, §25] of why Condition N-C is always satisfied for $N = 2$, i.e., for $\theta = 4p + 1$. As we quote Legendre, we caution that even his notation is very different; he uses n for the prime exponent that Germain, and we, call p . Legendre writes



One can also prove that when one has $\theta = 4n + 1$, these two conditions are also satisfied. In this case there are 4 residues r to deduce from the equation $r^4 - 1 = 0$, which divides into two others $r^2 - 1 = 0$, $r^2 + 1 = 0$. The second, from which one must deduce the number μ , is easy to resolve¹⁸; because one knows that in the case at hand θ may be put into the form $a^2 + b^2$, it suffices therefore to determine μ by the condition that $a + b\mu$ is divisible by θ ; so that upon omitting multiples of θ , one can make $\mu^2 = -1$, and the four values of r become $r = \pm(1, \mu)$.

From this one sees that the condition $r' = r + 1$ can only be satisfied in the case of $\mu = 2$, so that one has $\theta = 5$ and $n = 1$, which is excluded. ...



We largely leave it to the reader to understand Legendre's reasoning here. He does not use the congruence idea or notation that Germain had adopted from Gauss, he focuses his attention on the roots of unity from their defining equation, he makes no use of the 2-N- p condition, but he is interested in the consequences of the linear form $4n + 1$ necessarily having a certain quadratic form, although we do not see how it is germane to his argument. In the next case, for $N = 4$ and $\theta = 8n + 1$, he again focuses on the roots of unity equation, and claims that this time the prime $8n + 1$ must have the quadratic form $a^2 + 2b^2$, which then enters intimately into an argument related to a decomposition of the roots of unity equation. Clearly Legendre's approach is completely unlike Germain's. Recall that Germain

¹⁸From earlier in the treatise, we know that μ here means a primitive fourth root of unity, which will generate the four n -th powers.

disposed of all the cases $N = 1, 2, 4, 5$ in one fell swoop with the first application of her analysis of permuted placements of pairs of consecutive p -th powers, whereas Legendre laboriously builds his analysis of $2N$ -th roots of unity up one value at a time from $N = 1$. In short, Legendre focuses on the p -th powers as $2N$ -th roots of unity, one equation at a time, while Germain does not, instead studying their permutations as p -th powers more generally for what it indicates about their placement, and aiming for mathematical induction on N .¹⁹

Dickson rediscovers Germain’s permutation methods for Condition N-C

Many later mathematicians worked to extend verification of the N-C condition for larger values of N .²⁰ Their aim was to prove Case 1 of Fermat’s Last Theorem for more exponents by satisfying the hypotheses of Sophie Germain’s Theorem. In particular, in 1908 L. E. Dickson published two papers [Di, Di3, Di4] extending the range of verification for Condition N-C to $N < 74$, and also 76 and 128 (each N excepting certain values for p , of course), with which he was able to apply Sophie Germain’s theorem to prove Case 1 for all $p < 6,857$. In light of the fact that Germain and Legendre had completely different methods for verifying Condition N-C, one wonders what approach was taken by Dickson.

Dickson comments directly that his method for managing many cases together has “obvious advantages over the procedure of Legendre”. It is then amazing to see that his method is based directly (albeit presumably unbeknownst to him) on the same theoretical observation made by Sophie Germain, that pairs of consecutive p -th powers are permuted by two transformations of inversion and subtraction to produce six more. He recognizes that these transformations form a group of order six, which he calls the cross-ratio group (it consists of the transformations of the cross-ratio of four numbers on the real projective line obtained by permuting its variables [Sti, pp. 112–113]), and is isomorphic to the permutations on three symbols).

¹⁹Despite the apparently completely disjoint nature of the treatments by Germain and Legendre of the N-C condition, it is quite curious that their writings have a common mistake. The failure of N-C for $p = 3$ when $N = 7$ is overlooked in Legendre’s treatise, while in Germain’s manuscript we have already noted above that while she explicitly calculated the failure of $2-N-p$ (and thus of N-C) for this same combination, she then nonetheless mistakenly listed it as valid for N-C in her table.

²⁰Legendre went to $N = 8$ and Germain to $N = 10$, and actually to $N = 11$ in another very much rougher manuscript draft [Ge2, pp. 209 (right)–214 (left), 216 (right)–218 (left), 220 (right)–226 (right)].

Dickson observes that the general form of these transformations of an arbitrary p -th power are the roots of a sextic polynomial that must divide the roots of unity polynomial for any N . This then forms the basis for much of his analysis, and even the ad hoc portions have much the flavor of Germain's approach for $N > 5$. In sum, we see that Dickson's approach to the N-C condition more than three-quarters of a century later could have been directly inspired by Germain's, had hers not sat entirely unknown in her manuscripts. Might not further progress by later mathematicians on Case 1 of Fermat's Last Theorem have occurred decades earlier if Sophie Germain's approach to the nonconsecutivity condition had seen the light of day before now?

Revival of a proof by induction on N

Finally, work on verifying the N-C condition has continued up to the close of the twentieth century, largely with the aim of proving Case 1 using extensions of Sophie Germain's Theorem. By the middle of the nineteen eighties results on the distribution of primes had been combined with extensions of Germain's theorem to prove Case 1 of Fermat's Last Theorem for infinitely many prime exponents [AH, Fo]. It is also inspiring that at least one even more recent effort still harks back to what we have seen in Germain's unpublished manuscripts. Recall that Germain explained her intent to prove the N-C condition by induction on N . This is precisely what a recent paper by David Ford and Vijay Jha does [FJ], using some modern methods and computing power to prove by induction on N that Case 1 of Fermat's Last Theorem holds for any odd prime exponent p for which there is a prime $\theta = 2Np + 1$ with $3 \nmid N$ and $N \leq 500$.

2.4 Comparing Manuscripts A and D: Polishing for the prize competition?

Manuscripts A and D, of the same title, are extremely similar, with identical mathematical content and almost identical wording. Still, we will learn interesting things by comparing them.

Manuscript D gives the impression of an almost finished exposition of Germain's work on Fermat's Last Theorem, greatly polished in content and wording over the much rougher additional manuscript we mentioned in section 2. And it is perfectly readable. However, it is not yet physically beautiful, since Germain was clearly still refining her wording as she wrote it. In many places words are crossed out and she continues with different word-

ing, or words are inserted between lines or in the margins to alter what has already been written. There are also large parts of some pages left blank. By contrast, Manuscript A appears beautiful and perfect. It is copied word for word almost without exception from Manuscript D. It seems clear that Manuscript A was written specifically to provide a visually perfected copy of Manuscript D.

One aspect of Manuscript D is quite curious. Recall that Manuscript A contains a table with all the values for auxiliary primes satisfying Condition N-C for $N \leq 10$ and $3 < p < 100$. Germain explicitly introduces this table, referring both ahead and back to it in the text, where it lies on page 17 of 20. Manuscript D says all these same things about the table, but where the table should be there is instead simply a side of a sheet left blank. Thus Germain refers repeatedly to a table that is missing in what she wrote. This suggests that as Germain was writing Manuscript D, she knew she would need to recopy it to make it perfect, so she didn't bother writing out the table at the time, saving the actual table for Manuscript A.

Our comparison between Manuscripts A and D highlights the perfection of presentation Sophie Germain sought in producing Manuscript A. Is it possible that she was preparing this manuscript for submission to the French Academy prize competition on the Fermat problem, which ran from 1816 to 1820? We will discuss this further in our conclusion.

3 Large size of solutions

While German believed that her grand plan could prove Fermat's Last Theorem for infinitely many prime exponents, she recognized that it had not yet done so even for a single exponent. She thus wrote that she wished at least to show for specific exponents that any possible solutions to the Fermat equation would have to be extremely large.

In the last four pages of Manuscript A, Germain provides a theorem intended to accomplish this. She first recalls that any auxiliary prime satisfying Condition N-C will have to divide one of the numbers x, y, z in the Fermat equation, but observes that to produce significant lower bounds on solutions this way, one would need to employ rather large auxiliary primes. Then she says

“fortunately one can avoid such impediment by means of the following theorem:”²¹,

²¹ “heureusement on peut éviter un pareil embarras au moyen du théorème suivant:”

which we shall call

Theorem (Large Size of Solutions). *“For the equation $x^p + y^p = z^p$ to be satisfied in whole numbers, p being any [odd] prime number, it is necessary that one of the numbers $x + y$, $z - y$, and $z - x$ be a multiple of the $(2p - 1)^{\text{th}}$ power of the number p and of the p^{th} powers of all the prime numbers of the form $[\theta =]Np + 1$, for which one has, at the same time, that one cannot find two p^{th} power residues [mod θ] whose difference is one, and that p is not a p^{th} power residue [mod θ].”²²*

(N.B: The theorem implicitly requires that at least one such θ exists.)

It is this theorem to which Germain was undoubtedly referring when she wrote to Gauss that any possible solutions would consist of numbers “whose size frightens the imagination”. Early in Manuscript A she says that she will apply the theorem for various values of p using her table. She mentions here that even just for $p = 5$, the valid auxiliary primes $\theta = 11, 41, 71, 101$ show that any solution to the Fermat equation would require a number with at least 39 decimal digits.

We will soon see that, as given, the proof of her Large Size theorem is insufficient, and we will discuss approaches by Germain to remedy this, as well as an approach by Legendre to large size of solutions. But we will also see that Sophie Germain’s Theorem, the result she is actually known for today, validly falls out of her proof.

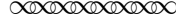
3.1 Germain’s approach to large size solutions

Note that the two hypotheses of Germain’s Large Size theorem are, first, the same N-C condition she already studied at length for her grand plan, and second, what we will call

Condition p -N- p (p is Not a p -th power). *p is not a p^{th} power residue, modulo θ .*

We now present a direct English translation of Germain’s proof. The proof implicitly begins with the fact that the N-C condition implies that one of the numbers x, y, z has to be divisible by θ . We also provide additional annotation, since Germain assumes the reader is already quite familiar with many aspects of her equations.

²² “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 $(2p - 1)^{\text{ième}}$ puissance du nombre p et des $p^{\text{ièmes}}$ puissances de tous les nombres premiers de la forme $Np + 1$, pour lesquels, en même tems [sic] que l’on ne peut trouver deux résidues $p^{\text{ièmes}}$ puissances dont la différence soit l’unité, p est non résidu puissance $p^{\text{ième}}$.”

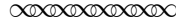


Assuming the existence of a single number subject to the double condition, I will prove first that the particular number x, y or z in the equation $x^p + y^p = z^p$ which is a multiple of the assumed number $[\theta]$, must necessarily also be a multiple of the number p^2 .

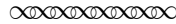
Indeed, if the numbers x, y, z are [assumed to be] relatively prime, then the [pairs of] numbers

$$\begin{array}{lll} x + y & \text{and} & x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + \text{etc} \\ z - y & \text{and} & z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 + \text{etc} \\ z - x & \text{and} & z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 + \text{etc.} \end{array}$$

can have no common divisors other than p .²³



For the first pair, this last claim can be seen as follows (and similarly for the other pairs). Denote the right hand expression on the first line by $\varphi(x, y)$. If some prime q other than p divides both numbers, then $y \equiv -x \pmod{q}$, yielding $\varphi(x, y) \equiv px^{p-1} \pmod{q}$. Then x and $x + y$ are both divisible by q , contradicting the assumption that x and y are relatively prime. This excludes all primes other than p as potential common divisors of $x + y$ and $\varphi(x, y)$.



If, therefore, the three numbers x, y , and z were all prime to p , then one would have, letting $z = lr$, $x = hn$, $y = vm$:²⁴

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

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

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

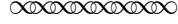
²³ “En supposant l’existence d’un seul des nombres assujettés à cette double condition, je prouverai d’abord que celui des nombres x, y et z qui dans l’équation $x^p + y^p = z^p$ sera multiple du nombre supposé, devra nécessairement être en même tems [sic] multiple du nombre p^2 .”

“En effet lorsque x, y et z sont premiers entr’eux, les nombres

$$\begin{array}{lll} x + y & \text{et} & x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + \text{etc} \\ z - y & \text{et} & z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 + \text{etc} \\ z - x & \text{et} & z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 + \text{etc.} \end{array}$$

ne peuvent avoir d’autres diviseurs communs que le nombre p .”

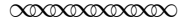
²⁴ “Si on voulait donc que les trois nombres x, y , et z fussent tous premiers a p on aurait, en faisant $z = lr$, $x = hn$, $y = vm$:



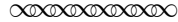
Equations like these were given by Barlow around 1810, and stated apparently independently by Abel in 1823 [Ri].

One can derive these equations as follows. In the first line, the assumption that x, y, z are each relatively prime to p , along with the Fermat equation, forces $x + y$ and $\varphi(x, y)$ to be relatively prime. It is this assumption that Germain is going to contradict. Since the product of $x + y$ and $\varphi(x, y)$ is equal to z^p , each of them must therefore be a p th power, as she writes. The other lines have parallel proofs.

Divisibility by p



Without loss of generality I assume that it is the number z which is a multiple of the prime number $[\theta]$ of the form $2Np + 1$, assumed to exist. One therefore has that $l^p + h^p + v^p \equiv 0 \pmod{2Np + 1}$. And since by hypothesis there cannot be, for this modulus, two p th power residues whose difference is 1, it will be necessary that it is l and not r , which has this modulus as a factor. Since $x + y \equiv 0 \pmod{2Np + 1}$, one concludes that $px^{p-1} \equiv r^p \pmod{2Np + 1}$, that is to say, because x is a p th power residue, p will also be a p th power residue, contrary to hypothesis; thus the number z must be a multiple of p .²⁵



The N-C condition and the congruence $l^p + h^p + v^p \equiv 0 \pmod{\theta = 2Np + 1}$ imply that either l , h , or v is divisible by θ . If one of h or v were, then x or y would also be divisible by θ , contradicting the assumption that

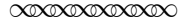
$$\begin{array}{ll} x + y = l^p & x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + \text{etc} = r^p \\ z - y = h^p & z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 + \text{etc} = n^p \\ z - x = v^p & z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 + \text{etc} = m^p. \end{array}$$

²⁵ "Pour fixer les idées je supposerai que c'est le nombre z qui est multiple du 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 $p^{\text{ièmes}}$ dont la différence soit l'unité, il faudra que ce soit l et nonpar r qui ait le même 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 $p^{\text{ième}}$ puissance, p aussi résidu $p^{\text{ième}}$ puissance, ce qui est contraire à l'hypothèse, il faut donc que le nombre z soit multiple de p ."

x, y, z are relatively prime. This implies that l is the number divisible by θ , and thus $y \equiv -x \pmod{\theta}$. Substituting, we have $\varphi(x, y) \equiv px^{p-1} \equiv r^p \pmod{\theta}$, as claimed. Furthermore, since $z \equiv 0 \pmod{\theta}$, we conclude from $z - x = v^p$ that x is a p th power modulo θ . Therefore, p is also a p th power modulo θ , a contradiction to the other hypothesis of the theorem.

Thus we have derived a contradiction to the assumption that x, y, z are all prime to p , which indeed forces one of x, y, z to be a multiple of p . But it is not clear yet why z , the number divisible by θ , has to be the one; this uncertainty is indicative of a flaw we will shortly observe. In order to continue the proof, Germain now in effect implicitly changes the assumption on z to be that z is the number known to be divisible by p , but not necessarily by θ , which in principle is fine, but must be kept very clear by us. She now replaces the first pair of equations by a new pair, reflecting this change. (The remaining equations still hold, since x and y must be relatively prime to p .)

Sophie Germain's Theorem as fallout



Setting actually $z = lrp$, the only admissible assumption is that

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

Because if, on the contrary, one were to assume that

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

then

$$(x + y)^{p-1} - \{x^{p-1} - x^{p-2}y + x^{p-3}y^2 + \text{etc}\}$$

would be divisible by p^{p-1} . Observe that in the equation $2z - x - y = h^p + v^p$ the form of the right-hand side forces it to be divisible by p or p^2 . Consequently, one sees that with the present assumptions z has to be a multiple of p^2 .²⁶

²⁶ "En prenant actuellement $z = lrp$, la seule supposition admissible est

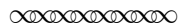
$$x + y = l^p p^{p-1}, \quad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + \text{etc} = pr^p,$$

car si on fesoit au contraire

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

$$(x + y)^{p-1} - \{x^{p-1} - x^{p-2}y + x^{p-3}y^2 + \text{etc}\}$$

seroit divisible par p^{p-1} , parconséquent si on observe que dans l'équation $2z - x - y = h^p + v^p$ la forme du second membre veut qu'il soit premier a p , ou multiple de p^2 on verra que, dans les suppositions presentes, z aussi doit être multiple de p^2 ."



To see Germain’s first assertion one can argue as follows. Since $z^p = x^p + y^p$ must be divisible by p , we need only show that $\varphi(x, y)$ is divisible by exactly the first power of p . If we set $x + y = s$, then

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

Now observe that all but the last summand of the right-hand side is divisible by p^2 , since p divides $s = x + y \equiv x^p + y^p = z^p \pmod{p}$ by Fermat’s Little Theorem, whereas the last summand is divisible by exactly p , since x is relatively prime to p .

Finally, to see that this forces z to be divisible by p^2 , observe that the equation $2z - x - y = h^p + v^p$ ensures that p divides $h^p + v^p$. Furthermore, p divides $h + v$ by Fermat’s Little Theorem, applied to h and v . Now note that, since $h \equiv -v \pmod{p}$, it follows that $h^p \equiv -v^p \pmod{p^2}$. Thus p^2 divides z , since p^2 divides $x + y$ by Germain’s new first pair of equations above.

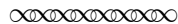
This much of her proof constitutes a valid demonstration of what we have identified as Sophie Germain’s Theorem.

A mistake in the proof



The only thing that remains to be proven is that all prime numbers of the form $[\theta =]2Np + 1$, which are subject to the same conditions as the number whose existence has been assumed, are necessarily divisors²⁷ of z .

In order to obtain this let us suppose that it is y , for example, and not z , that has one of the numbers in question as a factor. Then for this modulus we will have $h^p - l^p \equiv v^p$, consequently $v \equiv 0$, $z \equiv x$, $pz^{p-1} \equiv m^p$, that is to say, p is a p th power residue contrary to the hypothesis.²⁸



²⁷Germain wrote “multiples” here, but presumably meant “divisors”.

²⁸“La seule chose qui reste à prouver est que tous les nombres premier de la forme $2Np + 1$ qui sont assujettés aux mêmes conditions que celui de la même forme dont on a supposé l’existence sont nécessairement multiples [sic] de z .”

“Pour y parvenir supposons 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 residu puissance $p^{\text{ième}}$ contre l’hypothèse.”

Here Germain makes a puzzling mistake. Rather than using the equation (1'), resulting from the p -divisibility assumption on z , she erroneously uses the original equation (1) which required the assumption that all of x, y, z are relatively prime to p . Subtracting (1) from (2) and comparing the result to (3), she obtains the congruence $h^p - l^p \equiv v^p \pmod{\theta}$, since $y \equiv 0 \pmod{\theta}$. Although this congruence has been incorrectly obtained, we will follow how she deduces from it the desired contradiction, partly because we wish to see how the entire argument might be corrected. Since neither h nor l can be divisible by θ (since neither x nor z are), the N-C Condition implies that $v \equiv 0 \pmod{\theta}$, hence $z \equiv x$. Thus, $pz^{p-1} \equiv m^p$ follows from the right-hand equation of (3). Further, $z \equiv h^p$ follows from (2), since $y \equiv 0$, and, finally, this allows the expression of p as the residue of a p -th power, which contradicts the p -N- p Condition.

Except for the mistake noted, the proof of Germain's theorem is complete. If instead the correct new equation (1') had been used, then in place of the N-C Condition, the argument as written would need a condition analogous to N-C, but different, for the congruence

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

resulting from subtracting (1') from (2) instead of (1) from (2). That is, we could require the following additional hypothesis:

Condition N- p^{-1} (No p^{-1} differences). *There are no two nonzero p^{th} -power residues that differ by p^{-1} (equivalently, by $-2N$) modulo θ .*

Clearly, adding this condition as an additional hypothesis would make the proof of the theorem valid.

Germain's remedy?

Did Germain ever realize this problem, and attempt to correct it? To the left of the very well defined manuscript margin, at the beginning of the paragraph containing the error, are written two words in much smaller letters and a thicker pen. These words are either "voyez errata" or "voyez erratu".²⁹ This is one of only four places in Manuscript A where marginal notes mar its visual perfection. None of the content of these appears in Manuscript D, from which Manuscript A was meticulously copied. So Germain saw the

²⁹This is a good example of the challenge of original manuscripts, since it took many years before the authors could decipher these handwritten words, and therefore knew to look for an errata.

error in Manuscript A, but probably later, and wrote an errata about it. Where is the errata?

Most remarkably, not far away in the same archive of her papers, tucked apparently randomly in between sheets of the very much rougher draft of Manuscripts A and D mentioned in section 2, we find two sheets [Ge2, pp. 214 (right), 215 (left)] clearly titled “errata” or “erratu” in the same writing style as the marginal comment.

The moment one starts reading these sheets, it is clear that they address precisely the error Germain made. After writing the corrected equations (1'), (2), (3) (in fact she refines them even more, incorporating the p^2 divisibility she just correctly deduced) Germain notes that it is therefore a congruence of the altered form

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

that should hopefully lead to a contradiction. It is not hard to see that the $N-p^{-1}$ and $p-N-p$ conditions will suffice for this, but Germain observes right away that a congruence nullifying the $N-p^{-1}$ condition in fact exists for the very simplest case of interest to her, namely $p = 5$ and $N = 1$, since 1 and -1 are both 5-th powers, and they differ by $2N = 2$.³⁰ Germain then wisely embarks on an effort to prove her claim by other means, not relying on assuming the $N-p^{-1}$ condition. She develops arguments and claims based on knowledge of quadratic forms and quadratic reciprocity, but we find these hard to follow and have not been able fully to understand her efforts, including various marginal comments on these two sheets that we cannot fully decipher. There is more work to be done understanding her mathematical approach here. In the end it seems that Germain’s efforts may be inconclusive.

Verifying Condition $p-N-p$: Germain’s theoretical approach

We return now from Germain’s errata to consider the end of Manuscript A. Germain follows her Large Size of Solutions theorem with a method for finding auxiliary primes θ of the form $2Np + 1$ satisfying the two conditions (N-C and $p-N-p$) required for applying the theorem. Even though we now realize that her applications of the Large Size theorem are unjustified, since she did not succeed in providing a correct proof of the theorem, we will describe her methods for verifying its hypotheses, in order to show their

³⁰In fact the reader may check in various examples for small numbers that the $N-p^{-1}$ condition seems to hold rather infrequently compared with the N-C condition, so simply assuming the $N-p^{-1}$ condition as a hypothesis makes a true theorem, but perhaps not a very useful one.

skill, their application to Sophie Germain's theorem, and to compare them with the work of others.

Earlier in the manuscript Germain has already shown her methods for verifying Condition N-C for her grand plan. She now focuses on verifying Condition p -N- p , with application in the same range as before, i.e., for auxiliary primes $\theta = 2Np + 1$ using relevant values of $N \leq 10$ and odd primes $p < 100$.

Germain first points out that since $\theta = 2Np + 1$, therefore p will be a p -th power modulo θ if and only if $2N$ is also, and thus, due to the cyclic nature of the multiplicative units modulo θ , precisely if $(2N)^{2N} - 1$ is divisible by θ . Yet before doing any calculations of this sort, she obviates much effort by stating another theoretical result: For N of the form $2^a p^b$ in which $a + 1$ and $b + 1$ are prime to p , she claims that p cannot be a p -th power modulo θ provided 2 is not a p -th power modulo θ . Of course the latter is a condition (2-N- p) she already studied in detail earlier for use in her N-C analyses. Indeed the claim follows because $2^{a+1} p^{b+1} = 2Np \equiv (-1)^p$, which shows that 2 and p must be p -th powers together (although the hypothesis on b is not necessary for just the implication she wishes to conclude). Germain points out that this result immediately covers $N = 1, 2, 4, 8$ for all p . In fact, there is in these cases no need for Germain even to check the 2-N- p condition, since she already earlier verified N-C for these values of N , and 2-N- p follows from N-C. Germain easily continues to analyze $N = 5, 7, 10$ for Condition p -N- p by factoring $(2N)^{2N} - 1$ and looking for prime factors of the form $2Np + 1$. Astonishingly, by this method Germain deduces that there is not a single failure of Condition p -N- p for the auxiliary primes $\theta = 2Np + 1$ in her entire previously drawn table of values satisfying Condition N-C.

Germain ends Manuscript A by drawing conclusions on the minimum size of solutions to Fermat equations for $2 < p < 100$ using the values for θ in her table. Almost the most modest is her conclusion for $p = 5$. Since her techniques have verified that the auxiliaries 11, 41, 71, 101 all satisfy both Conditions N-C and p -N- p , Germain's Large Size theorem (if it were true) ensures that if $x^5 + y^5 = z^5$ were true in positive numbers, then one of the numbers $x + y$, $z - y$, $z - x$ must be divisible by $5^9 11^5 41^5 71^5 101^5$, which Germain notes has at least 39 decimal digits.

3.2 Comparing Germain on Condition p -N- p and Large Size with Legendre, Wendt, Dickson, Vandiver

Tables of residues for applying Sophie Germain's Theorem

Legendre's footnote credits Germain for Sophie Germain's Theorem and for applying it to prove Case 1 for odd primes $p < 100$ [Le]. For the application he exhibits a table providing, for each p , a single auxiliary prime satisfying both conditions N-C and p -N- p , based on examination of a raw numerical listing of all its p -th power residues. Thus he leaves the impression that Germain verified that her theorem was applicable for each $p < 100$ by brute force residue computation with a single auxiliary. In fact, there is even such a residue table to be found in Germain's papers [Ge2, p. 151 left], that gives lists of p -th power residues closely matching Legendre's table.³¹ Legendre's table could thus easily have been made from hers. This, however, is not the end of the story, contrary to the impression received from Legendre.

Theoretical approaches to Condition p -N- p

Both Legendre and Germain analyze theoretically the validity of Condition p -N- p as well as that of N-C for a range of values of N and p , even though, as with Germain's grand plan for proving Fermat's Last Theorem via Condition N-C, Legendre never indicates her efforts at proving large size for solutions by finding multiple auxiliary primes satisfying both Conditions N-C and p -N- p . Moreover, since all Legendre's work at verifying N-C and p -N- p comes after the footnote, he is mute about Germain developing techniques for verifying either condition. Rather, the clear impression his treatise leaves the reader is that Sophie Germain's Theorem and the brute force table are hers, while all the techniques for verifying Conditions N-C and p -N- p are his alone.

As we have seen, though, Germain qualifies auxiliaries to satisfy both N-C and p -N- p entirely by theoretical analyses, and her table in Manuscript A has no brute force listing of residues. In fact she developed general techniques for everything, with very little brute force computation evident, and

³¹There are a couple of small differences between Legendre's table of residues and the one we find in Germain's papers.

Germain states that she will not list the residues in the cases when $N \leq 2$ in the auxiliary prime, suggesting that she already knew that such auxiliary primes are always valid.

And while Germain, like Legendre, generally lists for each p the residues for only the single smallest auxiliary prime valid for both N-C and p -N- p , in the case of $p = 5$ she lists the residues for several of the auxiliaries that she validated in Manuscript A.

was very interested in verifying her conditions for many combinations of N and p , not just one auxiliary for each p . In short, the nature of Legendre's credit to Germain for proving Case 1 for $p < 100$ leaves totally invisible and unappreciated her much broader theoretical work that we have uncovered in Manuscript A.

We should therefore investigate, as we did earlier for Condition N-C, how Legendre's attempts at verifying Condition p -N- p compare with Germain's, to see if they are independent.

Legendre on Condition p -N- p

Legendre's approach to verifying Condition p -N- p for successive values of N is at first rather ad hoc, then based on the criterion whether θ divides $p^{2N} - 1$, slowly evolving to the equivalent divisibility of $(2N)^{2N} - 1$ instead, and appeals to his *Théorie des Nombres* for finding divisors of numbers of certain forms. Unlike Germain's methods, there is no recognition that many N of the form $2^a p^b$ are amenable to appeal to Condition 2-N- p . Suffice it to say that, as for Condition N-C, Legendre's approaches and Germain's take different tacks, with Germain starting with theoretical transformations that make verification easier, even though in the end they both verify Condition p -N- p for roughly the same ranges of N and p . There are aspects with both the N-C and p -N- p analyses where Germain goes further than Legendre with values of N and p , and vice versa.

Even their choices of symbols and notation are utterly different. Legendre never uses the congruence notation that Gauss had introduced a quarter century before, while Germain is fluent with it. Legendre quotes and relies on various results and viewpoints from the second edition of his *Théorie des Nombres*, and never considers Condition 2-N- p either for N-C or p -N- p analysis, whereas it forms a linchpin in Germain's approach to both. Germain rarely refers to Legendre's book or its results, but uses her implicit and intimate understanding of the group of units in the prime field, and its subgroups.

We are left surprised and perplexed by the lack of overlap in mathematical approach between Germain's Manuscript A and Legendre's treatise, even though the two are coming to the same conclusions page after page. There is nothing in the two manuscripts that would make one think they had communicated, except Legendre's footnote crediting Germain with the theorem that today bears her name. It is as though Legendre never saw Germain's Manuscript A, a thought we shall return to below. Four factors leave us greatly perplexed at this disparity. First, years earlier Legendre had

given Germain his strong mentorship during the work on elasticity theory that earned her a prize of the French Academy. Second, Legendre's own research on Fermat's Last Theorem was contemporaneous with Germain's. Third, Germain's letter to Gauss about the failure of N-C for $p = 3$ suggests detailed interaction. Fourth, we shall discuss later that Legendre's credit to Germain does match quite well with her Manuscript B. How could they not have been in close contact and sharing their results and methods? In the end, at the very least we can conclude that each did much independent work, and should receive separate credit for all the differing techniques they developed for analyzing and verifying the N-C and p -N- p conditions.

Wendt, Dickson, and Vandiver rediscover Germain's theoretical approach to Condition p -N- p

Later mathematicians were as unaware of Germain's theoretical analysis of Condition p -N- p as they were of her approach to Condition N-C, again because Legendre's published approach was very different and introduced nothing systematically helpful beyond basic calculation, and Germain's work was never published [BD]. In particular, the fact that for values of N of the form $2^a p^b$ for which p and a are relatively prime, Condition p -N- p follows from 2-N- p , which latter is automatic in the presence of Condition N-C, was essentially (re)discovered by Wendt in 1894 [We], and elaborated by Dickson [Di3] and Vandiver [Va] in the twentieth century. Again we wonder how progress on Fermat's Last Theorem might have been substantially advanced if Germain's theoretical idea had not languished in her unread papers.

Legendre's approach to large size of solutions

Legendre describes not just Sophie Germain's Theorem and applications, but also large size results similar to Germain's, although he makes no mention of his large size results having anything to do with her. Thus we should compare their large size work as well.

Germain presents a theorem about large size, and quite dramatic specific consequences, but the theorem is flawed and her attempts at general repair appear inconclusive. Legendre, like Germain, studies whether all qualifying auxiliary primes θ must divide the same one of x, y, z that p^2 does, which is where Germain went wrong in her original manuscript. Like Germain in her errata, Legendre recognizes that the N- p^{-1} condition would ensure the desired θ divisibility. But he too presses on in an alternative direction, since the condition is not necessarily (in fact perhaps not even often) satisfied.

But here, just as much as in his differing approach to verifying the N-C and p -N- p conditions, Legendre again chooses a completely different alternative approach than does Germain.

Legendre analyzes the placement of the p -th power residues more deeply in relation to the various expressions in equations (1'), (2), (3) above, and finds additional conditions, more delicate than that of $N-p^{-1}$, which will ensure the desired θ divisibility for concluding large size of solutions. Specifically, for example, when $p = 5$ Legendre has the same auxiliaries $\theta = 11, 41, 71, 101$ satisfying N-C and p -N- p as had Germain.³² However, as Germain explicitly pointed out for $\theta = 11$ in her errata, Condition $N-p^{-1}$ fails; in fact Legendre's calculations show that it fails for all four auxiliaries. While Germain attempted a general fix of her large size theorem using quadratic forms and quadratic reciprocity, Legendre's delicate analysis of the placement of 5-th powers shows that 11, 71, 101 (but not 41) must divide the same one of x, y, z as p^2 , and so he deduces that some sum or difference of two of the indeterminates must be divisible by $5^9 11^5 71^5 101^5$, i.e., must have at least 31 digits. This is weaker than the even larger size Germain incorrectly deduced, but it is a validly supported conclusion. Legendre successfully carries this type of analysis on to exponents $p = 7, 11, 13$, concluding that this provides strong numerical evidence for Fermat's Last Theorem. But he does not attempt a general theorem about large size of solutions, as did Germain. As with their work on Conditions N-C and p -N- p , we are struck by the disjoint approaches to large size of solutions taken by Germain and Legendre. It seems clear that they each worked largely independently, and there is no evidence in their manuscripts that they influenced each other.

4 Fermat's Last Theorem for exponents of form $2(8n \pm 3)$

Consider now what we call Manuscript B, entitled *Démonstration de l'impossibilité de satisfaire en nombres entiers à l'équation $z^{2(8n \pm 3)} = y^{2(8n \pm 3)} + x^{2(8n \pm 3)}$* . It seems clear that Germain has in mind that $p = 8n \pm 3$ be prime, and by the end of the manuscript, although it becomes difficult to decipher, she

³² Although Legendre never mentions the grand plan for proving Fermat's Last Theorem, he is interested in how many valid auxiliaries there may be for a given exponent. He claims that between 101 and 1000 there are no auxiliaries for $p = 5$ satisfying the two conditions, and that this must lead one to expect that 101 is the last. This presages Libri's claims that for each p there are only finitely many auxiliaries satisfying N-C, and is the one hint we find in Legendre of a possible interest in the grand plan.

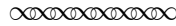
claims to have proven Fermat’s Last Theorem for all exponents of the form $2(8n \pm 3)$. Such a proof would be a stunning accomplishment.

Germain states and proves three theorems, and then has a final argument leading to the title claim. We shall analyze this manuscript for its approach, for its connection to her other manuscripts and to Legendre’s attribution to her, and for its correctness.

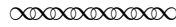
Although Germain does not spell out the big picture, leaving the reader to put it all together, it is clear that she is proceeding to prove Fermat’s Last Theorem via the division we make today, between Case 1 and Case 2, separately eliminating solutions in which the prime exponent $p = 8n \pm 3$ either does not or does divide one of x^2, y^2, z^2 in the Fermat equation $(x^2)^p + (y^2)^p = (z^2)^p$.

4.1 Case 1 and Sophie Germain’s Theorem

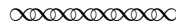
Germain begins by claiming to eliminate solutions in which none are divisible by p , and actually claims this for all odd prime exponents, writing



Theorem 1. *For any [odd] prime number p in the equation $z^p = x^p + y^p$, one of the three numbers $z, x, \text{ or } y$ will be a multiple of p^2 .*³³



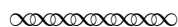
Today we name this Case 1 of Fermat’s Last Theorem, that solutions must be p -divisible (Germain claims a little more, namely p^2 divisibility). Note that there are no hypotheses as stated, since Germain wishes to evince that Case 1 is true in general, and move on to Case 2 for the exponents at hand. She does, however, immediately recognize that to prove this, she requires something else:



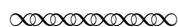
To demonstrate this theorem it suffices to suppose that there exists at least one prime number θ of the form $2Np + 1$ for which at the same time one cannot find two p^{th} power residues $[\text{mod } \theta]$ whose difference is one, and p is not a p^{th} power residue $[\text{mod } \theta]$.³⁴

³³ “Théorème premier. *Quelque soit le nombre premier p dans l’équation $z^p = x^p + y^p$ l’un des trois nombres z, x ou y sera multiple p^2 .*”

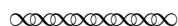
³⁴ “Pour démontrer ce théorème il suffit de supposer qu’il existe au moins un nombre premier θ de la form $2Np + 1$ pour lequel en même tems [sic] que l’on ne peut trouver deux residus puissances $p^{\text{ième}}$ dont la difference soit l’unité p est non residu puissance $p^{\text{ième}}$.”



Today we recognize this as the hypothesis of Sophie Germain’s Theorem, whereas for her it was not just a hypothesis, but something she believed was true and provable by her methods, since she goes on to say



Not only does there always exist a number θ satisfying these two conditions, but the course of calculation indicates that there must be an infinite number of them. For example, if $p = 5$, then $\theta = 2 \cdot 5 + 1 = 11$, $2 \cdot 4 \cdot 5 + 1 = 41$, $2 \cdot 7 \cdot 5 + 1 = 71$, $2 \cdot 10 \cdot 5 + 1 = 101$, etc.³⁵



Recall that Germain spends most of Manuscript A developing powerful techniques that support this belief in Conditions NC and p -N- p , and confirm them for $p < 100$, so it is not surprising that she wishes to claim to have proven Case 1 of Fermat’s Last Theorem, even though she still recognizes that there are implicit hypotheses she has not completely verified for all exponents.

Germain’s proof of her Theorem 1 is much like the beginning of her proof of the Large Size theorem of Manuscript A, which we laid out in section 3. Recall that the Large Size proof went awry only after the p^2 divisibility had been proven, so her proof here,³⁶ as there, proves p^2 divisibility without question. This is the closest to an independent statement and proof we find in her manuscripts of what today is called Sophie Germain’s Theorem. However, most curiously, at the end of the proof of Theorem 1 she claims also that the p^2 divisibility applies to the same one of x, y, z that is divisible by the auxiliary prime θ , which is the same as the claim, ultimately inadequately supported, where her Large Size proof in Manuscript A began to go wrong. While she makes no use of this additional claim here, so it is harmless to her line of future argument in this manuscript, it leads us to doubt a conjecture one could otherwise make about Manuscript B. One could imagine that Theorem 1 was written down as a means of salvaging what she could from the Large Size theorem, once she discovered the flaw in the latter part of its proof. But since the essence of the flawed claim there appears also here (without proof), even though without consequent maleffect, we cannot argue that this manuscript contains a corrected more limited version of the Large Size theorem argument.

³⁵ “Non seulement il existe toujours un nombre θ qui satisfait à cette double condition mais la marche du calcul indique qu’il doit s’entrouver une infinité $p = 5 \quad \theta = 2 \cdot 5 + 1 = 11$, $2 \cdot 4 \cdot 5 + 1 = 41$, $2 \cdot 7 \cdot 5 + 1 = 71$, $2 \cdot 10 \cdot 5 + 1 = 101$, etc.”

³⁶The proof of Theorem 1 in Manuscript B is largely reproduced, in translation, in [LP].

4.2 Case 2 for p dividing z

The rest of Manuscript B deals with Case 2 of Fermat's Last Theorem, which is characterized by equations (1'), (2), (3) in section 3.1. For completeness, we mention that Theorem 2 contains a technical result not relevant to the line of proof Germain is developing. Perhaps she placed it and its proof here simply because it was a result of hers about Case 2, which is the focus of the rest of the manuscript.³⁷

As we continue with Case 2, notice that, by involving squares, the equation $(x^2)^p + (y^2)^p = (z^2)^p$ has an asymmetry forcing separate consideration of z from x or y in proving Fermat's Last Theorem. Germain addresses the first of these, the p -divisibility of z , in her Theorem 3, which asserts that z cannot be a multiple of p , if p has the form $8n + 3$, $8n + 5$, or $8n + 7$. She proves Theorem 3 by contradiction, by assuming that z is divisible by p . Her proof actually begins with some equations that require some advance derivation. Using the relative primality of the key numbers in each pair of the Case 2 equations (1'), (2), (3) of Manuscript A, for pairwise relatively prime solutions x^2 , y^2 , z^2 (once the extra p^2 divisibility is built in), the reader may easily verify that the left trio of these equations becomes³⁸

$$\begin{aligned}x^2 + y^2 &= p^{4p-1}l^{2p} \\z^2 - y^2 &= h^{2p} \\z^2 - x^2 &= v^{2p}.\end{aligned}$$

The text of Germain's proof begins with these equations.

Germain quickly confirms Theorem 3 for $p = 8n + 3$ and $8n + 7$ using the fact, long known from Fermat's time, that a sum of squares can contain no prime divisors of these two forms. For $p = 8n + 5$ she must argue differently, as follows.

Because $z - y$ and $z + y$ (respectively $z - x$ and $z + x$) are relatively prime, one has $z + y = (h')^{2p}$ and $z + x = (v')^{2p}$, whence $y^2 \equiv (h')^{4p} \pmod{p}$ and $x^2 \equiv (v')^{4p} \pmod{p}$, yielding $(h')^{4p} + (v')^{4p} \equiv 0 \pmod{p}$ since $x^2 + y^2$ is divisible by p . This she points out is a contradiction, since -1 is not a biquadratic residue modulo $8n + 5$.

³⁷Theorem 2 asserts that in the equations (1'), (2), (3) pertaining in Case 2, the numbers r , m , n can have prime divisors only of the form $2Np + 1$, and that moreover, the prime divisors of r must be of the even more restricted form $2Np^2 + 1$. Legendre also credits this result to Germain in his footnote.

³⁸We do not see how she obtains $4p - 1$ as exponent, rather than just $2p - 1$, even after including the stronger p^2 divisibility; but $2p - 1$ suffices.

The unfortunate flaw in this proof is perhaps not obvious at first. The $2p$ -th power expressions for $z + y$ and $z + x$ rely on $z - y$ and $z + y$ (respectively $z - x$ and $z + x$) being relatively prime. This would be true from the pairwise relative primality of x, y, z , if the numbers in each difference had opposite parity, but otherwise their difference and sum have precisely 2 as greatest common divisor. Writing $(x^p)^2 + (y^p)^2 = (z^p)^2$ and recalling basics of Pythagorean triples, we see that opposite parity fails either for $z - y$ or $z - x$. Suppose without loss of generality that it is $z - y$. Then either $z - y$ or $z + y$ has only a single 2 as factor (since y and z are relatively prime), so it cannot be a $2p$ -th power. One can include this single factor of 2 and redo Germain's analysis to the end, but one then finds that it comes down to whether or not -4 is a biquadratic residue modulo $8n + 5$, and this unfortunately is true, rather than false as for -1 . So Germain's proof of Theorem 3 appears fatally flawed for $p = 8n + 5$.

4.3 Case 2 for p dividing x or y

In her final argument after Theorem 3, Germain finishes Case 2 for $p = 8n + 3$ and $8n - 3$ by dealing with the second possible situation, where either x or y is divisible by p . This argument again builds from enhanced versions of equations similar to (1'), (2), (3), but is considerably more elaborate, rising up through detailed study of the specific cases $p = 5, 13, 29$, until she is able to end with an argument applying to all $p = 8n + 3$ and $8n - 3$. However, since the argument proceeds initially as did the proof of Theorem 3, it too relies on the same mistaken assumption about relative primality that misses an extra factor of 2, and one finds that accounting for this removes the contradiction Germain aims for, no matter what value p has.

4.4 Manuscript B as source for Legendre?

In the end we must conclude that this proof of the bold claim to have proven Fermat's Last Theorem for many exponents fails due to an elementary mistake that any mathematician could make. But what is correct in Manuscript B fits extremely well with what Legendre wrote about Germain's work. The manuscript contains precisely the results Legendre credits to Germain, namely Sophie Germain's Theorem and the technical result of Theorem 2 about the equations in the proof of Sophie Germain's Theorem. Legendre does not mention the claims in the manuscript that turn out not to be validly proved. If Legendre used Germain's Manuscript B as his source for what he chose to publish as Germain's, then he vetted it and extracted the parts

that were correct.

5 Fermat’s Last Theorem for even exponents

Another tantalizing direction of Germain’s is provided by three pages that we call Manuscript C.³⁹ These pages contain highly polished statements with proof of two theorems.

The first theorem claims that the “near-Fermat” equation $2z^{2n} = y^{2n} + x^{2n}$ has no natural number solutions for any even exponent $2n$. In fact Germain claims that her proof applies to an entire family of similar equations in which the exponents are not always the same for all variables simultaneously. Her proof begins with a claimed parametric characterization of integer solutions to the “near-Pythagorean” equation $2c^2 = b^2 + a^2$, similar to the parametric characterization of Pythagorean triples (solutions to $c^2 = b^2 + a^2$) used by Euler in his proof of Fermat’s Last Theorem for exponent four [LP]. We are unfamiliar even with the beginning parametric description of Germain’s, and will not try to analyze her proof further here, nor pronounce any judgement on its correctness. Someone else may wish to pursue whether it is valid or not. However, we do not know of modern evidence of a theorem denying solutions to the near-Fermat equation $2z^{2n} = y^{2n} + x^{2n}$.

Germain’s second claim is to prove Fermat’s Last Theorem for all even exponents greater than two, and her proof relies directly on the previous theorem. However, it seems to us that her proof likely flounders, as did the proof above of Theorem 3 in Manuscript B, on another unjustified assumption of relative primality of two expressions, in this case the two factors $z - y$ and $z^{n-1} + yz^{n-2} + \dots + y^{n-2}z + y^{n-1}$ of $z^n - y^n$, under only the assumption that x , y , and z are pairwise relatively prime in the Fermat equation $z^{2n} = y^{2n} + x^{2n}$. It does seem to us that Germain’s proof is fine, though, for “Case 1” (modulo appeal to the previous theorem, of course), i.e., provided that no factor of n divides x , y , or z , in which case the two factors above will be relatively prime.

³⁹Yet one more manuscript, claiming to dispense with even exponents by quite elementary means, is [Ge2, p. 90 (left)–90 (right)]. It contains a mistake that Germain went back to, crossed out, and corrected. But she didn’t carry the corrected calculation forward, likely because it is then obvious that it won’t produce the desired result, so is not worth pursuing further.

6 Germain's approaches to Fermat's Last Theorem: précis and connections

Our analyses above of Sophie Germain's manuscripts have revealed a wealth of important unevaluated work on Fermat's Last Theorem, calling for a reassessment of her work and reputation. To prepare for our reevaluation and conclusion, we now summarize what we have discovered mathematically in these manuscripts, and see how it differs from the limited material upon which Germain's reputation has been built.

6.1 The grand plan to prove Fermat's Last Theorem

In Manuscript A, Germain pioneers a grand plan for proving Fermat's Last Theorem for any prime exponent $p > 2$ based on satisfying a modular non-consecutivity (N-C) condition for infinitely many auxiliary primes. She develops an algorithm verifying the condition within certain ranges, and outlines an induction on auxiliaries to carry her plan forward. Her techniques for N-C verification are completely different from, but just as extensive as, Legendre's, although his were for the purpose of proving Case 1, and were also more ad hoc than hers. That Germain, as opposed to just Legendre, even had any techniques for N-C verification, has been unknown to all subsequent workers who have labored for almost two centuries to extend N-C verification for proving Case 1. Germain likely abandoned further efforts at her plan after Legendre suggested to her that it would fail for $p = 3$. She sent him a proof confirming this, by showing that there are only finitely many valid N-C auxiliaries.

Unlike Legendre's, Germain's methods and terminology adopt Gauss' congruence language, and her techniques have in several respects an early group-theoretic flavor. Reading her manuscript, we find ourselves almost instinctively thinking in terms of the structure of the multiplicative group of units modulo p . Germain's approach for verifying N-C was independently discovered by L. E. Dickson in the twentieth century. He, or earlier workers, could easily have obtained a jump start on their own work by taking their cue from Germain's methods, had they known of them. Recent researchers have again approached N-C by induction, as did Germain.

6.2 Large size of solutions and Sophie Germain's Theorem

Also in Manuscript A, Germain writes a theorem and applications to force extremely large minimal sizes for solutions to Fermat equations, based on

satisfying both the N-C and p -N- p conditions. She later realized a flaw in the proof, and attempted to repair it using her knowledge of quadratic residues. The valid part of the proof yields what we call Sophie Germain's Theorem, which then allows proof of p^2 -divisibility of solutions, and therefore Case 1. Germain's efforts to satisfy the p -N- p condition are based on her theoretical result showing that it will often follow from the 2-N- p condition, which she has already studied for N-C. This then makes it in practice very easy to verify p -N- p , once again unlike Legendre's different and more ad hoc methods. Again, later researchers could have begun where Germain left off, had they known of her methods. Instead, her result obtaining p -N- p from 2-N- p was also independently discovered much later, by Wendt, Dickson, and Vandiver in their efforts to prove Case 1.

6.3 Exponents $2(8n \pm 3)$ and Sophie Germain's Theorem

In Manuscript B, Germain makes a very creditable attempt to prove Fermat's Last Theorem for all exponents $2p$ where $p = 8n \pm 3$ is prime. This would have been a major accomplishment. Germain begins with a proof of what we call Sophie Germain's Theorem, in order to argue for Case 1. Manuscript B provides us with our best original source for the theorem for which she is famous. Her subsequent argument for Case 2 boils down to knowledge about biquadratic residues. This latter contains a flaw related to relative primality. The manuscript fits well as a primary source for what Legendre credited to Germain.

6.4 Even exponents

In Manuscript C, Germain writes two theorems and their proofs to establish Fermat's Last Theorem for all even exponents, by methods completely unlike those in her other manuscripts. These, too, would be stunning achievements. She plans to prove Fermat's Last Theorem by showing first that a slightly different family of Diophantine equations has no solutions. So she begins by claiming that the "near-Fermat" equations $2z^{2n} = y^{2n} + x^{2n}$ (and whole families of related equations) have no positive solutions. Her proof of this claim begins by assuming that the reader is already familiar with a parametric characterization of "near-Pythagorean triples" satisfying $2c^2 = b^2 + a^2$, which we are not. While this proof may well be correct, her proof of Fermat's Last Theorem for even exponents, based on this "near-Fermat result," suffers from the same flaw for Case 2 as in Manuscript B, which would have been caught by careful collegial reading. For Case 1 it appears to be correct.

7 Reevaluation of Germain's work in number theory

7.1 Germain as strategist: theories and techniques

We see that Germain focused on big, general theorems applicable to infinitely many prime exponents, rather than simply tackling single exponents as usually done by others. In this work, she developed general theories and techniques quite multifaceted both in goal and methods. She did not focus overly on examples or ad hoc solutions. She also used to great advantage the modern point of view on number theory espoused by Gauss. The significance of Germain's theoretical techniques for verifying conditions N-C and p -N- p is indicated by their rediscovery and use much later by Wendt, Dickson, and Vandiver, and a very recent revival of the approach by mathematical induction. Moreover, her approach to these was more systematic and theoretical than Legendre's pre-Gaussian and completely different methods.

These features of her work demonstrate that, contrary to what has been thought by some, Sophie Germain was not a dabbler in number theory who happened to light upon one significant theorem. In fact, what we call Sophie Germain's Theorem is simply fallout from within two separate much grander engagements we find in her papers, fallout that we can retrospectively isolate, but which she did not. It seems that it is we and Legendre, not Germain, who have created "Sophie Germain's Theorem" as an entity.

We suggest that Sophie Germain would be disappointed to learn that for almost two hundred years, the aftereffect of Legendre singling out for publication a single provable "theorem" due to her, albeit presumably well-intended, rendered all her various mathematical attacks on Fermat's Last Theorem invisible and languishing in her unread and unpublished personal papers. It is also unfortunate that no one has known before now that all the results published by Legendre verifying conditions N-C and p -N- p , quoted and used extensively by others to the present, are due but uncredited to Germain, by more sophisticated and theoretical methods.

Germain's was an ambitious and bold mathematical agenda. She tackled what we know in retrospect was one of the hardest problems in mathematics. It should therefore be no surprise that her attempts at broad results probably never succeeded in actually proving Fermat's Last Theorem even for a single exponent, although she seems to have come close a number of times. Germain in a sense missed out on greater fame by aiming too high.

7.2 Interpreting the errors in Germain's manuscripts

Mathematicians often make errors in their private work, usually winnowed out before publication through their own revisions, reactions to presentations, informal review by supportive colleagues, or the process of publication. We have seen that several of Germain's manuscripts on Fermat's Last Theorem contain errors in her proofs. But there are several mitigating factors we must consider.

First, in a sense we are cheating and short-circuiting the normal processes by peeking at Germain's private papers, works she chose never to submit for publication, even had she shown them to anyone. Perhaps she knew of the errors we see, but chose to keep these papers in a drawer for later revival via new ideas, as any mathematician might do. We can see explicitly that she later recognized one big error, in her Large Size of Solutions proof, and wrote an errata attempting remedy. And we also see the retrospective correction of an error in another proof, of Fermat's Last Theorem for even exponents, then put aside because it left the rest of the proof irremediable.

Second, let us assess the mathematical nature of the mistakes in her manuscripts. In elasticity theory, where the holes in her societally forced self-taught education were serious and difficult to remediate on her own [BD], Germain suffered from persistent conceptual difficulties leading to repeated serious criticisms of her work. By contrast, number theory perhaps lent itself better than elasticity theory to effective independent work based on self-education, in part because it was essentially entirely reinvented in Gauss' single book. Germain had been able to train herself well from the books of both Legendre and Gauss, and she shows careful work based especially on Gauss' *Disquisitiones Arithmeticae* as her guide. The mistakes we have found in her number theory manuscripts are characteristic of those any mathematician might easily make, an annoying slip of the mind to be caught later in each case, rather than any conceptual misunderstanding. In particular, her entire grand plan for proving Fermat's Last Theorem, including algorithms for verifying Conditions N-C and p -N- p , were all on very sound footing. So her mistakes should be considered minor, even though they happen to leave her big claims about large size and proving Fermat's Last Theorem for various families of exponents unproven.

Further, we should ask what evaluation by peers Germain's manuscripts received, either by helpful individuals or institutions, that should have brought errors to her attention. Here we will encounter more a puzzle than an answer.

7.3 Review by others versus isolation

Germain's elasticity theory: praise and neglect

There is already solid evidence [BD] that during Germain's long process of working to solve the elasticity problem in mathematical physics,⁴⁰ she received ever decreasing collegial review and honest critique of her work. In fact, towards the end perhaps none. Publicly praised as genius and marvel, she was increasingly ignored privately and institutionally when it came to discourse about her elasticity work. There is no evidence of any individual intentionally wishing her harm, and indeed some tried personally to be quite supportive. But the existing system ensured that she lacked early solid training or sufficiently detailed and constructive critique that might have enabled her to be more successful in her elasticity research. Germain labored continually under marginalizing handicaps of lack of access to materials and normal personal or institutional discourse, strictures that male mathematicians did not experience [BD]. The evidence suggests that Germain in effect worked in substantial isolation much of the time.

Germain's interactions about Fermat's Last Theorem: the evidence

Given the social features dominating Germain's work in elasticity theory, what was the balance between collegial interaction and isolation in her work on Fermat's Last Theorem? Specifically, we will focus on what to make of the disparity between the techniques of Germain and Legendre for their many identical results on the Fermat problem. And we will ask what of Germain's work and results was seen by Legendre, or anyone?

We have no actually published work by Germain herself on Fermat's Last Theorem. Even though much of the work we have described in her manuscripts would have been eminently publishable, such as her theoretical means of verifying the N-C and p -N- p conditions for applying Sophie Germain's Theorem to prove Case 1, it never was. While we could speculate on reasons for this, it certainly means that it didn't receive any formal institutional review. Nor presumably could Germain easily present her work to the Academy of Sciences, like her male contemporaries.

⁴⁰The Academy's elasticity prize competition was announced in 1809, twice extended, and Germain eventually received the award in 1816. Thereafter she carried out efforts at personal, rather than institutional, publication of her work on elasticity theory, stretching long into the 1820s [BD].

Despite having analyzed a wealth of mathematics in Germain's manuscripts, we still have little to go on when considering her interactions with others. Germain's manuscripts say nothing directly about outside influences, so we must infer them from their mathematical content alone. And Germain's 1819 letter to Gauss focused on the broad scope of her work on Fermat's Last Theorem, but did not mention any direct contact with others, and apparently received no response from Gauss.

On the bright side, while Legendre's footnote is only a brief statement of credit, we can compare it very profitably with our study of the content of Germain's manuscripts. And we also have one highly relevant piece of correspondence, Germain's letter to Legendre confirming back to him from the previous day's conversation that her grand plan will not work. From these we can draw some important and interesting conclusions.

Legendre and Germain: A perplexing record

Legendre's footnote and Germain's letter to him indicate that they had mathematically meaningful contact about the Fermat problem, although we do not know how frequently, or much about its nature. What then does our study of her most polished manuscripts suggest? First, it is a real surprise to have found from Manuscript A that Germain and Legendre each had very extensive techniques for verifying Conditions N-C and p -N- p , but that they are completely disjoint approaches, devoid of mathematical overlap. Their methods were obviously developed completely independently, hardly what one would expect from two mathematicians in close contact. By contrast, Legendre's crediting footnote details exactly the results that are correct from Germain's Manuscript B, namely Sophie Germain's Theorem and an additional technical result about the equations in its proof. So while Manuscript B, along with her separate table of residues and auxiliaries, is an extremely plausible source for Legendre's credit to her, Germain's Manuscript A shows completely independent but parallel work left invisible by Legendre's treatise.

So where does this leave Manuscript A? It contains Germain's grand plan, along with all her methods and theoretical results for verifying N-C and p -N- p , and her large size theorem. This seems like her most substantial work, and yet we can find not a speck of evidence in Legendre's 1823 treatise suggesting that he had actually seen Germain's Manuscript A, despite it being placed by her letter to Gauss at considerably prior to 1819. The only evidence we have that Legendre knew of her grand plan is Germain's letter to him proving that it will not work for $p = 3$. But even if this failure

were his reason for not mentioning the grand plan at all in his treatise, why is Legendre mute about Germain through the many pages of results identical to hers that he proves, by completely different means, on Conditions N-C and p -N- p for establishing Case 1? Extensions of these results have been important to future work ever since, but no one has known that these were equally due to Germain, and by more powerful methods. If Legendre had seen Manuscript A, he knew all about Germain's methods, and could and should have credited her in the same way he did for what is in Manuscript B. We must therefore at least consider, did Legendre, or anyone else, ever see Manuscript A and so comprehend most of Germain's work on Fermat's Last Theorem, let alone provide her with constructive feedback? It is reasonable to be skeptical. Earlier correspondence with Legendre shows that, while he was a great personal mentor to her initially during the elasticity competition, and seems always to have been a friend and supporter, he withdrew somewhat from mentorship in frustration as the competition progressed [BD, p. 63]. Did this withdrawal carry over somehow to contact about Fermat's Last Theorem? Without finding more correspondence between them about the topic, we may never know whether Germain had much extensive or intensive communication with anyone about her work on Fermat's Last Theorem.

The Fermat prize competition

There was one final possible avenue for review of Germain's work on the Fermat problem. At the same session of the Academy of Sciences in 1816 at which Sophie Germain was awarded the prize for the competition on elasticity, a new competition was set, on the Fermat problem. Extended in 1818, it was retired in 1820 with no award, and Sophie Germain never made a submission [BD]. And yet, together, our manuscript evidence and the 1819 date of her letter to Gauss, strongly suggest that she was working hard on the problem during the years of the prize competition, perhaps even stimulated greatly by it.

Why did she not submit a manuscript for this new prize, given the enormous progress on the Fermat problem we have found in her manuscripts, and the meticulous and comprehensive appearance of her work in Manuscript A, which appears prepared for public consumption. Was Germain's reluctance due to previous frustrating experiences from her multiple submissions for the elasticity prize through its two extensions—a process that often lacked helpful critiques or suggested directions for improvement [BD]. Or, having been particularly criticized for incompleteness during the elas-

ticity prize competition, did she simply know she had not definitely proved Fermat's Last Theorem in full, and hence felt she had nothing yet sufficient to submit.

8 Conclusion

The impression to date has been that Germain could have accomplished so much more had she enjoyed the normal access to education, collegial interaction and review, professional institutions, and publication accorded to male mathematicians [BD]. Our study of her manuscripts bolsters this perspective. The evidence from Germain's manuscripts, and comparison of her work with that of Legendre and later researchers, displays dramatic, sophisticated, multifaceted, independent work on Fermat's Last Theorem, considerably more extensive than what we have from Legendre's crediting footnote. It corroborates the isolation within which she worked, and suggests that sadly much of this impressive work may never have been seen by others, certainly not by a wider audience like ourselves. We see that Germain was clearly a strategist, who singlehandedly created and pushed full-fledged programs towards Fermat's Last Theorem, and developed powerful theoretical techniques for carrying these out, such as her methods for verifying Conditions N-C and p -N- p . We are reminded again of her letter to Gauss: "I will give you a sense of my absorption with this area of research by admitting to you that even without any hope of success, I still prefer it to other work which might interest me while I think about it, and which is sure to yield results." Sophie Germain was a much more impressive number theorist than anyone has ever known.

References

- [AH] Adleman, L. M. and Heath-Brown, D. R., *The first case of Fermat's last theorem*, *Inventiones Mathematicae* **79** (1985), 409–416.
- [BD] Louis Bucciarelli and Nancy Dworsky, *Sophie Germain: an essay in the history of the theory of elasticity*, D. Reidel, Boston, 1980.
- [Ce] A. Del Centina, A. Fiocca, Giunia Adini, and Maria Luisa Tanganelli, *L'archivio di Guglielmo Libri dalla sua dispersione ai fondi della Biblioteca Moreniana = The archive of Guglielmo Libri from its dispersal to the collections at the Biblioteca Moreniana*, L. S. Olschki, Firenze, 2004.

- [Ce1] A. Del Centina, *Letters of Sophie Germain preserved in Florence*, *Historia Mathematica* **32** (2005), 60–75.
- [Ce2] A. Del Centina, *The manuscript of Abel’s Parisian memoir found in its entirety*, *Historia Mathematica* **29** (2002), 65–69 (and Corrigendum, *Historia Mathematica* **30** (2003), 94–95).
- [Ce3] A. Del Centina, *Abel’s surviving manuscripts including one recently found in London*, *Historia Mathematica* **33** (2006), 224–233.
- [Ce4] A. Del Centina, *Abel’s manuscripts in the Libri collection: their history and their fate*, In: *Il manoscritto parigino di Abel conservato nella Biblioteca Moreniana di Firenze*. Olschki, Florence, pp. 87–103 [Italian and English], 2002. Also at http://web.unife.it/progetti/geometria/storia/ManoscrittidiAbel_en.pdf
- [Di] L. E. Dickson, *History of the theory of numbers*, vol. II, Carnegie Institution, Washington DC, 1920; reprinted by Chelsea, New York, 1971.
- [Di1] L. E. Dickson, *On the congruence $x^n + y^n + z^n \equiv 0 \pmod{p}$* , *J. für Mathematik* **135** (1909), 134–141.
- [Di2] L. E. Dickson, *Lower limit for the number of sets of solutions of $x^n + y^n + z^n \equiv 0 \pmod{p}$* , *J. für Mathematik* **135** (1909), 181–188.
- [Di3] L. E. Dickson, *On the last theorem of Fermat*, *Messenger of Mathematics* **3** (1908), 15–32.
- [Di4] L. E. Dickson, *On the last theorem of Fermat (second paper)*, *Quarterly Journal of Pure and Applied Math.* **40** (1908), 27–45.
- [Ed] Harold M. Edwards, *Fermat’s Last Theorem: A genetic introduction to algebraic number theory*, Springer Verlag, New York, 1977.
- [FJ] David Ford and Vijay Jha, *On Wendt’s determinant and Sophie Germain’s theorem*, *Experimental Mathematics* **2** (1993), 113–120.
- [Fo] Étienne Fouvry, *Théorème de Brun-Titchmarsh; application au théorème de Fermat*, *Inventiones Mathematicae* **79** (1985), 383–407.
- [Ga1] Carl Friedrich Gauss, *Werke*, Teubner, Leipzig, 1863–1929.

- [Ga2] Carl Friedrich Gauss, *Commentationes Societatis Regiae Scientiarum Gottingensis* **16** (1808), Göttingen; also *Werke*, Göttingen, 1876, Band 2, pp. 1–8.
- [Ge1] Sophie Germain, *Unpublished letter to C. F. Gauss*, Niedersächsische Staats- und Universitätsbibliothek Göttingen.
- [Ge2] Sophie Germain, *Papiers de Sophie Germain*, MS. FR9114, Bibliothèque Nationale, Paris.
- [Ge3] Sophie Germain, *Papiers de Sophie Germain*, MS. FR9115, Bibliothèque Nationale, Paris.
- [Ge4] Sophie Germain, *Letter (undated) to A.M. Legendre, 3 pages plus address page*, in the Samuel Ward Papers of the Ward Family Papers (Box 7), New York Public Library.
- [Ge5] Sophie Germain, in the Nuovo Fondo Libri, Biblioteca Moreniana, Firenze, Italy.
- [LP] Reinhard C. Laubenbacher and David Pengelley, *Mathematical expeditions: chronicles by the explorers*, Springer, New York, 1999.
- [LP1] Reinhard C. Laubenbacher and David Pengelley, Gauß, Eisenstein, and the “third proof” of the Quadratic Reciprocity Theorem: Ein kleines Schauspiel, *Mathematical Intelligencer* **16** (1994), 67–72.
- [LP2] Reinhard C. Laubenbacher and David Pengelley, Eisenstein’s misunderstood geometric proof of the Quadratic Reciprocity Theorem, *College Mathematics Journal* **25** (1994), 29–34.
- [Le] Legendre, A. M., *Recherches sur quelques objets d’analyse indéterminée et particulièrement sur le théorème de Fermat*, Mém. Acad. Roy. des Sciences de l’Institut de France **6** (1823), Didot, Paris, 1827; also appeared as Second Supplément (1825) to *Essai sur la théorie des nombres*, Second edn., Paris, 1808; also reprinted in *Sphinx-Oedipe* **4** (1909), 97–128.
- [Li] G. Libri, *Mémoire sur la théorie des nombres*, *Journal für Mathematik* **9** (1832), 54–80, 169–188, 261–276.
- [Li1] G. Libri, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématique et de physique*, Florence, L. Ciardetti, 1829, pp. 47–140.

- [Li2] G. Libri, *Memoria di Guglielmo Libri sopra la teoria dei numeri*, Firenze, 1820.
- [Li3] G. Libri, *Mémoire sur la théorie des nombres*, in Mémoires présentés par divers Savants a l'Académie Royale des Sciences de l'Institut de France; sciences mathématiques et physiques, **5** (1838), 1–75; also published by Imp. Royale, Paris, 1833.
- [Pe] A. E. Pellet, *Mémoire sur la théorie algébrique des équations*, Bulletin de la Société Mathématique de France **15** (1886–87), 61–102.
- [Pe1] P. Pepin, *Étude sur la théorie des résidues cubiques*, J. Math. Pures et Appl. (3) **2** (1876), 313–324.
- [Pe2] P. Pepin, *Sur divers tentatives de démonstration du théorème de Fermat*, Comptes Rendus Acad. Sci. Paris **91** (1880), 366–367.
- [Po] L. Poinsoot, *Mémoire sur l'application de l'algèbre à la théorie des nombres*, Journal de l'École Polytechnique **11** (1820), 342–410; also in Mémoires de l'Académie des Sciences, Paris, IV (1819–1820), 99–184.
- [Ri] P. Ribenboim, *Fermat's last theorem for amateurs*, Springer, New York, 1999.
- [RM] P. Ruju and M. Mostert, *The life and times of Guglielmo Libri (1802–1869): scientist, patriot, scholar, journalist and thief; a nineteenth-century story*, Verloren Publishers, Hilversum, The Netherlands, 1995.
- [Sc] C. Schilling (ed.), *Wilhelm Olbers: sein Leben und seine Werke*, vol. 2, Berlin, Springer Verlag, 1900.
- [Sti] Stillwell, John, *The four pillars of geometry*, Springer, New York, 2005.
- [St] H^{te} Stupuy (ed.), *Oeuvres philosophiques de Sophie Germain*, Paul Ritti, Paris, 1879. New ed. Firmin-Didot, Paris, 1896.
- [Va] Vandiver, H. S., *Note on trinomial congruences and the first case of Fermat's Last Theorem*, Annals of Mathematics **27** (1926), 54–56.
- [We] E. Wendt, 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 auflösbar ist, *J. Reine und Angewandte Mathematik* **113** (1894), 335–347.