"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
reinhard@vbi.vt.edu

David Pengelley*
Mathematical Sciences
New Mexico State University
Las Cruces, NM 88003, USA
davidp@nmsu.edu

July 12, 2010

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 ideas and 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.

1

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 idées et resultats 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.

Contents

3

1 Introduction

Sophie Germain (Figure 1)[1] was the first woman known for important original research in mathematics.[2] While perhaps more famous for her work in mathematical physics that earned her a French Academy prize, Germain is also credited with an important result in number theory towards proving Fermat's Last Theorem. We will make a substantial reevaluation of her work on the Fermat problem, based on translation and mathematical interpretation of numerous documents in her own hand, and will argue that her accomplishments are much broader, deeper, and more significant than has been realized.

Fermat's Last Theorem refers to Pierre de Fermat's famous seventeenth century claim that the equation $z^p = x^p + y^p$ has no natural number solutions x, y, z for natural number exponents $p > 2$. The challenge of proving this assertion has had a tumultuous history, culminating in Andrew Wiles' success at the end of the twentieth century [46, XI.2].

Once Fermat had proven his claim for exponent 4 [14, p. 615ff] [54, p. 75ff], it could be fully confirmed just by substantiating it for odd prime exponents. But when Sophie Germain began working on the problem at the turn of the nineteenth century, the only prime exponent that had a proof was 3 [14, XXVI] [19, ch. 3] [46, I.6, IV] [54, p. 335ff]. As we will see, Germain not only developed the one theorem she has long been

---

[1]From [3, p. 17].

[2]A 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 Lawrence Bucciarelli and Nancy Dworsky [3].

Figure 1: Sophie Germain: a bust by Z. Astruc

known for towards proving part of Fermat's Last Theorem for all primes. Her manuscripts reveal a comprehensive program to prove Fermat's Last Theorem in its entirety.

1.1 Germain's background and mathematical development

Sophie Germain[3] was born on April 1, 1776 and lived with her parents and sisters in the center of Paris throughout the upheavals of the French Revolution. Even if kept largely indoors, she must as a teenager have heard, and perhaps seen, some of its most dramatic and violent events. Moreover, her father, Ambroise-François Germain, a silk merchant, was an elected member of the third estate to the Constituent Assembly convened in 1789 [3, p. 9ff]. He thus brought home daily intimate knowledge of events in the streets, the courts, etc.; how this was actually shared, feared, and coped with by Sophie Germain and her family we do not know.

Much of what we know of Germain's life comes from the biographical

---

[3]Much of our description here of Germain's background appears also in [42].

obituary [35] published by her friend and fellow mathematician Guglielmo Libri, shortly after her death in 1831. He wrote that at age thirteen, Sophie Germain, partly as sustained diversion from her fears of the Revolution beginning outside her door, studied first Montucla's *Histoire des mathématiques*, where she read of the death of Archimedes on the sword of a Roman soldier during the fall of Syracuse, because he could not be distracted from his mathematical meditations. And so it seems that Sophie herself followed Archimedes, becoming utterly absorbed in learning mathematics, studying without any teacher from a then common mathematical work by Étienne Bezout that she found in her father's library.

Her family at first endeavored to thwart her in a taste so unusual and socially unacceptable for her age and sex. According to Libri, Germain rose at night to work from the glimmer of a lamp, wrapped in covers, in cold that often froze the ink in its well, even after her family, in order to force her back to bed, had removed the fire, clothes, and candles from her room; it is thus that she gave evidence of a passion that they thereafter had the wisdom not to oppose further. Libri writes that one often heard of the happiness with which Germain rejoiced when, after long effort, she could persuade herself that she understood the language of analysis in Bezout. Libri continues that after Bezout, Germain studied Cousin's differential calculus, and was absorbed in it during the Reign of Terror in 1793–1794. It is from roughly 1794 onwards that we have some records of Germain interacting with the public world. It was then, Libri explains, that Germain did something so rashly remarkable that it would actually lack believability if it were mere fiction.

Germain, then eighteen years old, first somehow obtained the lesson books of various professors at the newly founded École Polytechnique, and was particularly focused on those of Joseph-Louis Lagrange on analysis. The École, a direct outgrowth of the French Revolution, did not admit women, so Germain had no access to this splendid new institution and its faculty. However, the École did have the novel feature, heralding a modern university, that its professors were both teachers and active researchers. Indeed its professors included some of the best scientists and mathematicians in the world. Libri writes that professors had the custom, at the end of their lecture courses, of inviting their students to present them with written observations. Sophie Germain, assuming the name of an actual student at the École Polytechnique, one Antoine-August LeBlanc, submitted her observations to Lagrange, who praised them, and learning the true name of the imposter, actually went to her to attest his astonishment in the most flattering terms.

Perhaps the most astounding aspect is that Germain appears to have entirely self-educated herself to at least the undergraduate level, capable of submitting written student work to Lagrange, one of the foremost researchers in the world, that was sufficiently notable to make him seek out the author. Unlike other female mathematicians before her, like Hypatia, Maria Agnesi, and Émilie du Châtelet, who had either professional mentors or formal education to this level, Sophie Germain appears to have climbed to university level unaided and entirely on her own initiative.

Libri continues that Germain's appearance thus on the Parisian mathematical scene drew other scholars into conversation with her, and that she became a passionate student of number theory with the appearance of Adrien-Marie Legendre's (Figure 2) *Théorie des Nombres* in 1798. Both Lagrange and Legendre became important personal mentors to Germain, even though she could never attend formal courses of study. After Carl Friedrich Gauss's *Disquisitiones Arithmeticae* appeared in 1801, Germain took the additional audacious step, in 1804, of writing to him, again under the male pseudonym of LeBlanc (who in the meantime had died), enclosing some research of her own on number theory, and particularly on Fermat's Last Theorem. Gauss entered into serious mathematical correspondence with "Monsieur LeBlanc". In 1807 the true identity of LeBlanc was revealed to Gauss when Germain intervened with a French general, a family friend, to ensure Gauss's personal safety in Braunschweig during Napoleon's Jena campaign [3, ch. 2, 3]. Gauss's response to this surprise metamorphosis of his correspondent was extraordinarily complimentary and encouraging to Germain as a mathematician, and quite in contrast to the attitude of many 19th century scientists and mathematicians about women's abilities:

> But how can I describe my astonishment and admiration on seeing my esteemed correspondent Monsieur LeBlanc metamorphosed into this celebrated person, yielding a copy so brilliant it is hard to believe? The taste for the abstract sciences in general and, above all, for the mysteries of numbers, is very rare: this is not surprising, since the charms of this sublime science in all their beauty reveal themselves only to those who have the courage to fathom them. But when a woman, because of her sex, our customs and prejudices, encounters infinitely more obstacles than men, in familiarizing herself with their knotty problems, yet overcomes these fetters and penetrates that which is most hidden, she doubtless has the most noble courage, extraordinary talent, and superior genius. Nothing could prove to me in a

Figure 2: Adrien-Marie Legendre

more flattering and less equivocal way that the attractions of that science, which have added so much joy to my life, are not chimerical, than the favor with which you have honored it.

The scientific notes with which your letters are so richly filled have given me a thousand pleasures. I have studied them with attention and I admire the ease with which you penetrate all branches of arithmetic, and the wisdom with which you generalize and perfect. [3, p. 25]

The subsequent arcs of Sophie Germain's two main mathematical research trajectories, her interactions with other researchers, and with the professional institutions that forced her, as a woman, to remain at or beyond their periphery, are complex. Germain's development of a mathematical theory explaining the vibration of elastic membranes is told by Bucciarelli and Dworsky in their mathematical biography [3]. In brief, the German physicist Ernst Chladni created a sensation in Paris in 1808 with his demonstrations of the intricate vibrational patterns of thin plates, and at the instigation of Napoleon, the Academy of Sciences set a special prize competition to find a mathematical explanation. Germain pursued a theory of vibrations of elastic membranes, and based on her partially correct submissions, the

Academy twice extended the competition, finally awarding her the prize in 1816, while still criticizing her solution as incomplete, and did not publish her work [3, ch. 7]. The whole experience was definitely bittersweet for Germain.

The Academy then immediately established a new prize, for a proof of Fermat's Last Theorem. While Sophie Germain never submitted a solution to this new Academy prize competition, and she never published on Fermat's Last Theorem, it has long been known that she worked on it, from the credit given her in Legendre's own 1823 memoir published on the topic [3, p. 87] [31, p. 189] [34]. Our aim in this paper is to analyze the surprises revealed by Germain's manuscripts and letters, containing work on Fermat's Last Theorem going far beyond what Legendre implies.

We will find that the results Legendre credits to Germain were merely a small piece of a much larger body of work. Germain pursued nothing less than an ambitious full-fledged plan of attack to prove Fermat's Last Theorem in its entirety, with extensive theoretical techniques, side results, and supporting algorithms. What Legendre credited to her, known today as Sophie Germain's Theorem, was simply a small part of her big program, a piece that could be encapsulated and applied separately as an independent theorem, as was put in print by Legendre.

1.2 Germain's number theory in the literature

Sophie Germain's principal work on the Fermat problem has long been understood to be entirely described by a single footnote in Legendre's 1823 memoir [14, p. 734] [19, ch. 3] [34, §22] [46, p. 110]. The memoir ends with Legendre's own proof for exponent 5, only the second odd exponent for which it was proven. What interests us here, though, is the first part of his treatise, since Legendre presents a general analysis of the Fermat equation whose main theoretical highlight is a theorem encompassing all odd prime exponents, today named after Germain:

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

Sophie Germain's Theorem can be applied for many prime exponents, by producing a valid auxiliary prime, 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 [1, 21], have been proven by building on the very theorem that Germain introduced.

Before proceeding further, we briefly give the minimum mathematical background needed to understand fully the statement of the theorem, and then an illustration of its application. The reader familiar with modular arithmetic may skip the next two paragraphs.

Two whole numbers a and b are called "congruent" (or "equivalent") "modulo θ" (where θ is a natural number called the modulus) if their difference $a-b$ is a multiple of θ; this is easily seen to happen precisely if they have the same remainder ("residue") upon division by θ. (Of course the residues are numbers between 0 and $\theta - 1$, inclusive.) We write $a \equiv b \pmod{\theta}$ and say "a is congruent to b modulo θ" (or for short, just "a is b modulo θ").[4] Congruence satisfies many of the same simple properties that equality of numbers does, especially in the realms of addition, subtraction, and multiplication, making it both useful and easy to work with. The reader will need to become familiar with these properties, and we will not spell them out here. The resulting realm of calculation is called "modular arithmetic", and its interesting features depend very strongly on the modulus θ.

In the statement of the theorem, when one considers whether two numbers are "consecutive modulo θ", one means therefore not that their difference is precisely 1, but rather that it is congruent to 1 modulo θ; notice that one can determine this by looking at the residues of the two numbers and seeing if the residues are consecutive. (Technically, one also needs to recognize as consecutive modulo θ two numbers whose residues are 0 and $\theta - 1$, since although the residues are not consecutive as numbers, the original numbers will have a difference congruent to $0 - (\theta - 1) = 1 - \theta$, and therefore to $1 \pmod{\theta}$. In other words, the residues 0 and $\theta - 1$ should be thought of as consecutive in how they represent numbers via congruence. However, since we are interested only in numbers with nonzero residues, this complication will not arise for us.)

We are ready for an example. Let us choose $p = 3$ and $\theta = 13$, both prime, and test the two hypotheses of Sophie Germain's Theorem by brute force calculation. We need to find all the nonzero residues of 3rd powers (cubic residues) modulo 13. A basic feature of modular arithmetic tells us

---

[4]The notation and language of congruences was introduced by Gauss in his *Disquisitiones Arithmeticae* in 1801, and Sophie Germain was one of the very first to wholeheartedly and profitably adopt it in her research.

Residue	1	2	3	4	5	6	7	8	9	10	11	12
Cube	1	8	27	64	125	216	343	512	729	1000	1331	1728
Cubic residue	1	8	1	12	8	8	5	5	1	12	5	12

Table 1: Cubic residues modulo 13

that we need only consider the cubes of the possible residues modulo 13, i.e., from 0 to 12, since all other numbers will simply provide cyclic repetition of what these produce. And since we only want nonzero results modulo θ, we may omit 0. Brute force calculation produces Table 1.

For instance, the residue of $8^3 = 512$ modulo 13 can be obtained by dividing 512 by 13, with a remainder of 5. However, there are much quicker ways to obtain this, since in a congruence calculation, any number (except exponents) may be replaced with anything congruent to it. So for instance we can easily calculate that $8^3 = 64 \cdot 8 \equiv (-1) \cdot (-5) = 5 \pmod{13}$.

Now we ask whether the two hypotheses of Sophie Germain's Theorem are satisfied? Indeed, no pair of the nonzero cubic residues 1, 5, 8, 12 modulo 13 are consecutive, and $p = 3$ is not itself among the residues. So Sophie Germain's Theorem proves that any solution to the Fermat equation $z^3 = x^3 + y^3$ would have to have one of x, y, or z divisible by $p^2 = 9$.

Returning to Legendre's treatise, after the theorem he 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 the Fermat equation for certain exponents would have to be extremely large.

For almost two centuries, it has been assumed that this theorem and its application to exponents less than 100, the basis of Germain's reputation, constitute her entire contribution to Fermat's Last Theorem. However, we will find that this presumption is dramatically off the mark as we study Germain's letters and manuscripts. 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 its enlarged scope and extent. Figures 8 and 9 in Section 7 show all the interconnected pieces of her work, and the place of Sophie Germain's Theorem in it. The ambitiousness and importance of Germain's work will prompt a major reevaluation, and recommend a substantial elevation of her reputation.

Before considering Germain's own writing, we note that the historical record based solely on Legendre's footnote has itself been unjustly portrayed. Even the limited results that Legendre clearly attributed to Germain have been 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 [51]. We will not list all these failings here. Fortunately a few books have correctly stated Legendre's attribution to Germain [14, p. 734] [19, ch. 3] [46, p. 110]. 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 [46] gives a good overall history of related developments, including windows into the intervening literature.

1.3 Manuscript sources, recent research, and scope

Bucciarelli and Dworsky's mathematical biography of Germain's work on elasticity theory [3] utilized numerous Germain manuscripts from the archives of the Bibliothèque Nationale in Paris. Many other Germain manuscripts are also held in the Biblioteca Moreniana in Firenze (Florence) [7, pp. 229–235, 239–241] [8].[5] While Bucciarelli and Dworsky focused primarily on her

---

[5]The story of how Germain's manuscripts ended up in the two archives is an extraordinary one, a consequence of the amazing career of Guglielmo (Guillaume) Libri, mathematician, historian, bibliophile, thief, and friend of Sophie Germain [7, 48].

Exactly how Libri originally obtained Germain's manuscripts remains uncertain. We note, however, that Germain was not affiliated with any institution that might naturally have taken them, while Libri was a good friend of hers. After 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.

work on elasticity theory, many of the manuscripts in these archives are on number theory. Their book also indicates there are unpublished letters from Germain to Gauss, held in Göttingen; in particular, there is a letter written in 1819 almost entirely about Fermat's Last Theorem.

It appears that Germain's number theory manuscripts have received little attention during the nearly two centuries since she wrote them. We began working with them in 1994, and published a translation and analysis of excerpts from one (Manuscript B below) in our 1999 book [31, p. 190f]. We demonstrated there that the content and proof of Sophie Germain's Theorem, as attributed to her by Legendre, is implicit within the much broader aims of that manuscript, thus substantiating in Germain's own writings Legendre's attribution. Since then we have analyzed the much larger corpus of her number theory manuscripts, and we present here our overall evaluation of her work on Fermat's Last Theorem, which forms a coherent theory stretching over several manuscripts and letters.

Quite recently, and independently from us, Andrea Del Centina [12] has also transcribed and analyzed some of Germain's manuscripts, in particular one at the Biblioteca Moreniana and its more polished copy at the Bibliothèque Nationale (Manuscripts D and A below). While there is some overlap between Del Centina's focus and ours, there are major differences in which manuscripts we consider, and in what aspects of them we concentrate on. In fact our research and Del Centina's are rather complementary in what they analyze and present. Overall there is no disagreement between the main conclusions we and Del Centina draw; instead they supplement each other. After we list our manuscript sources below, we will compare and contrast Del Centina's specific selection of manuscripts and emphasis with ours, and throughout the paper we will annotate any specifically notable comparisons of analyses in footnotes.

Nonetheless, it seems he ended up with almost all her papers [7, p. 142f], and it was entirely in character for him to manage this, since he built a gargantuan private library of important books, manuscripts, and letters [7].

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 [7, 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. These latter Germain materials are among those fortunate to have survived intact despite a long and tragic string of events following Libri's death in 1869 [7, 8]. Ultimately it seems that Libri was the good fortune that saved Germain's manuscripts; otherwise they might simply have drifted into oblivion. See also [9, 10, 11] for the story of Abel manuscripts discovered in the Libri collections in the Biblioteca Moreniana.

Germain's handwritten papers on number theory in the Bibliothèque Nationale are almost all undated, relatively unorganized, and unnumbered except by the archive. And they range all the way from scratch paper to some beautifully polished finished pieces. We cannot possibly provide a definitive evaluation here of this entire treasure trove, nor of all the manuscripts in the Biblioteca Moreniana. We will focus our attention within these two sets of manuscripts on the major claims about Fermat's Last Theorem that Germain outlined in her 1819 letter to Gauss, the relationship of these claims to Sophie Germain's Theorem, and on presenting a coherent and comprehensive mathematical picture of the many facets of Germain's overall plan of attack on Fermat's Last Theorem, distilled from the various manuscripts.

We will explain some of Germain's most important mathematical devices in her approach to Fermat's Last Theorem, provide a sense for the results she successfully obtained and the ones that are problematic, compare 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.

Our assessment is based on analyzing all of the following, to which we have given short suggestive names for reference throughout the paper:

- **Manuscript A** (Bibliothèque Nationale): An undated manuscript entitled *Remarques sur l'impossibilité de satisfaire en nombres entiers a l'équation $x^p + y^p = z^p$* [25, pp. 198r–208v] (20 sheets numbered in Germain's hand, with 13 carefully labeled sections). This is a highly polished version of Manuscript D (some, but not all, of the marginal notes added to Manuscript A have been noted in the transcription of Manuscript D in [12]);

- **Errata to Manuscript A** (Bibliothèque Nationale): Two undated sheets [25, pp. 214r, 215v] titled "errata" or "erratu";

- **Manuscript B** (Bibliothèque Nationale): An undated manuscript entitled *Démonstration de l'impossibilité de satisfaire en nombres entiers à l'équation $z^{2(8n\pm3)} = y^{2(8n\pm3)} + x^{2(8n\pm3)}$* [25, pp. 92r–94v] (4 sheets);

- **Manuscript C** (Bibliothèque Nationale): A polished undated set of three pages [26, pp. 348r–349r] stating and claiming a proof of Fermat's Last Theorem for all even exponents;

14

- **Letter from Germain to Legendre** (New York Public Library): An undated 3 page letter [27][6] about Fermat's Last Theorem;

- **Manuscript D** (Biblioteca Moreniana): A less polished version of Manuscript A [28, cass. 11, ins. 266] [7, p. 234] (25 pages, the 19th blank), transcribed in [12];

- **Letter of May 12, 1819 from Germain to Gauss** (Niedersächsische Staats- und Universitätsbibliothek Göttingen): A letter of eight numbered sheets [24], mostly about her work on Fermat's Last Theorem, transcribed in [12].

Together these appear to be Germain's primary pieces of work 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. 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.

Before beginning our analysis of Germain's manuscripts, we summarize for comparison Andrea Del Centina's recent work [12]. He first analyzes an appendix[7] to an 1804 letter from Germain to Gauss (for which he provides a transcription in his own appendix). This represents her very early work on Fermat's Last Theorem, in which she claims (incorrectly) a proof for a certain family of exponents; this 1804 approach was mathematically unrelated to the coherent theory that we will see in all her much later manuscripts. Then Del Centina provides an annotated transcription of the entire 1819 letter to Gauss, which provides her own not too technical overview for Gauss of her later and more mature mathematical approach. We focus on just a few translated excerpts from this 1819 letter, to provide an overview and to introduce key aspects of her various manuscripts.

---

[6]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. These papers include, according to the collection guide to the papers, "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.

[7]Held in the Biblioteca Moreniana.

Finally Del Centina leads the reader through an analysis of the mathematics in Manuscript D (almost identical with A), which he also transcribes in its entirety in an appendix. Although Manuscript A is our largest and most polished single source, we view it within the context of all the other manuscripts and letters listed above, since our aim is to present most of Germain's web of interconnected results in one integrated mathematical framework, illustrated in Figures 8 and 9 in Section 7. Also, even in the analysis of the single Manuscript A that is discussed in both Del Centina's paper and ours, we and Del Centina very often place our emphases on different aspects, and draw somewhat different conclusions about parts of the manuscript. We will not remark specially on numerous aspects of Manuscript A that are discussed either only in his paper or only in ours; the reader should consult both. Our footnotes will largely comment on differences in the treatment of aspects discussed in both papers.[8] Del Centina does not mention Germain's Errata to Manuscript A (noted by her in its margin), nor Manuscripts B or C, or the letter from Germain to Legendre, all of which play a major role for us.

1.4 Outline for our presentation of Germain's work

In Section 2 we will examine the interaction and mutual influences between Germain and Gauss, focusing on Fermat's Last Theorem. In particular we will display Germain's summary explanation to Gauss in 1819 of her "grand plan" for proving the impossibility of the Fermat equation outright, and her description of related successes and failures. This overview will serve as introduction for reading her main manuscripts, and to the big picture of her body of work.

The four ensuing Sections 3, 4, 5, and 6 contain our detailed analysis of the essential components of Germain's work. Her mathematical aims included a number of related results on Fermat's Last Theorem, namely her grand plan, large size of solutions, p^2-divisibility of solutions (i.e., Sophie Germain's Theorem, applicable to Case 1), and special forms of the exponent. These results are quite intertwined in her manuscripts, largely because the hypotheses that require verification overlap. We have separated our exposition of these results in the four sections in a particular way, explained below, partly for clarity of the big picture, partly to facilitate direct comparison with Legendre's treatise, which had a different focus but much

---

[8]In particular, in section 4.1.4 we examine a subtle but critical mistake in Germain's proof of a major result, and her later attempts to remedy it. In his analysis of the same proof, Del Centina does not appear to be aware of this mistake or its consequences.

apparent overlap with Germain's, and partly to enable easier comparison with the later work of others. The reader may refer throughout the paper to Figures 8 and 9 in Section 7, which portray the big picture of the interconnections between Germain's claims (theorems), conditions (hypotheses), and propositions and algorithms for verifying these conditions.

Section 3 will address Germain's grand plan. We will elucidate from Manuscripts A and D the detailed methods Germain developed in her grand plan, the progress she made, and its difficulties. We will compare Germain's methods with her explanation and claims to Gauss, and with Legendre's work. The non-consecutivity condition on p-th power residues modulo an auxiliary prime θ, which we saw above in the statement of Sophie Germain's Theorem, is key also to Germain's grand plan. It 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.

Section 4 will explore large size of solutions and p^2-divisibility of solutions. In Manuscripts A and D Germain proved and applied 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, a claim we will see she mentioned to Gauss in her 1819 letter. Germain's effort here is challenging to evaluate, since her proof as given in the primary manuscript is flawed, but she later recognized this and attempted to compensate. Moreover Legendre published similar results and applications, which we will contrast with Germain's. We will discover that the theorem on p^2-divisibility of solutions that is known in the literature as Sophie Germain's Theorem is simply minor fallout from her "Large size of solutions" analysis. And we will compare the methods she uses to apply her theorem with the methods of later researchers.

Section 5 addresses a large family of prime exponents for the Fermat equation. In Manuscript B, Germain claims proof of Fermat's Last Theorem for this family of exponents, building on an essentially self-contained statement of Sophie Germain's Theorem on p^2-divisibility of solutions to deal with Case 1 for all exponents first.

Section 6 considers even exponents. Germain's Manuscript C, using a very different approach from the others, claims to prove Fermat's Last Theorem for all even exponents based on the impossibility of another Diophantine equation.

We end the paper with three final sections: a précis and connections for

Germain's various thrusts at Fermat's Last Theorem, our reevaluation, and a conclusion. The reevaluation will take into account Germain's frontal assault 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 of the paths unknowingly taken in her footsteps by later researchers. We will conclude that a substantial elevation of Germain's contribution is in order.

2   Interactions with Gauss on number theory

Number theory held a 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 had first studied Legendre's *Théorie des Nombres*, published in 1798, and then devoured Gauss's *Disquisitiones Arithmeticae* when it appeared in 1801 [35]. Gauss's work was a complete departure from everything that came before, and organized number theory as a mathematical subject [30] [40], with its own body of methods, techniques, and objects, including the theory of congruences and the roots of the cyclotomic equation.

2.1   Early correspondence

Germain's exchange of letters with Gauss, initiated under the male pseudonym LeBlanc, lasted from 1804 to 1808, and gave tremendous impetus to her work. In her first letter [2][9] she sent Gauss some initial work on Fermat's Last Theorem stemming from inspiration she had received from his *Disquisitiones.*

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 [49, 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

---

[9]Relevant excerpts can be found in Chapter 3 of [3]; see also [51].

into resuming my beloved arithmetic investigations."[10] After LeBlanc's true identity was revealed to him, he wrote again to Olbers, on March 24, 1807 [49, 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's letter to Olbers of July 21 of the same year shows that Germain had become a valued member of his circle of correspondents [49, 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[11] is [the number] 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 [22, vol. 10, pp. 70–74]. Together with these theorems he also included, again without proof, another result now known as Gauss's Lemma, from which he says one can derive special cases of the Quadratic Reciprocity Theorem, the first deep result discovered and proven about prime numbers.[12] 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." [49, pp. 360] 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 [23], where he says he has finally found "the simplest and most natural way to its proof" (see also [32, 33]).

We shall see in Germain's manuscripts that the influence of Gauss's *Disquisitiones* on her work was all-encompassing; her manuscripts and letters use Gauss's congruence notion and point of view throughout, in contrast to

---

[10]Throughout the paper, any English translations are our own, unless cited otherwise.

[11]as modulus.

[12]Gauss was the first to prove quadratic reciprocity, despite major efforts by both its discoverer Euler and by Legendre.

her Paris mentor Legendre's style of equalities "omitting multiples" of the modulus. Her work benefits from the ease of writing and thinking in terms of arithmetic modulo a prime enabled by the *Disquisitiones* [30] [40, 56]. Germain also seems to have been one of the very first to adopt and internalize in her own research the ideas of the *Disquisitiones*. But her work, largely unpublished, may have had little influence on the next generation.

2.2   Letter of 1819 about Fermat's Last Theorem

On the twelfth of May, 1819, Sophie Germain penned a letter from her Parisian home to Gauss in Göttingen [24]. Most of this lengthy letter describes her work on substantiating Fermat's Last Theorem.

The letter provides a window into the context of their interaction on number theory from a vantage point fifteen years after their initial correspondence. It will show us how she viewed her overall work on Fermat's Last Theorem at that time, placing it in the bigger picture of her mathematical research, and specifically within her interaction with and influence from Gauss. And the letter will give enough detail on her actual progress on proving Fermat's Last Theorem to prepare us for studying her manuscripts, and to allow us to begin comparison with the published historical record, namely the attribution by Legendre in 1823 of Sophie Germain's Theorem.

Germain's letter was written after an eleven year hiatus in their correspondence. Gauss had implied in his last letter to Germain in 1808 that he might not continue to correspond due to his new duties as astronomer, but the visit of a friend of Gauss's to Paris in 1819 provided Germain the encouragement to attempt to renew the exchange [3, p. 86, 137]. She had a lot to say. Germain describes first the broad scope of many years of work, to be followed by details 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

Voici ce que j'ai trouvé:

L'ordre dans lequel les résidus (puissances égales à l'exposant)
se trouvent placés dans la série des nombres naturels
détermine les diviseurs nécessaires qui appartiennent

aux nombres entre lesquels on établit non seulement l'équation
de Fermat — mais encore beaucoup d'autres équations analogues
à 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, tout 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 série des nombres naturels divisera
nécessairement l'un des nombres x y et z.

Cela est évident, car l'équation donne $z^p = x^p + y^p$ donne
la congruance $1 \equiv r^{sp} - r^{tp}$ dans laquelle r représente une
racine primitive et s et t des entiers.

Figure 3: "Voici ce que ja'i trouvé:" From Germain's letter to Gauss, 1819

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.[13]

Germain continues the letter by explaining to Gauss her major effort
to prove Fermat's Last Theorem (Figure 3), including the overall plan, a
summary of results, and claiming to have proved the astronomically large
size of any possible solutions. She introduces her work to him with the words
"Voici ce que ja'i trouvé:" ("Here is what I have found:").

> Here is what I have found: [...]
> The order in which the residues (powers equal to the ex-
> ponent[14]) 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,[15] necessarily
> divides one of the numbers x, y, and z.

---

[13] "Quoique j'ai travaillé pendant quelque tems a la 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 donnerait necessairement un resultat
et qui pourtant m'interresse . . . quand j'y pense.

"Longtems avant que notre academie ait proposé pour sujet de prix la démonstration de
l'impossibilité de l'équation de Fermat cet espece de défi—porté aux théories modernes par
un géometre — qui fut privé des resources que nous possedons aujourd'hui me tourmentait
souvent. J'entrevoyais *vaguement* une liaison entre la théorie des residus et la fameuse
équation, je crois même vous avoir parlé anciennement de cette idée car elle m'a frappé
aussitôt que j'ai connu votre livre." (Letter to Gauss, p. 2)

[14] i.e., power residues where the power is equal to the exponent in the Fermat equation.

[15] Germain is considering congruence modulo an auxiliary prime $\theta = 2Np + 1$ that has
no consecutive nonzero p-th power residues. While the specified form of θ is not necessary
to her subsequent argument, she knows that only prime moduli of the form $\theta = 2Np + 1$
can possibly have no consecutive nonzero p-th power residues, and implicitly that Gauss
will know this too. (This is easy to confirm using Fermat's "Little" Theorem; see, for
instance, [46, p. 124].) Thus she restricts without mention to considering only those of
this form.

This is clear, since 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.[16] [...]

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 its success. But all that is still not enough; it takes the infinite and not merely the very large.[17]

---

[16] Here Germain is utilizing two facts about the residues modulo the prime θ. One is that when the modulus is prime, one can actually "divide" in modular arithmetic by any number with nonzero residue. So if none of x, y, z were divisible by θ, then modular division of the Fermat equation by x^p or y^p would clearly produce two nonzero consecutive p-th power residues. She is also using the fact that for a prime modulus, there is always a number, called a primitive root for this modulus, such that any number with nonzero residue is congruent to a power of the primitive root. She uses this representation in terms of a primitive root later on in her work.

[17] "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 lequels on établit 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, tout 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 suit delà que s'il y avoit un nombre infini de tels nombres l'équation serait 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 soit possible de l'exposer ici. Je n'oserais même pas affirmer que pour chaque valeur de p il n'existe pas une limite audela delaquelle tous les nombres de la forme $2Np + 1$ auraient deux résidus $p^{\text{ièmes}}$ placés de

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 nonzero 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). And she explains to Gauss that since each such auxiliary prime will have to divide one of x, y, z, the existence of infinitely many of them will make the Fermat equation impossible. 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 gives a few details of her particular methods of attack. The next two sections will examine the details of these claims in Germain's manuscripts.

3   The grand plan

Our aim in this section is to study Germain's plan for proving Fermat's Last Theorem, as outlined to Gauss, to show its thoroughness and sophistication, and to consider its promise for success.

As we saw Germain explain to Gauss, one can prove Fermat's Last Theorem for exponent p by producing an infinite sequence of qualifying auxiliary primes. Manuscript A (Figure 4) contains, among other things, the full details of her efforts to carry this plan through, occupying more than 16 pages of very polished writing. We analyze these details in this section, ending with a comparison between Manuscripts A and D.

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 serait possible qu'en nombres dont la grandeur effraye l'imagination ; Car elle est encore assujettie a bien d'autres conditions que je n'ai pas le tems d'énumérer a cause des details necessaire pour en établir la réussite. Mais tout cela n'est encore rien, il faut l'infini et non pas le très grand." (Letter to Gauss, pp. 2–4)

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

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

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

Figure 4: Beginning of Manuscript A

3.1   Germain's plan for proving Fermat's Last Theorem

We have seen that Germain's plan for proving Fermat's Last Theorem for exponent p hinged on developing methods to validate the following qualifying condition for infinitely many auxiliary primes of the form $\theta = 2Np + 1$:

Condition N-C (Non-Consecutivity). *There do **not** exist two nonzero consecutive p^{th} power residues, modulo θ.*

Early on in Manuscript A (Figure 5), Germain claims that for each fixed N (except when N is a multiple of 3, for which she shows that Condition N-C always fails[18]), there will be only finitely many exceptional numbers p for which the auxiliary $\theta = 2Np + 1$ fails to satisfy Condition N-C (recall from footnote 15 that only primes of the form $\theta = 2Np + 1$ can possibly satisfy the N-C condition). Much of Germain's manuscript is devoted to supporting this claim; while she was not able to bring this to fruition, Germain's insight was vindicated much later when proven true by E. Wendt in 1894 [14, p. 756] [46, p. 124ff] [55].[19]

---

[18]See [46, p. 127].

[19]Germain's claim would follow 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.

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

Figure 5: From the introduction of Manuscript A

Note that a priori there is a difference in impact between analyzing Condition N-C for fixed N versus for fixed p. To prove Fermat's Last Theorem for fixed p, one needs to verify N-C for infinitely many N, whereas Germain's approach is to fix N and aim to verify N-C for all but finitely many p. Germain was acutely aware of this distinction. After we see exactly what she was able to accomplish for fixed N, we will see what she had to say about converting this knowledge into proving Fermat's Last Theorem for particular values of p.

Before delving into Germain's reasoning for general N, let us consider just the case $N = 1$, i.e., when $\theta = 2p + 1$ is also prime, today called a "Germain prime". We consider $N = 1$ partly because it is illustrative and not hard, and partly to relate it to the historical record. Germain knew well that there are always precisely $2N$ nonzero p-th power residues modulo an auxiliary prime of the form $\theta = 2Np + 1$. Thus in this case, the numbers 1 and $2p = \theta - 1 \equiv -1$ are clearly the only nonzero p-th power residues, so Condition N-C automatically holds. Of course for $N > 1$, with more p-th power residues, their distribution becomes more difficult to analyze. Regarding the historical record, we remark that the other condition of Sophie Germain's Theorem for Case 1, namely that p itself not be a p-th power modulo θ, is also obviously satisfied in this case. So Sophie Germain's Theorem automatically proves Case 1 whenever $2p + 1$ is prime. This may shed light on why, as mentioned earlier, some writers have incorrectly thought that Sophie Germain's Theorem deals only with Germain primes as auxiliaries.

3.1.1 Establishing Condition N-C for each N, including 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

aware (expressed by us in modern terms) 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 following hypothesis:

Condition 2-N-p (2 is **N**ot 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, whose verification we shall discuss in Section 3.1.3, and also the always necessary condition mentioned above (Section 3.1) that N is not a multiple of 3, 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.[20]

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.[21] 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).[22]

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 nonzero

---

[20]In 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 [24], that from any one of the six pairs, her transformations will reproduce the five others.

[21]Del Centina [12, p. 367ff] provides details of how Germain proves this.

[22]Del Centina [12, p. 369ff] provides details for $N = 7, 8$.

consecutive p-th powers, x, $x + 1$, 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 the binomial expansion of this power of $x + 1$, 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"[23] of how she says the induction will work in general.[24]

It is difficult to understand fully this part of the manuscript. Germain's claims may in fact hold, but we cannot verify them completely from what she says. Germain's mathematical explanations often omit many details, leaving much for the reader to fill in, and in this case, there is simply not enough detail to make a full judgement. Specifically, 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. It seems clear that as this part of the manuscript ends, she is presenting only a sketch of how things could go, indicated by the fact that she explicitly states that her approach to induction is via the example of $N = 10$, which is not presented in a way that is obviously generalizable. Nonetheless, her instincts here were correct, as proven by Wendt.

3.1.2 The interplay between N and p

Recall from above that proving Condition N-C for all N, each with finitely many excepted p, does not immediately solve the Fermat problem.

What is actually needed, for each fixed prime p, is that 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 verification 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

---

[23](Manuscript A, p. 13)

[24]Del Centina [12, p. 369ff] also has commentary on this.

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"[25] 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 for which values. She herself then 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.

3.1.3   Verifying Condition 2-N-p

We conclude our exposition of Germain's grand plan in Manuscript A with her subsequent analysis of Condition 2-N-p, which was required for 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.[26] 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

---

[25](Manuscript A, p. 15)

[26]The 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.

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

3.1.4   Results of the grand plan

As we have seen above, Germain had a sophisticated and highly developed plan for proving Fermat's Last Theorem for infinitely many exponents.

It relied heavily on facility with the multiplicative structure in a cyclic prime field and a set (group) of transformations of consecutive p-th powers. She carried out her program on 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, as we shall see next.

3.2   Failure of the grand plan

Did Germain ever know that her grand plan cannot succeed? To answer this question we examine the published record, Germain's correspondence with Gauss, and a letter she wrote to Legendre.

Published indication that Germain's method cannot succeed in proving Fermat's Last Theorem, although not mentioning her by name, came in work of Guglielmo (Guillaume) Libri, a rising mathematical star in the 1820s. We now describe Libri's work in this regard.

3.2.1   Libri's claims that such a plan cannot work

It is a bit hard to track and compare the content of Libri's 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 [37]. One of these is titled *Mémoire sur la théorie des nombres*, republished later word for word as three papers in Crelle's Journal [36]. 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 [39], confusingly with the same title as the 1829 memoir. This presumably earlier document[27] 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.[28] Much later, P. Pepin [43, pp. 318–319] [44] and A.-E. Pellet [41, p. 93] (see [14, p. 750, 753] [46, pp. 292–293]) confirmed all of Libri's claims, and L. E. Dickson [15, 16] gave specific bounds.

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

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

---

[27]One 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.

[28]For completeness, we mention that Libri also published a memoir on number theory in 1820, his very first publication, with the title *Memoria sopra la teoria dei numeri* [38], but it was much shorter and does not contain the same type of study or results on the number of solutions to congruence equations.

exemplified by Manuscript A.[29] In the letter 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 dejá ancienne"[30]) that she has not had the time 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.[31] We know, too, that Germain wrote notes in 1822 on Libri's 1820 memoir,[32] 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 [3, p. 117] [7, p. 140], as well as frequent correspondents. It thus seems probable that sometime between 1819 and 1825 Germain would have come to realize from Libri's work that her grand plan could not work. However, we shall now see that she determined this otherwise.

---

[29]Near the end she even expresses to Gauss how a brand new work by L. Poinsot [45] 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 $x^{2N} - 1 = 0$. Poinsot'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 mod p. Del Centina [12, p. 361] also discusses this connection.

[30](Letter to Gauss, p. 5)

[31]Del Centina [12, p. 362] suggests that a letter from Legendre to Germain in late 1819, published in [51], shows that he believed at that time that Germain's work on Fermat's Last Theorem could not succeed. However, we are not certain that this letter is really referring to her program for proving Fermat's Last Theorem.

[32]Germain's three pages of notes [28, cass. 7, ins. 56] [7, 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 Poinsot's work, discussed in footnote 29.

3.2.3 Proof to Legendre that the plan fails for $p = 3$

Beyond arguing as above that Germain very likely would have learned from Libri's work that her grand plan cannot succeed, we have actually found separate direct evidence of Germain's realization that her method of proving Fermat's Last Theorem will not be successful, 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 [27] (described in the introduction) in which Germain actually proves the opposite for $p = 3$.

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 nonzero consecutive cubic residues. This amounts to saying that for $p = 3$, no auxiliary primes of the form $\theta = 2Np+1$ 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 excludes $p = 3$ for $N = 10$. So the claim by Legendre, mentioned in Germain's letter, that there are only two valid auxiliary primes for $p = 3$, is conceivably true. Germain immediately writes a proof for him.

Since this proof is highly condensed, we will elucidate her argument here in our own words, in modern terminology, and substantially expanded. Our aim is to verify her claim, and at the same time experience the mathematical level and sophistication of Germain's thinking. Figure 6 displays the end of the letter. The reader may notice that her last paragraph of proof takes us fully twice as long to decipher and explain below.

The grand plan cannot work for $p = 3$. *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 $1, \ldots, 6a$. 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

Après avoir prouvé que pour tout autre module
que 7 et 13 on trouvera nécessairement deux
résidus cubiques dont la différence sera 2, on verra
que r et r' étant deux résidus cubiques, si on
fait $2 = x^{3f \pm 1}$, $r - r' = 2$ on aura $r + r' = x^{3g \pm 1}$
En effet si on prenoit $r + r' = x^{3g \mp 1}$ on auroit
$2 r'' = x^{3(f+g)}$ contre l'hypothèse

soit donc $\left. \begin{array}{l} r - r' = x^{3f \pm 1} \\ r + r' = x^{3g \pm 1} \end{array} \right\}$ on en tire $2 r = x^{3f \pm 1} + x^{3g \pm 1}$

c'est-à-dire qu'en divisant par 2 on est encore
ramené à la supposition de deux résidus cubiques
dont la différence soit l'unité

Il ne me reste que la place de vous
prier d'excuser mon importunité de ne
pas prendre la peine de me répondre
et d'agréer, Monsieur, les respects
de votre servante   S. Germain

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 do not have difference 2. So they do not 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 $\theta > 13$.[33] 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, $\ldots$, $6a - 10$, $6a - 7$, $6a - 4$, $6a$, 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 missing numbers each, located at the beginning and end. To see this is absurd, consider first, for $\theta \geq 6 \cdot 5 + 1 = 31$, 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. Therefore 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 be 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 $r + r' \equiv 0$, then $2 = r - r' \equiv r - (-r) = 2r$, yielding $r \equiv 1$, and hence $r = 1$, which violates

---

[33]Germain writes that the list is (presumably omitting those at the ends) $1 + 4$, $5 + 3$, $8 + 3$, $11 + 3$, $14 + 3$, $\ldots$, $6a - 17$, $6a - 4$ [sic], $6a - 11$, $6a - 8$, $6a - 5$.

$r - r' = 2$. 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.

This is quite impressive for a proof developed overnight.

These dramatic failures of Condition N-C for $p = 3$ presumably greatly sobered Germain's previous enthusiasm for pursuing her grand plan any further. 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 in her 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 [46, p. 301].

3.3 Germain's grand plan in other authors

We know of no concrete evidence that anyone else ever pursued a 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. In this section we will see how and why other authors worked on Condition N-C, and compare with Germain's methods.

3.3.1 Legendre's methods for establishing Condition N-C

Legendre did not mention Germain's full scale attack on Fermat's Last Theorem via Condition N-C in his memoir of 1823, and we will discuss this later, when we evaluate the interaction between Germain and Legendre in Section 8.3.3. However, even ignoring any plan to prove Fermat's Last Theorem outright, 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 her results.

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 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.[34] We illustrate this by quoting Legendre's explanation 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 resolve[35]; 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 $r = \pm (1, \mu)$.

---

[34]Del Centina [12, p. 370] also remarks on this.

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

> 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. ... [34, §25]

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 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.[36]

3.3.2 Dickson rediscovers permutation methods for Condition N-C

Many later mathematicians worked to extend verification of the N-C condition for larger values of N.[37] 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 [17, 18] (also discussed in [14, p. 763]) extending the range of verification for Condition

---

[36]Despite 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 memoir, whereas in Germain's manuscript, as we noted above, she explicitly calculated the failure of 2-N-p (and thus of N-C) for this same combination, but then nonetheless mistakenly listed it as valid for N-C in her table.

[37]Legendre went to $N = 8$ and Germain to $N = 10$, and actually to $N = 11$ in another very much rougher manuscript draft [25, pp. 209r–214v, 216r–218v, 220r–226r].

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" [18, p. 27]. 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 [50, pp. 112–113]), and is isomorphic to the permutations on three symbols). 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 he known of it.

3.3.3   Modern approaches using Condition N-C

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 1980s 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 [1, 21]. It is also remarkable that at least one yet 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 [20], 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 $N \leq 500$.

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

We have analyzed Sophie Germain's grand plan to prove Fermat's Last Theorem, which occupies most of Manuscript A. Manuscript D has the same title and almost identical mathematical content and wording. Why did she write two copies of the same thing? We can gain some insight into this by comparing the two manuscripts more closely.

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 other much rougher versions amongst her papers. 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 wording, 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 essentially 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.

This 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 Section 8.3.4.

4 Large size of solutions

While Germain 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

Figure 7: Beginning of the final section of Manuscript A, p. 17

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 states, proves and applies a theorem intended to accomplish this (Figure 7). She actually states the theorem twice, first near the beginning of the manuscript (Manuscript A, p. 3), where she 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:[38]

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 $(2p-1)^{th}$ power of the number p and of the pth powers of all the prime numbers of the form $[\theta =]Np + 1$, for which, at the same time, one cannot find two p^{th} power residues [mod θ] whose difference is one, and p is not a pth power residue [mod θ]."*[39]

---

[38] "heureusement on peut éviter un pareil embarras au moyen du théorème suivant:" (Manuscript A, p. 3)

[39] "Pour que l'équation $x^p + y^p = z^p$ soit satisfaite en nombres entiers, p étant un nombre

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

It is this theorem to which Germain was undoubtedly referring when, as we noted earlier, 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 force a solution number to have at least 39 decimal digits.

We will see below that, as given, the proof of Germain's Large Size theorem is insufficient, and we will discuss approaches she made 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.

4.1 Germain's proof of large size of solutions

Note first that the two hypotheses of Germain's Large Size theorem are the same N-C condition she already studied at length for her grand plan, and a second:

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

Of course this is precisely the second hypothesis of Sophie Germain's Theorem.

We now present a direct English translation of Germain's proof.

4.1.1 The Barlow-Abel equations

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.

> 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

---

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 que l'on ne peut trouver deux résidus $p^{\text{ièmes}}$ puissances dont la difference soit l'unité, p est non résidu puissance $p^{\text{ième}}$." (Manuscript A, p. 3 and p. 17)

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

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

can have no common divisors other than p.[40]

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

---

[40] "En supposant l'existence d'un seul des nombres assujettis à cette double condition, je prouverai d'abord que celui des nombres x, y et z qui dans l'équation $x^p + y^p = z^p$ sera multiple du nombre supposé, devra necessairement être en même tems multiple du nombre p^2.

"En effet lorsque x, y et z sont premiers entr'eux, les nombres

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

ne peuvent avoir d'autres diviseurs communs que le nombre p." (Manuscript A, p. 18)

p, then one would have, letting $z = lr$, $x = hn$, $y = vm$:[41]

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

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

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

Equations like these were given by Barlow around 1810, and stated apparently independently by Abel in 1823 [46, ch. III].

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. Since the product of $x + y$ and $\varphi(x, y)$ is equal to z^p, each of them must therefore be a pth power, as she writes. The other lines have parallel proofs.

4.1.2 Divisibility by p

The next part of Germain's proof will provide a weak form of Sophie Germain's Theorem, proving that one of x, y, z must be divisible 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 $l^p + h^p + v^p \equiv 0$ (mod $2Np + 1$). And since by hypothesis there cannot be, for this modulus, two pth 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 $x + y \equiv 0$ (mod $2Np + 1$), one concludes that $px^{p-1} \equiv r^p$ (mod $2Np + 1$), that is to say, because x is a pth

---

[41] "Si on voulait donc que les trois nombres x, y, et z fussent tous premiers a p on aurait, en fesant $z = lr$, $x = hn$, $y = vm$:

$$x + y = l^p \qquad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + \text{ etc } = r^p$$
$$z - y = h^p \qquad z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 + \text{ etc } = n^p$$
$$z - x = v^p \qquad z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 + \text{ etc } = m^p."$$

(Manuscript A, p. 18)

power residue, p will also be a pth power residue, contrary to hypothesis; thus the number z must be a multiple of p.[42]

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 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 pth power modulo θ. Therefore, p is also a pth 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. This is already the weak form of Sophie Germain's Theorem. But it is not clear why z, the number divisible by θ, has to be the one divisible by p; 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 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.)

4.1.3 Sophie Germain's Theorem as fallout

Next in her proof comes the stronger form of Sophie Germain's Theorem.

> Setting actually $z = lrp$, the only admissible assumption is that
> $$x + y = l^p p^{p-1}, \qquad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + \text{etc} = pr^p. \tag{1'}$$
> Because if, on the contrary, one were to assume that
> $$x + y = l^p p, \qquad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + \text{etc} = p^{p-1}r^p,$$

---

[42] "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 difference soit l'unité, il faudra que ce soit l et non par 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." (Manuscript A, p. 18)

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.[43]

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

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

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 is called Sophie Germain's Theorem.

4.1.4   A mistake in the proof

Germain continues on to prove the further divisibility she claims by θ.

---

[43] "En prenant actuellement $z = lrp$, la seule supposition admissible est

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

car si on fesait au contraire

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

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

serait 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." (Manuscript A, p. 18)

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 multiples [sic][44] 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 pth power residue contrary to the hypothesis.[45]

Here Germain makes a puzzling mistake.[46] 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:

---

[44]Germain wrote "multiples" here, but presumably meant "divisors".

[45]"La seule chose qui reste à prouver est que tous les nombres premier de la forme $2Np + 1$ qui sont assujettis aux mêmes conditions que celui de la même forme dont en a supposé l'existence sont necessairement 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 $h^p - l^p \equiv v^p$, parconséquent $v \equiv 0$, $z \equiv x$, $pz^{p-1} \equiv m^p$, c'est a dire p residu puissance $p^{\text{ième}}$ contre l'hypothèse." (Manuscript A, pp. 18–19)

[46]Del Centina [12, p. 365ff] does not seem to notice this mistake.

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.

4.1.5 Attempted 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". This is one of only four places in Manuscript A where marginal notes mar its visual perfection. None of these appears in Manuscript D, from which Manuscript A was meticulously copied. So Germain saw the error in Manuscript A, but probably later, and wrote an erratum about it. Where is the erratum?

Most remarkably, not far away in the same archive of her papers, tucked apparently randomly in between other pages, we find two sheets [25, pp. 214r, 215v] 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 $2N = 2$.[47]

Germain then 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, including marginal comments that are difficult to interpret. There is more

---

[47]In 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.

work to be done understanding her mathematical approach in this erratum, which ends inconclusively. What Germain displays, though, is her versatility, in bringing in quadratic forms and quadratic reciprocity to try to resolve the issue.

4.1.6   Verifying Condition p-N-p: a theoretical approach

We return now from Germain's erratum to discuss 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 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.

4.2 Condition p-N-p and large size in other authors

Legendre's footnote credits Germain for Sophie Germain's Theorem and for applying it to prove Case 1 for odd primes $p < 100$ [34, §22]. 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 [25, p. 151v], that gives lists of p-th power residues closely matching Legendre's table.[48] Legendre's table could thus easily have been made from hers. This, however, is not the full story, contrary to the impression received from Legendre.

4.2.1 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 his footnote crediting Germain, he is mute about Germain developing

---

[48]There 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.

techniques for verifying either condition. Rather, the clear impression his treatise leaves to 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 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 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.

4.2.2 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 almost 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 instead her intimate understanding of the multiplicative structure of prime residues from Gauss's *Disquisitiones*.

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 Legendre about the failure of N-C for $p = 3$ demonstrates 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.

4.2.3 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 erratum, Legendre recognizes that the N-p^{-1} condition would ensure the desired θ divisibility. He, like Germain, also 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. Specifi-

cally, 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.[49] However, as Germain explicitly pointed out for $\theta = 11$ in her erratum, 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 at least 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.

4.2.4   Rediscovery of Germain's 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 [3, ch. 8].

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, was essentially (re)discovered by Wendt in 1894 [55], and elaborated by Dickson [17] and Vandiver[50] [53] in the twentieth century.

---

[49]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.

[50]For comprehensive views of Vandiver's contributions, especially in relation to Case 1, see [4, 5].

5   Exponents of form $2(8n \pm 3)$

We will consider now what we call Manuscript B, entitled *Démonstration de l'impossibilité de satisfaire en nombres entiers à l'équation $z^{2(8n\pm3)} = y^{2(8n\pm3)} + x^{2(8n\pm3)}$*. By the end of the manuscript, although it is written in a less polished fashion, it is clear that Germain has apparently proven Fermat's Last Theorem for all exponents of the form $2\,(8n \pm 3)$, where $p = 8n \pm 3$ is prime.

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 $\left(x^2\right)^p + \left(y^2\right)^p = \left(z^2\right)^p$.

5.1   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

> First Theorem. For any [odd] prime number p in the equation $z^p = x^p+y^p$, one of the three numbers z, x, or y will be a multiple of p^2.[51]

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 [mod

---

[51] "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 de p^2.*" (Manuscript B, p. 92r)

θ] whose difference is one, and p is not a pth power residue [mod θ].[52]

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 $\theta = 2 \cdot 5 + 1 = 11, \quad 2 \cdot 4 \cdot 5 + 1 = 41, \quad 2 \cdot 7 \cdot 5 + 1 = 71,$ $2 \cdot 10 \cdot 5 + 1 = 101$, etc.[53]

Recall that Germain spends most of Manuscript A developing powerful techniques that support this belief in Conditions N-C and p-N-p, and that 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 First Theorem is much like the beginning of her proof of the Large Size theorem of Manuscript A, which we laid out in Section 4. Recall that the Large Size proof went awry only after the p^2 divisibility had been proven, so her proof here,[54] 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 the First Theorem 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 that 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

---

[52] "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 que l'on ne peut trouver deux residus puissances $p^{\text{ième}}$ dont la difference soit l'unité p est non residu puissance $p^{\text{ième}}$." (Manuscript B, p. 92r)

[53] "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 $\quad p = 5 \quad \theta = 2 \cdot 5 + 1 = 11, \quad 2 \cdot 4 \cdot 5 + 1 = 41, \quad 2 \cdot 7 \cdot 5 + 1 = 71, \quad 2 \cdot 10 \cdot 5 + 1 = 101$, etc." (Manuscript B, p. 92r

[54] The proof of Theorem 1 in Manuscript B is largely reproduced, in translation, in [31, p. 189ff].

imagine that the First Theorem 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 confusion linked to 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.

5.2   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 4.1. 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.[55]

As we continue with Case 2, notice that, by involving squares, the equation $\left(x^2\right)^p + \left(y^2\right)^p = \left(z^2\right)^p$ 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 becomes[56]

$$x^2 + y^2 = p^{4p-1} l^{2p}$$
$$z^2 - y^2 = h^{2p}$$
$$z^2 - x^2 = v^{2p}.$$

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

---

[55]Theorem 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.

[56]We 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.

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 $8n + 5$.

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 $p = 8n + 5$.

5.3 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.

5.4 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. But what is correct in Manuscript B fits extremely well with what

Legendre wrote about Germain's work. The manuscript contains precisely the correct 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.

6   Even exponents

Another direction of Germain's is provided by three pages that we call Manuscript C.[57] These pages contain highly polished statements with proof of two theorems.

The first theorem claims that the "near-Fermat" equation $2z^m = y^m + x^m$ (which amounts to seeking three m-th powers in arithmetic progression) has no nontrivial natural number solutions (i.e., other than $x = y = z$) for any even exponent $m = 2n$ with $n > 1$. 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 parametric characterization of integer solutions to the "near-Pythagorean" equation $2c^2 = b^2 + a^2$ (via $c = z^n$, $b = y^n$, $a = x^n$), similar to the well-known 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 [31, p. 178]. The characterization of near-Pythagorean triples, stemming from a long history of studying squares in arithmetic progression, would have been well known at the time [14, ch. XIV].

We will not analyze Germain's proof further here, nor pronounce judgement on its correctness, except to say that it likely flounders in its fullest generality near the beginning, as did the proof above of Theorem 3 in Manuscript B, on another unjustified assumption of relative primality of two expressions. However, this would still allow it to apply for "Case 1", i.e., when x, y, z, are relatively prime to n. Someone else may wish to pursue deciphering whether the entire proof is valid in this case or not. There is a substantial history of research on the near-Fermat equation $2z^m = y^m + x^m$.

---

[57]Yet one more manuscript, claiming to dispense with even exponents by quite elementary means, is [25, pp. 90v–90r]. It contains a mistake that Germain went back to, crossed out, and corrected. But she did not carry the corrected calculation forward, likely because it is then obvious that it will not produce the desired result, so is not worth pursuing further.

It was finally proven in 1997 by Darmon and Merel [6] to have no nontrivial solutions for $m > 2$, after partial results by Ribet [47] and Dénes [13], among others. Much earlier, Euler had proved its impossibility for $m = 4$ [13] [14, ch. XXII] [47], and then for $m = 3$ [13] [14, ch. XXI]. So Germain's claim is now known to be true, and it would be interesting to understand her method of proof well enough to see if it is viable for Case 1.

Germain's second claim is to prove Fermat's Last Theorem for all even exponents greater than two, i.e., for $z^{2n} = y^{2n} + x^{2n}$ with $n > 1$, and her proof relies directly on the previous theorem. It seems to us that this proof too relies on the unsupported relative primality of two expressions, in this case the two factors $z - y$ and $z^{n-1} + yz^{n-2} + \cdots + y^{n-2}z + y^{n-1}$ of $z^n - y^n$, under only the assumption that x, y, and z are pairwise relatively prime. 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 x, y, z, are relatively prime to n, in which case the two factors above will be relatively prime. We note that it is under an almost identical hypothesis that Terjanian proved Case 1 of Fermat's Last Theorem for even exponents in 1977 [46, VI.4] [52].

7 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 achievements and reputation. To prepare for our reevaluation and conclusion, we first summarize (see Figures 8, 9) what we have discovered mathematically in these manuscripts, and how it is related to other documentary evidence.

7.1 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,

Consider $x^p + y^p = z^p$, for p an odd prime.
Let $\theta = 2Np + 1$ be an auxiliary prime, with N not divisible by 3.

Letter to Gauss, 1819

FLT
[Ms. A]

"Large size" of solutions
[Ms. A]

FLT for exponents 2(8n ±3)
[Ms. B]

"S. Germain's Thm." (Case 1)

Case 2

∞- many θ

several θ

a single θ

Condition N-C

Condition p-N-p

Key:
Ms. = Manuscript
Condition N-C = no consecutive p-th powers mod θ
Condition p-N-p = p is not a p-th power mod θ
FLT = Fermat's Last Theorem
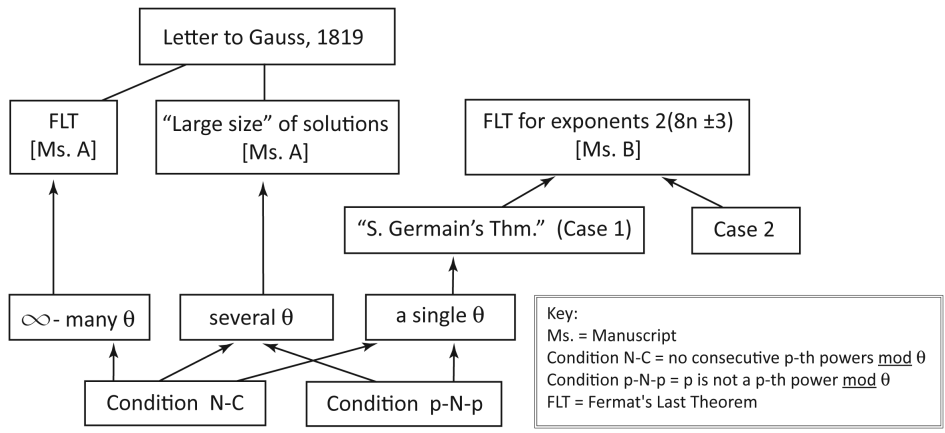
Figure 8: Conditions (hypotheses) for theorems

Condition N-C

Condition p-N-p

For each N, with finitely
many excepted p

If N = $2^a\ p^b$ for
gcd (a+1, p) =1

Condition 2-N-p
(special case of N-C)

Algorithm based on
permutations:
Verified for N=1,2,4,5,
continued by induction
for N=7,8,10,.....

Key:
Condition 2-N-p = 2 is not a p-th power mod θ
Condition N-C = no consecutive p-th powers mod θ
Condition p-N-p = p is not a p-th power mod θ
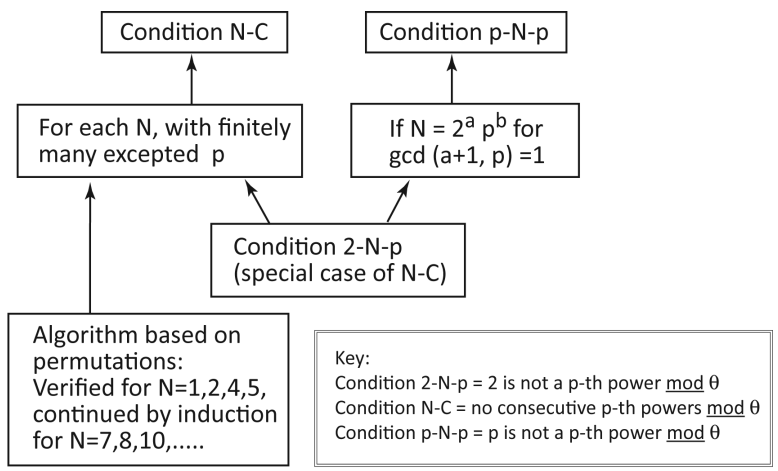
Figure 9: Algorithms and propositions for satisfying conditions

61

even had any techniques for N-C verification, has been unknown to all subsequent researchers who have labored for almost two centuries to extend N-C verification for proving Case 1. Germain likely abandoned further efforts at her grand 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 methods and terminology, Germain adopts Gauss's congruence language and points of view from his *Disquisitiones*, and thus her techniques have in several respects a more group-theoretic flavor. Germain's approach for verifying N-C was independently discovered by L. E. Dickson in the twentieth century. He, or earlier researchers, 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.

7.2 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 Case 1 by satisfying the two conditions.

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. Germain's 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.

7.3 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. 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 argument contains a flaw related to relative primality. The manuscript fits well as a primary source for what Legendre credited to Germain.

One could imagine that the appearance here of Sophie Germain's Theorem might indicate an effort to recover what she could from the flawed Large Size theorem in Manuscript A, but the details of the proof suggest otherwise, since they betray the same misunderstanding as in Manuscript A before Germain wrote its erratum.

7.4   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. 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 nontrivial positive solutions for $n > 1$. This has only very recently been proven in the literature. Her proof suffers from the same type of flaw for Case 2 as in Manuscript B, but may otherwise be correct. Her proof of Fermat's Last Theorem for even exponents, based on this "near-Fermat result," also suffers from the Case 2 flaw, but otherwise appears to be correct.

8   Reevaluation

8.1   Germain as strategist: theories and techniques

We have seen that Germain focused on big, general theorems applicable to infinitely many prime exponents in the Fermat equation, rather than simply tackling single exponents as usually done by others. She developed general theories and techniques quite multifaceted both in goal and methods. She did not focus overly on examples or ad hoc solutions. And 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 later rediscovery by others, and a recent reapproach by mathematical induction. Moreover, her approach was more systematic and theoretical than Legendre's pre-Gaussian and completely different methods.

For almost two hundred years, Germain's broad, methodical attacks on Fermat's Last Theorem have remained unread in her unpublished papers. And no one has known that all the results published by Legendre verifying conditions N-C and p-N-p, quoted and used extensively by others, are due but uncredited to Germain, by more sophisticated and theoretical methods.

These features of Sophie Germain's work demonstrate that, contrary to what has been thought by some, she 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 two much grander engagements in her papers, fallout that we can retrospectively isolate, but which she did not. It is we and Legendre, not Germain, who have created Sophie Germain's Theorem as an entity. On the other hand, Legendre in this sense also performed a great service to Germain and to future research, since he extracted from her work and published the one fully proven major theorem of an enduring and broadly applicable nature.

Germain's agenda was ambitious and bold. She tackled what we now know was one of the hardest problems in mathematics. It is no surprise that her attempts probably never actually proved Fermat's Last Theorem for even a single new exponent, although she seems to have come close at times.

8.2 Interpreting errors in the manuscripts

Mathematicians often make errors in their work, usually winnowed out through reactions to presentations, informal review by colleagues, or the publication refereeing process. We have found that several of Germain's manuscripts on Fermat's Last Theorem contain errors in her proofs. Let us examine these in light of the unusual context within which we have found them.

First, we are short-circuiting normal publication 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. We can see explicitly that she later recognized one big error, in her Large Size of Solutions proof, and wrote an erratum attempting remedy.

Second, let us consider 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 [3, p. 40ff], Germain suffered from persistent conceptual difficulties leading to repeated serious criticisms. By contrast, Germain was very successful at self-education and independent work in number theory. She was able to train herself well from the books of Legendre and Gauss, and she shows careful work based on thorough understanding of Gauss's *Disquisitiones Arithmeticae*, despite its highly technical nature. The mistakes in her number theory manuscripts do not stem from conceptual misunderstanding, but rather are

slips overlooking the necessity for relative primality in making certain deductions, even though elsewhere she shows clear awareness of this necessity. In particular, Germain's entire grand plan for proving Fermat's Last Theorem, including algorithms for verifying Conditions N-C and p-N-p, is all very sound. Even though Germain's mistakes were conceptually minor, they happen to have left 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, that should have brought errors to her attention. Here we will encounter more a puzzle than an answer.

8.3 Review by others versus isolation

8.3.1 Germain's elasticity theory: praise and neglect

There is already solid evidence [3, Ch. 5–9] that during Germain's long process of working to solve the elasticity problem in mathematical physics,[58] 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 research. Germain labored continually under marginalizing handicaps of lack of access to materials and to normal personal or institutional discourse, strictures that male mathematicians did not experience [3, Ch. 7–9]. The evidence suggests that Germain in effect worked in substantial isolation much of the time.

8.3.2 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?

---

[58]The 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.

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 actual published work by Germain on Fermat's Last Theorem. Even though much of the research 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 did not receive any formal institutional review. Nor presumably could Germain present her work to the Academy of Sciences, like her male contemporaries.

Despite having analyzed a wealth of mathematics in Germain's manuscripts, we still have little to go on when considering her interactions with others. Her manuscripts say nothing directly about outside influences, so we must infer them from mathematical content.

Germain's 1819 letter to Gauss focused on the broad scope of her work on Fermat's Last Theorem, but did not mention direct contact with others, and apparently received no response from Gauss. Gauss had earlier made clear his lack of interest in the Fermat problem, writing on March 21, 1816 to Olbers [49, p. 629]: "I am very much obliged for your news concerning the [newly established] Paris prize. But I confess that Fermat's theorem as an isolated proposition has very little interest for me, because I could easily lay down a multitude of such propositions, which one could neither prove nor dispose of." This could by itself explain why Germain did not receive a response from Gauss to her 1819 letter.

Thus the Fermat problem was in a very curious category. On the one hand, from 1816–1820 it was the subject of the French Academy's prize competition, thereby perhaps greatly attracting Germain's interest. After all, with no access to presenting her work at the Academy, her primary avenues for dissemination and feedback were either traditional journal publication or the Academy prize competition, which she had won in elasticity. On the other hand the Fermat problem was considered marginal by Gauss and others, and topics such as the investigation of higher reciprocity laws certainly involved developing important concepts with much wider impact. So Germain's choice to work mostly on Fermat's Last Theorem, while understandable, contributed to her marginalization as well.

Regarding Germain's interaction with Legendre about her work on Fermat's Last Theorem, we have two important pieces of evidence. First, while Legendre's published footnote crediting Sophie Germain's Theorem to her

is brief, we can correlate it very precisely with content found in Germain's manuscripts. Second, we have one critical piece of correspondence, Germain's letter to Legendre confirming that her grand plan will not work. Starting from these we will now draw some interesting conclusions.

8.3.3 Legendre and Germain: A perplexing record

Legendre's footnote and Germain's letter to him indicate that they had mathematically significant 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.

This phenomenon dovetails with a counterview about the effects of isolation suggested to us by Paulo Ribenboim. If one works in isolation, one is not so much influenced by others, so one has the advantage of originality, provided one has fresh, good ideas. Clearly Germain had these, since we have seen that she developed her own powerful theoretical techniques for verifying Conditions N-C and p-N-p, not derived from anyone else's.

In contrast to Manuscript A, 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 only a single speck of circumstantial evidence in Legendre's 1823 treatise suggesting that he might even be aware of the mathematics in Germain's Manuscript A, despite her manuscript being placed by her letter to Gauss at prior to 1819. But even this speck is perplexing and can be viewed in opposing ways, as follows.

Recall from footnote 49 that Legendre, in his treatment of large size of solutions, comments that for $p = 5$ his data makes him "presume" that

there are no auxiliary primes larger than 101 satisfying Condition N-C. This indicates that he was at least interested in whether there are infinitely many auxiliaries, although he does not mention why. Why would he even be interested in this issue, if it weren't for interest in the grand plan? And why would he even imagine that there might only be finitely many, unless he already had some evidence supporting that, such as Germain's letter to him proving failure of the grand plan for $p = 3$? On the other hand, if he had her letter before writing his 1823 memoir, why did he not say something stronger for $p = 5$, such as that he knew that for $p = 3$ there are only finitely many primes satisfying N-C, supporting his presumption for $p = 5$?

The only direct evidence we have that Legendre knew of Germain's grand plan is her letter to him proving that it will not work for $p = 3$. But even if Germain's letter proving failure of the grand plan for $p = 3$ occurred before Legendre's 1823 treatise, so that the known failure was his reason for not mentioning the plan 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 and large size of solutions? 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, 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 [3, p. 63]. Did this withdrawal carry over somehow to contact about Fermat's Last Theorem? Without finding more correspondence, we may never know whether Germain had much extensive or intensive communication with anyone about her work on Fermat's Last Theorem.

8.3.4 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 elasticity competition prize, 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 [3, p. 86]. 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.

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 [3, Ch. 5–9]? Or, having been particularly criticized for incompleteness during the elasticity prize competition, did she simply know she had not definitely proved Fermat's Last Theorem in full, and hence felt she had nothing sufficient to submit?

8.4   Amateur or professional?

Goldstein [29] analyzes the transformation of number theory from the domain of the amateur to that of the professional during the 17th to 19th centuries. By Germain's time this transformation had shifted number theory mostly to the professional world, and to be successful Germain needed to interact and even compete with degreed professionals at institutions. Was she herself an amateur or a professional?

Germain had many of the characteristics of a professional, attained through highly unusual, in fact audacious, personal initiatives injecting herself into a professional world that institutionally kept her, as a woman (and therefore by definition uncertified), at arm's length. Her initiatives would hardly be dreamt of by anyone even today. She attained some informal university education first through impersonation of LeBlanc, a student at the École Polytechnique, an institution that would not admit women, leading to mathematicians like Lagrange and Legendre serving as her personal mentors. She devoured much professional mathematical literature in multiple disciplines, to which however she presumably had only what access she could obtain privately. And she initiated an also impersonated correspondence with Gauss. Germain appears to have devoted her adult life almost entirely to mathematical research, having no paid employment, spouse, or children. She competed against professional mathematicians for the Academy prize on elasticity, she achieved some professional journal publications, and she

self-published her elasticity prize research when the Academy would not.

On the other hand, Germain had some of the characteristics of amateurs typical of earlier periods, such as great reliance on personal contact and letters. Most importantly, she was not employed as a professional mathematician. And after her death no institution took responsibility for her papers or their publication, one substantial reason why much of her extensive work has remained unknown. However, it seems that all this was ultimately due precisely to her being a woman, with professional positions closed to her. One could say that Germain was relegated to something of the role of an amateur by a world of professionals and institutions that largely excluded her because of her sex, a world to which she aspired and for which she would have otherwise been perfectly qualified.

9   Conclusion

The impression to date, the main thesis of [3], 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. Our study of her manuscripts and letters bolsters this perspective.

The evidence from Germain's manuscripts, and comparison of her work with that of Legendre and later researchers, displays bold, sophisticated, multifaceted, independent work on Fermat's Last Theorem, much more extensive than the single result, named Sophie Germain's Theorem, that we have had from Legendre's published crediting footnote. It corroborates the isolation within which she worked, and suggests that much of this impressive work may never have been seen by others. We see that Germain was clearly a strategist, who single-handedly 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."[59] Sophie Germain was a much more impressive number theorist than anyone has ever known.

---

[59](Letter to Gauss, p. 2)

Acknowledgements

References

[1] L.M. Adleman, D.R. Heath-Brown, The first case of Fermat's last theorem, Inventiones Mathematicae 79 (1985) 409–416.

[2] B. Boncompagni, Cinq Lettres de Sophie Germain à Carl-Frederic Gauss, B. Boncompagni, Berlin, 1880.

[3] L. Bucciarelli, N. Dworsky, Sophie Germain: An Essay in the History of the Theory of Elasticity, D. Reidel, Boston, 1980.

[4] C. Corry, Number crunching vs. number theory: computers and FLT, from Kummer to SWAC (1850-1960), and beyond, Archive for History of Exact Sciences 62 (2008) 393–455.

[5] C. Corry, Fermat Comes to America: Harry Schultz Vandiver and FLT (1914–1963), Mathematical Intelligencer 29 (2007) 30–40.

[6] H. Darmon, L. Merel, Winding quotients and some variants of Fermat's last theorem, Journal für die Reine und Angewandte Mathematik 490 (1997) 81–100.

[7] A. Del Centina, A. Fiocca, G. Adini, M.L. 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.

[8] A. Del Centina, Letters of Sophie Germain preserved in Florence, Historia Mathematica 32 (2005) 60–75.

[9] 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).

[10] A. Del Centina, Abel's surviving manuscripts including one recently found in London, Historia Mathematica 33 (2006) 224–233.

[11] A. Del Centina, Abel's manuscripts in the Libri collection: their history and their fate, in: A. Del Centina, Il Manoscritto Parigino di Abel Conservato Nella Biblioteca Moreniana di Firenze, Olschki, Florence, 2002, pp. 87–103 [Italian and English]. Also at `http://web.unife.it/progetti/geometria/storia/ManoscrittidiAbel_en.pdf`

[12] A. Del Centina, Unpublished manuscripts of Sophie Germain and a revaluation of her work on Fermat's Last Theorem, Archive for History of Exact Sciences 62 (2008) 349-392.

[13] P. Dénes, Über die Diophantische Gleichung $x^l + y^l = cz^l$, Acta Mathematica 88 (1952) 241–251.

[14] L.E. Dickson, History of the Theory of Numbers, vol. II, Carnegie Institution, Washington DC, 1920; reprinted by Chelsea, New York, 1971.

[15] L.E. Dickson, On the congruence $x^n + y^n + z^n \equiv 0 \pmod{p}$, Journal für Mathematik 135 (1909) 134–141.

[16] L.E. Dickson, Lower limit for the number of sets of solutions of $x^n + y^n + z^n \equiv 0 \pmod{p}$, Journal für Mathematik 135 (1909) 181–188.

[17] L.E. Dickson, On the last theorem of Fermat, Messenger of Mathematics 3 (1908) 15–32.

[18] L.E. Dickson, On the last theorem of Fermat (second paper), Quarterly Journal of Pure and Applied Mathematics 40 (1908) 27–45.

[19] H.M. Edwards, Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory, Springer Verlag, New York, 1977.

[20] D. Ford and V. Jha, On Wendt's determinant and Sophie Germain's theorem, Experimental Mathematics 2 (1993) 113–120.

[21] É. Fouvry, Théorème de Brun-Titchmarsh; application au théorème de Fermat, Inventiones Mathematicae 79 (1985) 383–407.

[22] C.F. Gauss, Werke, Teubner, Leipzig, 1863–1929.

[23] C.F. Gauss, Theorematis arithmetici demonstratio nova, Commentationes Societatis Regiae Scientiarum Gottingensis 16 (1808); also in Werke, Band 2, Göttingen, 1876, pp. 1–8.

[24] S. Germain, Letter dated May 12, 1819 to Carl Friedrich Gauss, Cod. Ms. Gauß Briefe A : Germain, Nr. 9, Abteilung Handschriften und seltene Drucke, Niedersächsische Staats- und Universitätsbibliothek Göttingen, Göttingen, Germany.

[25] S. Germain, Papiers de Sophie Germain, MS. FR9114, Bibliothèque Nationale de France, Paris.

[26] S. Germain, Papiers de Sophie Germain, MS. FR9115, Bibliothèque Nationale de France, Paris.

[27] S. Germain, Letter (undated) to A.M. Legendre, 3 pages plus address page, in Box 7 of the Samuel Ward papers, 1647–1912, Manuscripts and Archives Division, The New York Public Library. Astor, Lenox and Tilden Foundations.

[28] S. Germain, in the Nuovo Fondo Libri, Biblioteca Moreniana, Firenze, Italy.

[29] C. Goldstein, Le métier des nombres aux XVIIe et XIXe siècles, in: M. Serres (Ed.), Éléments d'Histoire des Sciences, Bordas, Paris, 1989.

[30] C. Goldstein, N. Schappacher, A book in search of a discipline (1801–1860), and Several disciplines and a book (1860–1901), Chapters I.1 and I.2 in: C. Goldstein, N. Schappacher, J. Schwermer (Eds.), The Shaping of Arithmetic: After C.F. Gauss's Disquisitiones Arithmeticae, Springer, Berlin, 2007, pp. 3–66, 67–103.

[31] R.C. Laubenbacher, D Pengelley, Mathematical Expeditions: Chronicles by the Explorers, Springer, New York, 1999.

[32] R.C. Laubenbacher, D. Pengelley, Gauß, Eisenstein, and the "third proof" of the Quadratic Reciprocity Theorem: Ein kleines Schauspiel, Mathematical Intelligencer 16 (1994) 67–72.

[33] R.C. Laubenbacher, D. Pengelley, Eisenstein's misunderstood geometric proof of the Quadratic Reciprocity Theorem, College Mathematics Journal 25 (1994) 29–34.

[34] A.M. Legendre, 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 A.M. Legendre, Essai sur la Théorie des Nombres, Second edn., Paris, 1808; also reprinted in Sphinx-Oedipe 4 (1909) 97–128.

[35] G. Libri, Notice sur Mlle Sophie Germain, in: A-J. Lherbette (Ed.), S. Germain , Considérations Générales sur l'État des Sciences et des Letters, aux Différentes Époques de leur Culture, Imprimerie de Lachevardière, Paris, 1833, pp. 11–16, reprinted from Journal des Débats, 18 May, 1832.

[36] G. Libri, Mémoire sur la théorie des nombres, Journal für Mathematik 9 (1832) 54–80, 169–188, 261–276.

[37] G. Libri, Mémoire sur la théorie des nombres, in: Mémoires de Mathématique et de Physique, L. Ciardetti, Florence, 1829, pp. 47–140.

[38] G. Libri, Memoria di Guglielmo Libri sopra la Teoria dei Numeri, Firenze, 1820.

[39] 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.

[40] O. Neumann, Carl Friedrich Gauss, Disquisitiones Arithmeticae (1801), in: I. Grattan-Guinness (Ed.), Landmark Writings in Western Mathematics 1640–1940, Elsevier, Amsterdam, 2005, ch. 22, pp. 303–315.

[41] A.E. Pellet, Mémoire sur la théorie algèbrique des équations, Bulletin de la Societé Mathématique de France 15 (1886–87) 61–102.

[42] D. Pengelley, Book review of Sophie's Diary (author Dora Musielak), Mathematical Intelligencer, to appear.

[43] P. Pepin, Étude sur la théorie des résidues cubiques, Journal de Mathématiques Pures et Appliquées (3) 2 (1876) 313–324.

[44] P. Pepin, Sur divers tentatives de démonstration du théorème de Fermat, Comptes Rendus de l'Académie des Sciences, Paris 91 (1880) 366–367.

[45] L. Poinsot, 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'Academie des Sciences, Paris, IV (1819–1820), 99–184.

[46] P. Ribenboim, Fermat's Last Theorem for Amateurs, Springer, New York, 1999.

[47] K. Ribet, On the equation $a^p + 2^\alpha b^p + c^p = 0$, Acta Arithmetica 79 (1997) no. 1, 7–16.

[48] P. Ruju, 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.

[49] C. Schilling (ed.), Briefwechsel zwischen Olbers und Gauss, Erste Abteilung, in Wilhelm Olbers: sein Leben und seine Werke, vol. 2, Berlin, Springer Verlag, 1900; reprinted as Carl Friedrich Gauss - Heinrich Wilhelm Matthias Olbers Briefwechsel I, in Carl Friedrich Gauss, Werke, Ergänzungsreihe IV, Briefwechsel C.F. Gauss - H.W.M. Olbers, Georg Olms Verlag, Hildesheim, New York, 1976.

[50] J. Stillwell, The Four Pillars of Geometry, Springer, New York, 2005.

[51] H$^{\text{te}}$ Stupuy (ed.), Oeuvres philosophiques de Sophie Germain, Paul Ritti, Paris, 1879. New ed. Firmin-Didot, Paris, 1896.

[52] G. Terjanian, Sur l'équation $x^{2p} + y^{2p} = z^{2p}$, Comptes Rendus de l'Académie des Sciences, Paris, Sér. A-B 285 (1977) no. 16, A973–A975.

[53] H.S. Vandiver, Note on trinomial congruences and the first case of Fermat's Last Theorem, Annals of Mathematics 27 (1926) 54–56.

[54] A. Weil, Number Theory: An Approach Through History; From Hammurapi to Legendre, Birkhäuser, Boston, 1984.

[55] 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, Journal für die Reine und Angewandte Mathematik 113 (1894) 335–347.

[56] H. Wussing, The Genesis of the Abstract Group Concept, MIT Press, Cambridge, Mass., 1984.