

---

The correspondence between Sophie Germain and Carl Friedrich Gauss

Author(s): Andrea Del Centina, Alessandra Fiocca, Ch.Fr. Gauss, Le Blanc and Sophie Germain

Source: *Archive for History of Exact Sciences*, Vol. 66, No. 6 (November 2012), pp. 585–700

Published by: Springer

Stable URL: <https://www.jstor.org/stable/23319292>

Accessed: 19-05-2020 12:06 UTC

---

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at  
<https://about.jstor.org/terms>



Springer is collaborating with JSTOR to digitize, preserve and extend access to *Archive for History of Exact Sciences*

JSTOR

## The correspondence between Sophie Germain and Carl Friedrich Gauss

Andrea Del Centina · Alessandra Fiocca

Received: 9 January 2012 / Published online: 10 August 2012  
© Springer-Verlag 2012

**Abstract** This paper publishes the correspondence between S. Germain and C.F. Gauss. The mathematical notes enclosed in her letters are published for the first time. These notes, in which she submitted some of her results, proofs and conjectures to Gauss for his evaluation, were inspired by her study of the *Disquisitiones Arithmeticae*. The interpretation of these mathematical notes not only shows how deeply she went into Gauss's treatise and mastered it long before any other mathematician, but also, more importantly, shows that she obtained interesting results in the theory of power residues that have never previously been attributed to her.

### Contents

|   |     |
|---|-----|
| 1 Introduction . . . . .  | 586 |
| 2 Sophie Germain's life and work . . . . .                                    | 587 |
| 3 The consistency of the Germain–Gauss correspondence . . . . .               | 591 |
| 4 The discovery of the correspondence . . . . .                               | 595 |
| 5 The editorial project of Boncompagni . . . . .                              | 599 |
| 6 Gauss's <i>Disquisitiones Arithmeticae</i> . . . . .                        | 602 |
| 7 The <i>Disquisitiones</i> in the first three decades of the 1800s . . . . . | 607 |
| 8 Gauss's results on cubic and biquadratic residues . . . . .                 | 609 |
| 9 The mathematical content of Germain's letters and notes . . . . .           | 614 |

---

Communicated by: Umberto Bottazzini.

A. Del Centina (✉) · A. Fiocca  
Dipartimento di Matematica, Università di Ferrara,  
via Machiavelli 45, 44100 Ferrara, Italy  
e-mail: a.delcentina@unife.it

A. Fiocca  
e-mail: a.fiocca@unife.it

|   |     |
|---|-----|
| Appendix: Transcription of the correspondence . . . . . | 636 |
| References . . . . .                                    | 696 |

## 1 Introduction

Sophie Germain is known for original research in Mathematical Physics and Number Theory. While she earned fame as a recipient of the French Academy prize for her work on elasticity in 1816, she produced her best results in Number Theory. A.-M. Legendre credited her with an important step toward proving the first case of Fermat's Last Theorem (Legendre 1827, art. 22; see also Edwards 1977, Chap. 3; Ribenboim 1999, p. 110).

It is well known that Sophie Germain initiated a correspondence with Gauss in 1804, under the pseudonym of "Le Blanc." She wrote ten letters, eight in the period 1804–1809 and the remaining two, respectively, in 1819 and in 1829. The first five were published (in facsimile) by Boncompagni (1880). Excerpts from these five and the one dated 1829 have been published in English in Bucciarelli and Dworsky (1980). The others, except for the one dated 1819 (already published in Del Centina 2008), are unedited.

In the first five letters, Germain enclosed extended mathematical notes, and submitted to Gauss's evaluation some new proofs, theorems and conjectures inspired by the study of his *Disquisitiones Arithmeticae*. These mathematical notes, which consisted of more than 22 pages (larger than A4), full of mathematical formulas, computations and statements, were believed to be lost forever (see Bucciarelli and Dworsky 1980, p. 21; Sampson 1990; Ribenboim 1999, p. 203). Luckily, it is not the case, and they have been preserved, together with Germain's letters to Gauss, at the Niedersächsische Staats- und Universitätsbibliothek in Göttingen.<sup>1</sup>

The interpretation of these mathematical notes reveals that she studied the *Disquisitiones Arithmeticae* and she mastered it in a relatively short time, long before other more experienced mathematicians could do. What is more, she obtained interesting results on the whole matter of Gauss's treatise. If she is well known for the result pertaining to Fermat's Last Theorem, which Legendre credited to her and can be dated around 1820, she is not known for her achievements on  $n$ -ary quadratic forms,  $n$ th-power residues, etc., obtained in the early years of her correspondence with Gauss. For these reasons we believe that her letters and mathematical notes deserved to be published in their entirety. We hope this paper will contribute to complete the reevaluation of Sophie Germain as a number theorist, initiated with Del Centina (2008) and Laubenbacher and Pengelley (2010).

This paper is divided into two parts.

The first, consisting of eight sections, is devoted to a presentation of Sophie Germain's life and work, as well as of her correspondence with Gauss. This includes a discussion of the mathematical content of her letters. The second part consists of the

<sup>1</sup> Cod. ms. Gauss Briefe A: Germain, n. 9. Abteilung Handschriften und Seltene Drucke.

Appendix, completely devoted to the annotated transcription of all Germain’s letters, including the mathematical notes, and Gauss’s responses. More specifically:

In Sect. 2, we give an account of Sophie Germain’s life and work, stressing the fact that she learned mathematics by herself and—although she benefitted from the advice of Lagrange and Legendre and from the correspondence with Gauss—she worked in almost complete isolation.

In Sect. 3, we present the epistolary exchange between Germain and Gauss in its chronological development, and we comment briefly on it.

In Sect. 4, we discuss the discovery of the correspondence between 1877 and 1880, and the interest that the publication of some of these letters aroused in European mathematical and historical circles.

In Sect. 5, we discuss the editorial project of a complete edition of the correspondence that Prince Baldassare Boncompagni aimed to publish, but never did.

Section 6 is devoted to a short summary of the *Disquisitiones Arithmeticae*, focusing specifically on what is needed for explaining Germain’s results and introducing Gauss’s notation which she used in her mathematical notes. We hope this may aid the reader in understanding the mathematical content of the correspondence.

In Sect. 7, we give an account of the impact the *Disquisitiones* had in Europe from the time of its publication to the time of Sophie Germain’s death in 1831.

In Sect. 8, we briefly describe the work of Gauss on cubic and biquadratic residues, especially his first memoir on this topic (Gauss 1828a), which is important in discussing Germain’s sixth and seventh letters.

Finally, in Sect. 8, Germain’s letters and mathematical notes are analyzed and commented upon, giving special attention to certain results, namely those on cubic and biquadratic residues, which have never previously been attributed to her.

## 2 Sophie Germain’s life and work

Marie-Sophie Germain was born in Paris the April 1, 1776, the middle daughter of Ambroise-François and Marie-Madeleine Gruguelu. Her father, a rich silk-merchant, was elected a deputy in the National Assembly in 1789 and 3 years later, he became a member of the Constitutional Assembly.<sup>2</sup>

In the years of the Great Revolution, she was in her teens. Forced to stay at home when the Terror began in 1793, she found diversion from her fear in reading. In her father’s library, she found the *Histoire des Mathématiques* by J.E. Montucla, and she read it with great interest. Fascinated by the story about Archimedes’s fate, she decided to devote herself to mathematics and science. She studied with great passion and indomitable will, in opposition to her parents, who found her desire foreign to her gender and social class.<sup>3</sup>

<sup>2</sup> For the genealogy and other information on her family, see Stupuy (1879, 1896).

<sup>3</sup> Much of what we know about her youth, personality and attitude come from the biographical obituary written by her friend and fellow mathematician Guglielmo Libri, shortly after her death in 1831 (Libri 1832). Other information comes from her correspondence published in Stupuy (1879, 1896), and partly translated into English in Bucciarelli and Dworsky (1980). For her correspondence with Libri see also Del Centina (2005).

Sophie began to learn mathematics by studying the *Cours des mathématiques* by Étienne Bézout, and then the *Calcul différentiel et calcul integral* by Joseph Cousin. She also learned Latin by herself to read the works of Newton and Euler.

With the establishment of the École Centrale des Travaux Publics (later École Polytechnique) in 1794, to which women were not admitted, Sophie obtained the lecture notes of various professors for her own use. Fourcroy's chemistry and Lagrange's analysis especially attracted her interest. The students were typically invited to present the professors with written observations pertaining to the course topics. She used the name of an actual student, Antoine-August Le Blanc, to submit her own observations. Joseph Louis Lagrange praised Le Blanc's essays profoundly, and wanted to meet him; he was really surprised when he discovered that Le Blanc was a young lady, and he then went to her home to demonstrate to her all his astonishment and good will.

The appearance of a young woman talented in mathematics caused curiosity among men of science. Many were eager to aid in her education, and Mademoiselle Germain did not wait long before receiving scientists of great merit. Nevertheless, not all those encounters were pleasant, comfortable and encouraging. Sometimes she felt somehow intellectually diminished by them, as was the case with the astronomer Joseph Lalande, who gallantly proposed that she read his *Astronomie des dames*. Irritated, she responded that she had already read Laplace's *Système du monde* (Bucciarelli and Dworsky 1980, pp. 12–13).

Sophie Germain became known in Parisian intellectual circles as a sort of prodigy over which to marvel, rather than as a student to be taught. What she needed was a proper education, both in basic mathematics and in judging the nature of mathematical questions, rather than the admiration of scholars. However, at that time, regular studies were available only to men. This not only prevented her having a scientific career, but also influenced her personality.

In 1798, Adrian-Marie Legendre published his *Essai sur la théorie des nombres*, and Sophie Germain began to study number theory with great fervor.

We do not know when or how Sophie learned of Gauss's *Disquisitiones Arithmeticae*, which was published in 1801, but certainly she was amazed by the originality of this work. In it she found new stimulus toward number theory. For a couple of years she studied Gauss's treatise, solving many exercises and trying to give her own proofs of some of the theorems therein. Then, eager for acknowledgment and encouragement, on November 21, 1804, she wrote her first letter to Gauss. She signed it "Mr. Le Blanc," fearing the ridicule attached to the title of "femme savant."

After having praised the *Disquisitiones Arithmeticae*, which had long been the object of her admiration and study, Sophie Germain disclosed some of her ideas and results. Gauss replied after a seven-month interlude, but in his letter, he showed appreciation for the work of the young Parisian geometer. In fact, Gauss had already written to his friend H.W. Olbers on December 7, 1804, saying (Schilling 1990, p. 237):

Neulich habe ich die Freude gehabt, einen Brief von einem jungen Geometer aus Paris Le Blanc zu erhalten, der sich mit Enthusiasmus mit der höheren Arithmetik vertraut macht, und mir Proben gegeben hat, dass er in meine Disquis. Arith. tief eingedrungen ist [Today, I received with pleasure a letter from a young

geometer of Paris, Le Blanc, who has studied the higher arithmetic with great enthusiasm, and has given me evidence of having penetrated very deeply into my *Disquisitiones Arithmeticae*].

Sophie Germain, under the name of Le Blanc, wrote three letters to Gauss, and Gauss numbered Le Blanc among his correspondents. Although Gauss's praises were sincere, as clearly demonstrated in some letters, he wrote to Olbers, and despite Germain's solicitousness, he scarcely commented on her work.

In February 1807, as a consequence of the Franco-Prussian War, she had to reveal her true identity to Gauss. This time he responded promptly and at length, and with even more praise than before.

Gauss wrote his last letter to Germain in January 1808. In it, Gauss seems to be saying that he would no longer have time to correspond with her. Germain addressed to Gauss three other letters, to which he probably never replied, and she stopped writing to him in 1809.

In 1808, after a series of spectacular experiments performed in Paris by the German physicist E.F. Chladni on the intricate vibrational patterns of thin plates, the Paris Academy of Sciences announced a contest for the best memoir—supported by experimental evidence—on the mathematical theory of vibrating elastic surfaces.

Sophie Germain set aside her beloved number theory, and began to study this problem intensely. In 1811, assisted by Legendre, she presented, as the only competitor, her first contribution to the Academy. Unfortunately, the memoir she offered, based on a generalization of Euler's theory of vibrating beams, was marred by a significant mistake. However, the contest was extended for 2 years. Helped by her mentors, Lagrange and Legendre, she submitted to the Academy an amended version of her first memoir in 1813, again as the sole competitor. This time, although the way she came to her fundamental equation was still judged completely incorrect, the memoir was awarded an "honorable mention," for the part regarding the comparison of the theory with the experimental data.

The competition was extended again until October 15, 1815. Sophie Germain's third memoir, presented again as only competitor, was different in many respects from the previous one. For instance she tried to extend her research to curved surfaces, but her work, although interesting in intent, was still fundamentally deficient. Nevertheless, the commission, consisting of Poisson, Laplace, Legendre, Poinsot, and Biot, decided to award her the prize with reservation. In their motivation, the members of the board stated that her (correct) fundamental equation was not clearly deduced from the hypothesis, but the comparison—made with the results observed by Chladni—and the new experiments carried out to test the indications of the theory, appeared to merit the prize.

In 1821, Germain published her prize-winning memoir at her own expense (Germain 1821).<sup>4</sup>

<sup>4</sup> For a detailed analysis of Sophie Germain's works in elasticity see Bucciarelli and Dworsky (1980), Dahan-Dalmédico (1987), and Truesdell (1991).

In late December 1815, the Academy of Paris established a new contest and prize, aimed at the proof of Fermat's Last Theorem (FLT), i.e., the impossibility of solving in nonzero integers the equation  $x^n + y^n = z^n$  when  $n \geq 3$ . The competition was extended in 1818, and withdrawn in 1820. Probably, only after the second call for FLT, did Sophie Germain return with force to work on this challenging question, which she had been considering since 1804—the time of her first letter to Gauss. She not only was convinced that the theory of congruences and power residues, developed by Gauss in the *Disquisitiones*, was the right tool for solving that old problem, but in 1818, the memoir by Louis Poinsot *Sur l'application de l'algèbre à la théorie des nombres*, gave her new encouragement to address the question.<sup>5</sup>

In May 1819, the visit she received from H.C. Schumacher, a friend of Gauss, gave her the occasion to address a new letter to him. In it, she put forth her ideas and her progress toward the resolution of Fermat's problem.

For a long time, her only contribution to FLT had been entirely described by the so-called Sophie Germain theorem (see Dickson 1971, II, p. 734; Edwards 1977, Chap. 3; Ribenboim 1999, p. 110). Legendre attributed this to her in a footnote of his paper (Legendre 1827).<sup>6</sup> Only very recently, through the study of some of her unpublished manuscripts, it has been recognized that her results related to FLT went far beyond the content of that simple footnote (Del Centina 2008; Laubenbacher and Pengelley 2010).

In the early 1820s, through the work of S.-D. Poisson, J. Fourier, C.-L. Navier, and A.-L. Cauchy, a new theory of elastic surfaces emerged. It was impossible for Sophie Germain to take part in its development, not only because of her lack of knowledge of mathematical analysis, but also because of lack of access to the sessions of the Academy, the difficulties she encountered in getting information about the works of others, and the arrogance with which she was treated. She had never been included in serious scientific discussions. All this put her in an isolated and uncomfortable position (Bucciarelli and Dworsky 1980, Chap. 9).

In May 1825, during one of the Thursday parties given by François Arago at the Observatory, Sophie Germain met Guglielmo Libri.<sup>7</sup> Germain and Libri had many

<sup>5</sup> From a letter of Germain to Poinsot dated July 2nd 1819, and published in Del Centina (2005, p. 63), we deduce that she received from Poinsot a manuscript copy of this memoir, already announced to the Academy in 1818 by Delambre and published one year later (Poinsot 1820).

<sup>6</sup> Legendre read this paper to the Paris Academy in 1823.

<sup>7</sup> Guglielmo Libri, count of Bagnano [1802–1869], was born in Florence. He had an excellent education and enrolled at the University of Pisa in 1816. He graduated in Mathematics in 1820, and the same year he wrote his first paper *Memoria sulla teoria dei numeri* [Memoir on Number Theory], which he sent to Legendre and Cauchy. In 1823, he became professor of Mathematical Physics in Pisa. In the winter of 1824, already known as a talented young mathematician to Legendre and Cauchy for having corresponded with them, he went to Paris to present in person his memoirs to the Academy. Libri remained in Paris until August 1825, when he returned to Florence. He returned to Paris in 1830. In 1833, Libri became a French citizen, and the same year he was named a member of the Academy. In 1843, Libri also became a professor at the Sorbonne. In 1848, accused of being involved in thefts from several French public libraries, he fled to London, where he continued his trade in books and manuscripts. He returned to Florence in December 1868. He died the following year in Fiesole, a small town in the hills surrounding Florence (Maccioni Ruju and Monstert 1995; Del Centina and Fiocca 2010).

interests in common, most importantly a real passion for Number Theory and FLT, and—although he was 26 years her junior—their friendship immediately grew. They met several times during Libri's stay in Paris. In the summer, Libri went back to Florence, and he started to correspond with her (Del Centina 2005).

In 1826, Sophie Germain presented to the Academy a new memoir on elasticity, which she considered a clearer version of her third entry. Cauchy was designated to review her paper. He encouraged her to publish it, to relieve the Academy of the embarrassment of having to deal with her work (Bucciarelli and Dworsky 1980, p. 107), and her memoir appeared in *Annales de Chimie* in 1828 (Germain 1828).

In 1829, Sophie Germain wrote her last letter to Gauss. The occasion arose from the visit she received from Mr. Bader, a pupil of Gauss's, who delivered a copy of Gauss's *Theoria residuorum biquadraticorum* (published a year earlier) to her.

The same year, Sophie Germain became afflicted with breast cancer, and was unable to do real work anymore.

In June of 1830, Libri returned to Paris, and visited her. According to him, it was during the week of fighting of the July Revolution that she wrote her last paper on elasticity (Germain 1831a). In December the same year, Libri returned to Florence. Then, in February 1831, she told him she had found the energy to write a short note on a question she had presented to Gauss in her first letter more than 25 years earlier (Germain 1831b). She wrote to him again in April and in May. From her words, it seems that only by thinking of her friends could she obtain some relief (Del Centina 2005). She died on June 17, 1831, at one o'clock in the morning.

In addition to mathematics, Sophie Germain studied natural sciences and philosophy. Her philosophical writings *Considérations générales sur l'état des sciences et des lettres aux différentes époques de leur culture* and *Pensées diverses*, were published posthumously. The first was edited by her nephew Jacques-Amant Lherbette, 2 years after her death (Germain 1833) (also in Stupuy 1879, 1896). It was highly appreciated by the philosopher Auguste Comte (see Comte 1864, II, p. 415). The second, which is a list of reflections on the history of science and mathematics, was published together with a few letters, by Hyppolite Stupuy and appears in Stupuy (1879, 1896).

### 3 The consistency of the Germain–Gauss correspondence

The known correspondence between Sophie Germain and Carl Friedrich Gauss consists of 14 letters, ten by Germain and four by Gauss.

We can be quite sure that if any letter has been lost, it is much more probably a letter by Gauss rather than by Germain, because the letters of Germain were preserved by Gauss himself and reached the Academy of Göttingen after his death. On the other hand, after Germain's death a large part of her papers fell into the hands of Libri, and the letters suffered the fate of the dispersal of his archives (Del Centina and Fiocca 2004). When, in 1848, Libri fled to London, he brought with him a large part, but not all, of his vast collection. Many papers were confiscated by the French authorities

in his apartment at the Sorbonne. Likely among them, there were writings by Sophie Germain and letters addressed to her.<sup>8</sup>

To each of the first five letters, Sophie Germain added extensive mathematical notes, in which she submitted to Gauss's judgement some new proofs, theorems and conjectures inspired by his *Disquisitiones arithmeticæ*.

The work of Boncompagni (Boncompagni 1880) has long caused us to think that there were only five letters of hers held in Göttingen. Bucciarelli and Dworsky, despite acknowledging the existence of Germain's unpublished letters (Bucciarelli and Dworsky 1980, pp. 114–115, 143), believed the mathematical notes to have been lost (Bucciarelli and Dworsky 1980, p. 21) (see also Sampson 1990; Ribenboim 1999, p. 203). However, the letters of Sophie Germain, numbered from 1 to 10, the first four by Gauss himself, together with the enclosed five mathematical notes, are held, as already stated, at the Niedersächsische Staats- und Universitätsbibliothek of Göttingen.<sup>9</sup> The first-named author was really surprised some years ago when, in answer to a request to Göttingen for copies of Germain's letters, he also got copies of the mathematical notes.

Gauss's letters are preserved in Paris at the Bibliothèque Nationale (Fonds Français n. 9118), except for the one dated April 30, 1807. Of this letter, listed as n. 40 art. 605 in the *Catalogo della insigne biblioteca appartenuta a B. Boncompagni* (Boncompagni 1895), the Library of the University of Göttingen has only a photolithographic reproduction. This copy was a gift from Prince Boncompagni. In a handwritten note posted on that reproduction, we read:

Die Manuskripten Sammlung des Prinzen Boncompagni und damit wahrscheinlich auch das Original des dritten Gaussischen Briefes an Sophie Germain gehört jetzt dem Professor Mittag-Leffler in Stockholm. Im Archiv! [The collection of manuscripts belonged to Prince Boncompagni and so, probably, also Gauss's third letter to Germain now belongs to Professor Mittag-Leffler in Stockholm. In the Archive! (added by another hand)].

This note suggests that all the letters of Boncompagni's collection are likely held at the Mittag-Leffler Institute in Stockholm, but this is not true (see Del Centina and Fiocca 2004, pp. 189, 211, 232). In any case, recent searches by Folkerts have not confirmed the presence of that letter by Gauss in Stockholm (Folkerts 2003).

The first three letters by Germain—dated, respectively, November 21, 1804, July 21, and November 16, 1805—are signed “Le Blanc.” In the first letter she asked Gauss to send his reply to the address of Sylvestre de Sacy, who would have forwarded it to her.

<sup>8</sup> Autographs by Sophie Germain are preserved at the Bibliothèque Nationale (see Bucciarelli and Dworsky 1980) and at the Biblioteca Moreniana in Florence (see Del Centina and Fiocca 2004), where drafts of letters to Gauss can be found. In 1859, manuscripts by Sophie Germain were donated to the French Academy by her sister Angelique-Ambroise madam Dutrochet and Jacques-Amant Lherbette, son of her eldest sister Marie-Madeleine (Bertrand 1859).

<sup>9</sup> Gauss used the notation “Nro 1,” “Nro 2,” etc. for Germain's first four letters and “Ad. 1,” “Ad. 2,” etc. for the mathematical notes. We presume that “Ad.” stands for the Latin “Additamentum” or for the German “Addition.” The same notation has been used by another hand for the remaining six letters and the fifth mathematical note. We have adopted the term “Addendum.”

Gauss responded to the first letter after almost 7 months, on June 16, 1805, while to the second, he replied more promptly, on August 20, 1805. Both times Gauss praised “Mr. Le Blanc” for his results and progress in the difficult field of higher arithmetic. Gauss’s reply to Sophie’s third letter, if it ever existed, has not been found.

As we have already stated, it was only with the fourth letter that Sophie Germain disclosed her true identity to Gauss. The circumstances were as follows:

In October 1806, the success of the Napoleonic Army at Jena opened the way for the invasion of a large part of Prussia, and French troops occupied Brunswick, Gauss’s hometown. Sophie, fearing for Gauss’s safety, asked General Pernety (a family friend and commander of the French artillery in the Prussian campaign, responsible for the siege of Breslau) the favor of discovering Gauss’s whereabouts and ensuring that he was not mistreated. The General ordered *Chef de Bataillon* Chantal to ride two hundred miles west to Brunswick and carry out this mission. The meeting between Chantal and Gauss is described in the letter that the former sent to his General once he had fulfilled his duty; the letter is published in Stupuy (1879). When Chantal revealed to Gauss the name of his protector “Mademoiselle Sophie Germain,” Gauss replied that he had not had the honor of knowing her. Informed of these events by General Pernety (Stupuy 1879, 1896) on February 20, 1807, Sophie wrote her fourth letter to Gauss, finally revealing her true identity.<sup>10</sup>

Gauss responded promptly with a long letter containing many mathematical suggestions and even more praise than before for his correspondent.

The epistolary exchange between the two continued with a letter from Germain dated June 27, 1807, the reply by Gauss dated January 19, 1808, and a new letter from Germain dated March 19, 1808.

The letter of January 1808 is likely the last Gauss addressed to Sophie Germain. In this letter, he seems to be saying that, due to various circumstances, he would no longer have much time for corresponding with her, although, as is clear from his words, he maintained great esteem for her talent.

In the first months (probably in the spring) of 1809, Gauss forwarded to Sophie Germain, through Legendre, a copy of his memoir *Summatio quarundam serierum*, a work that he had presented to the Academy of Göttingen the year before. In the letter dated May 22, after having thanked Gauss for this gift, she professed admiration for Gauss’s memoir *Theorematis arithmeticci demonstratio nova*,<sup>11</sup> a copy of which Gauss had sent to her on January 19, 1808:

En étudiant votre mémoire du 15 Janvier 1808, qui m’a inspiré tant d’admiration et d’étonnement par la simplicité des formules qu’il contient et par les belles conclusions que vous en avez déduites, je me suis avisée de chercher ce qu’elles

<sup>10</sup> The letter of Chantal to Pernety and that of Pernety to Germain, are held at the Bibliothèque Nationale of Paris, MS Fr. 9118, pp. 266 and 269. A copy of the first, probably requested by E. Schering (see next section), is in the Universitätsbibliothek of Göttingen with the Gauss–Germain correspondence. For an English translation of these letters, see Bucciarelli and Dworsky (1980, pp. 23–24).

<sup>11</sup> In this paper, Gauss gave a new, shorter proof of his “Fundamental Theorem,” as he called it in the *Disquisitiones*, and that is today known as “Quadratic Reciprocity Law” (see Sect. 8).

donneraient si on les appliquaient aux résidus biquarrées... [While studying your memoir of January 15, 1808, which left me in complete astonishment and admiration for the simplicity of the formulae therein and the beautiful conclusions you have deduced from them, I have tried to see what they may yield when applied to biquadratic residues...]

She then put forth her results concerning biquadratic residues. In closing her letter, she added “vous me promettez une ouvrage plus étendu sur l’astronomie” [you promised me a more extended work on astronomy]. This phrase causes one to think that Gauss included, with the complimentary copy of his paper *Summatio...*, the written promise to send her a copy of his tract on the motion of planets, *Motus corporum coelestium* .... The existence of his accompanying letter is further suggested in the next one which she wrote. On May 26, she received from the printer the awaited copy of Gauss’s tract that she had ordered long before, and, immediately, she addressed a new letter to Gauss. Explaining the reasons for having sent two letters in so short a time, she wrote

Je n’avais pas voulu differer plus longtemps de répondre à la lettre et au présent dont vous m’avez honorée et cependant j’ai cru vous témoigner d’avantage le cas que je fais de vos ouvrages [I had not wanted to delay anymore to reply to your letter and present with which you have honored me, and at the same time to show you even more how much I value your works]

She also implored him to maintain his generosity by sending her some of his memoirs which were more difficult for her to find.

Soon Sophie Germain informed Legendre about the content of Gauss’s tract, and on May 31, Legendre wrote to Gauss saying:<sup>12</sup>

Je pense, Monsieur, que Mad.lle Germain se sera acquittée auprès de vous de la commission dont elle avait bien voulu se charger, qui était de vous faire tous mes remerciements du mémoire que vous avez bien voulu m’envoyer sur la sommation de quelques séries. Vos écrits sur une matière que j’ai toujours affectionnée ne peuvent que m’intéresser beaucoup et j’ai remarqué dans celui-ci la fécondité de votre génie qui a vous fait trouver un quatrième ou cinquième démonstration de la proposition à laquelle j’ai donné le nom de loi de réciprocité entre deux nombres premiers. Depuis peu de jours M.lle Germain a reçu d’Allemagne votre Theoria motus corporum coelestium; Elle même donné communication et dans le peu que j’ai pu lire, je vois que ce ouvrage est digne de votre réputation ... J’ai vu avec plaisir que vous étiez tombé par vos méditations sur la même méthode que j’ai appelé *méthode des moindres quarrées* dans mon ouvrage sur les comètes. Je vous avues que j’attache quelques prix à cette petite trouvaille. Je ne vous dissimulerai donc pas, Monsieur, que j’ai éprouvé quelque regret de voir qu’en citant mon mémoire pag. 221, vous dites *principium nostrum quo jam inde ab anno 1795 usi sumus, etc.*

<sup>12</sup> The letter of Legendre is held at the Niedersächsische Staats- und Universitätsbibliothek in Göttingen, but only a short extract has been published in Gauss (1917, 1, p. 380).

[I imagine Sir, that Mademoiselle Germain will have delivered the message which she kindly agreed to take, which was to thank you very much for the paper which you were kind enough to send me on the summation of certain series. Your writings on a subject of which I have always been fond could not fail to interest me deeply, and I noted in these the fecundity of your genius which led you to discover a fourth or fifth demonstration of the proposition to which I have given the name of law of reciprocity between two prime numbers. Since a few days ago M.lle Germain received from Germany your *Theoria motus corporum coelestium*; she herself had passed on extracts, and from the little I have managed to read, I can see that this work is worthy of your reputation ... It was with pleasure that I saw that in the course of your meditations you had hit on the same method which I called *Méthode des moindres quarrés* in my memoir on comets ... I confess to you that I do attach some value to this little finding. I will therefore not conceal from you, Sir, that I felt some regret to see that in citing my memoir p. 221 you say *principium nostrum quo jam inde ab anno 1795 usi sumus etc.*].<sup>13</sup>

In the following years, Sophie Germain became more and more involved in her studies on elasticity and vibrating surfaces. She put aside her beloved number theory and stopped writing to Gauss.

Sophie Germain wrote again to Gauss on May 12, 1819. The occasion was Gauss's friend H.C. Schumacher's visit to her.<sup>14</sup> This letter is very important, because in it, she explains at some length her ideas and progress toward a proof of FLT. This was a question of great interest for her, but, as is well known, not for Gauss (Del Centina 2008).

The last letter Germain addressed to Gauss is dated May 28, 1829.

It is very likely that Gauss never responded to these two letters.

#### 4 The discovery of the correspondence

Libri, in his short biography of Sophie Germain (Libri 1832), was the first to make mention of an exchange of letters between Germain and Gauss. However, the existence of a further letter of Sophie Germain to Gauss emerged in 1877.

During the celebrations for the first centenary of Gauss's birthday, Ernst Schering (1833–1897), one of the editors of Gauss's works, gave an official speech to the Academy of Science of Göttingen. This was published together with some letters from Gauss's archives (Schering 1877). Among these was Sophie Germain's letter that Gauss dated February 20, 1807. According to Schering, the reason for publishing this letter was to reveal the true identity of the "Mr. Le Blanc" cited in Gauss's letter written to Olbers on September 3, 1805.

The same year, Schering informed the Academy of Sciences of Paris that the library and the archive of Gauss had been acquired by the Academy of Science of Göttingen.

<sup>13</sup> Gauss's remark led to a long controversy with Legendre on priority for the discovery of the Method of Least Squares, see Plackett (1972), where an English translation of the whole letter has been published (a translation of which we have used an excerpt).

<sup>14</sup> See the letter that Schumacher wrote to Gauss from Paris on May 10, 1819 (Peters 1860, pp. 157–159).

Schering also sent to Paris copies of some letters by Lagrange, Laplace, Delambre, and Germain addressed to Gauss. Along with this was a request that copies of letters, manuscripts, and documents concerning Gauss (owned by Parisian scientists, collectors, and institutions) might be sent to Göttingen to be included in the new volumes of Gauss's works that he was preparing. Schering's request was presented to the Parisian Academy of Science by Bertrand (1877).

In 1879, Hypolite Stupuy included in his reevaluation of Sophie Germain's philosophical works (Stupuy 1879) some letters from her correspondence. Among these were three letters by Gauss and two undated letters signed "Le Blanc." In Stupuy's work, Gauss's first letter was erroneously dated June 16, 1806, and moreover Stupuy did not mention the whereabouts of these documents. Stupuy's work was reviewed by Bertrand (1879), and by Charles Henry, who expressed severe criticisms (Henry 1879).

Still in 1879, Baldassarre Boncompagni published the photolithographic reproduction of Gauss's letter to Germain of April 30, 1807 (Boncompagni 1879).<sup>15</sup> This letter came from Libri's archives, which had been dispersed in a series of private and public sales before and after his death (in 1869). The letter was acquired the following year, together with 160 pounds of paper, by the engineer Tommaso Montanari. He, in turn, sold it to Boncompagni on December 2, 1878 (Del Centina and Fiocca 2004).

In October of the same year, Boncompagni sent two copies of his publication to Angelo Genocchi, a member of the Turin Academy of Sciences—one for personal use and one for the Academy.<sup>16</sup> Boncompagni also informed Genocchi that Gauss's letter was in his hands and he intended to write a note, with all the details of the lucky purchase, to be published in the memoirs of the *Accademia Pontificia dei Nuovi Lincei*. Boncompagni requested Genocchi's advice in order to understand the profound mathematical questions that Gauss was dealing with in the letter. However, the note that Boncompagni had planned to write never saw the light of day. Nevertheless, this was the beginning of a close epistolary exchange between Boncompagni and Genocchi, focused on the Germain–Gauss correspondence which, as we will see, was revealed in its entirety only later and bit by bit.<sup>17</sup>

In November 1879, Ernst Schering presented Boncompagni's work to the Academy of Science of Göttingen. Schering stressed the importance of that letter, not only because it was the first that Gauss had addressed to Germain after having been informed of her true identity, but mainly because it allowed him to date Gauss's studies on biquadratic residues (Schering 1879).

<sup>15</sup> Baldassarre Boncompagni (1821–1894), prince of Piombino, is well known for his research in the history of mathematics. He founded the *Bullettino di bibliografia e di storia delle Scienze matematiche e fisiche*, also known as *Bullettino* of Boncompagni.

<sup>16</sup> Angelo Genocchi (1817–1889), who is considered the most qualified Italian number theorist of the nineteenth century, was one of the first Italian mathematicians to learn the new methods of the *Disquisitione Arithmeticae*. His paper *Sur la théorie des résidus quadratiques* (Genocchi 1852), gave him an international reputation.

<sup>17</sup> Most of the letters that Boncompagni addressed to Genocchi are preserved in the "Passerini-Landi" Public Library of Piacenza, whereas those of Genocchi to Boncompagni are dispersed.

Michel Chasles, in presenting Boncompagni's publication to the French Academy of Science (Chasles 1879), remarked the historical and scientific relevance of the letter, but inverted Schering's order of importance:

Cette lettre offre un très grand intérêt, non seulement par les questions les plus élevées de l'analyse des résidus cubiques et des résidus bicarrés, et de la mention des travaux astronomiques auxquels Gauss se livrait depuis cinq ans, mais surtout au point de vue historique des relations qu'il croyait depuis six [sic] ans avec un élève de l'École Polytechnique [This letter is of great interest, not only for the highest questions concerning the analysis of cubic and biquadratic residues, and for the mention of the work in astronomy to which Gauss has devoted himself since five years previous, but above all from the historical point of view for the epistolary communications he had had for six [sic] years with a student of the École Polytechnique].

According to this note, Charles thought, without supporting evidence, that the correspondence between the two initiated the same year that the *Disquisitiones Arithmeticae* were issued.

The Belgian mathematician Paul Mansion (1844–1919) also commented on Gauss's letter published by Boncompagni (Mansion 1880a). He remarked (a) how Sophie Germain revealed her identity to Gauss, (b) that Gauss detected some errors in her theorems, (c) that, at that time, Gauss had developed enough the theory of cubic and biquadratic residues to fill up a volume as large as the *Disquisitiones*, and (d) on the statement of the theorem—today known as Gauss's lemma—which had given Gauss the means to discover a new concise proof of the Quadratic Reciprocity Law. Mansion concluded his review by observing that

L'admiration que Gauss exprime ainsi, à la fin comme au début de sa lettre, ne doit pas nous étonner. A part Sophie Germain, personne ne semblait, en effet, s'occuper des *Disquisitiones* ni leur accorder l'attention dont elles étaient dignes. Il est tout naturel que le jeune Géomètre hanovrien, encore peu connu à cette époque, éprouvât et exprimât un vif contentement d'avoir trouvé, en Sophie Germain, un lecteur conscientieux et compétent [The admiration expressed by Gauss, at the end as at the beginning of his letter, should not surprise us. Aside from Sophie Germain, nobody seemed to take an interest in the *Disquisitiones*, nor to dedicate to these the attention they deserved. It was natural that the young Hanoverian geometer, still not very well known at that time, felt and expressed a strong pleasure at having found in Sophie Germain such a conscientious and competent reader].

Summing up, at the end of 1879, only seven letters of the Germain–Gauss correspondence were known to the public: (1) the two undated drafts, by Germain; (2) three letters by Gauss dated June 16, August 20, 1805, and January 19, 1808 published by Stupuy; (3) Germain's letter dated February 20, 1807 published by Schering; and (4) Gauss's response dated April 30, 1807 published by Boncompagni. In particular, at that time, nobody knew of the existence of the mathematical notes that Sophie Germain had enclosed in her letters, except Schering.

The existence of a mathematical note enclosed in Germain's first letter, as published by Stupuy, was suggested to Genocchi by Germain's phrase, "J'ai ajouté à cet article autres considerations. La dernière est relative à la célèbre équation de Fermat" [I have added to this article some other considerations. The last is related to Fermat's celebrated equation]. Despite these words, nothing about FLT was present in the letter. Then, Genocchi asked Schering about the existence of mathematical notes by Germain among the correspondence from Gauss. At the same time, searches were commissioned by Boncompagni, in order to find the originals of the letters between Germain and Gauss published by Stupuy. Three letters by Gauss were finally rediscovered at the Bibliothèque Nationale in Paris.

On March 3, 1880, Schering informed Genocchi:<sup>18</sup>

Parmi les papiers de Gauss se trouvent dix lettres de Sophie Germain. Aux cinq premières lettres appartiennent des notes mathématiques spéciales, repoussant un assez grand nombre de feuilles; les cinq autres lettres contiennent elles mêmes des recherches étendues dans les mathématiques. J'ai l'intention de publier ces lettres et ces écrits scientifiques, en tant qu'ils sont exactes. [Among Gauss's papers there are ten letters by Sophie Germain. To the first five are attached special mathematical notes, filling up many sheets, the other five also contain extended mathematical research. I am planning to publish these letters and scientific writings, since they are exact].

One month earlier, Boncompagni, via Julius Jochens, secretary of the Royal Library in Berlin, had convinced Schering to allow a photolithographic reproduction to be made of Germain's letters which had already been edited. The work, financed by Boncompagni, was done in Berlin. It includes, actually, the first five letters, which were published both in facsimile and in printed version, but without the additional mathematical notes (Boncompagni 1880). Schering presented Boncompagni's new work to the Academy of Science of Göttingen (Schering 1880).

Thanks to this publication, it became clear that the two undated letters signed "Le Blanc," published by Stupuy, were drafts of the actual letters dated November 21, 1804 and November 16, 1805, held in Göttingen. Genocchi also corrected the misprint of the date of the first letter by Gauss (June 16, 1806 instead of June 16, 1805 in Stupuy's edition). The misprint had induced Schering to believe that Gauss's response to Germain's first letter was still to be found (Schering 1880). To thank Genocchi, he sent some excerpts from Germain's mathematical notes.

On May 30, 1880, Genocchi, while presenting Boncompagni's new editorial work to the Academy of Science of Turin, announced his own yet-to-be-published writing on the correspondence between Germain and Gauss. The note appeared the same year in the memoirs of the Academy of Turin, with the title *Il carteggio di Sofia Germain e Carlo Federico Gauss* (Germain 1880). With it, Genocchi revealed to the community of mathematicians and historians that the (known) correspondence consisted of ten letters by Germain—five with extended mathematical notes—and four by Gauss. He also informed of the exact location of the letters, and commented briefly on the

<sup>18</sup> Schering's letters to Genocchi are preserved at the "Passerini-Landi" Public Library of Piacenza.

letters published up to that time. He remarked on the importance of Gauss's letter of April 30, 1807, for the two theorems on cubic and biquadratic residues that Gauss had stated therein. According to Genocchi, especially the theorem on cubic residues was noteworthy because

quantunque già si sapesse fin dal 1805 il Gauss aveva fatto studii intorno a tali residui non era noto alcun teorema speciale da lui trovato,<sup>19</sup> e nessun cenno se ne rinvenne nelle sue carte, non vedendosene traccia nell'edizione delle sue Opere postume [even if it was known that Gauss had conducted research on such residues since 1805, no special theorem found by him was known, nor has any hint of them been found among his papers, because there is no trace in the edition of his posthumous works].

Schering did not agree with this claim, and in his letter of September 26, 1880, he reminded Genocchi of what he had already written on this subject (Gauss 1863, p. 375):

Die in den Anzeigen erwähnten Untersuchungen über cubiche Reste werden wohl nicht zur Ausarbeitung gelangt sein; aufgezeichnet finden sich davon die mit den Hülfsmitteln, welche die Abhandlung *Disquisitionum circa aequationes puras ulterior evolutio* bietet, durchgeföhrten Beweise der Reciprocitysätze für zwei Primzahlen, von denen die eine reell ist [The research on cubic residues indicated in the announcements had probably not reached a conclusion;<sup>20</sup> the proof of the theorem of reciprocity for two primes, one of which real, can be found [among the handwritten notes of Gauss], where the proof is given with the methods developed in the tract *Disquisitionum circa aequationes puras ulterior evolutio*.]<sup>21</sup>

## 5 The editorial project of Boncompagni

Boncompagni requested a copy of all the letters and notes by Germain, and on March 3, 1880, Schering replied:

Cependant ayant maintenant parcouru les papiers de Sophie Germain je me sens d'abord obligé à vous dire que selon mon opinion ce qu'ils continent d'intérêt purement mathématique est déjà publié. Les autres me semblent avoir moins d'importance pour les mathématiques pures que pour l'histoire et quelques unes des démonstrations contenant des erreurs. Pour soumettre cette circonstance à votre propre jugement j'ai fait hier une petite liste sur les lettres et les notes mathématiques ainsi que sur leur contenu scientifique; je me permets de l'ajouter ici. Vous y voyez que de la note à la lettre numéro 1 (la même que j'ai

<sup>19</sup> Genocchi is referring to what Gauss wrote in his memoir *Theorematis fundamentalis in doctrina de residuis quadratici...* (Gauss 1818, 1863, p. 50).

<sup>20</sup> *Göttingische Gelehrte Anzeigen*, 10 März 1817 (see Gauss 1863, p. 161).

<sup>21</sup> Gauss's handwritten notes concerning his research on cubic residues were published only in 1900 in the 8 volume of Gauss's works, see Gauss (1900, pp. 5–20).

mentionnée dans ma dernière lettre) la première partie, quant à ce qui concerne son contenu essentiel est déjà imprimée dans le Journal de Crelle VII, 1831. De la seconde partie contenant un essai de démontrer un cas du dernier théorème de Fermat je vous envoie une copie exacte à l'originale quoique cette [est incorrecte]<sup>22</sup> [Having now read the papers of Sophie Germain, I must say to you that, in my opinion, what they contain of pure mathematical interest is already published. The other things seem to me less important for pure mathematics than for history, moreover some proofs have mistakes. To submit these circumstances to your judgment, yesterday I made a short list of the letters, the mathematical notes, and their scientific content; which I add here. You see that what is essential in the first part of the note in letter number 1 (the same that I mentioned in my previous letter) has already been published in the Crelle's Journal VII, 1831. Regarding the second part containing an attempt to prove a special case of Fermat's last theorem, I am sending you an exact copy, even if it was wrong].<sup>23</sup>

In our opinion, Schering neither read all Germain's mathematical notes nor did he do so with great attention.

Hence, on the same day in which Schering wrote to Genocchi about his plan to publish all the letters and notes by Germain (see the previous footnote), he changed his mind. The reason for such a rapid retraction is not clear.

On July 13, Boncompagni informed Genocchi that he had finally received a copy of the five unedited letters and all the mathematical notes by Germain. In his letter, Boncompagni declared his intention of publishing the correspondence in its entirety, mathematical notes included—in the form of a little book to be entitled *Carteggio tra Sofia Germain e Gauss*—and asked Genocchi's opinion of the project.

In contrast with Schering, Genocchi was convinced that the notes were worthy of publication. He also suggested that Boncompagni publish them in printed form and not in facsimile. Boncompagni agreed, and hoped to publish the volume in the first half of 1881.

In the middle of November 1880, the proofs were ready. They consisted of 69 printed pages in all, 26 for Germain's letters, seven for those of Gauss, and 36 for the mathematical notes.<sup>24</sup> Boncompagni invited Genocchi to cooperate in the correction of the proofs and especially, being well aware of his own lack of knowledge in number theory, to help him with mathematics. The correction of the proofs lasted a couple of months, and during this time Genocchi visited Boncompagni in Rome.

In 1880, two reviews of Boncompagni (1880) appeared (Henry 1880; Mansion 1880b,c). In the second, a note signed by Eugène Catalan at the end of Mansion's article announced Boncompagni's plan for the publication of the Germain–Gauss correspondence in its entirety.

<sup>22</sup> This document ends with the words “quoique cette,” “est incorrecte” was written on another sheet which has been lost. In the letter of Schering to Genocchi dated March 3, 1880, is written “Je vous envoie maintenant une copie de l'essai de démonstration de Sophie Germain pour le cas mentionnée du dernier théorème de Fermat quoique cette démonstration est incorrecte”.

<sup>23</sup> This passage of Schering's letter to Boncompagni on Mars 3, 1880, was copied and enclosed in Boncompagni's letter to Genocchi dated July 13.

<sup>24</sup> We do not know if these proofs still exist.

One more review appeared in 1881 (Günther 1881). In this review, the author claimed that the letters already published constituted the entire correspondence between Germain and Gauss, and that the mathematical notes had been lost.

It is clear that the existence of still unpublished letters and mathematical notes by Sophie Germain was not known to everyone who wrote about the Germain–Gauss correspondence. In the Italian translation of Günther’s article, published in the *Bullettino* (Günther 1882), the editor (in a footnote signed “B.B.”), rectified Günther’s claim:

L’illustre Società Reale di Göttingen possiede dieci lettere di Sofia Germain, cinque delle quali sono qui menzionate dal sig. Günther, ed altre cinque finora inedite saranno da me in breve date in luce. Unitamente a queste cinque lettere inedite pubblicherò cinque note matematiche di Sofia Germain, di ciascuna delle quali la medesima Società delle Scienze di Göttingen possiede un esemplare autografo. Tali note sono annesse alle prime 5 delle dieci suddette lettere di Sofia Germain

[The Royal Society of Göttingen possesses ten letters by Sophie Germain, five of which are mentioned here by Mr. Günther, and the other five, still unedited, I will publish shortly. Together with these five letters I will publish five mathematical notes by Sophie Germain, the originals of which are also held by the same Society. These notes are attached to the first five letters of the above mentioned letters by Sophie Germain]

Boncompagni had himself planned to write an introduction to the *Carteggio*, but because of the duties involved in managing his *Bullettino*, and the printing of the *Regula Abaci* by Adelard of Bath that took more time than expected (for one reason or another), he was unable to find the time to complete it. From what appears in Boncompagni (1879–1880) we may deduce that he presented a note entitled *Intorno al carteggio tra Sofia Germain e Carlo Federico Gauss* to the *Pontificia Accademia dei Nuovi Lincei*. This was probably a draft version of the planned introduction that he withdrew shortly after, with the aim of perfecting it.

A few years later, Boncompagni published the paper (Boncompagni 1884)<sup>25</sup> in which he commented on and annotated at great length (as was his style), Gauss’s letter to Olbers of September 3, 1805 [this letter had already appeared in facsimile (Boncompagni 1883)]. As in the letter to Olbers, Gauss again mentioned his correspondent “Le Blanc” with great appreciation, so Boncompagni had the opportunity to comment on the first two letters by Germain to Gauss and their *addenda*. In particular, Boncompagni stressed the fact that in the second *addendum* she gave a new proof that 2 is a quadratic residue for primes of the form  $8k + 1$  and  $8k + 7$  and a nonresidue for those of the form  $8k + 3$  and  $8k + 5$ .

<sup>25</sup> Here, Boncompagni also gave detailed information about the contents of Gauss’s correspondence held by the Academy of Sciences of Göttingen. The letters addressed to Gauss by 164 authors were distributed in alphabetical order in 180 portfolios contained in 19 cardboard folders. The letters by Sophie Germain were contained in the fourth folder numbered 98, covered in dark green paper, and inside the second portfolio numbered 38. On the spine of the folder was written, in golden letters and digits, “98 Gauss Nachlass 98 Briefe Fuss–Harding,” and on the portfolio, in Schering’s handwriting, was written “38, Sophie German Leblanc 1804–1829.” The drafts of the letters written by Gauss were in alphabetical order, and distributed in portfolios contained in 19 folders numbered 95b–113b.

Genocchi, who had read with great attention and interest the letters exchanged by Germain and Gauss, wrote in 1884 two other notes on the subject (Genocchi 1884a,b, 1885; Genocchi and Realis 1884). In his papers, he credited Germain with certain results contained in her mathematical notes (see Sect. 9).

However, Boncompagni never completed his project, and a few years after the initial interest aroused by the first incomplete edition of the correspondence, the still-unpublished letters by Germain to Gauss, along with her mathematical notes, were completely forgotten, and—what is worse—believed to have been lost forever.

## 6 Gauss's *Disquisitiones Arithmeticae*

The *Disquisitiones Arithmeticae* (in the following also “D.A.” for short), were published in the summer of 1801 in Leipzig. The content of this innovative treatise of 665 pages on number theory—or better on Higher Arithmetic (as Gauss himself loved to call this branch of mathematics)—is divided into seven sections (or chapters) and 366 articles (or paragraphs).<sup>26</sup> We will adopt Gauss's notation.

The first section, which is very short, is devoted to establishing some new concepts—in large part elementary—and notation such as that for *congruence with respect to a number*, in symbols  $a \equiv b \pmod{n}$ ,  $a$  and  $b$  (are congruent or not) with respect to  $n$  if  $a - b$  is divisible (or not) by  $n$ . Gauss called  $n$  the *modulus* and  $b$  a *residue* of  $a$ , and showed the compatibility of congruences with arithmetic operations.

Section 3 contains several theorems on integers, such as the unique factorization theorem and the Chinese remainder theorem. It also includes a treatment of linear congruences and Lagrange's result that a polynomial congruence cannot have more solutions than its degree.

In Sect. 4, Gauss treats *power residues*, or the sequence  $1, a, a^2, a^3, \dots$  modulo a prime  $p$  ( $a$  is a number not divisible by  $p$ ). He discusses the *periods* of  $a$  modulo  $p$  and Fermat's Little Theorem according to which  $a^{p-1} \equiv 1 \pmod{p}$ . He also shows the existence of *primitive roots* and introduces the use of *indices* of  $1, 2, \dots, p-1$  modulo  $p$  with respect to a fixed primitive root. Let us recall that an integer  $a$  is a primitive root for the prime  $p$  if for every integer  $b$  not divisible by  $p$  we have  $b \equiv a^\alpha \pmod{p}$  for some exponent  $\alpha$  which is the index of  $b$ . In particular, if  $a$  is a primitive root for the prime  $p$ , then  $a, a^2, \dots, a^{p-1}$  are all distinct, and their minimal residues coincide (not necessarily in that order), with  $1, 2, \dots, p-1$ . Moreover he treats  $n$ th-power roots modulo  $p$  and gives proofs of Wilson's theorem, i.e.,  $1 \cdot 2 \cdots (p-1) \equiv -1 \pmod{p}$ . Finally he characterizes those integers  $n$  for which there exists a primitive root modulo  $n$ .

In Sect. 5, Gauss develops a systematic theory of *quadratic residues*. In general, if the congruence  $x^m \equiv a \pmod{p}$  has a solution, then  $a$  is called a  $m$ th-power residue modulo  $p$ , so a quadratic residue is a 2nd-power residue, i.e., a residue of a perfect square. He also proves the *Quadratic Reciprocity Law* that he states in the form:  $\pm p$  is a quadratic residue or nonresidue (the sign + or − to be taken depending on whether

<sup>26</sup> For more details on the *Disquisitiones Arithmeticae*, and in-depth historical studies concerning it, see the recent papers (Goldstein et al. 2007).

$p$  is of the form  $4n + 1$  or  $4n + 3$ ) of any prime  $p'$  which is a residue or a nonresidue of  $p$ . He uses the notation  $aRa'$  or  $aNa'$ , to mean that  $a$  is a residue or a nonresidue modulo  $a'$ , respectively. This law relates the occurrence of a prime  $p$  as a quadratic residue of a prime  $p'$  to the occurrence of  $p'$  as quadratic residue of  $p$ .

The Quadratic Reciprocity Law, at least in particular cases, was known to Euler, and was stated in the general form by Legendre, who named it the *loi de reciprocité* and introduced a new symbol to express it, namely  $\left(\frac{k}{p}\right)$  defined to be 1 or  $-1$  depending on whether the integer  $k$  is a quadratic residue or a quadratic nonresidue  $(\bmod p)$  today known as *Legendre's symbol*.<sup>27</sup> With this, the quadratic reciprocity for two odd primes is easily expressed by the formula:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{[(p-1)/2][(q-1)/2]}.$$

In the *Disquisitiones*, Gauss calls this result the “fundamental theorem.”<sup>28</sup>

The Sect. 6, which occupies more than half of the volume, is devoted mostly to the theory of binary quadratic forms (or indeterminate equations of second degree), i.e.,

$$ax^2 + 2bxy + cy^2$$

which he also denotes by  $(a \ b \ c)$ . Gauss defines the *determinant* of a binary quadratic form to be the number  $D := b^2 - ac$ , showing that  $D$  is a quadratic residue of any integer primitively represented by the form, i.e., which can be represented as  $ax^2 + 2bxy + cy^2$  with  $x, y$  being two coprime integers.

The problem of the representation of numbers by means of a quadratic form is reduced to the classification of forms of a given determinant, and the first half of Sect. 6 is devoted to this question. Gauss defines two quadratic forms to be equivalent if they can be transformed into one another by a linear transformation of the variables, namely,  $(x, y) \mapsto (\alpha x + \beta y, \gamma x + \delta y)$  where  $\alpha, \beta, \gamma$ , and  $\delta$  are integers and  $L := \alpha\delta - \beta\gamma = \pm 1$  (i.e., a unimodular transformation with integer coefficients). The equivalence is said to be *proper* or *improper* depending on whether the value of  $L$  is  $+1$  or  $-1$ . Basing his argument on a finer classification of binary forms, Gauss addresses the general problem of representing numbers by quadratic forms, and shows (art. 200) how to solve the equation  $t^2 + Du^2 = m^2$ , where  $D$  is the determinant of the given form and  $m$  is the  $\gcd(a, 2b, c)$ . In particular, in art. 201, he gives the possible values of  $m$  for a given  $D$ . For instance,  $m = 1$  is always possible if  $D$  is not a square, and  $m = 2$  is possible only if  $D$  is of the form  $4k$  or  $4k + 1$ .

In art. 215 Gauss shows that if  $f = ax^2 + 2bxy + cy^2$  has determinant 0, then  $f := m(gx + hy)^2$ , where  $g, h$  are integers and  $m = \gcd(a, c)$ , which is to say:  $f$  can be reduced to the square of a linear form.

<sup>27</sup> See Legendre (1785, 1798), in the latter of which Legendre introduced his symbol.

<sup>28</sup> It seems that as attested in his diary, Gauss had known this result since 1796. He was so proud of the discovery that he named it *theoremata aureum* [the Golden Theorem]. For the history and the genesis of this theorem, see Lemmermeyer (2000).

In art. 266, Gauss introduces ternary quadratic forms:

$$f := ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'xx'' + 2b''xx',$$

which he also denotes

$$\begin{pmatrix} a & a' & a'' \\ b & b' & b'' \end{pmatrix}.$$

He defines the *adjoint* of  $f$  to be the ternary form  $F$  represented by

$$\begin{pmatrix} A & A' & A'' \\ B & B' & B'' \end{pmatrix},$$

where  $A := b^2 - a'a'', A' := b'^2 - aa'', A'' := b'' - aa', B := ab - b'b'', B' := a'b' - bb'', B'' := a''b'' - bb'$ , and thus easily shows that the adjoint of  $F$  is the form

$$\begin{pmatrix} aD & a'D & a''D \\ bD & b'D & b''D \end{pmatrix},$$

where  $D := ab^2 + a'b'^2 + a''b''^2 - aa'a'' - 2bb'b''$  is the determinant of the form  $f$ . Gauss devotes arts. 266–285 to the study of ternary quadratic forms of  $D \neq 0$ .

Gauss excludes treating ternary quadratic forms with  $D = 0$ , postponing the problem: “We will show at another time, when we will treat more completely the theory of ternary forms, that these forms [those for which  $D = 0$ ] are only *apparently* ternary. All them are, in fact, equivalent to binary forms” (Gauss 1801, art. 267). This claim, as we will see, attracted the attention of Sophie Germain.

Then, he quickly generalizes the basic theory of binary quadratic forms to ternary ones. In particular, in art. 271, he gives conditions for a ternary quadratic form to be *positive* or *negative definite* or even *indefinite*, depending on whether it can represent only positive or only negative numbers, or both, i.e., if for any choice of  $x, x', x''$  we have  $f(x, x', x'') > 0, < 0$  or  $\geq 0$ .

In art. 278, Gauss says that a ternary quadratic form  $f(x, x', x'')$  represents the binary quadratic form  $\varphi(t, u)$  if there are integers  $m, n, m', n', m''$  and  $n''$  such that by the linear transformations  $x = mt + nu, x' = m't + n'u$ , and  $x'' = m''t + n''u$ , then we have  $f(x, x', x'') = \varphi(t, u)$ . If  $\varphi$  of determinant  $D$  is represented by  $f$ , then (see art. 280), by a direct computation or by applying the method of art. 268, it can be shown that  $D$  can be represented by the adjoint  $F(X, X'X'')$  of  $f$  by putting  $X = m'n'' - m''n'$ ,  $X' = mn'' - m''n$  and  $X'' = mn' - m'n$ . Gauss calls this representation of  $D$  the *adjoint representation* of the representation of  $\varphi$  by  $f$ .

Section 7 is devoted to computational applications such as, for instance, partial fraction decomposition, decimal expansion, and primality tests.

The final Sect. 8 is that which attracted major attention when the D.A. appeared, chiefly because it contains the solution of the longstanding question of the construction of regular polygons with a ruler and compass. Not by chance does Sophie Germain’s first letter to Gauss mainly concern this section.

Here, Gauss studies the equation:

$$X := \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1 = 0,$$

( $n$  being a prime number  $\geq 3$ ) related to the problem of the division of the circle in  $n$  equal parts.

Gauss denotes the set of all roots of  $X = 0$  by  $\Omega$ . It is clear that if  $r$  is any root of  $X = 0$ , then  $r^n = r^{2n} = \cdots = 1$  and that  $\{r, r^2, \dots, r^{n-1}\}$  is the set  $\Omega$ . In particular, for any  $e$  not divisible by  $n$ , then one has  $r^e + r^{2e} + \cdots + r^{(n-1)e} = -1$ . Let  $g$  be a primitive root modulo  $n$ , and let us denote by  $[1], [h], \dots, [h^{n-2}]$ , where  $h := g^e$ , the roots of  $X = 0$ . Let  $\lambda$  be any number not divisible by  $n$ . For any factorization  $n - 1 = ef$ , Gauss divides the set  $\Omega$  into  $e$  subsets of  $f$  roots, which he calls *periods* and denotes  $(f, \lambda), (f, \lambda g), (f, \lambda g^2), \dots, (f, \lambda g^{e-1})$ , whose union coincides with  $\Omega = (f, 1) = (f, g^0)$ . Gauss also observes that the sum of the roots of a period, say  $(f, \lambda) = \{[\lambda], [\lambda h], [\lambda h^2], \dots, [\lambda h^{f-1}]\}$ , does not depend on the choice of the primitive root  $g$ , and he calls even this sum *period*, denoting it by the same symbol  $(f, \lambda)$ .

Let the roots,  $[\lambda], [\lambda h], [\lambda h^2], \dots, [\lambda h^{f-1}]$ , be denoted by  $\lambda, \lambda', \lambda'', \dots$ . Then in art. 345 Gauss proves that

$$(f, \lambda)(f, \mu) = (f, \lambda + \mu) + (f, \lambda' + \mu) + (f, \lambda'' + \mu) + \cdots,$$

and, in particular, he shows that any such product can be reduced to the form:

$$af + b(f, 1) + b'(f, g) + \cdots + b^{(e-1)}(f, g^{e-1}).$$

Let  $p := (f, \lambda), p' := (f, \lambda g^2), \dots, p^{(e-1)} := (f, \lambda g^{e-1})$ . Thus he then proves in the following article 346 that  $(f, \mu), \mu$  not divisible by  $n$ , is always a linear combination of the periods  $p := (f, \lambda), p' := (f, \lambda g^2), p'' := (f, \lambda g^3), \dots, p^{(e-1)} := (f, \lambda g^{e-1})$  with rational coefficients. In particular, the polynomial  $X$  can be factorized into the product of  $e$  polynomials  $z, z', z'', \dots$  of degree  $f$  with integral coefficients, roots of which are precisely those found in the periods  $(f, 1), (f, g), \dots, (f, g^{e-1})$ .

In art. 348, Gauss gives a method to compute the factors of the polynomial  $X$  and shows that, if one of the periods (sums) is known, then all the others can be obtain rationally.

Then, in art. 356, he studies the distribution of the roots in  $\Omega$  into two periods  $(m, 1)$  and  $(m, g)$  where  $m = (n - 1)/2$ . The first contains the roots  $[1], [g^2], [g^4], \dots, [g^{n-3}]$  associated to the minimal residues  $R, R', R'', \dots$  and the second, the roots  $[g], [g^3], [g^5], \dots, [g^{n-2}]$  with minimal residues  $N, N', N'', \dots$ . Hence,  $(m, 1)$  coincides with  $\{[1], [R], [R'], \dots\}$  and  $(m, g)$  with  $\{[N], [N'], [N''], \dots\}$ . Clearly  $1, R, R', \dots$  are quadratic residues modulo  $p$ , while  $N, N', N'', \dots$  are not.

Article 357 is devoted to showing that for any prime  $n$ , the equation

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

is solvable, i.e., to show that polynomials  $Y, Z$  always exist satisfying that equation. This result, which in modern language means that the fields generated by the  $n$ th roots of unity contains the quadratic irrationality  $\sqrt{\pm n}$ , is among the deepest of the D.A. To prove this, Gauss used his theory of periods of the cyclotomic polynomial  $X = (x^n - 1)/(x - 1)$  and the trigonometrical sums defined in art. 356, today known as *Gauss sums*.

Suppose that

$$z = x^m - ax^{m-1} + bx^{m-2} - \dots = 0$$

is the equation having the roots of the period  $(m, 1)$ , then  $a = (m, 1)$ ,  $b$  is the sum of the products of the roots in  $(m, 1)$  two at time,  $c$  is the sum of the products of the roots in  $(m, 1)$  three at time, and so on. By the results of art. 348, if we denote by  $S_k$  the sum of the  $k$ th-powers of the roots, we have  $2b = aS_1 - S_2$ ,  $3c = bS_1 - aS_2 + S_3$ , etc., so that  $b, c$ , etc., are (see art. 345) always of the form  $\mathfrak{A} + \mathfrak{B}(m, 1) + \mathfrak{C}(m, g)$  with  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$  being integers. It follows that  $z$  can always be reduced to the form:

$$z = R + S(m, 1) + T(m, g),$$

where  $R, S$ , and  $T$  are polynomials in  $x$  with integer coefficients, and so  $z' = R + S(m, g) + T(m, 1)$ . Gauss then shows that the polynomials  $Y := 2R - S - T$  and  $Z := T - S$  satisfy  $4X = Y^2 \pm nZ^2$ , where the sign is  $+$  or  $-$  according as  $n$  is of the form,  $4k + 3$  or  $4k + 1$ .

In the subsequent article 358, Gauss considers  $n = 3m + 1$  and studies the distribution of the roots of  $X = 0$  into three periods, namely:  $(m, 1)$ ,  $(m, g)$ , and  $(m, g^2)$ ,  $g$  being any primitive root for the prime  $n$ . It is clear that the first contains the roots  $[1], [g^3], [g^6], \dots, [g^{n-4}]$ , the second  $[g], [g^4], [g^7], \dots, [g^{n-3}]$  and the third  $[g^2], [g^5], [g^8], \dots, [g^{n-2}]$ . He denotes their sums respectively  $p, p'$ , and  $p''$ . If the equation roots of which are  $p, p'$ , and  $p''$  is  $X^3 - Ax^2 + Bx - C = 0$ , one has  $A = p + p' + p'' = -1$ ,  $B = pp' + p'p'' + p''p$  and  $C = pp'p''$ . To find the others' coefficients, Gauss proceeds as follows: Let  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$  be the minimal residues of the numbers  $g^3, g^6, g^9, \dots$  modulo  $n$  and let  $\mathfrak{K}$  their set together with the number 1. Similarly, one defines  $\mathfrak{A}', \mathfrak{B}', \mathfrak{C}', \dots, \mathfrak{A}'', \mathfrak{B}'', \mathfrak{C}'', \dots$ , and  $\mathfrak{K}', \mathfrak{K}''$ . Gauss observes that  $n - 1$  lies in  $\mathfrak{K}$ , and that the numbers  $h$  and  $n - h$  always belong to the same of the sets  $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}''$ . Gauss denotes by  $(\mathfrak{KK})$  the number of those numbers in the sequence  $1, 2, 3, \dots, n - 1$  which belong to  $\mathfrak{K}$  by themselves and when increased by 1. Similarly,  $(\mathfrak{KK}')$  denotes the number of those integers in  $1, 2, 3, \dots, n - 1$  which belong to  $\mathfrak{K}$  and belong to  $\mathfrak{K}'$  when increased by 1. The meaning of the symbols  $(\mathfrak{KK}'')$ ,  $(\mathfrak{K}'\mathfrak{K})$ ,  $(\mathfrak{K}'\mathfrak{K}')$ ,  $(\mathfrak{K}'\mathfrak{K}'')$  and so on is clear. One has  $(\mathfrak{KK}') = (\mathfrak{K}'\mathfrak{K})$ ,  $(\mathfrak{KK}'') = (\mathfrak{K}''\mathfrak{K})$ , and  $(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}')$ . Then, applying the method of art. 345, he finds  $B = -m$  and  $C = a^2 - bc$  where  $a := (\mathfrak{K}'\mathfrak{K}'')$ ,  $b := (\mathfrak{K}'\mathfrak{K})$ ,  $c := (\mathfrak{K}''\mathfrak{K})$ .

Finally, in the remaining articles, Gauss applies this theory to show the constructibility with a ruler and compass of regular  $n$ -gons for any Fermat's prime  $n = 2^k + 1$ .

## 7 The *Disquisitiones* in the first three decades of the 1800s

The *Disquisitiones Arithmeticae* were presented to the French Academy in January of the year 1802, by Adrien-Marie Legendre. Legendre, Joseph-Louis Lagrange, Sylvestre François Lacroix, and Pierre-Simon Laplace were among the first readers of Gauss's treatise.

On May 31, 1804, Lagrange wrote to Gauss: “Vos *Disquisitiones* vous ont mis de suite au rang des premiers géomètres et je regarde la dernière section comme contenant la plus belle découverte analytique qui ait été faite depuis longtemps” [Your *Disquisitiones* have raised you immediately into the ranks of the first-order geometers and I consider the last section as containing the most beautiful analytic discovery in a long time] (Lagrange 1867–1892, 14, p. 299).

The same year, Lacroix, in the third edition of his *Complément des Éléments d'algèbre*, presented, “d'après M. Gauss,” the theory of residues and its application to the resolution of the cyclotomic equation (see Lacroix 1804, p. 296). He also used, as he added on pag. 307, “quelques remarques que M. de La Place a bien voulu me communiquer”[Some remarks that M. de La Place has communicated to me]. Lacroix concluded by inviting the reader to consult Legendre's *Essai sur la théorie des nombres* and “les *Disquisitiones Arithmeticae* de M. Gauss desquelles j'ai tiré ce qui précède”[and the D.A. of M. Gauss from which I extracted the preceding]. Lacroix's words suggest that Laplace had also read Gauss's treatise.

Therefore, it seems that, at first, the attention to the D.A. of the mathematical establishment focused on the resolution of the equation  $x^n - 1 = 0$ , and the construction of regular polygons.

We cannot be sure how Germain knew of the D.A., if Legendre or Lagrange suggested that she read it, or if she initiated the reading by personal initiative. At any rate, as in the Autumn of 1804 she addressed Gauss, saying “Vos *Disquisitiones Arithmeticae* font depuis longtemps l'objet de mon admiration et de mes études” [Your D.A. have long been the object of my admiration and my studies], it is clear that she was among the first readers of Gauss's book. Actually, as we will see, she not only read the D.A. but, unlike others, she proceeded in a systematic study of Gauss treatise, and in a few years, she had mastered it in its entirety.

In the spring of 1805, the project for a French edition of the D.A. started, and Gauss, on June 16 (the same day he replied to the first letter of Germain, as Le Blanc), wrote to the translator of the *Disquisitiones Arithmeticae* A.-C. M. Poulet-Delisle (De Jonquieres 1896, p. 829):

Il m'est aussi doux que flatteur que les recherches contenues dans mon ouvrage, auxquelles j'avais dévoué la plus belle partie de ma jeunesse, et qui ont été la source de mes plus douces jouissances, aient acquis tant d'amis en France; sort bien inégal à celui qu'elles ont trouvé en Allemagne où le goût pour les parties plus difficiles des mathématiques pures n'est la propriété que d'un fort petit nombre de personnes [It is for me as sweet as it is flattering that the investigations contained in my work, to which I devoted the best part of my youth, and which were the source of my sweetest joys, have acquired so many admirers in France; a fate quite different from what they found in Germany where the taste

for the most difficult parts of pure mathematics has but a very small number of adherents.]

He used almost the same words to her (see Gauss's reply to Germain's letter of November 21, 1804). The French edition appeared only in 1807, printed in Paris by Coursier.

Legendre in the introduction to the second edition of his *Essai sur la théorie des nombres*, which appeared in 1808, wrote:

Enfin il a été ajouté une cinquième partie où on expose avec tout le détail nécessaire, la belle théorie de la résolution de l'équation  $x^n - 1 = 0$ , donnée par M. Gauss, dans ses *Disquisitiones arithmeticæ*... On aurait désiré enrichir cet Essai d'un plus grand nombre des excellens matériaux qui composent l'ouvrage de M. Gauss: mais les méthodes de cet auteur lui sont tellement particulières qu'on n'aurait pu, sans des circuits très-étendus, et sans s'assujétrir au simple rôle de traducteur, profiter de ses autres découvertes [Finally a fifth part has been added, where one expounds in all necessary detail the beautiful theory of the resolution of the equation  $x^n - 1 = 0$  given by Mr. Gauss in his *Disquisitiones arithmeticæ*... One would have desired to enrich this essay with a larger number of the excellent topics of which the work of Mr. Gauss is composed: but the methods of this author are so unique to him that, without extensive digressions and without becoming a simple translator, one could not benefit from his other discoveries].

In the second edition of his *Traité de la résolution des équations numériques de tous les degrés*, printed in 1808, Lagrange included, as a final note, a discussion and a simplification of art. 360. of the D.A.

Ten years after the appearance of the D.A., Gauss's treatment of the cyclotomic equation was still the topic of major appeal. Peter Barlow in the preface of his book, *An Elementary Investigation of the Theory of Numbers* (Barlow 1811), wrote: “[the D.A.] has opened a new field of inquiry, by the application of the properties of numbers to the solution of the binomial equation of the form  $x^n - 1 = 0$  on the solution of which depends the division of the circle into  $n$  equal parts” and devoted the last chapter of his book to it.

Charles Babbage spoke of “the celebrated theorem of Gauss on the resolution of the equation  $x^n - 1 = 0$ ” in recommending the D.A. to the newly founded Cambridge Analytical Society (Babbage and Herschel 1813, also Babbage 1989).

The first who used concepts and notation from the D.A. unrelated to the cyclotomic equation, such as those of determinant and adjoint, was in Cauchy (1815).

In 1818, Louis Poinsot presented his *Mémoire sur l'application de l'algèbre à la théorie des nombres* (Poinsot 1820) to the Paris Academy, in which, developing simultaneously the congruence  $x^n \equiv 1 \pmod{p}$  and the equation  $x^n - 1 = 0$ , he gave an analytic representation of power residues by means of imaginary roots of unity. Poinsot's memoir had a great influence on Germain's work on Fermat's Last Theorem (see below and also Del Centina 2005, 2008).

Legendre was never too inclined toward Gauss's use of the symbol  $\equiv$  introduced in the D.A. in place of the somewhat contradictory  $=$  which was in use (equality up to multiples), or did he distinguish congruences as a topic which needed a separate

treatment. Still, in his *Recherches sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat* Legendre claimed that there is no “besoin de signes nouveaux d'égalité ni des denominations nouvelles assez incongrues, dont quelques géomètres font usage [need of new signs of equality nor of new, and somewhat incongruous, names of which some geometers make use]” (Legendre 1827, p. 15). Germain, on the contrary, was immediately and strongly in favor of Gauss's notation, as she confirmed in her letter to him of 1819: “the simple substitution of congruence represented by the symbol  $\equiv$  seems to me important. The notion of equality elsewhere denoted = always seemed to me in contradiction with the progress of analysis, and I cannot express the clarity and consequently the facility I have found in this branch of computation with the use of your notation.”

Because of the fame of the D.A. and the fact that its reading does not require many prerequisites, the mathematicians born shortly after 1801 became familiar with Gauss's treatise early on in their lives.

Niels Henrik Abel, born in 1802, read it in his early youth, during the first year at university in Christiania [Oslo].

In 1819, Guglielmo Libri (also born in 1802) brought a copy of the D.A. with him to Pisa, and, like Sophie Germain, attempted to apply the theory of congruences to prove FLT (Del Centina and Fiocca 2010). Libri, who showed a good understanding of Gauss's D.A., proved some interesting results concerning various types of congruence equations (Libri 1829).

Carl Gustav Jacob Jacobi was born in 1804, and graduated from the University of Berlin. In 1827, he published the first paper on cubic residues (Jacobi 1827), a subject—together with that of biquadratic residues—which Gauss had started to study in the years 1805–1807 (see Gauss 1900, pp. 5–11 and the correspondence with Germain). Some years later, in 1834, Jacobi published his first work on quadratic forms (Jacobi 1834), and perfected the theory of determinants (Jacobi 1841).

Johann Peter Gustav Lejeune Dirichlet, born in 1805, after graduating in Cologne, went to Paris in 1822, where he attended the lectures at the *Collège de France* and at the *Faculté des Sciences*. He set off for France with his copy of the D.A., which he kept with him constantly. Dirichlet's understanding of Gauss's work was profound, and in 1825, he was able to prove some theorems on biquadratic residues stated without proof by Gauss (Lejeune-Dirichlet 1828). The same year Dirichlet returned to Germany, where he contributed strongly to the renewal of German mathematics.

According to Klein (1826, p. 27), the reason why the D.A. exerted its deserved influence in Germany was due, above all, to Dirichlet's interpretative lectures. There can be no doubt that, at that time, the D.A. was a difficult book to read. But, thanks to Dirichlet's lectures, many young Prussian mathematicians became familiar with Gauss's treatise, and number theory emerged in that country as a significant topic upon which to determine the value of a mathematician (Goldstein et al. 2007, p. 25).

## 8 Gauss's results on cubic and biquadratic residues

Although the first sign of cubic residues appears in a footnote in art. 358 of the D.A., Gauss asserted that he began to study cubic and biquadratic residues in 1805 (Gauss

1818, 1863b, p. 50). However, in his mathematical diary, on February 15, 1807, he recorded: “Theoria cubicorum et biquadraticorum incepta” [Beginning of the theory of cubic and biquadratic residues] (Gauss 1917, p. 665). Likely, it was in the winter of 1807 that Gauss began to settle that theory. In fact, in his letter to Germain of April 30 of that year he affirmed: “Last winter I even succeeded in adding an entirely new branch to it. This is the theory of cubic and biquadratic residues, brought to an equal level of perfection as the theory of quadratic residues,” and announced, for the first time, two theorems regarding the cubic and the biquadratic characters of the number 2.

In the years following, seeking a better understanding of the behavior of cubic and biquadratic power residues, Gauss was led to penetrate more deeply into the theory of quadratic residues and to give new proofs of his fundamental theorem—the Quadratic Reciprocity Law (Gauss 1808, 1818). In particular, in Gauss (1818, 1863b, p. 50), he wrote:

Alia adhuc affuit ratio, quae ut novas demonstrationes, novem iam abhinc annos promissas, nunc potissimum promulgarem, efficit. Scilicet quum inde ab anno 1805 theoriam residuorum cubicorum atque biquadraticorum, argumentum longe difficilius, perscrutari coepisse, similem fere fortunam, ac olim in theoria residuorum quadraticorum, expertus sum. Protinus quidem theorematum ea, quae has quaestiones prorsus exhauiunt, et in quibus mira analogia cum theorematibus ad residua quadratica pertinentibus eminet, per inductionem detecta fuerunt, quam primum via idonea quaesita essent: omnes vero conatus, ipsorum demonstrationibus ex omni parte perfectis potiundi, per longum tempus irriti manserunt. Hoc ipsum incitamentum erat, ut demonstrationibus iam cognitis circa residua quadraticia alias aliasque addere tantopere studerem, spe fultus, ut ex multis methodis diversis una vel altera ad illustrandum argumentum affine aliquid conferre posset. Quae spes neutram vana fuit, laboreisque indefessum tandem successus prosperi sequuti sunt [Another reason is also at the origin of the new proof, published here and promised nine years ago. Since 1805, when I began to be involved in the research on cubic and biquadratic residues, a more difficult topic than that of the quadratic residues, I have become an expert, by a similar fortune, as once of the theory of quadratic residues. Actually, the theorems that respond to all these questions and which seem highly analogous to the theorems on quadratic residues, were first found by induction before they were properly proved. I have to say that all my efforts to prove them, conducted in every direction, remained fruitless for a long time. This was the true incentive for striving so hard to add new proofs to those already known on quadratic residues, sustained by the hope that by using many different methods, one or another would convey something toward the clarification of the argument [for cubic and biquadratic residues]. This hope has not been in vain, finally by the indefatigable work I have obtained promising results. Soon, I will bring the fruit of this research into public view].

All this leads us to think that, in contrast with what he wrote to Germain in 1807, Gauss proceeded slowly in the development of that theory, in particular, with what concerns the discovery of a reciprocity law for cubic and biquadratic residues. In fact,

Gauss's first publication on biquadratic residues, *Theoria residuorum biquadraticorum, commentatio prima*, appeared only in 1828.<sup>29</sup>

According to Gauss (1828, 1863b, pp. 67–68), the theory of cubic and biquadratic residues was more difficult to develop than that of quadratic residues, and he soon came to the recognition that the hitherto employed tools of higher arithmetic would in no way suffice to establish a general theory (i.e., to state a reciprocity law), and that this necessarily required enlarging the domain of arithmetic by the introduction of complex numbers.

In this first memoir, Gauss only presented those studies on biquadratic residues which can be carried out without such expansion, and he gave a criterion for detecting the biquadratic character of the number 2, i.e., determining for which primes the number 2 is a biquadratic residue or nonresidue.

Let us briefly look at how Gauss proceeds.

First of all, he observes that every biquadratic residue  $(\bmod p)$  is a quadratic residue  $(\bmod p)$  and every quadratic nonresidue  $(\bmod p)$  is a biquadratic nonresidue  $(\bmod p)$  for any prime number  $p$ . Then, he proves that the claim can be inverted whenever  $p = 4n + 3$ , so that in further investigation, one needs to consider only primes of the form  $p = 4n + 1$ .

If  $p = 4n + 1$ , Gauss proves that the set of numbers  $\{1, 2, \dots, p-1\}$  is divided into four subsets, or *classes*,  $A$ ,  $B$ ,  $C$ , and  $D$ , in such a way that each number appears in only one class, each containing  $(p-1)/4$  elements. Moreover, he shows that  $A$  is the set of biquadratic residues,  $B$  the set of all the least positive residues of the products  $eA$  where  $e$  is an arbitrary chosen quadratic residue, and likewise  $C$  and  $D$  are the sets of the least positive residues of the products  $e^2A$  and  $e^3A$   $(\bmod p)$ . Since the product of two biquadratic residues is always a biquadratic residue, the least positive residue of the product of two elements of  $A$  is always in  $A$ .

Gauss also remarks that the previous results can be easily obtained by using the theory of power residues. In fact, if  $g$  is a primitive root for the modulus  $p$ , we immediately have  $A = \{1, g^4, g^8, \dots, g^{p-5}\}$ ,  $B = \{g, g^5, g^9, \dots, g^{p-4}\}$ ,  $C = \{g^2, g^6, g^{10}, \dots, g^{p-3}\}$  and  $D = \{g^3, g^7, g^{11}, \dots, g^{p-2}\}$ .

Then Gauss observes that since 2 is quadratic residue for all primes of the form  $8n + 1$  (see D.A. art. 114), the number 2 is in  $A$  for these primes, and furthermore that, since  $-1$  is always a biquadratic residue for primes of the form  $8n + 1$  (see D.A. art. 115), the number  $-2$  is also a biquadratic residue  $(\bmod 8n + 1)$ . Moreover, he recalls that any prime  $4n + 1$  can be brought to the form  $a^2 + b^2$  in one and only one way (see D.A. art. 182), where  $a$  is assumed as odd and  $b$  even.

After examining all cases for primes  $p = 4n + 1$  less than 100 (Gauss 1828, arts. 11–13), he concludes inductively that 2 must be included in the class  $A$  for all those  $p$  for which  $b = 8m$  (Gauss 1828, art. 14).<sup>30</sup> Let us stress that this claim is the second

<sup>29</sup> In 1827, Jacobi published *De residuis cubicis commentatio numerosa* (Jacobi 1827), wherein two theorems related to the cubic reciprocity law are stated by means of complex numbers.

<sup>30</sup> Precisely, Gauss's statement is as follows: the number 2 is in class  $A$  for all moduli in which  $b = 8m$ , and is in class  $C$  for all moduli in which  $b = 8m + 4$ . He also added: "Sed hoc theorema longe altioris indaginis est, quam id, quod in art. praec. eruimus. demonstratione plures disquisitiones praealiminares sunt praemittendae, ordinem, quo numeri complexuum  $A$ ,  $B$ ,  $C$ ,  $D$  se invicem sequuntur, spectantes" [Nevertheless this theorem asks for a much deeper investigation than that of the previous article, and its proof

of the three theorems that Gauss proposed to Germain in his letter of April 1807. In the subsequent articles 15–21 of his work, Gauss proves this result.<sup>31</sup>

He denotes the number of numbers  $h$  from the class  $A$  such that  $h + 1$  is in  $A, B, C$  or  $D$ , by (00), (01), (02), and (03), respectively, the number of numbers  $h$  from the class  $B$  such that  $h + 1$  is in  $A, B, C$ , or  $D$  by (10), (11), (12), or (13), respectively, and, analogously, there are the numbers (20), (21), (22), . . . , (32), (33).

The symbol (00) denotes in how many different ways the equation  $1 + \alpha = \alpha'$  can be satisfied when  $\alpha, \alpha'$  denote undetermined numbers from the class  $A$ . Since, for the modulus  $p = 8n + 1$ ,  $\alpha'$ , and  $p - \alpha'$  belong to the same class, we can also say that (00) is the number of solutions of the equation  $1 + \alpha + \alpha' = p$ , or (which is the same) of the congruence

$$1 + \alpha + \alpha' \equiv 0 \pmod{p}.$$

Likewise, the numbers (01), (02), (03), etc., denote, respectively, the number of solutions of the congruences:

$$\begin{aligned} 1 + \alpha + \beta &\equiv 0 \pmod{p}, \\ 1 + \alpha + \gamma &\equiv 0 \pmod{p}, \\ 1 + \alpha + \delta &\equiv 0 \pmod{p}, \\ 1 + \beta + \beta' &\equiv 0 \pmod{p}, \\ &\vdots \end{aligned}$$

where  $\beta, \beta'$  denote numbers from  $B$ , and  $\gamma, \gamma'$  denote numbers from  $C$ , etc. From this arise immediately the following six equalities (10) = (01), (02) = (20), (03) = (30), (12) = (21), (13) = (31), and (23) = (32).

From every given solution of the congruence  $1 + \alpha + \beta \equiv 0$  arises a solution of the congruence  $1 + \delta + \delta' \equiv 0$ , provided  $\delta$  is chosen in  $\{1, \dots, p - 1\}$  so that  $\beta\delta \equiv 1$  (which is certainly from  $D$ ), and  $\delta'$  is the least residue of  $\alpha\delta$  (which is also in  $D$ ). This correspondence can be reversed by choosing  $\beta$  such that  $\beta\delta \equiv 1$  and  $\alpha$  such that  $\alpha \equiv \beta\delta'$ . Therefore, one has (01) = (33). Similarly one gets (02) = (22), and (11) = (03).

Finally, in a analogous way, he derives from the congruence  $1 + \beta + \gamma \equiv 0$  the congruence  $1 + \beta' + \delta \equiv 0$ , as well as the congruence  $1 + \gamma' + \delta' \equiv 0$ , from which he gets (12) = (13) = (23).

Taking all this into account, the 16 quantities (00), (01), . . . , (10), (11), . . . , (23), (33) are now reduced to only six unknowns, and they can be ordered in the following  $4 \times 4$  matrix:

---

Footnote 30 continued

needs many preliminary results, which are related to the order in which the numbers follow one each other in the sets,  $A, B, C, D$ .

<sup>31</sup> Actually, Gauss proves the following complete result: the number 2 belongs to the class  $A, B, C$ , or  $D$  depending on whether  $b$  is of the form  $8m, 8m + 2, 8m + 4$ , or  $8m + 6$ , but we omit this, as the same is not essential to our discussion.

$$\begin{pmatrix} h & i & k & l \\ i & l & m & m \\ k & m & k & m \\ l & m & m & i \end{pmatrix}$$

Gauss finds three other equations among the six remaining unknowns.

Since each number in the class  $A$ , excluding  $p - 1$ , must be followed by a number in the classes  $A, B, C$ , or  $D$ , Gauss observes that

$$(00) + (01) + (02) + (03) = 2n - 1$$

and similarly, starting from a number in  $B, C$  or  $D$ , he also gets

$$\begin{aligned} (10) + (11) + (12) + (13) &= 2n, \\ (20) + (21) + (22) + (23) &= 2n, \\ (30) + (31) + (32) + (33) &= 2n. \end{aligned}$$

The first three equations yield the following:

$$\begin{aligned} h + i + k + l &= 2n - 1, \\ i + l + 2m &= 2n, \\ k + m &= n \end{aligned}$$

and the fourth becomes identical to the second. Clearly with these relations Gauss reduces the unknowns to only two.

In order to obtain a complete determination, Gauss computes the number of solutions of the congruence  $1 + \alpha + \beta + \gamma \equiv 0 \pmod{p}$ , where  $\alpha, \beta$ , and  $\gamma$  are undetermined numbers from  $A, B$ , and  $C$  in two different ways. Comparing the two expressions thus obtained for the same number, and taking into account the equations above, with some computation he gets

$$8n + 1 = [4(k - m) + 1]^2 + 4(l - i)^2,$$

so that if  $x^2 + 64y^2$ , one must have  $x = 4(k - m) + 1$  and  $b = 2(l - i)$ . Putting  $x = 4q + 1$  and  $b = 4r$ , from  $16h = 8n + 1 - 64(k - m) + 1 - 11$ , he finally obtains

$$h = q^2 - q + r - 1,$$

and, since  $q^2 - q$  is always even,  $h = (00)$  is odd if and only if  $r$  is even, i.e.,  $b = 8y$ .

As already observed, when  $p = 8n + 1$ , the number 2 will appear either in the class  $A$  or in the class  $C$ , and in the former case, it can easily be seen that  $(p - 1)/2$  and  $(p + 1)/2$  also belong to  $A$ , while in the latter case, they belong to  $C$ . Hence, if  $h$  and  $h + 1$  are in  $A$  then also  $p - h$  and  $p - h - 1$  are in  $A$ , then  $(00)$  is always even unless a number thus associated with itself exists, i.e.,  $(p - 1)/2$  belongs to  $A$ . One concludes that  $(00)$  is odd whenever 2 is a biquadratic residue  $\pmod{p}$ .

In his second work on biquadratic residues, Gauss went more deeply into the theory and stated a reciprocity law for them. In this respect, he wrote (Gauss 1832, 1863b, p. 102):

ita theorematum circa residua biquadratica tunc tantum in summa simplicitate ac genuina venustate resplendet, quando campus arithmeticæ ad quantitates *imaginarias* extenditur [thus the theorems on biquadratic residues gleam in their greatest simplicity and genuine beauty only when the field of arithmetic is extended to the *imaginary quantities*].

Gauss begins his memoir by exposing the elementary theory of complex numbers, and of the ring  $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ , and in particular, he introduces the concepts of (a) *associated* complex numbers (any  $a + ib$  and the product of it by the units  $-1, i, -i$ ), and (b) *primary* complex number, to distinguish a particular one in the set of the four associated complex numbers—as the positive is distinguished between  $n$  and  $-n$  in  $\mathbb{Z}$ . In other words, a non-unit  $a + ib$  is called primary if and only if either  $a \equiv 1(\text{mod } 4)$ ,  $b \equiv 0(\text{mod } 4)$  or  $a \equiv 3(\text{mod } 4)$ ,  $b \equiv 2(\text{mod } 4)$  [or, equivalently,  $a + ib \equiv 1 \pmod{(2+i2)}$ ]. Then, after having established the quadratic reciprocity law in  $\mathbb{Z}[i]$  in section 67, on the basis of induction, he finally states the following biquadratic reciprocity theorem: *let  $a + ib$  and  $a' + ib'$  be two distinct primary complex primes, then the biquadratic character of the first with respect to the second is the same as that of the second with respect to the first if at least one is  $\equiv 1(\text{mod } 4)$ , but the biquadratic character differs by 2 if both are  $\equiv (3+i2)(\text{mod } 4)$ .*

Of this theorem, Gauss wrote (Gauss 1832, 1863b, p. 139):

At non obstante summa huius theorematis simplicitate, ipsius demonstratio inter mysteria arithmeticæ sublimioris maxime recondita referenda ext [Although this theorem can be stated with great simplicity, its proof is one of the deepest mysteries of higher arithmetic]

and he promised a third memoir on the subject, which never appeared.

Let us remark that the proof of the biquadratic reciprocity law as stated by Gauss was given by Eisenstein (1844a).

The cubic reciprocity law, never stated by Gauss, was announced and proved by Eisenstein (1844b).<sup>32</sup>

## 9 The mathematical content of Germain's letters and notes

The mathematics which Sophie Germain expounds in the letters and enclosed notes (the *addenda*) is sometimes difficult to follow or understand. The results that she presented to Gauss do not have the appearance of polished or well-organized works,

<sup>32</sup> Jacobi also gave a proof of the cubic reciprocity law in his lectures at Königsberg during the year 1837, as he attested in a footnote in his *Über die Kreistheilung und ihre Anwendung aus die Zahlentheorie* (Jacobi 1846, p. 172). This note, in which Jacobi accused Eisenstein of plagiarism, gave rise to a bitter dispute over priority between the two. For the history of the cubic and biquadratic reciprocity law see Smith (1965), Collison (1977), and Lemmermeyer (2000).

and her writing (especially in the symbols) is not always easy to interpret. Moreover, her mathematical explanations sometimes omit details, leaving the reader to complete the work, or they consist of lengthy computations sometimes containing trivial mistakes. For these reasons, we have not been able to completely check all of Germain's claims, but suffice it is to say that the letters and mathematical notes contain many interesting results, and we will focus on them.

### 9.1 First letter

Let us recall that in art. 357 of the D.A., Gauss proved that if  $n$  is any prime  $> 2$ , then the equation:

$$4 \frac{x^n - 1}{x - 1} = Y^2 \pm nZ^2, \quad (9.1)$$

where  $Y$  and  $Z$  are polynomials in  $x$  with integer coefficients and the sign on the right is  $+$  or  $-$  depending on whether  $n$  is of the form  $4k + 3$  or  $4k + 1$ .

In the first part of the *addendum*, Sophie Germain extends this result to the case of the more general equation:

$$4 \frac{x^{n^s} - 1}{x - 1} = Y^2 \pm nZ^2, \quad (9.2)$$

where  $s$  is any positive integer, and  $Y$  and  $Z$  are still polynomials in  $x$  with integer coefficients. To this end, she uses the following recursive argument. Suppose  $s = 2$ , from

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

by Eq. (9.1), we have

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

and since the second member is equal to  $(YY' \pm nZZ')^2 \pm n(Y'Z \pm YZ')^2$ , if we put  $YY' \pm nZZ' = 2f$  and  $Y'Z \pm YZ' = 2\varphi$ , taking into account the divisibility by 4, then we finally get

$$\frac{4(x^{n^2} - 1)}{x - 1} = f^2 \pm n\varphi^2.$$

The same reasoning applied to the last equation and (9.1) gives the case  $s = 3$ , and so on.

Sophie Germain observes that due to the ambiguity of the signs, there are  $2^{s-1}$  different polynomials  $Y$  and  $2^{s-1}$  different polynomials  $Z$  satisfying (9.2).

Let  $m = (n - 1)/2$ , then  $z = x^m - ax^{m-1} + bx^{m-2} - \text{etc.} = 0$  be the equation solutions of which belong to the period  $(m, 1)$ . So, by art. 348 of the D.A., we have  $a = (m, 1)$  and the coefficients  $b$ , etc. are of the form  $\mathfrak{A} + \mathfrak{B}(m, 1) + \mathfrak{C}(m, g)$ , where  $\mathfrak{A}$ ,  $\mathfrak{B}$ , and  $\mathfrak{C}$  are integers. Let  $z'$  be the transformation of  $z$  when the periods  $(m, g)$  and  $(m, g^2)$  are, respectively, substituted for  $(m, 1)$  and  $(m, g)$  into the coefficients of  $z$ , then the roots of  $z' = 0$  are those contained in the period  $(m, g)$ , and it follows that

$$zz' = \frac{x^n - 1}{x - 1}. \quad (9.3)$$

Thus, by art. 357 of the D.A.,  $z$  can be reduced to the form  $R + S(m, g) + T(m, 1)$ , where  $R$ ,  $S$ , and  $T$  are polynomials with integer coefficients, and consequently,  $z'$  reduces to the form:  $z' = R + S(m, 1) + T(m, g)$ . From these reductions, it is possible to determine the coefficients of  $Y$  and  $Z$ . Gauss writes: "It is easy to see that the two terms of higher degree in the function  $Y$  will always be  $2x^m + x^{m-1}$  and that of highest degree in the function  $Z$ , will always be  $x^{m-1}$ . All the remaining coefficients will be integers which depend on  $n$ , and it is not possible to give a general analytic formula for them."

In the *addendum*, Sophie Germain, imitating Gauss's method by replacing  $r = \cos \frac{kP}{n} + i \sin \frac{kP}{n}$  by  $R = \cos \frac{kP}{n^s} + i \sin \frac{kP}{n^s}$ , extends the above result to the case of Eq. (9.2). In other words, she shows that—even in this case—the coefficients of the corresponding  $z$  and  $z'$ , which are now polynomials of degree  $(n^s - 1)/2$ , can be expressed in terms of the periods  $(m, 1)$ ,  $(m, g)$ . The proof given seems to be correct, and to see its development, we refer directly to the *addendum* transcribed in the Appendix. This property obviously also holds true for the polynomials  $Y$  and  $Z$ .

The reasoning followed by Germain allows her to determine, although in a complicated way in general, the coefficients of the polynomials  $Y$  and  $Z$  for certain values of  $n$  and  $s$  (see the examples she gives in the *addendum*).

Sophie Germain also remarks: *if  $n = 4k + 1$ , then the coefficients of  $Y$  and  $Z$  are the same, and of the same signs, starting from  $x^m$  as well as starting from 1, i.e., if  $N$  is the coefficient of  $x^{m-h}$  in  $Y$  or in  $Z$  then  $N$  is the coefficient of  $x^h$*  [she say *homogeneous function* of  $x$  and 1].

Moreover, she observes *if  $n = 4k + 3$ , the same holds with opposite sign, i.e., if  $N$  is the coefficient of  $x^{m-h}$ , then  $-N$  is the coefficient of  $x^h$*  [*homogeneous function* of  $x$  and  $-1$ ] (see the examples given by Gauss in art. 357 of the D.A.).

To show this, she proceeds as follows. Let  $g$  denote a primitive root for the modulus  $n$ , and let  $[1], [g], \dots, [g^{n-2}]$  denote the set of all roots of the equation  $zz' = X = 0$ . She notes that the coefficients of  $Y$  and  $Z$  depend on those of  $z$  and  $z'$ . According to Gauss's theory of periods,  $z = 0$  can be put in the form  $z = (x - [1])(x - [g^2])(x - [g^4]) \cdots (x - [g^{n-3}]) = 0$ . Since  $[1][g^2][g^4] \cdots [g^{n-3}] = [1 + g^2 + g^4 + \cdots + g^{n-3}] = [0] = 1$ , one can multiply the second member of the above equation by  $([1][g^2][g^4] \cdots [g^{n-3}])^{m-1}$  without changing the first, and one can do this in such a way that each single factor is multiplied by all roots excluding those appearing in that same factor. This process allows one to write the above equation in the form:  $z = ([-1] - 1)(x[-g^2] - 1) \cdots (x[-g^{n-3}] - 1)$ .

When  $n = 4k + 1$ ,  $-1$  is a quadratic residue, then the last equation reduces to  $z = (x[1] - 1)(x[g^2] - 1) \cdots (x[g^{n-3}] - 1)$ , and since the number of factors  $m = 2k$  is even, one can change all the signs, obtaining  $z = (1 - x[1])(1 - x[g^2]) \cdots (1 - x[g^{n-3}])$ , which shows  $z$  to be a homogeneous function of  $x$  and  $1$  as defined by Germain. The same reasoning can be applied to  $z'$ , and one gets  $z' = (x - [g])(x - [g^3])(x - [g^5]) \cdots (x - [g^{n-2}]) = 0$ . It follows that  $zz'$  is a homogeneous function of  $x$  and  $1$ . Here, she claims that  $Y$  and  $Z$  are also homogeneous functions of  $x$  and  $1$ .

When  $n = 4k + 3$ , one can proceed in a similar way (but remembering that in this case  $-1$  is not a quadratic residue) to show that  $zz'$  is a homogeneous function of  $x$  and  $-1$ . Then, she claims that  $Y$  (and  $Z$ ) is homogeneous function of  $x$  and  $-1$ , without explanation.

At any rate, we can see that the stated property of the polynomial  $Y$  holds.

Legendre, in the second edition of his *Théorie des nombres*, gave two methods for obtaining the coefficients of  $Y$  and  $Z$  for Eq. (9.1) (Legendre 1827, arts. 509–512). The first he showed by using the theory of periods, and so this method is in some sense similar to Germain's above line of thought. The second was based on a very simple remark that we now describe.

In the development of  $(x - 1)^n$ , all the coefficients, except the first and the last, are divisible by  $n$ . Thus, one can write  $(x - 1)^n = x^n - 1 - nT$ , with  $T$  a suitable polynomial of degree  $n - 1$ . Then, remembering equation (9.1), one has  $4X(x - 1) = 4(x - 1)^n + 4nT = (x - 1)(Y^2 \pm nZ^2)$ . Hence, by omitting the multiples of  $n$ , one gets  $4(x - 1)^n = (x - 1)Y^2$  and then  $Y = 2(x - 1)^m$ ; so, in order to determine the coefficients of  $Y$ , one has only to reduce  $(\bmod n)$  the coefficients of the development of  $2(x - 1)^m$ .

The property of the coefficients of  $Y$ , noticed by Germain, was remarked upon by Legendre as a byproduct of his first method (Legendre 1827, p. 194).

Germain returned to the subject of Eq. (9.2) with the note (Germain 1831b) which she published in the year of her death. In this paper, by using the above-mentioned result of Legendre—which she refers to as “useful for establishing immediately that  $Y$  in Eq. (9.1) is a homogeneous polynomial of  $x$  and  $1$ ”—she determines the form of the general power of  $x$  in the polynomials  $Y'$  and  $Z'$  when  $s = 2$ .

Almost at the end of the *addendum*, Sophie Germain gives, by using the method of art. 345 of the D.A., a new proof of the fact that  $2$  is a residue for primes of the form  $8k + 1$  and  $8k + 7$ , and a nonresidue for primes of the form  $8k + 3$  and  $8k + 5$ . This is the only result that Gauss commented on in his response to Germain's letter: “your new proof for the primes of which  $2$  is residue or nonresidue gave me extreme pleasure. It is very clever, although it seems peculiar, and not applicable to other numbers.”

In the last part of the *addendum*, Germain reports on what is probably her first approach to FLT. She claims to have proven FLT for the exponent  $p - 1$  when  $p$  is a prime of type  $8n + 7$ . Since this part of the *addendum* has already been commented upon in Del Centina (2008), we will not give much detail here.

Let  $p$  be a prime  $> 3$  and set  $2p' := p - 1$ . If  $x, y, z$  is a primitive solution of the equation  $x^{p-1} + y^{p-1} = z^{p-1}$ , then  $x^{p'}, y^{p'}, z^{p'}$  satisfy  $X^2 + Y^2 = Z^2$ , so that either  $x$  or  $y$  must be even, and the other odd. She first proves the following two results. (1) if  $x, y$ , and  $z$  are pairwise relatively prime integers satisfying Fermat's equation, then  $p$  divides the even one of  $x$  and  $y$ , and moreover  $z$  is odd and is not divisible by  $p$  (see Gandhi 1966, also Ribenboim 1999, p. 206). Supposing  $y = 2phf$ , she then

proves  $x^{p'} = f^{2p'} - 2^{2p'-2} p^{2p'} h^{2p'}$ . From this, she gets (2) if  $x, y, z$  are as in (1); then  $x^{p'} = fx$  is a quadratic residue (mod  $p$ ) (see Raina 1969, also Ribenboim 1999, p. 207).

Let  $x = f^2 + mp^{2p'}$  where  $m$  is not divisible by  $p$ . By developing the  $p'$ -th power of  $x$ , one has  $f^{2p'} - 2^{2p'-2} p^{2p'} h^{2p'} = f^{2p'} + p' f^{2p'-2} m p^{2p'} + \dots$ , from which, she asserts, one has  $m = k^{2p'}$  and then  $-2 \equiv f^2 \pmod{p}$ . It follows that  $x^{p-1} + y^{p-1} = z^{p-1}$  is not solvable in integers when  $-2$  is not a quadratic residue (mod  $p$ ), that is, for primes of the form  $8n + 5$  and  $8n + 7$  (D.A. art. 113). In the first case,  $p - 1$  is always divisible by 4, and then the result also follows from the impossibility of  $x^4 + y^4 = z^4$ , but in the second case,  $p - 1$  is never divisible by 4 and is not always divisible by 3. Hence, FLT for the exponent  $p - 1$  when  $p = 8n + 7$  would follow.

Unfortunately, one cannot assert that  $m$  necessarily is a  $(2p')$ -th-power, and her reasoning fails (see Del Centina 2008, p. 355). However, we would like to stress that this was the very first attempt to apply the theory of congruences and residues to prove FLT for some exponent. Likely, Sophie Germain continued to study FLT in the following years, but she never returned to this topic in her letters to Gauss until 1819.

## 9.2 Second letter

In her second letter to Gauss, Germain, after an introduction concerning her own research on ternary quadratic forms of determinant zero, tells him of the very recent publication of the fourth volume of Laplace's *Mécanique céleste* and describes the content of it. Moreover, she reviews Legendre's memoir on the orbits of comets, *Nouvelle méthodes pour la détermination des orbites des comètes*, which appeared in March (Legendre 1806).<sup>33</sup> Her comments on it prove that Sophie Germain had an extensive knowledge of mathematical astronomy.

In the *addendum*, she gives some details of her work on quadratic forms.

In art. 267 of the D.A., Gauss claims that a ternary quadratic form

$$f = ax^2 + a'x'^2 + a''x''^2 + 2b''xx' + 2b'xx'' + 2b''xx',$$

of determinant

$$\mathcal{D} = ab^2 + ab'^2 + a''b''^2 - aa'a'' - 2bb'b''$$

equal to zero, can be reduced to a binary quadratic form, up to a linear change of variables. Gauss also asserts that he would prove this result in the future, when presenting a complete theory of ternary quadratic forms. Gauss never published a tract on ternary quadratic forms, but he sketched a proof of the above claim in an handwritten note dated around the year 1800 (Gauss 1917, pp. 87–88).

In the first part of the *addendum* to her second letter, Germain attempts a proof of Gauss' claim for quadratic ternary forms. Let

<sup>33</sup> In this memoir, Legendre expounded the method of least squares for the first time (see also Sect. 3).

$$\begin{pmatrix} A & A' & A'' \\ B & B' & B'' \end{pmatrix}$$

represent the adjoint form  $F$  of  $f$ .

Since  $\mathcal{D} = 0$ ,  $F$  is the null form, and one gets the following six equations:

$$\begin{aligned} BB - A'A'' &= 0, & AB - B'B'' &= 0, \\ B'B' - AA'' &= 0, & A'B' - BB'' &= 0, \\ B''B'' - AA'' &= 0, & A''B'' - BB' &= 0. \end{aligned}$$

At this point Sophie Germain seems to be saying that by taking  $B = m\alpha\beta$ ,  $B' = m\delta\beta$ , and  $B'' = m\alpha\delta$  and then  $A = m\delta^2$ ,  $A' = m\alpha^2$ , and  $A'' = m\beta^2$ , the above equations are satisfied. How she got these expressions for  $B$ ,  $B'$ , and  $B''$  and  $A$ ,  $A'$ , and  $A''$  is not clear, but on the basis of what she also wrote in the third *addendum* (where she extends these results to the case of quaternary quadratic forms), we may argue that she proceeded as follows. Let  $m$  be  $\gcd(A, A', A'')$ , since by the above equations  $A'A''/m^2 = (B/m)^2$ ,  $AA''/m^2 = (B'/m)^2$ , and  $AA'/m^2 = (B''/m)^2$ . Then, by a well-known result,  $A/m$ ,  $A'/m$  and  $A''/m$  are squares (but for this, it is necessary that  $A/m$ ,  $A'/m$ , and  $A''/m$  are pairwise coprimes). Hence, one can suppose that  $A = m\delta^2$ ,  $A' = m\alpha^2$ , and  $A'' = m\beta^2$ . Thus, again by the above equations and taking only positive numbers, one has  $B = m\alpha\beta$ ,  $B' = m\delta\beta$ , and  $B'' = m\alpha\delta$ . It is clear that this cannot be realized for “any”  $f$  with  $\mathcal{D} = 0$ . In order to perform the desired reduction, Sophie Germain has to also suppose (but without saying so) that  $B$ ,  $B'$ , and  $B'' \neq 0$ , i.e.,  $\alpha$ ,  $\beta$ , and  $\delta \neq 0$ , which, of course, is not always true. Under these hypotheses (which only hold for a “general”  $f$  with  $\mathcal{D} = 0$ ), by some computation, she obtains the following relations:

$$\begin{cases} a'\alpha^2 = a\delta^2 + 2b'\delta\beta + a''\beta^2 \\ a''\beta^2 = a\delta^2 + 2b''\delta\alpha + a'\alpha^2 \\ a\delta^2 = a'\alpha^2 + 2b\alpha\beta + a''\beta^2 \end{cases}$$

(see the *addendum*). Then, multiplying by  $\delta^2$  the form  $f$ , and taking into account the equations above, she is able to reduce  $f$  to the form:

$$a'(\alpha x - \delta x')^2 + a''(\beta x - \delta x'')^2 + 2b(\alpha x - \delta x')(\beta x - \delta x''),$$

which, by putting

$$\begin{cases} u = \alpha x - \delta x' \\ v = \beta x - \delta x'', \end{cases}$$

can be written as

$$a'u^2 + a''v^2 + 2bu v,$$

or, which is to say,  $(a', b, a'')$  (see Gauss 1917, pp. 87–88). She observes that this reduction can be done in two other ways, obtaining the binary quadratic forms  $(a, b', a'')$ , and  $(a, b'', a')$ .

This is perhaps the most interesting remark of the *addendum*.

In art. 201 of the D.A., Gauss had shown that the equation  $t^2 - \mathcal{D}u^2 = 4$  is solvable in integers only if  $\mathcal{D}$  is  $4k$  or  $4k + 1$ . In the second part of the *addendum*, Sophie Germain considers in detail the case when  $\mathcal{D}$  is one of the following:  $8k$ ,  $8k + 1$ , or  $8k + 5$ . She gives some explicit formulae.

Next she extends Gauss's result of article 115 from second powers to the  $(2^s)$ th-powers. Precisely, Gauss showed that among the numbers  $1, 2, \dots, 4m$  there are  $m$  biquadratic residues for the prime  $p = 4m + 1$ , and  $3m$  not biquadratic residues. Using Gauss's method, Sophie Germain proves that for the prime  $p = 2^s m + 1$ , among the numbers  $1, 2, \dots, 2^s m$ , there are  $m$  which are  $(2^s)$ th-power residues and  $(2^s - 1)m$  which are  $(2^s)$ th-power nonresidues. In fact, since  $-1$  is always a quadratic residue, i.e.,  $f^2 \equiv -1 \pmod{p}$ , let  $z$  be any number not divisible by  $p$ . From  $f^{2^{s-1}} \equiv -1$ , it follows that the  $2^s$  numbers  $z, -z, zf, -zf, \dots, zf^{2^{s-1}}$ , and  $-zf^{2^{s-1}}$  are congruent  $\pmod{2^s m + 1}$ . From this, she deduces that for the primes of the form  $2^{2^i} + 1 = 2^{i+1}2^{2^i-i-1} + 1$ , there are  $2^{i+1}$   $(2^{2^i-i-1})$ -th power residues, and because  $2^{2^{i+1}} \equiv 1 \pmod{2^i + 1}$ ,  $2$  is a  $(2^{2^i-i-1})$ -th-power residue.

Finally, Sophie Germain claims that by using the method of art. 98 in the D.A., the first two parts of the theorem (same article) on the product of two quadratic residues or nonresidues, also holds true for  $(2^s)$ th-power  $\pmod{2^s m + 1}$ , i.e., the product of two  $(2^s)$ th-power residues is a  $(2^s)$ th-power residue, and the product of a  $(2^s)$ th-power residue with a  $(2^s)$ th-power nonresidue is a  $(2^s)$ th-power nonresidue. She also claims that the third part of theorem, the one about the product of two nonresidues, extends to  $(2^s)$ th-powers only if both nonresidues are  $(2^{s-1})$ th-power residues  $\pmod{2^s m + 1}$ .

### 9.3 Third letter

At the beginning of the *addendum*, Sophie Germain shows that a quaternary quadratic form

$$f := \begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b'''' \end{pmatrix},$$

of determinant  $D$  equal to zero, can be reduced to a ternary one. To this end she performs a long computation following the method used in the case of ternary quadratic forms. She put

$$F := \begin{pmatrix} \mathcal{A} & \mathcal{A}' & \mathcal{A}'' & \mathcal{A}''' \\ \mathcal{B} & \mathcal{B}' & \mathcal{B}'' & \mathcal{B}'''' \end{pmatrix}$$

which is the adjoint form of  $f$ , and expresses the coefficients of  $F$  in terms of those of  $f$ . Then, from  $D = 0$ , she gets  $\mathcal{A} = m\delta^2$ ,  $\mathcal{A}' = m\alpha^2$ ,  $\mathcal{A}'' = m\beta^2$ , and  $\mathcal{A}''' = m\nu^2$ ,

where  $m = \text{mcd}(\mathcal{A}, \mathcal{A}', \mathcal{A}'', \mathcal{A}''', \text{etc})$ . Hence, her proof does not hold for all quaternary quadratic forms with determinant zero but only for “general ones.”

Next, Germain observes: *under the same hypothesis for  $f$ , the adjoint  $F$  can be reduced to a perfect square multiplied by the maximal common divisors of its coefficients.* She also remarks that  $f(\delta, \alpha, \beta, v) = 0$ .

Let us stress that Gauss, in a handwritten note (Gauss 1917, Part I, pp. 86–88), used this fact to prove the reducibility of a ternary quadratic form of determinant zero to a binary one.

Then, Germain computes the adjoint of the adjoint  $F$  of a quaternary quadratic form  $f$  with  $D \neq 0$ :

$$\begin{pmatrix} aD^2 & a'D^2 & a''D^2 & a'''D^2 \\ bD^2 & b'D^2 & b''D^2 & b'''D^2 \end{pmatrix}$$

and observes that the determinant of  $F$  is  $D^3$ .

Following the case of ternary quadratic forms which Gauss discussed in art. 271 of the D.A., Sophie Germain observes: *the quaternary quadratic form  $f$  (with  $a \neq 0$ ) is definite, if the ternary quadratic form*

$$\begin{pmatrix} A^v & A''' & A'' \\ -B & -B' & -B'' \end{pmatrix},$$

*where  $b^v b^v - aa' = A^v$ ,  $ba - b''b''' = B$ ,  $b'''b''' - aa'' = A'''$ ,  $b'a - b''b^v = B'$ ,  $b''b'' - aa''' = A''$  and  $b'''a - b'''b^v = B''$ , is negative definite. In particular  $f$  is positive definite if  $a > 0$  and negative definite if  $a < 0$ .*

In fact, we have

$$af = (ax + b^v x' + b'''x'' + b''x'''^2) + (A^v x'^2 + A'''x''^2 + A''x'''^2 - 2Bx'''x'' - 2B'x'''x' - 2Bx''x').$$

By the results of art. 271, the conditions for  $\begin{pmatrix} A^v & A''' & A'' \\ -B & -B' & -B'' \end{pmatrix}$  (of determinant  $\mathfrak{D} \neq 0$ ) to be negative are  $B''^2 - A^v A''' < 0$ ,  $A^v \mathfrak{D}$  and  $A^v$  all  $< 0$ . Since, after some computation, we see that  $B''^2 - A^v A''' = a\mathcal{A}'''$  and  $\mathfrak{D} = -a^2\mathcal{D}$ , Germain finally obtains that those conditions reduce to  $A^v, a\mathcal{A}'''$ , and  $\mathfrak{D}$  are all  $< 0$ . She also proves that under these conditions, the adjoint  $F$  is definite. Thus, she concludes that if  $af$  is definite, then  $F$  is definite too, and, because  $\mathcal{A}''' < 0$ , if  $f$  is negative definite, then  $F$  is positive definite, and viceversa.

Next, Sophie Germain states a proposition on the representation of the determinant of a ternary quadratic form, similar to that in art. 280 of the D.A., as follows: *if the ternary quadratic form  $\begin{pmatrix} A & A' & A'' \\ B & B' & B'' \end{pmatrix}$ , of determinant  $\mathcal{D}$ , is represented by the quaternary quadratic form*

$$a \begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b''' \end{pmatrix},$$

with variables  $x = ps + mt + nu$ ,  $x' = p's + m't + n'u$ ,  $x'' = p''s + m''t + n''u$ ,  $x''' = p'''s + m'''t + n'''u$ , then  $\mathcal{D}$  is representable by the adjoint of that form.

She claims (as Gauss does in art. 280 of the D.A. for ternary quadratic forms) that this proposition can be easily proven by direct computation, but actually she only performs it in a particular case.

At the end of the *addendum*, on the basis of the earlier results, Sophie Germain conjectures that *an  $n$ -ary quadratic form with determinant equal to zero, can be always reduced, in  $n$  different ways, to an  $(n - 1)$ -ary quadratic form*. She verifies it by a direct computation in the case of quinary forms. Let us remark that, lacking a general theory of matrices and determinants, these computations are very long and impossible to perform in general.

Finally, in light of what she knows about ternary, quaternary, and quinary quadratic forms, she argues that *if  $\mathcal{D}$  is the determinant of an  $n$ -ary quadratic form  $f$ , then  $\mathcal{D}^{n-1}$  is the determinant of the adjoint form*.

Let us stress that this general result was proved by Cauchy some years later (Cauchy 1815, p. 82).

#### 9.4 Fourth letter

The first claim of Sophie Germain is

- (A) *Let  $n = 4k + 3$  be a prime, and suppose that  $N = x + y$  can be put in the form  $f^2 + nh^2$  with  $f, h$  being integers, then there are two integers  $F, H$  such that  $x^n + y^n = F^2 + nH^2$ .*

To prove this she argues as follows. She knows that from *addendum I*, the polynomial  $Y$ , of degree  $m = (n - 1)/2$ , which satisfies  $4\frac{x^n-1}{x-1} = Y^2 + nZ^2$ , is of the form  $Y = 2x^m + x^{m-1} + ax^{m-2} + \dots - ax^2 - x - 2$ . The same property holds true for the polynomial  $Y'$  in the equation  $4\frac{x^n+y^n}{x+y} = Y'^2 + nZ'^2$ , so  $Y' = 2x^m + x^{m-1}y + ax^{m-2}y^2 + \dots - ax^2y^{m-2} - xy^{m-1} - 2y^m$ . From this it is clear that, for any  $x, y$ , the value of  $Y'$  is divisible by 2. This is true also for  $Z'$ , as follows immediately from  $Z'^2 = (4X' - Y'^2)/n$  (here  $X' := \frac{x^n+y^n}{x+y}$ ). Then,  $\frac{x^n+y^n}{x+y} = (Y'/2)^2 + n(Z'/2)^2$ . To conclude, it is enough to remember the identity  $(a^2 + nb^2)(c^2 + nd^2) = (ac - nbd)^2 + n(ad + bc)^2$  (see also Waterhouse 1994, p. 142).

The second claim is the converse of (A), as follows:

- (B) *If  $x^n + y^n$  is of the form  $f^2 + nh^2$ , then  $x + y$  is of that form as well.*

Unfortunately, this assertion does not hold: in fact her proof, based on the theory developed by Gauss in art. 235 of the D.A., is valid for “forms” and not for “numbers.” In his response to the letter, Gauss provides a numerical counterexample and explains how  $x + y$  cannot be of the prescribed form, and adds that the proposition holds true under the restriction that  $x + y$  be a prime number. For a complete proof of this fact and a generalization, see Genocchi (1884a, p. 247). Gauss’s counterexample is also discussed in MacKinnon (1990) and Waterhouse (1994). Next, Germain considers the analogue of proposition (A) for the case of primes  $n = 4k + 1$ . In this case, one has to take into account equation  $4\frac{x^n-1}{x-1} = Y^2 - nZ^2$ ,

quadratic forms of type  $f^2 - nh^2$  instead of  $f^2 + nh^2$ , and consider the identity  $(a^2 - nb^2)(c^2 - nd^2) = (ac + nbd)^2 - n(ad + bc)^2$ .

She erroneously claims that the analogue of (B) holds true.

Finally, she asserts (without proof) that propositions (A) and (B) can be extended to the case of Eq. (9.2).

### 9.5 Fifth letter

In the kind and lengthy response to Germain's fourth letter—the one in which she revealed her true identity—Gauss stated two theorems are “linked,” as he wrote, “to delicate research” concerning the theory of cubic and biquadratic residues, a theory that, he added, “I developed in the past winter to the same degree of perfection as that of quadratic residues.” Precisely,

- I. *Let  $p$  be a prime number of the form  $3n + 1$ . I claim that  $2$  (i.e.,  $+2$  and  $-2$ ) is cubic residue of  $p$ , if  $p$  can be reduced to the form  $xx + 27yy$ , and that  $2$  is not cubic residue of  $p$  if  $4p$  can be reduced to the same form.*
- II. *Le  $p$  be a prime number of the form  $8n + 1$ . I claim that  $+2$  and  $-2$  are biquadratic residues or nonresidues of  $p$ , depending on whether  $p$  is or is not of the form  $xx + 64yy$ .*

In the same letter, Gauss also stated a theorem regarding quadratic residues, “whose proof,” he remarked, “is less hidden [than the others], I will not include it here to not deprive you of the pleasure of finding it by yourself”:

*Let  $p$  be a prime number and denote by  $A$  and  $B$  (respectively) the two sets  $\{1, 2, 3, 4, \dots, (p-1)/2\}$  and  $\{(p+1)/2, (p+3)/2, (p+5)/2, \dots, p-1\}$ . Let  $a$  be any integer not divisible by  $p$ . Consider the minimal residues (mod  $p$ ) of all numbers in  $A$  multiplied by  $a$  and let  $\alpha$  be the number of those belonging to  $A$ ,  $\beta$  the number of those belonging to  $B$ , so that  $\alpha + \beta = (p-1)/2$ . I claim that  $a$  is a quadratic residue of  $p$  if  $\beta$  is even, and it is not a quadratic residue of  $p$  if  $\beta$  is odd.*

This theorem, today known as “Gauss's lemma,” gives a condition for an integer to be a quadratic residue, and is of great theoretical significance. Gauss used this result to produce a new proof of his “fundamental theorem” in Gauss (1808). In fact a few weeks after having replied to Germain, Gauss wrote to Olbers (Schilling 1990, pp. 359–360):

Neulich, als ich ihr antwortete und einige Arithmetica mittheilte, wurde ich dadurch veranlasst, wieder eine Untersuchung vorzunehmen und gleich zwei Tage nachher gelang mir eine äusserst angenehme neue Entdeckung. Es ist eine neuer sehr zierlicher und kurzer Beweis des Fundamentalsatzes Art. I (sic) [8, 9, 12 Mai 1807] [Recently, when I replied to a letter of hers, explaining some Arithmetic, I undertook to study again the question and, two days later, I made a very pleasant discovery. This is a new, very elegant proof of the fundamental proposition of Art. I (sic)].

A month later, with her fifth letter, Sophie Germain submitted the proofs of these theorems and some of her own findings to Gauss. She wrote “I had already tried to examine residues of higher powers than squares, but I have not been able to penetrate this theory, which remains the object of my curiosity. Therefore here is the small number of propositions I have reached.” Among them, we consider the following two.

- (1) *Let  $p$  be a prime, and  $q$  a natural number. If  $(q, p - 1) = 1$ , then all numbers in the sequence  $1, 2, \dots, p - 1$  are  $q$ th-power residues. On the contrary if  $p - 1 = qs$ , then in the sequence  $1, 2, \dots, qs$  there are  $s$  residues and  $p - s - 1$  nonresidues (mod  $p$ ).*

We observe that the “contrary” of the previous case  $(q, p - 1) = 1$  should be  $d = (q, p - 1) \neq 1$ . For this case, see Sierpiński (1964, Theorem 14 at p. 257) where it is proved that the number of different residues is  $(p - 1)/d + 1$  (including 0), and so Germain’s second claim is a particular case of this result, while the first is an immediate corollary (see Sierpiński 1964, p. 258).

- (2) *The product of two  $q$ th-power residues (mod  $p = qs + 1$ ) is a  $q$ th-power residue same modulo. In general, the product of  $a \equiv r^m$  and  $b \equiv r^n$ ,  $r$  primitive root, is a residue or a nonresidue depending on whether or not  $(m + n) \equiv 0 \pmod{q}$ .*

In the *addendum* to her letter she expounded the “proofs” of Gauss’s theorems.

The proof of theorem I seems to be correct. Let  $p = 3n + 1$  be a prime number, so that  $n$  is even. Let, as in the D.A. art. 358 (Gauss 1801, 1863a, p. 445),  $g$  be a primitive root modulo  $p$  and denote by  $\mathcal{R}$  the set of minimal residues of  $g^3, g^6, \dots, g^{p-4}$  together with 1, by  $\mathcal{R}'$  the set of minimal residues of  $g, g^4, \dots, g^{p-3}$ , and by  $\mathcal{R}''$  the set of minimal residues of  $g^2, g^5, \dots, g^{p-2}$ . Let  $(\mathcal{R}\mathcal{R})$  be the number of integers in the set  $\{1, 2, \dots, p - 1\}$  such that  $h \in \mathcal{R}$  and  $h + 1 \in \mathcal{R}$ ,  $(\mathcal{R}\mathcal{R}')$  the number of those that  $h \in \mathcal{R}$  and  $h + 1 \in \mathcal{R}'$ , and similarly  $(\mathcal{R}\mathcal{R}'')$ ,  $(\mathcal{R}'\mathcal{R}'')$ , and so on. Let  $a = (\mathcal{R}\mathcal{R}'')$ ,  $b = (\mathcal{R}\mathcal{R}')$ ,  $c = (\mathcal{R}'\mathcal{R}'')$ . One has  $n = a + b + c$  and  $(\mathcal{R}\mathcal{R}) = a - 1$ . In art. 358 (p. 447), it is proved that  $4p = (6a - 3b - 3c - 2)^2 + 27(b - c)^2$ . If  $p = x^2 + 27y^2$  (so  $x, y$  are of different parity), then it follows that  $6a - 3b - 3c - 2 = 2x$ , and  $b - c = 2y$ . From  $n = a + b + c$ , if  $b + c$  is even,  $a$  is also even, so  $(\mathcal{R}\mathcal{R}) = a - 1$  is odd. In general if  $h, h + 1$  are in  $\mathcal{R}$ , then  $p - h - 1$  and  $p - h$  are in  $\mathcal{R}$ , so  $(\mathcal{R}\mathcal{R})$  is even unless  $p - h - 1 = h$ , i.e.,  $p - 1 = 2h$  and, concludes Germain, since  $p - 1$  is a cubic residue, 2 is also a cubic residue.

In the *addendum* to her letter, Sophie Germain also gave a proof of theorem II, a “proof” she wrote, “that requires several preambles, since in the D.A., there is no result that can be used directly.”

She follows the route traced by Gauss in art. 358 of the D.A., in the case in which the roots are divided into three periods. Let  $g$  be a primitive root for the prime modulo  $p = 8n + 1$ , and denote the four periods  $(2n, 1)$ ,  $(2n, g)$ ,  $(2n, g^2)$ , and  $(2n, g^3)$  by  $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}''$ , and  $\mathfrak{p}'''$  respectively. We have  $\mathfrak{p} = \{[1], [g^4], \dots, [g^{p-5}]\}$ ,  $\mathfrak{p}' = \{[g], [g^5], \dots, [g^{p-4}]\}$ , and so on. Also, let  $\mathcal{R}$  denote the set of the minimal remains of the powers  $g^4, g^8, \dots, g^{p-5}$  including 1,  $\mathcal{R}'$  the set of the minimal remains of the powers  $g, g^5, \dots, g^{p-4}$ , and similarly, define  $\mathcal{R}''$ ,  $\mathcal{R}'''$ . Clearly, these sets are mutually disjoint, and their union is the set  $\{1, 2, 3, \dots, p - 1\}$ . We have that  $p - 1$  is in  $\mathcal{R}$  and both  $h$  and  $p - h - 1$  belong to the same set among  $\mathcal{R}, \mathcal{R}', \mathcal{R}''$ , and  $\mathcal{R}'''$ . Again as in art. 358 of the D.A., denote by  $(\mathcal{R}\mathcal{R})$  the number of those integers  $h$  in

the set  $\{1, 2, \dots, p - 1\}$  such that  $h \in \mathfrak{K}$  and also  $h + 1 \in \mathfrak{K}$ . Denote by  $(\mathfrak{K}\mathfrak{K}')$  the number of those integers  $h$  such that  $h \in \mathfrak{K}$  and  $h + 1 \in \mathfrak{K}'$ , and similarly define the numbers  $(\mathfrak{K}\mathfrak{K}''), (\mathfrak{K}\mathfrak{K}'''), \dots, (\mathfrak{K}''\mathfrak{K}'''), (\mathfrak{K}'''\mathfrak{K}'''')$ .

Since  $-1$  is biquadratic residue for the modulus  $p = 8n + 1$ , we have  $(\mathfrak{K}\mathfrak{K}') = (\mathfrak{K}'\mathfrak{K})$ ,  $(\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K})$ ,  $\dots$ ,  $(\mathfrak{K}''\mathfrak{K}''') = (\mathfrak{K}'''\mathfrak{K}'')$ .  $\mathfrak{K}$  is the set of all biquadratic residues  $(\bmod p)$ . If  $h$  and  $h + 1$  are in  $\mathfrak{K}$  also  $p - h$  and  $p - h - 1$  are in  $\mathfrak{K}$ , then  $(\mathfrak{K}\mathfrak{K})$  is always even unless there exists  $h \in \mathfrak{K}$  such that  $p - h - 1 = h$ , i.e.,  $(p - 1)/2 = h$ , which means  $(p - 1)/2$  is a biquadratic residue. In this case, since  $p - 1$  is a biquadratic residue,  $2$  must be a biquadratic residue.

Thus, Germain's strategy for proving theorem II was to prove that  $(\mathfrak{K}\mathfrak{K})$  is always odd when  $p = 8n + 1$  is of the form  $x^2 + 64y^2$ . She proceeds as follows.

Let  $a := (\mathfrak{K}\mathfrak{K})$ ,  $b := (\mathfrak{K}\mathfrak{K}')$ ,  $c := (\mathfrak{K}\mathfrak{K}'')$ ,  $d := (\mathfrak{K}\mathfrak{K}''')$ ,  $e := (\mathfrak{K}'\mathfrak{K}')$ ,  $f := (\mathfrak{K}''\mathfrak{K}')$ ,  $d' := (\mathfrak{K}'\mathfrak{K}'')$ ,  $e' := (\mathfrak{K}'\mathfrak{K}''')$ ,  $e'' := (\mathfrak{K}''\mathfrak{K}''')$ ,  $b' := (\mathfrak{K}'''\mathfrak{K}'''')$ . With the 16 numbers  $(\mathfrak{K}\mathfrak{K}), (\mathfrak{K}\mathfrak{K}'), \dots, (\mathfrak{K}'\mathfrak{K}), \dots, (\mathfrak{K}''\mathfrak{K}''')$  we can construct the following matrix:<sup>34</sup>

$$\begin{pmatrix} a & b & c & d \\ b & d' & e & e' \\ c & e & f & e'' \\ d & e' & e' & b' \end{pmatrix}.$$

Moreover, for the nature of the numbers  $a, b, c, \dots, b'$ , we have the following obvious relations among them:

$$\begin{aligned} 2n - 1 &= a + b + c + d \\ 2n &= d' + b + e + e' \\ 2n &= f + c + e + e'' \\ 2n &= b' + d + e' + e'' \end{aligned}$$

By developing, as in art. 345 (see also art. 358) of the D.A., the products of two, three and four periods she gets a number of relations among the numbers  $a, b, c, \dots, b'$  (see the transcription of the *addendum* in the appendix), so that the matrix above can be reduced to the form:

$$\begin{pmatrix} a & b & c & d \\ b & d & e & e \\ c & e & c & e \\ d & e & e & b \end{pmatrix}.$$

<sup>34</sup> Germain does not introduce this matrix, but we think this will be useful for the reader comparing her proof with that of Gauss (Gauss 1828, art. 15–20). See the next subsection in which we compare the two proofs.

Thus, the relations above become

$$\begin{aligned} 2n - 1 &= a + b + c + d \\ 2n &= b + d + 2e \\ n &= c + e, \end{aligned}$$

and we also have  $b - d = 2(c - d)$ .<sup>35</sup> In performing this reduction, she obtains also the relation:

$$ec + e^2 = (2c - 2d)c + d^2 + e(2e - c - 1),$$

from which one easily deduces

$$4(8n + 1) = 64(c - e)^2 + 32(c - e) + 4 + 64(c - d)^2$$

or, equivalently,

$$p = 8n + 1 = [4(c - e) + 1]^2 + 16(c - d)^2.$$

From this, if  $p = x^2 + 64y^2$ , we must have  $x = 4(c - e) + 1$  and  $2y = c - d$ . Thus, the question is reduced to prove that  $a$  is odd when  $c - d$  even.

To this end, let us observe that 2 and  $4n = (p - 1)/2$  are quadratic residues for  $p = 8n + 1$ .<sup>36</sup> This means that, remarks Germain, there is an odd number, say  $Q$ , of integers  $h$  in the sequence 1, 2, ...,  $p - 1$  such that  $h, h + 1$  are quadratic residues  $(\bmod p)$ . In fact, on the contrary, an  $h$  exists satisfying the equation  $h = (p - 1)/2$ , i.e.,  $h = 4n$  and then  $4n$  would be a nonresidue.

Suppose  $h$  and  $h + 1$  are quadratic residues, then either  $h, h + 1 \in \mathfrak{K}$ , or  $h, h + 1 \in \mathfrak{K}''$  or one of those is in  $\mathfrak{K}$  and the other is in  $\mathfrak{K}''$ . She claims that  $Q = (\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}'') + (\mathfrak{K}''\mathfrak{K}'') = a + c + d$ , and then she concludes that, since  $c + d$  must be even,  $a$  is necessarily odd. Unfortunately, the last claim is false, as she recognizes in the subsequent sixth letter to Gauss, where she correctly writes  $Q = (\mathfrak{K}\mathfrak{K}) + 2(\mathfrak{K}\mathfrak{K}'') + (\mathfrak{K}''\mathfrak{K}'') = a + 3c$ , and gave another argument to conclude her proof.

We postpone the examination of the amended version for when we discuss the sixth letter.

In the *addendum*, Germain also gave a proof of the third theorem, which is substantially identical to that published by Gauss in *Theorematis arithmeticci demonstratio nova* (Gauss 1808).

To Germain's fifth letter, written on June 27, 1807, Gauss responded after 7 months, but on July 21, after a journey that had led him to Nienburg, Hannover, and Bremen (where he visited Olbers); after having returned home, he wrote this letter (Schilling 1990, pp. 376–377):

<sup>35</sup> Germain does not observe this.

<sup>36</sup> D.A., Section 4, art. 94–114.

Bei meiner Zurückkunft habe ich hier einige Briefe aus Paris vorgefunden von Bouvard, Lagrange und Sophie Germain. [...] Lagrange interessirt sich noch mit vieler Wärme für die Astronomie und höhere Arithmetik; die beiden Probe-Theoreme (in welchen Primzahlen 2 ein kubischer oder ein biquadratischer Rest ist) die ich auch Ihnen vor einiger Zeit mittheilte, hält er für “ce qu’il peut y avoir de plus beau et de plus difficile à demontrer.” Aber die Sophie Germain hat mir die Beweise derselben geschickt; noch habe ich sie zwar nicht durchgehen können, ich glaube aber, dass sie gut sind; wenigstens hat sie die Sache von der rechten Seite angegriffen, nur etwas weitläufiger sind sie als nöthig sein wird [On my return I found several letters from Paris, from Bouvard, Lagrange, and Sophie Germain. [...] Lagrange still shows great interest in astronomy and higher arithmetic, he considers the two theorems (for which primes 2 is a cubic or a biquadratic residue) which I told you about some time ago, “what one can have that is most beautiful and difficult to prove.” But Sophie Germain has sent me the proofs of them; although I have not yet been able to look carefully through them, I think they are good, at least she has approached the problem in the right direction, they are only somewhat longer than they need be.]

We do not know if Gauss found the time to read Germain’s proofs of his theorems carefully, especially that of theorem II, but on September 2, 1808, writing to Bolyai, he confirmed his great esteem for her (Schmidt and Stäckel 1899, pp. 93–94):

Von Personen, die jenes Werk mit Erfolg studirt hätten, kenne ich bis jetzt nur wenige; oben an steht die Demoiselle Sophie Germain in Paris (habe ich dir von ihr geschrieben?) ein gewisser Poulet-de-l’Isle in Orleans hat es ins französische übersetzt, Lagrange hat einen Paragraph in der neuen Auflage seines *Traité de la resolution numerique des equations* commentirt, indess auf eine Art der ich nicht in allen Stücken meinen Beifall geben kann ... [I know very few people who have studied this work [the D.A.] with profit, above all Miss Sophie Germain of Paris (have I written to you about her?), a certain Poulet-de- l’Isle of Orleans, who translated my work into French, Lagrange commented on it in a section of his work *Traité de la resolution numerique des equations*, although in a way that I do not completely agree with ...].

## 9.6 Sixth letter

First of all, we examine the revised version of the proof of theorem II.

Let us recall that Germain aims to prove that  $a = (\mathfrak{K}\mathfrak{K})$  is always odd when  $p = 8k + 1$  is of the form  $x^2 + 64y^2$ . To this end, Germain goes back to the equations

$$2n - 1 = a + b + c + d, \quad 2n = b + d + 2e,$$

and she observes that among the numbers  $a, b, c$ , and  $d$  only one is odd and the others are even. This does not seem justified at this point, but in the continuation of the letter (see below) she affirms that, since only one among  $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}'',$  and  $\mathfrak{K}'''$  contains 2, only one among  $a = (\mathfrak{K}\mathfrak{K}), b = (\mathfrak{K}\mathfrak{K}'), c = (\mathfrak{K}\mathfrak{K}''),$  and  $d = (\mathfrak{K}\mathfrak{K}''')$  is odd. Hence, to finish her proof, she claims that, since  $c - d$  is even (because  $c - d = 2y$ ), both  $c$  and

$d$  must be even and, by the second equation above,  $b$  is also even. Therefore, from the first equation,  $a$  must be odd.

Let us show that, at this point, she could have completed the proof of theorem II precisely as at the end of Gauss's proof.

From the first equation, we have

$$a = 2n - 1 - b - c - d$$

and with some computation, we obtain

$$8a = 4n - 3[4(c - e) + 1] - 5$$

which can be put in the form:

$$16a = 8n + 1 - 6[4(c - e) + 1] - 11$$

When  $p = 8n + 1$  is of the form  $x^2 + 64y^2$ , as we have seen in discussing the fifth letter, we must have  $x = 4(c - e) + 1$  and  $c - d = 2y$ . Hence, from above, putting  $q := c - e$  and  $r = c - d$ , we easily obtain

$$a = q^2 - q - 1 + r^2,$$

and since  $q^2 - q$  is always even and  $r$  is also even, it follows that  $a$  is odd as required.

Gauss, after having proved theorem II, commented as follows (Gauss 1828, Sect. 22):

In *Disquisitiones Arithmeticae* theoriam generalem divisionis circuli, atque solutionis aequationis  $x^p - 1 = 0$  explicavimus, interque alia docuimus, si  $\mu$  sit divisori  $p - 1$ , functionem  $(x^p - 1)/(x - 1)$  in  $\mu$  factores ordinis  $(p - 1)/\mu$  resolvi posse adiumento aequationis auxiliaris ordinis  $\mu$ . Prater theoriam generalem huius resolutionis simul casus speciales, ubi  $\mu = 2$  vel  $\mu = 3$ , in illo opere artt. 356 — 358 seorsim consideravimus, aequationemque auxiliarem a priori assignare docuimus, i.e., absque evolutione schematis residuorum minimorum potestum alicuius radicis primitiae pro modulus  $p$ . Iam vel nobis non monentibus lectores attenti facile percipient nexus arctissimus casus proximi istius theoriae, puta pro  $\mu = 4$ , cum investigationibus hic in artt. 15–20 explicatis, quarum adiumento ille quoque sine difficultate complete absolvvi poterit. [In the D.A., we have presented the general theory of the division of the circle and the solution of the equation  $x^p - 1 = 0$ , and demonstrated, among other things, that if  $\mu$  is a divisor of the number  $p - 1$ , the function  $(x^p - 1)/(x - 1)$  can be decomposed into  $\mu$  factors of order  $(p - 1)/\mu$ , with the aid of the auxiliary equation of order  $\mu$ . Out of the general theory of these solutions, we have considered separately the special cases where  $\mu = 2$  or  $\mu = 3$ , in articles 356–358 of the work, and we have learned to establish the auxiliary equation a priori, i.e., without the development of the schema of the least residues of the powers of some primitive root of the modulus  $p$ . Now, without our having to refer to that, the attentive reader will recognize the close dependence of the next case of that theory, i.e., the case  $\mu = 4$ , on the investigation here laid out in articles

15–20, with the aid of which this case can be determined completely without any difficulty.]

This is precisely the path followed by Sophie Germain.

In her sixth letter to Gauss, Germain gave a new method for finding the first relations among the quantity  $a, b, c, \dots, b'$  which avoids the long computation of the products of the periods. This is a very interesting part of the letter, but, at the same time, her explanations are very difficult to follow, in view of being extremely concise. Hence, we are not sure if we have completely understood her argument.

Let  $P = 2Q + 1 = 2Nn + 1$  be a prime number, then  $-1$  is a quadratic residue as well as an  $n$ -power residue  $(\bmod P)$ . Let  $S$ , and  $T$  be any two positive numbers less than  $2Q$ , and  $r$  be a primitive root for the modulo  $P$ . The solutions of the equation  $r^S + 1 = r^T$  are as many as the solutions of the congruence  $1 + r^S + r^T \equiv 0 \pmod{P}$ . Since we have  $r^{2Q} \equiv 1 \pmod{P}$  and  $r^Q \equiv -1 \pmod{P}$ , from the congruence  $-r^S - r^T \equiv -1 \pmod{P}$  (and forgetting  $(\bmod P)$ ), we have

$$r^{Q+T-S} - r^{-S} \equiv 1.$$

If we write  $Y, Y'$  for  $-S, -T$ , we obtain

$$r^{Q+Y-Y'} - r^Y \equiv 1.$$

From this congruence, we easily get the following five equations as well:

$$\begin{aligned} r^{Q+Y'-Y} - r^{Y'} &\equiv 1, \\ r^{Q+Y} - r^{Y-Y'} &\equiv 1, \\ r^{Q+Y'} - r^{Y'-Y} &\equiv 1, \\ r^{Q-Y} - r^{2Q-Y'} &\equiv 1, \\ r^{Q-Y'} - r^{2Q-Y} &\equiv 1. \end{aligned}$$

From any one of the above six congruences, we can obtain the other five. Let us denote by  $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}'', \mathfrak{K}''', \dots$  the periods containing the  $n$ th,  $(n+1)$ th,  $(n+2)$ th,  $(n+3)$ th, etc. powers of the primitive root, and by  $[\mathfrak{K}\mathfrak{K}'], [\mathfrak{K}\mathfrak{K}''],$  etc. the number of congruences that belong to the same system of six, first member of which is the difference between an  $n$ th-power and an  $(n+1)$ th-power, an  $n$ th-power and an  $(n+2)$ th-power, etc. Then, by solving  $Y = yn + \delta$  and  $Y' = yn + \delta'$ , we obtain  $[\mathfrak{K}\mathfrak{K}^\delta] = [\mathfrak{K}^{n-\delta}\mathfrak{K}^{n-\delta}]$ . Since each system containing the difference of the  $n$ th and  $(n+\delta)$ th powers gives the same equation, it follows that  $(\mathfrak{K}\mathfrak{K}^\delta) = (\mathfrak{K}^{n-\delta}\mathfrak{K}^{n-\delta})$ , where  $(\mathfrak{K}\mathfrak{K}^\delta)$ , etc., denotes the number of numbers in  $\mathfrak{K}$  which, increased by 1, belong to  $\mathfrak{K}^\delta$ , etc.

Since only one among  $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}'', \mathfrak{K}''', \dots$  contains 2, these conditions imply that only one of the numbers  $(\mathfrak{K}\mathfrak{K}^\delta)$  is odd.<sup>37</sup>

<sup>37</sup> This is the justification for the claim, made above: “among the numbers  $a, b, c$ , and  $d$ , only one is odd”.

If we now take  $Y = yn + d$  and  $Y' = yn + \delta'$ , we obtain, by a similar reasoning that  $(\mathfrak{K}^{n+d-\delta}\mathfrak{K}^{n+d}) = (\mathfrak{K}^{n-d}\mathfrak{K}^{n-\delta}) = (\mathfrak{K}^{n+\delta-d}\mathfrak{K}^{n+\delta})$ .

We can also see that, considering the systems of the six congruences, that  $(\mathfrak{K}, \mathfrak{K})$  is either of the form  $6h + 3$  or of the form  $6h$ , depending on whether 2 is an  $n$ th-power residue or nonresidue.

For  $n = 4$ , as in the case of the theorem II, she gets the conditions:

$$(\mathfrak{K}\mathfrak{K}') = (\mathfrak{K}'''\mathfrak{K'''}), \quad (\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}''), \quad (\mathfrak{K}\mathfrak{K}''') = (\mathfrak{K}'\mathfrak{K}')$$

and

$$(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}''') = (\mathfrak{K}'''\mathfrak{K}'),$$

already obtained by confronting the different forms of the same products of periods, namely:  $b = b'$ ,  $c = f$ ,  $d = d'$ , and  $c = e' = e''$ .

The case  $n = 2$  gives Germain a new proof that 2 is quadratic residue for the primes of the form  $8n + 1$  and  $8n + 7$ , and nonresidue for primes of the form  $8n + 3$  and  $8n + 5$ .<sup>38</sup>

Germain's new approach to the last part of the proof of theorem II seems to be a generalization of what Gauss developed, and which we have summarized in the previous section (see Gauss 1828, art. 17).

## 9.7 Seventh letter

Germain was certainly fascinated by the theory of cubic and biquadratic residues, but in this letter, she expresses the strong belief that a reciprocity law, analogous to Gauss's fundamental theorem, does not exist for cubic and biquadratic residues. She bases her conviction on the differences observed between these power residues and the quadratic residues. In fact, in the letter, she writes: "although is true that every number which is not a positive square is a quadratic nonresidue for the modulo  $2k + 1$ , it is not true that every number which is not a positive quartic power is a biquadratic nonresidue for some prime numbers of the form  $4k + 1$ . In fact,  $-4$  is biquadratic residue for all these numbers, since  $-1$  and  $4$  are either both biquadratic residues or both simply quadratic residues. Actually I think that  $4$ , taken with the minus sign, is the only square which is a biquadratic residue for all prime of the form  $4k + 1$ ."

Germain's skepticism, though not entirely justified, is understandable. As we know, it took some years before Gauss was able to state the biquadratic reciprocity law, and it required the introduction of complex numbers into arithmetic (Gauss 1828a, 1917, pp. 65–69).

Let us show how Germain proves the above:

(1)  $-4$  is biquadratic residue for the prime numbers of the form  $4k + 1$ .<sup>39</sup>

<sup>38</sup> Gauss also gave a new proof of this result in Gauss (1808).

<sup>39</sup> Lemmermeyer in his article (Lemmermeyer 2000, p. 256) refers to this result as "Germain's result," quoting Genocchi.

Let  $g$  be a primitive root for the prime  $p$  of the form  $8k + 1$  or  $8k + 5$ , then  $g^{(p-1)/2} = g^{4k} \equiv -1 \pmod{p}$  or  $g^{(p-1)/2} = g^{4k+2} \equiv -1 \pmod{p}$ . In the first case, 2 is a quadratic residue, so  $2 \equiv g^{2n} \pmod{p}$  and so  $4 \equiv g^{4n} \pmod{p}$ . Taking into account that  $-1$  is biquadratic residue, one obtains  $-4 \equiv g^{4(k+n)} \pmod{p}$ , and hence  $-4$  is a biquadratic residue. In the second case, 2 is not a quadratic residue, so  $2 \equiv g^{2n-1} \pmod{p}$ , and this implies that  $4 \equiv g^{4n-2} \pmod{p}$ . Taking into account that  $-1$  is biquadratic residue, one again has  $-4 \equiv g^{4(k+n)} \pmod{p}$ . In both cases,  $-4$  is a biquadratic residue.

In this letter, Germain proves other interesting theorems on biquadratic residues that we now present.

- (2) *Any odd square  $(2h + 1)^2$  taken with the minus sign is not a biquadratic residue for any prime of the form  $8k + 5$ .*

Let us follow her proof. The number  $N := (2h + 1)^2 + 4$  is the sum of two coprime squares and is of type  $8k' + 5$ . If  $N$  is not a prime, then any prime factor must be the sum of two squares, so it is necessarily of the forms  $8k + 1$  and  $8k + 5$ . Let  $p$  be a divisor of the form  $8k + 5$ , then  $N \equiv -4 \pmod{p}$ . On the other side (as above),  $2 \equiv g^{2n-1} \pmod{p}$  and  $g^{4k+2} \equiv -1 \pmod{p}$ ; hence,  $4 \equiv g^{4n-2} \pmod{p}$ ,  $-N \equiv 4 \equiv \pmod{p}$ . Since  $N \equiv -4 \equiv g^{4(k+n)} \pmod{p}$ , it follows that  $N$  is a biquadratic residue of  $p$ , and  $-N$ , being congruent to an even power of  $g$  but not divisible by 4, is a quadratic residue but not a biquadratic residue.

From these theorems, Germain deduces the following.

Let  $n^2$  be the maximal square in  $k$ , so that  $k = n^2q$  and  $q$  is free from squares. Because  $-4n^2q \equiv 1 \pmod{p}$ ,  $-4n^2q$  is an  $m$ th-power residue  $\pmod{p}$  for any  $m$  and so,  $-4$  being a biquadratic residue mod  $p$ ,  $n^2q$  is also a biquadratic residue  $\pmod{p}$ . It follows from  $p = 4n^2q + 1$  that for any odd prime factor  $r$  of  $n$ , one has  $p \equiv 1 \pmod{r}$  and so, by the quadratic reciprocity law,  $r$  is quadratic residue  $\pmod{p}$ . If 2 is a divisor of  $n$ , then  $p$  is of type  $8k + 1$ , and so 2 is a quadratic residue  $\pmod{p}$ . Hence,  $n^2$  is a biquadratic residue  $\pmod{p}$ . Hence,  $n^2$  and  $n^2q$  being biquadratic residues;  $q$  is also biquadratic residue  $\pmod{p}$ , and taking  $q = 2$ , she correctly deduces

- (A) *2 is a biquadratic residue for primes of type  $8n^2 + 1$ .*

Then she claims

- (B) *a number of the form  $8n^2 + 1$  may be prime only if  $n^2$  satisfies the equation  $n^2 = (y^2 + y)/2 + 8x^2$ .*

This holds true, as observed in Genocchi (1884a). In fact—in *Theoria residuorum biquadraticorum, commentatio prima* (1828)—Gauss proves that  $\pm 2$  is a biquadratic residue for primes of type  $p = 8k + 1$ . Gauss gets this by reducing  $p$  to the forms  $g^2 + 2h^2$  and  $e^2 + f^2$  then, one has that  $\pm 2$  are biquadratic residues of  $p$  when  $g$  is of the form  $8m \pm 1$ , and are nonresidues when  $g$  is of the form  $8m \pm 5$ . Also, one has that  $\pm 2$  are biquadratic residues of  $p$  when, assuming  $f$  even and  $e$  odd,  $f$  is of the form  $8m$ , and are nonresidues when  $f$  is of the form  $8m + 4$ . As the prime  $p = 8n^2 + 1$  corresponds to  $g = 1$  and  $h = 2n$ , for the first criterion, it actually has  $\pm 2$  among its biquadratic residues. The same number  $p$  is the sum of two squares  $e^2 + f^2$ , where we can suppose  $e = 2y + 1$ , and necessarily  $f = 8m$ ,  $\pm 2$  being biquadratic residues. Then, if we put  $f = 8x$ , we have  $8n^2 + 1 = (2y + 1)^2 + 64x^2$ ,

which is Germain's assertion. Gauss's result was not available to Germain in 1809, and so she likely deduced the above equation from theorem II: as proved by Germain, since 2 is a biquadratic residue of primes  $p = 8n^2 + 1$ , according to theorem II,  $p$  can be put in the form  $v^2 + 64x^2$  where, necessarily,  $v = 2y + 1$ , and the required equation follows immediately.

Let us remark that from Germain's result (A), we can deduce that 2 is a biquadratic residue for many primes not of the form  $8n^2 + 1$ , as the following example shows. We have  $20^4 \equiv -8 \pmod{113}$ ; so  $-8$  is a biquadratic residue of 113, (recall Gauss's example); since 113 is of the form  $4k + 1$ , by the first theorem of Germain, we have that  $-4$  is a biquadratic residue of 113, and so, since  $-8 = -4 \times 2$ , 2 is also a biquadratic residue of 113.

Genocchi (1884b), reviewed Germain's results on biquadratic residues very positively, and of the theorem of point (2) above he wrote: "I do not know of printed books where this theorem is proved or even stated."

In spite of Genocchi's review, she was never credited for them, and in Dickson (1971) there is no trace of Germain's theorems on biquadratic residues.

## 9.8 Eighth, ninth, and tenth letter

Germain wrote her eighth letter to Gauss to inform him that she had just received the awaited copy of his work on planetary motion from Germany. She admired the clearness that pervaded all of the work and, at the same time, the simplicity with which the computations were performed. She said this was very useful for practical purposes. She ended the letter with a *post scriptum* in which she renewed the desire to know more about Gauss's results on biquadratic residues.

The ninth letter to Gauss was written in May of 1819.

She had received a visit from Schumacher, who had brought her a copy of Gauss's paper, *Theorematis fundamentalis in doctrina residuis quadraticis, demonstrationes et applicationes novae* (Gauss 1818). This encouraged Sophie Germain to try renewing, after an interlude of ten years, the epistolary exchange with Gauss.

The lengthy letter is very interesting in many respects, but mainly because, as we will see, she describes the progress she had made on FLT since 1804.

She confessed that during her studies and experiments on the theory of vibrating surfaces, she never stopped thinking about number theory, "a field" she writes "that I prefer, even without any hope of success, to a work which produces results almost automatically." As we know, she had started to think about FLT, which to her eyes appeared a challenge by an ancient geometer, during her first reading of the D.A., when immediately she perceived a connection between Fermat's equation and the theory of congruences and power residues.

In the years of her correspondence with Gauss, she probably went much deeper into those studies, although, after her first letter, she had never returned to this subject with him. The contest and the prize established by the French Academy for the best work on FLT in late 1815—and renewed in 1818—probably was an opportunity to reconsider her old writing on Fermat's equation.

Germain continues her letter by explaining, with some details, her plan for addressing FLT, not just for a single or isolated exponent  $p$ , but—for the first time in history—an entire class of them.

Before we go on to briefly describe her plan,<sup>40</sup> it is useful to state Germain's theorem on the first case of FLT (see for instance Ribenboim 1999, p. 109 and following).<sup>41</sup>

*For an odd prime  $p$ , if there exists an auxiliary prime  $\theta$  such that there are no two nonzero consecutive  $p$ th-power residues (mod  $\theta$ ), nor is  $p$  itself a  $p$ th-power residue for the same modulus, then for any solution of  $x^p + y^p = z^p$  the product  $xyz$  must be divisible by  $p$ .*

If the equation  $x^p + y^p = z^p$  is impossible, i.e., it does not have nontrivial integer solutions, then every prime number  $\theta$  of the form  $2Np + 1$ , for which there are no two consecutive  $p$ th-power residues in the sequence of natural numbers, necessarily divides one of the numbers  $x$ ,  $y$  or  $z$ . In fact, if  $r$  is a primitive root, this equation yields the congruence  $1 \equiv r^{sp} - r^{tp} \pmod{\theta}$  with  $s, t$  integers, which implies the existence of two consecutive  $p$ th-power residues (mod  $\theta$ ). It follows that if there are infinitely many such primes  $\theta$ , Fermat's equation would be impossible, because one of the numbers  $x$ ,  $y$ , and  $z$  would be larger than any given number.

Let us observe that, to prove the first case of FLT, the existence of only one such auxiliary prime is required.

Germain's plan for proving FLT for the exponent  $p$  was then hinged on the development of a method capable of producing infinitely many  $\theta = 2Np + 1$  for which: (N–C) *there are no two nonzero consecutive  $p$ th-power residues mod  $\theta$* . But, as she writes to Gauss, she had never been able to arrive “at the infinity,” although she had pushed back the limit quite far.

She does not explain in detail the method she had implemented “being too long,” as she writes, “to be described in the letter,” and affirms only that she was helped by the use of a system of six congruences “having the property that from each of them can the other five be rediscovered” and that, when 2 is not a  $p$ th-power residue (mod  $\theta$ ), the number of congruences in that system cannot be reduced to less than six. Let us recall that a similar system has been discussed in the previous section.

In the letter, Germain also tells Gauss that she had found an explanation, “la métaphysique,” of her method in the paper that Poinsot had communicated to the French Academy in 1818 (Poinsot 1820), and that—she assumed—Gauss had on hand.<sup>42</sup> She thinks that this work would give her another reason to continue her efforts to confirm the condition (N–C) by providing a new way of working with the  $p$ th-powers (mod  $\theta$ ), which she considered as solutions of the binomial equation  $x^{2N} - 1$ .<sup>43</sup>

<sup>40</sup> Since this letter has been extensively studied and commented upon in Del Centina (2008) and Laubenbacher and Pengelley (2010), in the specific context of her work on FLT, we will not go into details here; for the details, we refer the readers to these papers.

<sup>41</sup> The first case of FLT is when the non-zero integers  $x$ ,  $y$ , and  $z$  are such that  $xyz$  is not a multiple of  $p$ ; the second case is when  $xyz$  is a multiple of  $p$ .

<sup>42</sup> Let us recall that this letter was entrusted to Schumacher, together with a copy of Poinsot's memoir.

<sup>43</sup> Two months later, Germain also wrote to Poinsot: “L'emploi des racines imaginaires...c'est un phanal placé sur la grand route: il éclaire les sentiers détournés” [the use of the imaginary roots...is a light placed on the road: it illuminates the misguided paths] (see Del Centina 2005).

In fact, Poinsot's memoir takes the point of view that the  $(\text{mod } \theta)$  solutions of this equation can be obtained by first considering the equation in the complex field, and then considering these roots as  $(\text{mod } \theta)$  integers by replacing  $\sqrt{-1}$  with an integer whose square is  $\equiv -1 \pmod{\theta}$ .

At the end of the letter, Germain asks Gauss if her ideas might have some importance. She is especially interested to know what his thinking was on her deductions about the positions in which the residues appear in the sequence of natural numbers.

Once again, she was not confident enough in her own judgement to decide if her approach was worthy of being pushed forward, but Gauss never answered this letter, and Germain never knew his longed-for and esteemed opinion.

In 1819, writing to Gauss, Sophie Germain was enthusiastic about her method and confident of the possibility that her plan could yield to a proof of FLT. But her plan could never be successful.<sup>44</sup> Nevertheless, in her attempt to prove FLT, she produced many interesting results that have never been credited to her (see Del Centina 2008, also Laubenbacher and Pengelley 2010).

The tenth letter she addressed to Gauss was written on the occasion of the visit she received from Gauss's pupil Bader, who brought to her a copy of *Theoria residuorum biquadraticorum commentatio prima*. This contained, as we know, Gauss's long-awaited results on biquadratic residues. She did not comment on Gauss's work, but she very much regretted having been so long deprived of his correspondence, to which she never ceased to attach the highest value.

Bader had also brought with him a copy of Gauss's work on the curvature of surfaces, *Disquisitiones generales circa superficies curvas* (Gauss 1828b), in which Gauss computes the curvature of a given surface by means of a map to a sphere of unit radius. As is known, Sophie Germain had introduced the concepts of *principal curvatures* at a point  $p$  of a surface  $S$ , which correspond to the maximal and minimal curvature of the curves on  $S$  through  $p$ , and that of *mean curvature*  $(k_1 + k_2)/2$  instead

<sup>44</sup> A first published indication that her method cannot lead to a proof of FLT is contained in *Mémoire sur la théorie des nombres* (Libri 1829, p. 139). In a final note on p. 140, Libri writes that all the results of his work were presented to the French Academy in 1823 and 1825. In January of 1824, Libri presented the French Academy with a memoir on the theory of numbers, divided in three articles, one of which was on the theory congruences. From the report of the referees, Cauchy and Ampère, we know that this latter essentially contained new results on congruences [a method here developed by Libri was used by Cauchy in his *Sur la resolution des équations dont les modules se réduisent à des nombres premiers* (Cauchy 1829)]. The paper that Libri presented to the Academy was never published, but the results it contains appeared later in Libri (1829). On p. 139, Libri also writes "Nous faisons cette observation, parceque nous avons motif de croire que plusieurs analystes ont tenté ce genre de démonstration [of FLT], et puis parceque nous avons vu qu'un géomètre distingué, n'a pu démontrer dans aucun cas le théorème que nous avons découverte" [We make this observation because we have reason to believe that several analysts have attempted this kind of proof [of FLT], and also because we have seen that a distinguish geometer could not prove any case of the theorem we have discovered] (see also Del Centina and Fiocca 2010, part 2). To whom is Libri referring? Laubenbacher and Pengelley have brought to light an undated letter of Germain to Legendre, from which one deduces that Legendre informed her that all numbers of the form  $6a + 1$  larger than 13 have a pair of consecutive nonzero cubic residues, thus implicitly affirming that her method cannot succeed for  $p = 3$ . Germain's letter contains the proof of this claim; a proof that she developed overnight and forwarded in the morning to Legendre. It is likely that she became aware of the failure of her plan in 1823, or shortly before then (Laubenbacher and Pengelley 2010, pp. 25–27).

of the *total curvature* or *Gaussian curvature*  $k_1 k_2$ . In the letter she explained her point of view on this argument to Gauss.<sup>45</sup>

Bader only showed Germain this paper. She remained astonished, and at the same time, she was happy at seeing that so esteemed a geometer had the same idea as she had. But she only had the possibility to look briefly at that paper, and not to study it, and so in her letter to Gauss, she essentially mentioned her approach to curvature in relation to his, remarking what was most similar to her own work, namely the use of a referent sphere. She seemed unaware of the definition of “Gaussian curvature.” Nevertheless, she perceived the important difference between their works. In the letter, she also announced a new paper by her on the subject.

## 9.9 Conclusions

The reading of the letters and mathematical notes which Sophie Germain wrote to Gauss show that she was quick to grasp—long before any others—the content of the D.A. She not only was able to learn the techniques and theorems of Gauss’s work, but also—a testament to her merit—to reach on her own initiative new results that were, by no means trivial, and to develop ideas and conjectures that demonstrate a strong taste for generalization.

Unfortunately, due to her gender, she was prevented from attaining an adequate university instruction. Still worse, she was denied even the possibility of working in the academic world, as would have been possible for a man of her ability. Thus, apart from the benevolence of Lagrange and Legendre—largely due to the respect due to a woman—she worked in almost total isolation, often without being guaranteed access to the scientific information and debates within the Academy.

She saw in her correspondence with Gauss the possibility of escaping from the bell jar under which she felt herself eternally banished rather than protected. Gauss greatly appreciated her intelligence and admired the wisdom with which she knew how to confront and demonstrate theorems which he himself had deemed to be among the most difficult and enigmatic. However, she would have certainly needed more support and interaction with Gauss to develop all her potential for number theory.

Nothing better than the words with which she closed her last letter to Gauss can express better the sentiment which forever hung over her: “I regret that I am deprived of the advantage that I would find in enjoying your learned conversation, as Mr. Bader does. What he told me does not astonish me, but it is an object of my envy. Apart from what I could learn from you, I regret again that I can’t submit for your judgement so many ideas which I have not published, and which would be too long to explain in letter form.”

We believe that the analysis found within the correspondences with Gauss reinforces the conviction—already extolled, on the basis of the study of other unedited writings by her, in Del Centina (2008) and Laubenbacher and Pengelley (2010)—that Sophie Germain should be placed right among the professional number theorists, as

<sup>45</sup> For a detailed discussion of Germain’s point of view see Dahan-Dalmédico (1987).

Gauss himself seems to have affirmed when he said that she would deserve an honorary degree if she were still alive.<sup>46</sup>

**Acknowledgments** The first author would like to express his gratitude to the Niedersächsische Staats- und Universitätsbibliothek in Göttingen, for allowing him, several years ago, to have copies of Germain's letters and mathematical notes. Both the authors express their warmest thanks to Mrs. Bärbel Mund, the person in charge of the Library, and to Mr. Ulrich Hunger, the person in charge of the Historical Archive of the University of Göttingen, for their kindness and the cooperation offered during the preparation of this research article. Finally our warmest thanks go to David Pengelley for having read the paper and corrected some typos and misprints.

## Appendix: Transcription of the correspondence

In the transcription of Germain's letters, we kept close to the original texts with few exceptions. We have employed the modern use of the accented letters and the morphology of some words, as *pouvait* instead of *pouvoit*, *temps* instead of *tems*, *faisant* instead of *fesant*. Moreover, we have written in italics those words and phrases which in the text appeared underlined. For three of the four responses of Gauss, we have reproduced the text given by Stupuy (1879, pp. 302–307, 318–320). For Gauss's reply of the April 30, 1807, we have used the facsimile published by Boncompagni (1879).<sup>47</sup>

### I

Paris, ce 21 novembre 1804 Monsieur

Vos *Disquisitiones Arithmeticae* font depuis longtems l'objet de mon admiration et de mes études. Le dernier chapitre de ce livre renferme, entr'autres choses remarquables, le beau théorème contenu dans l'équation

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

je crois qu'il peut être généralisé ainsi,

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

$n$  étant toujours un nombre premier et  $s$  un nombre quelconque. Je joins à ma lettre deux démonstrations de cette généralisation. Après avoir trouvé la première j'ai cherché comment la méthode que vous avez employé art. 357, pouvait être appliquée

<sup>46</sup> When the matter of honorary degrees came up in 1837 at the centenary celebration of the University of Göttingen, it seems that Gauss regretted exceedingly that Sophie Germain was no longer alive, and declared "She proved to the world that even a woman can accomplish something worthwhile in the most rigorous and abstract of the sciences and for that reason would have well deserved an honorary degree" (Dunnington 1955, p. 68). Among the documents for the centenary celebration preserved at the Historical Archives of the University of Göttingen, no record of Gauss's words has been found.

<sup>47</sup> The present transcription is a revised version of the first one provided by Tiberio Antolini in his thesis: *Le lettere di Sophie Germain a Carl Friedrich Gauss (1804–1828)*, Tesi di Laurea in Matematica, relatori Prof. A. Fiocca and Prof. A. Del Centina, Università di Ferrara, a.a. 2009–2010.

au cas que j'avais à considérer; j'ai fait ce travail avec d'autant plus de plaisir, qu'il m'a fourni l'occasion de me familiariser avec cette méthode, qui, je n'en doute pas, sera dans vos mains l'instrument de nouvelles découvertes.

J'ai ajouté à cet art. quelques autres considérations. La dernière est relative à la célèbre équation de Fermat  $x^n + y^n = z^n$ , dont l'impossibilité en nombres entiers n'a encore été démontrée que pour  $n = 3$  et  $n = 4$ : je crois être parvenu à prouver cette impossibilité pour  $n = p - 1$ ,  $p$  étant un nombre premier de la forme  $8k + 7$ . Je prends la liberté de sousmettre ces essais à votre jugement persuadé que vous ne dédaignerez pas d'éclairer de vos avis un amateur enthousiaste de la science que vous cultivez avec de si brillants succès.

Rien n'égale l'impatience avec laquelle j'attends la suite du livre que j'ai entre les mains, je me suis fait informer que vous y travailliez en ce moment et je ne négligerais rien pour me la procurer aussi tôt qu'elle paraîtra. Malheureusement l'étendue de mon esprit ne répond pas à la vivacité de mes goûts, et je sens qu'il y a une sorte de témérité à importuner un homme de génie lorsqu'on a d'autre titre à son attention qu'une admiration nécessairement partagée par tous ses lecteurs.

En relisant la mémoire de M. de La Grange (Berlin 1775)<sup>48</sup> j'ai vu avec étonnement qu'il n'a pas su réduire la quantité

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

(pag. 352) à la forme  $t^2 - 11u^2$ , car

$$\begin{aligned} & s^{10} - 11(s^8 - 4s^6r^2 + 7s^4r^4 - 5s^2r^6 + r^8)r^2 \\ &= s^{10} - 2 \cdot 11 \cdot s^6r^4 + 11(5+6)r^8s^2 - 11(s^8 - 6s^6r^2 + 7s^4r^4 + 6s^2r^6 + r^8)r^2 \\ &= s^{10} - 2 \cdot 11s^6r^4 + 11^2r^8s^2 - 11(s^8 - 6s^6r^2 + 9s^4r^4 - 2s^2r^6 + r^8)r^2 \\ &= (s^5 - 11sr^4)^2 - 11(s^4 - 3s^2r^2 - r^4)^2, \end{aligned}$$

cette remarque<sup>49</sup> est une nouvelle preuve de l'avantage de votre méthode qui s'appliquant à toutes les valeurs de  $n$ , donne pour chaque cas des valeurs de  $Y$  et  $Z$  indépendantes du talonnement.

Si, connaissant les valeurs de  $Y$  et  $Z$  dans l'équation

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

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

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

<sup>48</sup> *Recherches d'Arithmétique, seconde partie*, Nouveaux Mémoire de l'Academie Royale des Sciences et Belles-Lettres de Berlin, année 1804–1828 (Lagrange 1867–1892, 3, pp. 759–795: 772).

<sup>49</sup> S. Germain forgot to multiply by  $r^2$ , so the last term should be equal to  $-11(s^4r - 3s^2r^3 - r^5)^2$ .

il est clair qu'il suffirait de changer les signes de tous les termes de  $Y$  et  $Z$  qui contiennent des puissances de  $x$  dont l'exposant est impair.

Je n'ai pas voulu fatiguer votre attention en multipliant les remarques dont votre livre a été pour moi l'occasion: si je puis espérer que vous acceuilliez favorablement celles que j'ai l'honneur de vous communiquer et que vous ne les trouviez pas entièrement indignes de répondre veuilliez l'adresser À Monsieur Sylvestre de Sacy membre de l'Institut national, Rue Sante Famille À Paris, qui me la remettra.<sup>50</sup>

Croyez, Monsieur au prix que j'attacherais à un mot d'avis de votre part et recevez l'assurance du profond respect de

votre très humble serviteur  
et très assidu lecteur  
Le Blanc

### Addendum

On peut toujours satisfaire à l'équation  $\frac{4(x^n - 1)}{x - 1} = Y^2 \pm nZ^2$ ,  $n$  étant un nombre premier et  $s$  un nombre quelconque. Car la proposition étant démontrée pour le cas où  $s = 1$  il en résulte qu'elle a lieu aussi pour  $s = 2$ . En effet soit  $\frac{4((x^n)^s - 1)}{x^n - 1} = \frac{4(x^{n^2} - 1)}{x - 1} = Y'^2 \pm nZ'^2$ , il est clair que  $Y'$  et  $Z'$  sont composées des  $x^n$  comme  $Y$  et  $Z$  le sont de  $x$  dans l'équation  $\frac{4(x^n - 1)}{x - 1} = Y^2 \pm nZ^2$ , on a donc  $\frac{16(x^{n^2} - 1)}{x - 1} = \frac{4[(x^n)^s - 1]}{x^n - 1} \cdot \frac{4(x^n - 1)}{x - 1} = (Y'^2 \pm nZ'^2) \cdot (Y^2 \pm nZ^2) = (YY' \pm nZZ') \pm n(Y'Z \mp YZ')$ .

À cause de  $Y'^2 \pm nZ'^2$  et  $Y^2 \pm nZ^2$  multiples de 4, il faut que  $Y'$  et  $Z'$  soient pairs ou impairs en même temps et que  $Y$  et  $Z$  satisfassent aux mêmes conditions, d'où nous concluons  $YY' \pm nZZ' = 2f : x$ ,  $Y'Z \mp YZ' = 2\psi : x$  et par conséquent  $\frac{4(x^{n^2} - 1)}{x - 1} = (f : x)^2 \pm n(\psi : x)^2$ .

On trouve de même

$$\begin{aligned} \frac{4((x^{n^2})^n - 1)}{x^{n^2} - 1} &= Y''^2 \pm nZ''^2; \\ \frac{16(x^{n^3} - 1)}{x - 1} &= \frac{4[(x^{n^2})^n - 1]}{x^{n^2} - 1} \cdot \frac{4(x^{n^2} - 1)}{x - 1} \\ &= (Y''^2 \pm nZ''^2) \cdot ((f : x)^2 \pm n(\psi : x)^2) \\ &= (Y''f : x \pm nZ''\psi : x)^2 \pm n(Y''\psi : x \mp Z''f : x)^2 \end{aligned}$$

d'où nous concluons

$$\begin{aligned} Y''f : x \pm nZ''\psi : x &= 2f' : x, \\ Y''\psi : x \mp Z''f : x &= 2\psi' : x, \end{aligned}$$

<sup>50</sup> Antoine-Isaac Silvestre de Sacy (1758–1838), professor of Arabic at the École des Langues orientales, and, from 1806, also professor of Persian at the Collège de France.

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

et ainsi de suite.

### Exemples

$$\begin{aligned}\frac{4(x^9 - 1)}{x - 1} &= (2x^4 + x^3 + x + 2)^2 + 3(x^3 - x)^2, \\ \frac{4(x^{27} - 1)}{x - 1} &= (2x^{13} + x^{12} + x^{10} + 2x^9 + x^4 + 2x^3 - x + 1)^2 \\ &\quad + 3(x^{12} - x^{10} - x^4 - x - 1)^2, \\ \frac{4(x^{25} - 1)}{x - 1} &= (2x^{12} + x^{11} + 2x^{10} + x^7 + 3x^6 + x^5 + 2x^2 + x + 2)^2 \\ &\quad - 5(x^{11} + x^7 + x^6 + x^5 + x)^2.\end{aligned}$$

Nous observons qu'il y a toujours au moins  $2^{s-1}$  valeurs différentes de  $Y$  et  $Z$  dans l'équation  $\frac{4(x^{n^s} - 1)}{x - 1} = Y^2 \pm nZ^2$ ; car, l'ambiguité des signes dans les quantités  $YY' \pm nZZ'$ ,  $Y'Z \pm YZ'$  fournit deux valeurs différentes pour les quantités  $f : x$ ,  $\psi : x$  qui répondent à  $s = 2$ : ces deux valeurs pouvant être mises dans les quantités  $Y''f : x \pm nZ''\psi : x$ ,  $Y''\psi : x \mp Z''f : x$  donnent, à cause de la nouvelle ambiguïté des signes, 4 valeurs pour  $f'' : x$ ,  $\psi'' : x$  qui répondent à  $s = 3$ ; de sorte qu'en continuant le même raisonnement, on trouve que  $s$  augmentant d'une unité, le nombre des valeurs de  $Y$  et  $Z$  qui satisfont pour la précédente valeur doit être multiplié par 2. D'où il résulte  $2^{s-1}$  pour l'expression générale de ce nombre.



En suivant la démonstration du théorème exprimé par l'équation  $4zz' = 4\frac{x^n - 1}{x - 1} = Y^2 \pm nZ^2$  (art. 357) on voit qu'elle est fondée sur la forme de  $z = R + S(m, 1) + T(m, g)$  et que cette forme elle-même résulte de ce que les coefficients  $a = q = (m, 1)$ ,  $b = \frac{aq - q'}{2} = \frac{(m, 1)^2 - (m, 2)}{2}$ , etc. de l'équation du  $m$ -ième degré  $z = x^m - ax^{m-1} + bx^{m-2} - \dots - 0$ , ne sont composés que des quantités 1,  $(m, 1)$ ,  $(m, g)$  prises un nombre de fois déterminé par la valeur de  $m$ .

Pour étendre ce théorème au cas où l'exposant de  $x$  est une puissance quelconque d'un nombre premier c'est-à-dire, pour démontrer l'équation  $4zz' = 4\frac{x^{n^s} - 1}{x - 1} = Y^2 \pm nZ^2$ , il suffit donc d'établir que les coefficients de l'équation du  $\left(\frac{n^s - 1}{2}\right)$ -ième =  $(mn^{s-1} + mn^{s-2} + \dots + mn + m)$ -ième [ $m = (n - 1)/2$ ] degré

$$\begin{aligned}z &= x^{mn^{s-1} + mn^{s-2} + \dots + m} - Ax^{mn^{s-1} + mn^{s-2} + \dots + m-1} + Bx^{mn^{s-1} + mn^{s-2} + \dots + m-2} \\ &\quad - \dots \pm Vx^{mn^{s-1} + \dots + mn} \mp A'x^{mn^{s-1} + \dots + mn-1} \pm B'x^{mn^{s-1} + \dots + mn-2} \mp \dots \\ &\quad + V'x^{mn^{s-1} + \dots + m(n-1)} - A'x^{mn^{s-1} + \dots + m(n-1)-1} + B'x^{mn^{s-1} + \dots + m(n-1)-2} - \dots\end{aligned}$$

$$\begin{aligned}
& \vdots \\
& + V^n x^{mn^{s-1}+\dots+mn^2} - A^{n+1} x^{mn^{s-1}+\dots+mn^2-1} + B^{n+1} x^{mn^{s-1}+\dots+mn^2-2} - \dots \\
& \pm V^{n+1} x^{mn^{s-1}+\dots+m(n^2-1)} \mp A^{n+2} x^{mn^{s-1}+\dots+m(n^2-1)-1} \\
& \mp B^{n+2} x^{mn^{s-1}+\dots+m(n^2-1)-2} \mp \dots \\
& \vdots \\
& (\pm \text{ ou } +) V^{n^{s-1}+n^{s-2}+\dots+n-1} x^m (\mp \text{ ou } -) A^{n^{s-1}+n^{s-2}+\dots+n} x^{m-1} (\pm \text{ ou } +) \\
& B^{n^{s-1}+n^{s-2}+\dots+n} x^{m-2} (\pm \text{ ou } - \dots) \\
& (+ \text{ ou } \pm) V^{n^{s-1}+n^{s-2}+\dots+n} = 0
\end{aligned}$$

ne contiennent que les quantités 1,  $(m, 1)$ ,  $(m, g)$  prises un nombre de fois déterminé par la valeur de  $n$  et par celle de  $s$ .

(N.<sup>o</sup>te) Les signes + et - devant être alternatifs dans cette équation on voit que les signes supérieurs se rapportant au cas où  $m$  est pair et les inférieurs à celui où  $m$  est impair; on voit en outre que suivant que l'indice de  $V$  est pair ou impair les termes de la ligne à laquelle il appartient, ont ou n'ont pas, de doubles signes).

Ainsi il s'agit de choisir  $m + mn + mn^2 + \dots + mn^{s-2} + mn^{s-1}$  racines parmi les  $n^s - 1$  racines de l'équation  $\frac{x^{n^s}-1}{x-1} = 0$ , de manière que  $A, A', \dots, B, B', \dots$  satisfassent aux conditions indiquées.

Pour cela il faut que la somme de ces racines, celle de leurs quarrés, et en général celle de leurs puissances quelconques, ne soient fonctions que des quantités  $(m, 1)$ ,  $(m, g)$  et de l'unité.

A l'imitation de ce qui a été pratiqué pour l'équation  $\frac{x^n-1}{x-1} = 0$  prenons pour racines de l'équation  $\frac{x^{n^s}-1}{x-1} = 0$ , toutes les puissances de  $R$  moindres que  $n^s$ , c'est-à-dire,  $R, R^2, \dots, R^n, R^{n+1}, \dots, R^{n^s-1}$  en observant qu'au lieu de  $r = \cos \frac{kP}{n} + i \sin \frac{kP}{n}$  on a ici  $R = \cos \frac{kP}{n^s} + i \sin \frac{kP}{n^s}$ .

Parmi ces racines nous prenons pour l'équation  $z = 0$ , d'abord les  $m$  puissances de  $R$  exprimées par les résidus quadratiques (mod  $n$ ) multipliés par  $n^{s-1}$ , par exemple si on a  $g^4 \equiv a \pmod{n}$  [alors]  $R^{an^{s-1}}$  sera une de ces racines; leur somme sera  $(m, 1)$ ; car  $(m, 1)$  est la somme de toutes les puissances de  $r = \cos \frac{kP}{n} + i \sin \frac{kP}{n}$  exprimées par les résidus quadratiques (mod  $n$ ) et il est clair que  $R^{n^{s-1}} = (\cos \frac{kP}{n^s} + i \sin \frac{kP}{n^s})^{n^{s-1}} = \cos \frac{kP}{n} + i \sin \frac{kP}{n}$ .

Nous prenons ensuite les  $mn$  puissances de  $R$  exprimées par les résidus quadratiques (mod  $n$ ) augmentés du nombre  $n$ , multiplié par  $0, 1, 2, \dots, n-1$  et multipliés par  $n^{s-2}$ , par exemple si on a  $g^4 \equiv a \pmod{n}$  [alors]  $R^{(a+hn)n^{s-2}}$  sera une de ces racines,  $n$  étant un quelconque des nombres  $0, 1, 2, \dots, n-1$ . Si on fait  $r' = \cos \frac{kP}{n^2} + i \sin \frac{kP}{n^2}$  et que l'on prenne  $(m, \frac{1}{n})$  pour la somme des puissances de  $r'$  exprimées par les résidus quadratiques (mod  $n$ ) on aura pour la somme des  $mn$  racines,  $(m, \frac{1}{n})(1 + r'^m + r'^{2n} + r'^{3n} + \dots + r'^{(n-1)n})$  et réservant  $r$ , pour exprimer les racines de l'équation  $\frac{x^n-1}{x-1} = 0$ , cette quantité deviendra  $(m, \frac{1}{n})(1 + r + r^2 + r^3 + \dots + r^{n-1})$  qui est visiblement égale à zéro, puisqu'elle est multipliée par la somme des racines de l'équation  $x^n - 1 = 0$ .

La somme de ces racines peut encore être considérée comme celle des puissances de  $r'$  exprimées par les résidus quadratiques  $(\bmod n^2)$ , car ces résidus ne peuvent différer de ceux  $(\bmod n)$  que de la quantité  $n$  prise un nombre de fois moindre que  $n$ , et sous ce point de vue, elle peut être mise sous la forme  $[1] + [g^2] + [g^4] + \cdots + [g^{n(n-1)-2}] = (mn, 1)$ .

Nous prenons de même les  $mn^2$  puissances de  $R$  exprimées par les résidus quadratiques  $(\bmod n^2)$  augmentés du nombre  $n^2$ , multiplié par  $0, 1, \dots, n-1$  et multipliées par  $n^{s-3}$ , par exemple, si on a  $y^4 \equiv a + hn (\bmod n^2)$  [alors]  $R^{(a+hn+h'n^2)n^{s-3}}$  sera une de ces racines. Si on fait  $r'' = \cos \frac{kP}{n^3} + i \sin \frac{kP}{n^3}$ , et que l'on prenne  $(mn, \frac{1}{n})$  pour la somme  $i$ -ième puissances de  $r''$  exprimées par les résidus quadratiques  $(\bmod n^2)$ , on aura pour la somme des  $mn^2$  racines  $(mn, \frac{1}{n})(1 + r''^{m^2} + r''^{2n^2} + \cdots + r''^{(n-1)n^2}) = (mn, \frac{1}{n})(1 + r + \cdots + r^{n-1}) = 0$ .

La somme des ces racines peut encore être considérée comme celle des puissances de  $r''$  exprimées par les résidus quadratiques  $(\bmod n^3)$ , car ces résidus ne peuvent différer de ceux  $(\bmod n^2)$  que de la quantité  $n^2$  prise un nombre de fois moindre que  $n$ , et sous ce point de vue elle peut être mise sous la forme  $[1] + [g^2] + [g^4] + \cdots + [g^{n^2(n-1)-2}] = (mn^2, 1)$ .

On trouvera de même que la somme des  $mn^3$  racines doit être exprimée par  $(mn^3, 1)$  et qu'ayant aussi  $1 + r + r^2 + \cdots + r^{n-1}$  pour facteur elle est égale à zéro; il en est de même des  $mn^4$  racines et de  $mn^5, mn^6, \dots, mn^{s-1}$  racines.

Aussi la somme des  $m + mn + mn^2 + \cdots + mn^{s-1}$  racines de l'équation  $z = 0$  sera  $(m, 1) + (mn, 1) + (mn^2, 1) + \cdots + (mn^{s-1}, 1)$ , et elle se réduira, à cause de  $(mn, 1) = 0, (mn^2, 1) = 0, \dots, (mn^{s-1}, 1) = 0$ , à  $(m, 1)$ .

Il est visible par la nature des périodes  $(mn, 1), (mn^2, 1), \dots, (mn^{s-1}, 1)$  qu'elles seroient encore égal à zéro, si on élevait tous leur termes à une puissance quelconque  $q$  ( $q$  étant premier à  $n$ ) car elle resteront toujours multipliées par la quantité  $1 + r + r^2 + \cdots + r^{n-1}$ , d'où il résulte que  $(mn, g), (mn^2, g), \dots, (mn^{s-1}, g)$  seront également nulles, c'est-à-dire que la somme des racines de l'équation  $z' = 0$ , se réduit à  $(m, g)$ . Il en résulte encore que la somme des puissances  $q$ -èmes des racines c'est-à-dire  $(m, q) + (mn, q) + \cdots + (mn^{s-1}, q)$  se réduit à  $(m, q)$ ; car  $(mn, q), (mn^2, q), \dots, (mn^{s-1}, q)$  sont = 0.

Si on élevait tous les termes des périodes  $(mn, 1), (mn, g)$  à la puissance  $n$  on aurait  $(mn, n) = n(m, 1), (mn, ng) = n(m, g)$ , puis à la puissance  $n^2$  on aurait  $(mn, n^2) = n(m, n) = n, (mn, n^2g) = n(m, gn) = n$ , les périodes  $(mn^2, n), \dots, (mn^2, ng)$  sont nulles mais  $(mn^2, n^2) = n^2(m, 1), (mn^2, g^2n^2) = n^2(m, g)$  en poursuivant les mêmes calculs on voit que les coefficients des équations  $z = 0, z' = 0$  satisfont aux conditions exigées.

### Exemples

Soit  $n = 3, s = 2$ ,

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

On trouve en employant pour calculer les coefficients  $V, V', \dots$  la méthode de l'art. 349:

$$V = (1, 1), \quad V' = 0, \quad V'' = (1, 1), \quad V''' = (1, 2),$$

$$z = x^4 - (1, 1)x^3 - (1, 1)[x] + (1, 2),^{51}$$

$$\begin{aligned} R &= x^4, \quad S = -x^3 - x, \quad T = 1, \quad Y = 2R - S - T = 2x^4 + x^3 + x - 1, \\ Z &= T - S = x^3 + x + 1 \end{aligned}$$

↔

[Soit]  $n = 3, s = 3,$

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

[On trouve]  $V = (1, 1); V' = 0, V'' = (1, 1), V''' = (1, 2), V'''' = 0, V^v = 0, V^{vi} = 0, V^{vii} = 0, V^{viii} = (1, 1), V^ix = (1, 2), V^x = 0, V^{xi} = (1, 2), V^{xii} = 1;$

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

↔

[Soit]  $n = 5, s = 2;$

$$\begin{aligned} z &= x^{2 \cdot 5 + 2} - Ax^{2 \cdot 5 + 1} + Vx^{2 \cdot 5} - A'x^{2 \cdot 5 - 1} + V'x^{2(5-1)} - A''x^{2(5-1)-1} + V''x^{2(5-2)} \\ &\quad - A'''x^{2(5-2)-1} + V'''x^{2(5-2)} - A''''x^{2(5-2)-s} + V''''x^2 - A^v x + V^v = 0. \end{aligned}$$

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

$$\begin{aligned} z &= x^{12} - (2, 1)x^{11} + x^{10} - (2, 1)x^7 + [(2, 2) + 2]x^6 - (2, 1)x^5 + x^2 - (2, 1)x + 1 = 0. \\ R &= x^{12} + x^{10} + 2x^6 + x^2 + 1, \quad S = -x^{11} - x^7 - x^5 - x, \quad T = x^6, \\ Y &= 2x^{12} + x^{11} + 2x^{10} + [x^7] + 3x^6 + x^5 + 2x^2 + x + 2, \quad Z = x^{11} + x^7 + x^6 + x^5 + x.^{52} \end{aligned}$$

↔

En examinant la manière dont se forment les coëfficien[t]s de l'équation  $z = 0$ , nous avons remarqué que les  $m + mn + mn^2 + \dots + mn^{s-2}$  premiers coëfficien[t]s de l'équation du  $(m + mn + mn^2 + \dots + mn^{s-1})^{\text{ième}}$  degré sont égaux à ceux de l'équation du  $(m + mn + mn^2 + \dots + mn^{s-2})^{\text{ième}}$  degré, que les  $m + mn + mn^2 + \dots + mn^{s-2}$  suivants sont égaux à zéro, et que le  $(2m + 2mn + 2mn^2 + \dots + 2mn^{s-2})^{\text{ième}}$  est  $(m, 1)$  de sorte que si on connaît les coëfficients de l'équation  $z = 0$  du  $(\frac{n^{s-1}-1}{2})^{\text{ième}}$

<sup>51</sup> In Germain's manuscript appears  $(1, 1)x^2$  instead of  $(1, 1)x$ .

<sup>52</sup> The term  $x^7$  was erroneously skipped in writing to Gauss.

degré on a sans calcul les  $2m + 2mn + 2mn^2 + \cdots + 2mn^{s-2} + 1 = n^{s-1}$  premiers, de l'équation  $z = 0$  du  $(\frac{n^s-1}{2})$ ième degré.

On trouve aussi par cette méthode qu'il y a au moins  $2^{s-1}$  valeurs différentes de  $Y$  et  $Z$ : car, en reprenant la somme  $(m, 1) + (mn, 1) + (mn^2, 1) + \cdots + (mn^{s-1}, 1)$  des racines de l'équation  $z = 0$ , on voit que l'on peut changer  $(mn, 1)$  en  $(mn, g)$  sans que les précédentes conclusions soient [soyent] altérées, et comme il y a  $s - 1$  quantités  $(mn, 1), (mn^2, 1) + \cdots + (mn^{s-1}, 1)$  et que les mêmes changements peuvent être faits 1 à 1, 2 à 2, etc. on a en ajoutant 1 pour le cas où il n'y a aucun changement  $1 + s - 1 + \frac{(s-1)(s-2)}{2} + \frac{(s-1)(s-2)(s-3)}{2 \cdot 3} + \text{etc. } = 2^{s-1}$  pour le nombre des différentes formes de cette somme. Ces changements n'influencent à la vérité que sur les puissances  $n, n^2$ , etc. des racines à cause de  $(mn, n) = n(m, 1), (mn^2, n^2) = n^2 = n^2(m, 1)$ , etc. mais cela suffit à y donner des valeurs différentes pour  $R, T$  et  $S$  et par conséquent aussi pour  $Y$  et  $Z$ .



Nous avons remarqué que les coefficients des termes de  $Y$  et  $Z$  art. 357 sont, pour  $n = 4k + 1$  les mêmes et de mêmes signes à partir de  $x^m$  qu'a partir de 1; c'est-à-dire, que si on a  $N$  pour coefficient de  $x^{m-h}$  dans  $Y$  ou  $Z$ ,  $N$  sera aussi coefficient de  $x^h$  dans la même quantité. Pour  $n = 4k + 3$  les mêmes coefficients sont de signes contraires; c'est-à-dire, que si on a  $N$  pour coefficient de  $x^{m-h}$  dans  $Y$  ou  $Z$ ,  $-N$  sera coefficient des  $x^h$  dans la même quantité.<sup>53</sup>

Pour démontrer cette règle nous observerons que les coefficients de  $Y$  et  $Z$  dépendent de ceux des différents termes de  $z = 0$  et  $z' = 0$ ; or l'équation  $z = 0$ , peut être mise sous cette forme  $z = (x - [1])(x - [g^2])(x - [g^4]) \cdots (x - [g^{n-3}]) = 0$ , et à cause de  $[1][g^2][g^4] \cdots [g^{n-3}] = [1 + g^2 + g^4 + \cdots + g^{n-3}] = [0] = 1$ . On peut donc multiplier le second nombre par  $([1][g^2][g^4] \cdots [g^{n-3}])^{m-1}$  sans que le premier reçoive aucun changement.

Effectuant donc cette multiplication de manière que chaque facteur se trouve multiplié par le produit de toutes les racines  $[1], [g^2]$ , etc. moins celle qui entre dans ce facteur, et réduisant l'équation devient  $z = (x[-1] - 1)(x[-g^2] - 1)(x[-g^4] - 1) \cdots (x[-g^{n-3}] - 1)$

Lorsque  $n = 4k + 1, -1$  étant résidu quadratique, l'équation se transforme ainsi:  $z = (x[1] - 1)(x[g^2] - 1)(x[g^4] - 1) \cdots (x[g^{n-3}] - 1)$  et comme le nombre  $m = 2k$  des facteurs est pair on peut changer tous les signes ce qui donne  $z = (1 - x[1])(1 - x[g^2])(1 - x[g^4]) \cdots (1 - x[g^{n-3}])$ .

Cette forme comparée à la première montre que  $z$  est fonction homogène de  $x$  et de 1.<sup>54</sup>

Lorsque  $n = 4k + 3, -1$  est non résidu, ainsi la valeur de  $z$  doit être mise sous la forme  $z = (x[g] - 1)(x[g^3] - 1)(x[g^5] - 1) \cdots (x[g^{n-2}] - 1)$ : qui étant comparée à

<sup>53</sup> This is not true for  $Z$ , as clearly appears by looking at the table in art. 357 of the D.A. For polynomial  $Z$  it seems to hold the property that  $x^{m-h}$  and  $x^h$  have always the same coefficient with the same sign.

<sup>54</sup> It is not clear to us how she may deduce that  $Y$  and  $Z$  are homogeneous functions of  $x$  and 1.

celle de  $z'$ , savoir  $z' = (x - [g])(x - [g^3])(x - [g^5]) \cdots (x - [g^{n-2}])$  montre que  $zz''$  et par conséquent aussi  $Y$  et  $Z$  sont fonctions homogènes de  $x$  et  $-1$ .<sup>55</sup>



La méthode de l'art. 345 donne après les réductions convenables. Pour  $n = 4k + 1$   $q^2 = m + (m, 2) + 2\{(m, 1+g^2) + (m, 1+g^4) + (m, 1+g^6) \cdots + (m, 1+g^{m-2})\}$ . Et on tire de la considération des deux équations  $(p-q)^2 = n$ ,  $(p+q)^2 = 1$  cette autre valeur de  $q^2$ ,  $q^2 = k + 1 + p$ : donc si  $k + 1$  est pair, il faut que  $(m, 2) = p = (m, g)$ , c'est-à-dire que 2 soit non résidu: au contraire si  $k + 1$  est impair il faut que  $(m, 2) = (m, 1)$  car  $1 - (m, 1) = -2(m, 1) - (m, g) = -2(m, 1) - p$ , c'est-à-dire que 2 soit résidu. Ainsi 2 est résidu des nombres premiers de la forme  $8k' + 1$  et non résidu de ceux de la forme  $8k' + 5$ .

La comparaison des deux valeurs de  $q^2$  relatives à  $n = 4k + 3$  donne de même  $-k + p = (m, 2) + 2\{(m, 1+g^2) + (m, 1+g^4) + \cdots + (m, 1+g^{m-1})\}$  et par conséquent  $p = (m, 2)$  lorsque  $k$  est pair et  $q = (m, 2)$  lorsque  $k$  est impair c'est-à-dire 2 non résidu pour les nombres de la forme  $8k' + 3$  et résidu pour ceux de la forme  $8k' + 7$ .

Les précédents théorèmes sont démontrés dans plusieurs endroits du livre, par des méthodes qui diffèrent toutes de celle-ci.



On peut démontrer l'impossibilité de satisfaire en nombres entiers à l'équation  $x^{p-1} + y^{p-1} = z^{p-1}$ ,  $p$  étant un nombre premier de la forme  $8n + 7$ .<sup>56</sup>

En effet, si on veut satisfaire à l'équation  $x^{p-1} + y^{p-1} = z^{p-1}$ ,  $p$  étant un nombre premier quelconque, il faut prendre pour  $x$  ou  $y$  un multiple de  $p$ . Car faisant d'abord  $x$ ,  $y$  et  $z$  premiers à  $p$  et mettant la proposée sous la forme  $x^{p-1} - 1 + y^{p-1} - 1 = z^{p-1} - 2$ , il en résultera, à cause de  $z^{p-1} - 1 \equiv 0 \pmod{p}$ ,  $\equiv 0$ , et faisant ensuite  $x$  et  $y$  premiers à  $p$  et  $z$  multiples de ce nombre on sera mené à conclure  $-2 \equiv 0$ .

Soit donc  $x$  impair et multiple de  $p$ , en mettant  $2p'$  au lieu de  $p - 1$  et  $phf$  à la place de  $x$  la proposée devient  $(phf)^{2p'} + y^{2p'} = z^{2p'}$ , où  $z^{2p'} - y^{2p'} = (phf)^{2p'}$  d'où on tire  $y^{p'} \pm z^{p'} = (pf)^{2p'}$ ,  $y^{p'} \mp z^{p'} = h^{2p'}$ ,  $2y^{p'} = (pf)^{2p'} + h^{2p'}$ ,  $h$  étant premier à  $p$ ,  $h^{2p'} - 1 \equiv 0 \pmod{p}$  donc aussi  $2y^{p'} - 1 \equiv 0 \pmod{p}$ , et à cause de  $y^{2p'} - 1 \equiv 0$ ,  $y^{p'} \equiv 2$ ,  $y^{2p'} \equiv 4 \equiv 1$  d'où résulte  $p = 3$ .

Supposons donc  $y = 2pfh$ , la proposée deviendra  $(2pfh)^{2p'} = x^{2p'} - z^{2p'}$ . Examinons d'abord le cas où  $x^{p'} \pm z^{p'} = 2p^{2p'}f^{2p'}, x^{p'} \mp z^{p'} = 2^{2p'-1}h^{2p'}$  d'où on tire  $2x^{p'} = 2p^{2p'}f^{2p'} + 2^{2p'-1}h^{2p'}$  et  $(2h)^{2p'} \equiv 1 \pmod{p}$ ,  $4x^{p'} \equiv 2^{2p'}h^{2p'}$ ,  $4x^{p'} \equiv 1 \equiv x^{2p'}$ ,  $4 \equiv x^{p'}$ ,  $16 \equiv x^{2p'} \equiv 1$  c'est-à-dire  $15 \equiv 0$  et par conséquent  $p = 3$  ou  $p = 5$ .

Supposons enfin  $x^{p'} \pm z^{p'} = 2f^{2p'}, x^{p'} \mp z^{p'} = 2^{2p'-1}p^{2p'}h^{2p'}$ , d'où on tire  $2x^{p'} = 2f^{2p'} + 2^{2p'-1}p^{2p'}h$  ou  $x^{p'} = f^{2p'} + 2^{2p'-2}p^{2p'}h^{2p'}$  soit  $x = f^2 + mp^{2p'}$  le développement donne  $f^{2p'} + p'f^{2p'-2}(mp^{2p'}) + \cdots \equiv f^{2p'} + 2^{2p'-2}p^{2p'}h^{2p'}$ ,  $p'f^{2p'-2}(mp^{2p'}) + \cdots = 2^{2p'-2}p^{2p'}h^{2p'}$  ou  $p'f^{2p'-2}(m) + \cdots = 2^{2p'-2}h^{2p'}$  comme tous les termes suivants du développement de  $f^2 + mp^{2p'}$  sont multiples de  $m$ , il faut que  $h^{2p'}$  soit divisible par ce nombre et comme tous les facteurs de  $h^{2p'}$  sont élevés

<sup>55</sup> It is not clear to us how she may deduce that  $Y$  is a homogeneous functions of  $x$  and  $-1$ .

<sup>56</sup> This part of the addendum has been already published and commented on in Del Centina (2008).

à la puissance  $2p'$  on doit faire  $m = k^{2p'}$ . L'équation devient  $p'f^{2p'-2}k^{2p'} + \dots = 2^{2p'-2}h^{2p'}$  ou  $4p'f^{2p'-2}k^{2p'} \equiv 2^{2p'}h^{2p'} \equiv 1 \pmod{p}$  et à cause de  $k^{2p'} \equiv 1$ ,  $4p'f^{2p'-2} \equiv 1 \equiv f^{2p'}$  d'où on tire  $4p' \equiv f^2$  mais à cause de  $2p' + 1 = p$ ,  $4p' \equiv -2$  d'où résulte  $-2 \equiv f^2$ .

Ainsi l'équation  $x^{p-1} + y^{p-1} = z^{p-1}$  est impossible lorsque  $-2$  est non résidu quadratique: c'est ce qui a lieu pour les nombres premiers des formes  $8n + 5$ ,  $8n + 7$ . Mais nous avons vu plus haut que le cas  $p = 5$  échape à notre méthode et d'ailleurs l'impossibilité de l'équation  $x^4 + y^4 = z^4$  a été démontrée ainsi elle est uniquement applicable aux nombres  $8k + 7$ .

### Gauss's reply.

Brunswick 16 juin 1805

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

J'ai lu avec plaisir les choses que vous m'avez bien voulu communiquer ; je me félicite que l'arithmétique acquiert en vous un ami assez habile. Surtout votre nouvelle démonstration pour les nombres premiers, dont 2 est résidu ou non résidu, m'à extrêmement plu ; elle est très fine, quoiqu'elle semble être isolée et ne pouvoir s'appliquer à d'autre nombres. J'ai très souvent considéré avec admiration l'enchaînement singulier des vérités arithmétiques. Par exemple, le théorème que je nommé fondamental (art. 131) et les théorèmes particuliers concernant les résidus  $1 \pm 2$ , s'entrelacent à une foule d'autres vérités où l'on les aurait jamais cherché! Outre les deux démonstrations que j'ai données dans mon ouvrage, je suis en possession de deux ou trois autre, qui du moins ne le cèdent pas à celle-là en question d'élégance.

Je remarque avec beaucoup de regret que les autres occupations où je suis engagé ne me permettent point du tout de me livrer à présent à mon amour pour l'arithmétique. Ce ne sera peut-être qu'après plusieurs années que je pourrai penser à la publication de la suite de mes recherches qui rempliront aisément un ou deux volumes semblables ou premier. Mais je croirais n'avoir pas assez vécu, si je mourrais sans avoir achevé toutes les recherches intéressantes auxquelles je me suis une fois livré. Au reste, chez nous en Allemagne, la publication d'un tel ouvrage a ses difficultés : quoiqu'on en dise, le goût pour les mathématiques pures, si l'on cherche de la profondeur, n'est pas trop général. Nos libraires ne se mêlent guère de ces sortes de livres, et je ne suis pas assez riche pour faire à mes frais l'impression et me soumettre à la malhonnêteté des libraires étrangers, comme il m'est arrivé à l'occasion du premier volume. Un M.\*\*\*,

par exemple libraire à Paris, a reçu de moi, il y a presque trois ans, des exemplaires pour la valeur de six cent quatre-vingt francs ; mais jamais je n'ai reçu un sou de lui, et il ne s'est même pas donné la peine de répondre à mes lettres.

Peut-être vous pourriez me donner des renseignements par quel moyen, on pourrait engager cet homme à faire son devoir.

Agréez, Monsieur, l'expression de ma haute considération.

Ch.Fr. Gauss

## II

Paris 21 julliet 1805

Monsieur

je dois sans doute à votre indulgence la réponse flatteuse que vous avez bien voulu faire à ma lettre; vous me donnez l'espérance de vous entretenir avec moi de l'objet de vos études; rien au monde ne pourrait me faire plus de plaisir qu'une semblable correspondance, mais je sens que j'en suis bien peu digne. Quelle différence en effet entre les faibles essais dont je suis capable et les méthodes ingénieuses dont l'invention vous est familière! Cependant puisque vous avez acceuilli avec bonté les notes que je vous ai communiquées je pren[ds] la liberté de vous en soumettre de nouvelles.

Vous promettez (n. 267) de prouver dans une autre occasion que les formes ternaires dont la déterminante est zéro sont équivelantes aux formes binaires; j'ai cherché à faire la réduction indiquée et j'ai trouvé que dans ce cas la forme adjointe se réduit à un carré multiplié par  $m$ , ce qui est absolument la même forme que celle que prennent les formes binaires lorsqu'on suppose leurs déterminantes égales à zéro.

Je vois avec regret qu'il nous faudra attendre, peut-être plusieurs années la publication de vos nouvelles recherches arithmétiques; il est impossible de connaître le premier volume sans désirer avec impatience d'en voir la suite; ce sera pour moi une consolation si vous daignez m'en communiquer quelques parties.

Le libraire Duprat sur lequel vous me demandez des renseignements a cédé son fond et est en banqueroute déclarée depuis 18 mois environ; je sais que plusieurs savans ont été dupés avec lui ce qui est de très mauvais augure pour votre créance: cependant Mr. de Sacy qui a l'habitude de traiter avec les libraires m'a promis de faire des démarches, pour découvrir si il n'y aurait pas quelques moyens de vous faire payer, il vous fera savoir ce qu'il apprendra d'utile. Si jamais pareil cas se représent[er]ait il ne faudrait pas attendre un temps aussi long pour réclamer le payement car ici les créances ne gagnent pas à viellir.

J'aurais désiré avoir de meilleures nouvelles à vous donner, je crains que le résultat fâcheux de l'envoi que vous avez fait ne nous privent de connaître les nouveaux ouvrages que vous pourrez publier, je vous demande comme une grâce de vouloir bien m'indiquer les titres de ceux que vous écrirez en latin, car n'entendant pas l'Allemand je suis forcé de borner là ma curiosité.

Je pense que vos travaux astronomiques ne consistent pas seulement dans des calculs d'éléments de planètes, vous devez presqu'involontairement trouver de nouvelles méthodes; l'esprit d'invention semble vous être si naturel, que quelques soient les

objets dont vous vous occupez, je croirais avoir beaucoup gagné si je parvenais à connaître vos recherches.

Puisque vous vous occupez d'astronomie vous connaissez sans doute la *Mécanique Céleste* par Mr. de Laplace, le 4-ième volume a paru il y a environ deux mois il contient: la théorie des satellites de Jupiter de Saturne et d'Uranus; la théorie des perturbations des comètes, des recherches sur les réfractions astronomiques, l'intégration de l'équation différentielle du mouvement de la lumière suivant différentes hypothèses; un chapitre sur l'extinction de la lumière des astres dans l'atmosphère; sur la mesure des hauteurs par le baromètre; sur la chute des corps qui tombent d'une grande hauteur; et un, sur les alterations que les mouvements des planètes et des comètes peuvent éprouver par la résistance des milieux qu'elles traversent et par la transmission successive de la pesanteur.

Mr. Le Gendre a publié aussi il y a quelques temps, un mémoire sur la détermination des orbites des comètes. Après avoir fait l'analyse du problème il simplifit les formules générales par la supposition de l'égalité des temps entre les observations: il s'attache à déterminer les limites de  $r =$  rayon de la comète et de  $\rho =$  distance de la comète à la terre. Pour le cas où le rayon  $R$  de la terre est  $< r$  les limites reviennent à celles trouvées par Mr. de la Grange (*Mémoires de Berlin* 1778 n.° 22).<sup>57</sup> Mais pour celui où  $r < R$  il tira de la considération de l'équation  $r^2 = R^2 - 2R\rho \cos(c) + \rho^2$  (dans laquelle  $c$  est l'angle entre le soleil et la comète)  $\rho > 0$  et  $\rho < 2R \cos(c)$  puis en mettant cette équation sous la forme  $r^2 = R^2 \sin^2(c) + (\rho - R \cos(c))^2$  il a  $r > R \sin(c)$ , ce qui est beaucoup plus simple que les résultats de Mr. de la Grange.

L'auteur reprend ensuite le cas général, où les temps entre les observations peuvent être inégaux et il parvient à des équations de mêmes formes que celles qu'il a obtenues dans la supposition de leur égalité. Enfin il fait l'application de sa méthode à la 2-ème comète de 1781 et à celle de 1769.

Si il vous est agréable de connaître les ouvrages qui paraîtront ici je me ferai un plaisir de vous tenir sur les avis; ce serait pour moi un motif d'espérer jouir de votre correspondance, car je sens que j'ai bien peu de moyens de la mériter par moi-même et que je ne suis en être digne que par l'admiration et le profond respect avec lequel j'ai l'honneur d'être

Monsieur

Votre très humble serviteur Le Blanc.

La lettre qui était incluse dans celle que vous avez adressée a été mise à la poste.

## Addendum

Réduction des formes ternaires aux formes binaires lorsque la déterminante est zéro (nr. 267).

<sup>57</sup> S. Germain is referring to *Sur le problème de la détermination des orbites des comètes d'après trois observations I, II, Nouv. Mémoires Ac. R. des Sci. et Belles-lettres de Berlin* 1778 (Lagrange 1867–1892, 4, pp. 437–496).

Lorsque l'on suppose  $\mathcal{D} = 0$  les équations

$$\begin{aligned} BB - A'A'' &= a\mathcal{D}, & AB - B'B'' &= b\mathcal{D}, \\ B'B' - AA'' &= a'\mathcal{D}, & A'B' - BB'' &= b'\mathcal{D}, \\ B''B'' - AA' &= a''\mathcal{D}, & A''B'' - BB' &= b''\mathcal{D}, \end{aligned}$$

se réduisent à  $BB = A'A''$ ,  $B'B' = AA''$ ,  $B''B'' = AA'$ ;  $AB = B'B''$ ,  $A'B' = BB''$ ,  $A''B'' = BB'$ ; on peut y satisfaire en faisant  $B = m\alpha\beta$ ,  $B' = m\delta\beta$ ,  $B'' = m\alpha\delta$ ; la substitution de ces valeurs dans les trois dernières équations donne  $Am\alpha\beta = m^2\alpha\beta\delta^2$ ,  $A'm\delta\beta = m^2\delta\beta\alpha^2$ ,  $A''m\alpha\delta = m^2\alpha\delta\beta^2$ ; d'où on tire  $A = m\delta^2$ ,  $A' = m\alpha^2$ ,  $A'' = m\beta^2$ ;

mettant ces valeurs dans

$$\begin{pmatrix} A & A' & A'' \\ B & B' & B'' \end{pmatrix}$$

forme adjointe de

$$\begin{pmatrix} a & a' & a'' \\ b & b' & b'' \end{pmatrix}$$

on trouvera

$$\begin{aligned} Ax &+ A'x'x' + A''x''x'' + 2Bx'x'' + 2B'xx'' + 2B''x'x \\ &= m(\{\delta^2xx + \alpha^2x'x' + \beta^2x''x'' + 2\alpha\beta x'x'' + 2\delta\beta xx'' + 2\alpha\delta x'x\} \\ &= m(\delta x + \alpha x' + \beta x'')^2. \end{aligned}$$

Reprenant ensuite l'équation

$$\mathcal{D} = abb + a'b'b' + a''b''b'' - aa'a'' - 2bb'b'' = 0,$$

on a à cause de

$$\begin{aligned} abb - a''a'a &= Aa = am\delta^2, & abb - bb'b'' &= Bb = bm\alpha\beta \\ a'b'b' - a''a'a &= A'a' = a'm\alpha^2, & a'b'b' - bb'b'' &= B'b' = b'm\delta\beta \\ a''b''b'' - a''a'a &= A''a'' = a''m\beta^2, & a''b''b'' - bb'b'' &= B''b'' = b''m\alpha\delta; \\ Aa + B'b' + B''b'' &= \mathcal{D} = am\delta^2 + b'm\delta\beta + b''m\alpha\delta = 0, \\ A'a' + Bb + B''b'' &= \mathcal{D} = a'm\alpha^2 + bm\alpha\beta + b''m\alpha\delta = 0, \\ A''a'' + Bb + B'b' &= \mathcal{D} = a''m\beta^2 + bm\alpha\beta + b'm\delta\beta = 0, \end{aligned}$$

ou

$$\left. \begin{aligned} a\delta + b'\beta + b''\alpha &= 0 \\ a'\alpha + b\beta + b''\delta &= 0 \\ a''\beta + b\alpha + b'\delta &= 0 \end{aligned} \right\} \quad (1)$$

On trouve en faisant usage des mêmes équations

$$\begin{aligned} Aa + 2B'b' + A''a'' - A'a' &= \mathcal{D} = am\delta^2 + 2b'm\delta\beta + a''m\beta^2 - a'm\alpha^2 = 0, \\ Aa + 2B''b'' + A'a' - A''a'' &= \mathcal{D} = am\delta^2 + 2b''m\delta\alpha + a'm\alpha^2 - a''m\beta^2 = 0, \\ A'a' + 2Bb + A''a'' - Aa &= \mathcal{D} = a'm\alpha^2 + 2bm\alpha\beta + a''m\beta^2 - am\delta^2 = 0, \end{aligned}$$

ou

$$\left. \begin{aligned} a\delta^2 + 2b'\delta\beta + a''\beta^2 &= a'\alpha^2 \\ a\delta^2 + 2b''\delta\alpha + a'\alpha^2 &= a''\beta^2 \\ a'\alpha^2 + 2b\alpha\beta + a''\beta^2 &= a\delta^2 \end{aligned} \right\} \quad (2)$$

Multipliant la forme ternaire par  $\delta^2$  et mettant ensuite pour  $a\delta^2$  sa valeur donnée par la troisième des équations (2) et pour  $2b'\delta^2$ ,  $2b''\delta^2$  leurs valeurs  $-2(a''\beta\delta + b\alpha\delta)$ ,  $-2(a'\alpha\delta + b\beta\delta)$ , tirées des équations (1) multipliées par  $2\delta$  on trouve

$$\begin{aligned} a\delta^2xx + a'\delta^2x'x' + a''\delta^2x''x'' + 2b\delta^2x'x'' + 2b'\delta^2xx'' + 2b''\delta^2xx' \\ = (a'\alpha^2 + 2b\alpha\beta + a''\beta^2)xx + a'\delta^2x'x' + a''\delta^2x''x'' + 2b\delta^2x'x'' \\ - 2(a''\beta\delta + b\alpha\delta)xx'' - 2(a'\alpha\delta + b\beta\delta)xx' \\ = a'[\alpha^2xx + \delta^2x'x' - 2\alpha\delta xx'] + a''[\beta^2xx + \delta^2x''x'' - 2\beta\delta xx''] \\ + 2b[\alpha\beta xx + \delta^2x'x'' - \alpha\delta xx'' - \beta\delta xx'] \\ = a'(\alpha x - \delta x')^2 + a''(\beta x - \delta x'')^2 + 2b[(\alpha x - \delta x')\beta x + (\delta x' - \alpha x)\delta x''] \\ = a'(\alpha x - \delta x')^2 + a''(\beta x - \delta x'')^2 + 2b(\alpha x - \delta x')(\beta x - \delta x''). \end{aligned}$$

On trouverait de même

$$\alpha^2 \begin{pmatrix} a & a' & a'' \\ b & b' & b'' \end{pmatrix} = (a, b', a''), \quad \beta^2 \begin{pmatrix} a & a' & a'' \\ b & b' & b'' \end{pmatrix} = (a, b'', a')$$

Les équations (1) montrent que  $a, b', b''; b'', a', b; b', b, a'';$  sont les valeurs de  $x, x', x''$  qui dans le cas où  $\mathcal{D} = 0$  rendent

$$\begin{pmatrix} A & A' & A'' \\ B & B' & B'' \end{pmatrix} = 0,$$

l'addition des trois équations (2) donnent  $a\delta^2 + a'\alpha^2 + a''\beta^2 + 2b\alpha\beta + 2b'\delta\beta + 2b''\delta\alpha = 0$ , c'est-à-dire que dans le même cas  $\delta, \alpha, \beta$  sont les valeurs de  $x, x', x''$  qui rendent

$$\begin{pmatrix} a & a' & a'' \\ b & b' & b'' \end{pmatrix} = 0$$



Nr. 201: 2 est une valeur de  $m$  dans le cas seulement où  $\mathcal{D}$  est de l'une ou l'autre des formes  $4k$ ,  $4k + 1$ .

Lorsque  $\mathcal{D}$  est de l'une ou l'autre des formes  $8k$ ,  $8k + 1$ , les valeurs de  $t$  et  $u$  dans l'équation  $t^2 - \mathcal{D}u^2 = 4$ , ne sont d'autre chose que les valeurs correspondantes de  $x$  et  $y$  dans l'équation  $x^2 - \mathcal{D}y^2 = 1$ , multipliées par 2. Car alors  $t$  et  $u$  sont nécessairement des nombres pairs.

Examinons d'abord l'équation  $t^2 - 8ku^2 = 4$ .  $t$  ne peut être qu'un nombre impair-pair, par conséquent  $t^2$  est de la forme  $32n + 4$ , et pour que  $8ku^2 + 4$  soit de la même forme il faut que  $u$  soit un nombre pair.

A l'égard de l'équation  $t^2 - (8k + 1)u^2 = 4$ , il est visible que  $t$  et  $u$  sont pairs et impairs en même temps; mais si on supposait  $t$  et  $u$  impair le premier nombre serait divisible par 8; donc  $t$  et  $u$  sont nécessairement des nombres pairs.

Lorsque  $\mathcal{D} = 8k + 4$ ,  $t$  est un nombre pair, mais  $u$  peut être impair: dans ce cas  $T$  et  $U$  étant les moindres valeurs  $t$  et  $u$  dans l'équation  $t^2 - \mathcal{D}u^2 = 4$  et  $p$  et  $q$  les moindres valeurs de  $x$  et  $y$  dans l'équation  $x^2 - \mathcal{D}y^2 = 1$  on a  $p = \frac{T^2 - 2}{2}$ ,  $q = \frac{UT}{2}$ .

Car  $2p$ ,  $2q$  doivent être les moindres valeurs paires de  $t$ ,  $u$ ; et les formules générales du nr. 200 donnent en faisant  $m = 2$ ,  $e = 2$

$$2p = \left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^2 + \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right)^2 = \frac{1}{2}(T^2 + U^2\mathcal{D}) = \frac{1}{2}(2T^2 - 4) = T^2 - 2$$

$$2q = \frac{1}{\sqrt{\mathcal{D}}} \left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^2 - \frac{1}{\sqrt{\mathcal{D}}} \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right) = TU$$

On tire encore de là:

$$p + q\sqrt{\mathcal{D}} = \frac{\left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^2 + \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right)^2 + \left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^2 - \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right)^2}{2}$$

$$= \left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^2,$$

$$p - q\sqrt{\mathcal{D}} = \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right)^2;$$

$$\frac{(T + U\sqrt{\mathcal{D}})(p + q\sqrt{\mathcal{D}})^n + (T - U\sqrt{\mathcal{D}})(p - q\sqrt{\mathcal{D}})^n}{2}$$

$$= \left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^{2n+1} + \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right)^{2n+1}$$

$$\frac{\left(T + U\sqrt{\mathcal{D}}\right)(p + q\sqrt{\mathcal{D}})^n - (T - U\sqrt{\mathcal{D}})(p - q\sqrt{\mathcal{D}})^n}{2\sqrt{\mathcal{D}}}$$

$$= \frac{1}{\sqrt{\mathcal{D}}} \left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^{2n+1} - \frac{1}{\sqrt{\mathcal{D}}} \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right)^{2n+1},$$

formules relatives au cas où  $t$  est pair et  $u$  impair.

Lorsque  $\mathcal{D} = 8k + 5$ ,  $t$  et  $u$  peuvent avoir des valeurs impaires et on a dans ce cas

$$p = \frac{T(T^2 - 3)}{2}, \quad q = \frac{U(T^2 - 1)}{2},$$

car

$$\begin{aligned} 2p &= \left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^3 + \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right)^3 = \frac{1}{4}(T^3 + 3TU^2\mathcal{D}) \\ &= \frac{1}{4}[T^3 + 3T(T^2 - 4)] = T(T^2 - 3), \\ 2q &= \frac{1}{\sqrt{\mathcal{D}}} \left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^3 - \frac{1}{\sqrt{\mathcal{D}}} \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right)^3 = \frac{1}{4}(3T^2U + U^3\mathcal{D}) \\ &= \frac{1}{4}[3T^2U + U(T^2 - 4)] = U(T^2 - 1) \end{aligned}$$

on a donc

$$\begin{aligned} p + q\sqrt{\mathcal{D}} &= \frac{\left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^3 + \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right)^3 + (\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}})^3 - (\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}})^3}{2} \\ &= \left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^3, \\ p - q\sqrt{\mathcal{D}} &= \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right)^3, \end{aligned}$$

et à cause de

$$\begin{aligned} &\left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)\left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right) = 1; \\ &\frac{(T \pm U\sqrt{\mathcal{D}})(p + q\sqrt{\mathcal{D}})^n + (T \mp U\sqrt{\mathcal{D}})(p - q\sqrt{\mathcal{D}})^n}{2} \\ &= \left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^{3n+1} + \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right)^{3n+1}, \\ &\frac{(T \pm U\sqrt{\mathcal{D}})(p + q\sqrt{\mathcal{D}})^n - (T \mp U\sqrt{\mathcal{D}})(p - q\sqrt{\mathcal{D}})^n}{2\sqrt{\mathcal{D}}} \\ &= \frac{1}{\sqrt{\mathcal{D}}} \left(\frac{T}{2} + \frac{U}{2}\sqrt{\mathcal{D}}\right)^{3n+1} - \frac{1}{\sqrt{\mathcal{D}}} \left(\frac{T}{2} - \frac{U}{2}\sqrt{\mathcal{D}}\right)^{3n+1} \end{aligned}$$

formules relative au cas où  $t$  et  $u$  sont impairs.



On peut démontrer par la méthode employée nr. 115 que pour tout nombre premier de la forme  $2^sm + 1$  il y a parmi les nombres  $1, 2, 3, 4, \dots, 2^sm$ ,  $m$  résidus  $2^s$ -iéme puissance et  $(2^s - 1)m$  non résidu même puissance.

Pour cela il suffit d'observer que  $-1$  est toujours résidu  $2^{s-1}$ -ième puissance  $(\text{mod } 2^s m + 1)$  car à cause de  $f^{2^{s-1}} \equiv -1$  les  $2^s$ -ième puissance des  $2^s$  nombres  $+z, -z, +zf, -zf, +zf^2, -zf^2, \dots, +zf^{2^{s-1}-1}, -zf^{2^{s-1}-1}$ , sont congruentes entre elles  $(\text{mod } 2^s m + 1)$ .

Ainsi, par exemple, pour les nombres premiers de la forme  $2^{2^i} + 1 = 2^{i+1} \cdot 2^{2^i-i-1} + 1$  il y a  $2^{i+1}$  résidus  $(2^{2^i-i-1})$ -ième puissance et à cause  $2^{2^{i+1}} \equiv 1 (\text{mod } 2^i + 1)$ ,  $2$  est résidu  $(2^{2^i-i-1})$ -ième puissance: les  $2^{i+1}$  résidus, même puissance, sont donc  $1, 2, 2^2, 2^3, \dots, 2^{2^i-1} : -1, -2, -2^2, -2^3, \dots, -2^{2^i-1}$ .

Il résulte de là que l'on sait *a priori* que dans la résolution de l'équation du second degré dont la somme des racines est exprimée par la période  $(2^{i+1}, 1)$  le signe  $+$  du radical appartient à la période  $(2^i, 1)$  et par conséquent le signe  $-$  à la période  $(2^i, g^{2^{2^i-i-1}})$ .

En effet on a en dernière analyse

$$\begin{aligned}(2^i, 1) &= 2 \left\{ \cos \frac{P}{n} + \cos \frac{2^2 P}{n} + \cos \frac{2^4 P}{n} + \cos \frac{2^6 P}{n} + \cdots + \cos \frac{2^{2^i-2} P}{n} \right\} \\ &= 2 \left\{ \cos \frac{2^2 P}{4n} + \cos \frac{2^4 P}{4n} + \cos \frac{2^6 P}{4n} + \cos \frac{2^8 P}{4n} + \cdots + \cos \frac{2^{2^i-2} P}{4n} \right\}, \\ (2^i, g^{2^{2^i-i-1}}) &= 2 \left\{ \cos \frac{2P}{n} + \cos \frac{2^3 P}{n} + \cos \frac{2^5 P}{n} + \cos \frac{2^7 P}{n} + \cdots + \cos \frac{2^{2^i-1} P}{n} \right\}.\end{aligned}$$

En comparant ces valeurs termes à termes on voit évidemment que  $(2^i, 1)$  est  $> (2^i, g^{2^{2^i-i-1}})$  car tous les termes de la valeur de  $(2^i, 1)$  sont positifs et plus grands que leurs correspondants dans la valeur de  $(2^i, g^{2^{2^i-i-1}})$ , dont le dernier est même négatif.

On trouve de même

$$(2^{i-1}, 1) > (2^{i-1}, g^{2^{2^i-i-1}}) > (2^{i-1}, g^{2^{2^i-i}}) > (2^{i-1}, g^{3 \cdot 2^{2^i-i-1}})$$

et encore

$$\begin{aligned}(2^{i-2}, 1) &> (2^{i-2}, g^{2^{2^i-i-1}}) > (2^{i-2}, g^{2^{2^i-i}}) > (2^{i-2}, g^{3 \cdot 2^{2^i-i-1}}) \\ &> (2^{i-2}, g^{2^{2^i-i+1}}) > (2^{i-2}, g^{5 \cdot 2^{2^i-i-1}}) > (2^{i-2}, g^{3 \cdot 2^{2^i-i+1}}) > (2^{i-2}, g^{7 \cdot 2^{2^i-i-1}}).\end{aligned}$$

Il en est de même pour les périodes de  $2^{i-3}, 2^{i-4}$ , etc. termes de sorte que la valeur de ces périodes est d'autant plus grande qu'elles contiennent des puissances de  $g$  moins élevées.



Pour les nombres premiers  $2^{2^i} + 1$ , 3 est toujours racine primitive car pour les nombres de cette forme tous les non résidus jouissent de cette propriété (nr. 117) 3 est non résidus pour les nombres premiers de la forme  $12n + 5$  et on trouve  $2^{2^i} + 1 = 4(2^{2^i-2} - 1) + 5 = 4 \cdot 2(2^{2^i-3} - 2^{2^i-4} + 2^{2^i-5} \dots + 2 - 1) + 5$ .



Les deux premières parties du théorème n° [art.] 98 sont également vraies pour les résidus et non résidus  $2^s$ -ième puissances ( $\text{mod } 2^s m + 1$ ) et elles peuvent être démontrées par des raisonnements analogues à ceux employés n° cité.

A l'égard de la troisième la méthode du même n° prouverait seulement que le produit de deux résidus  $2^{s-1}$ -ième puissance, si ils sont un et l'autre non résidus  $2^s$ -ième puissance ( $\text{mod } 2^s m + 1$ ) est résidu  $2^s$ -ième puissance, même modul.

En effet il y a  $2m$  résidus puissance  $2^{s-1}$ -ième et parmi ces nombres la moitié sont résidus et la moitié non résidus  $2^s$ -ième puissance. Si donc  $A$  et  $B$  sont non résidus et que l'on multiplie les  $m$  nombres résidus par  $A$ , on aura  $m$  nombres non résidus et incongruants entre eux; maintenant le produit  $AB$  n'est congruant à aucun de ces nombres et il est nécessairement résidu puissance  $2^{s-1}$ -ième, puisque  $A$  et  $B$  sont l'un et l'autre résidus pour cette puissance: si donc il était en même temps non résidu puissance  $2^s$ -ième, il y aurait parmi les  $2m$ , nombres  $m + 1$  non résidus puissance  $2^s$ -ième et par conséquent seulement  $m - 1$  résidus.

Mais en général le produit  $hh'$  sera résidu  $2^s$ -ième puissance si  $h$  étant  $\equiv R^{2^sx+r} (\text{mod } 2^s m + 1)$  et  $h' = R^{2^sy+r'} \text{ on a } r + r' \equiv 0 (\text{mod } 2^s)$ .

### Gauss's reply.

Brunswick, 20 août 1805

Je profite de la complaisance de M. Grégoire pour vous offrir,<sup>58</sup> avec beaucoup de remerciements pour toutes les communications de votre dernière lettre, un exemplaire d'un petit mémoire que j'ai publié en 1799 et qui probablement vous sera encore inconnu.<sup>59</sup> Vous souhaitez de savoir tout ce que j'ai écrit en latin. Cette pièce est la seule outre mes recherches arithmétiques, et en même temps celle qui a paru la première, quoique alors l'impression de mes *Disquisitiones* eût été portée au-delà de la moitié.

Je suis à présent occupé à perfectionner quelques méthodes nouvelles par rapport aux calculs des perturbations planétaires : celles-ci et les méthodes dont je me suis servi pour calculer les éléments elliptiques des différentes nouvelles planètes, fourniront probablement les matériaux pour mon premier ouvrage.

Je vous salue cordialement

Ch. Fr. Gauss

<sup>58</sup> Likely Henry Grégoire, also known as "Abbé Grégoire" [1750–1831], member of the Comité d'instruction publique and founder of the Conservatoire des Arts et métiers and of the Bureau des longitudes.

<sup>59</sup> Gauss is referring to *Demonstratio nova theorematis: omnem functionem algebraicam rationalem integrum unius variabilis in factores reales primi vel secundi gradus resolvi posse* [Gauss 1799].

### III

Paris 16 novembre 1805

Monsieur

Je dois vous paraître bien coupable d'avoir tardé si longtemps à vous remercier de la lettre dont vous m'avez honoré et de l'envoi du mémoire que vous avez bien voulu y joindre; cependant il n'y a pas de ma faute, le paquet ne m'a été remis qu'il y a huit jours, Mr. De Sacy était en voyage depuis plus de 2 mois et on avait négligé chez lui de me le faire tenir; il est vrai que n'espérant pas de vous une réponse si prompte je n'avais mis aucun soin à m'informer des lettres qui m'étaient adressées.

Votre mémoire m'a fait d'autant plus de plaisir que je le connaissais déjà par une lecture rapide que m'avait procurée l'un des savans auxquels vous l'avez envoyée, et qu'ayant toujours eu le désir de l'étudier, comme on doit le faire de tous les ouvrages qui sortent de votre plume je l'avais inutilement fait demander à Leipsik, d'où j'avais reçu pour réponse que l'édition était épuisée.

L'indulgence que vous continuez de me témoigner m'encourage à vous communiquer encore quelques unes de mes nouvelles recherches.

Après avoir réduit suivant que vous l'indiquez, les formes ternaires dont la déterminante est zéro aux formes binaires, j'ai cherché si cette propriété s'étendait aux formes quaternaires, c'est-à-dire, si ces formes étaient susceptibles de se réduire aux formes ternaires lorsque leur déterminante est zéro et j'ai examiné ensuite quelques autres propriétés des mêmes formes et de leurs adjointes.

Je crois que si  $\mathcal{D}$  est la déterminante d'une forme composée de  $n$  variables  $\mathcal{D}^{n-1}$  sera la déterminante de l'adjointe de cette forme: c'est ainsi que vous avez trouvé  $\mathcal{D}^2$  pour la déterminante de l'adjointe ternaire et que, d'après mes calculs  $\mathcal{D}^3$  est la déterminante de l'adjointe quaternaire. Cette analogie n'est sans doute pas suffisante pour établir la généralité de la proposition mais on voit au moins que la déterminante de la forme étant composée de produits de l'ordre  $n$  et les coefficients de son adjoint l'étant de produits de l'ordre  $n - 1$ ,  $\mathcal{D}^{n-1}$  est du même ordre que la déterminante de l'adjointe; c'est-à-dire de l'ordre  $n(n - 1)$ .

Ces deux propositions, savoir: que la déterminante d'une forme est composée de produits des coefficients de ses termes de l'ordre qui exprime le nombre des variables dont elle est composée et que les coefficients de l'adjointe le sont de produits de l'ordre immédiatement inférieur; m'ont paru résulter de la nature générale des formes et de leurs adjointes.

Je regarde comme une faveur, la permission que vous voulez bien m'accorder de vous communiquer mes faibles efforts persuadé que vous aurez assez de bonté pour m'avertir des erreurs qui pourraient m'échapper, dans un genre de recherches où vous êtes le seul juge éclairé que l'on puisse consulter.

Les nouveaux renseignements que j'ai pris au sujet du libraire Duprat ne sont rien moins que satisfaisants: son successeur a dit avoir depuis longtemps terminé ses paiements dont le produit a été aussitôt divisé : il est retiré dans une petite ville où il vit du revenu d'un médiocre emploi et l'avis général de toutes les personnes que j'ai consultées a été qu'il est à peu près impossible de tirer de l'argent de lui.

Je n'avais pas jugé nécessaire de vous communiquer ces résultats parce que je ne vois pas que vous puissiez en tirer parti: et j'attendais pour vous écrire de nouveau

que vous m'eussiez accordé la permission: le retard qu'a éprouvé la remise de votre lettre m'a privé de vous faire plustôt tous mes remerciements et les protestations de mon profond respect

Le Blanc

### Addendum

*La forme quaternaire:*

$$\begin{aligned} & axx + a'x'x' + a''x''x'' + a'''x'''x''' + 2bx'''x'' + 2b'x'''x' \\ & + 2b''x'''x + 2b'''x''x' + 2b'''x''x + 2b^v x'x \\ & = \begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b''' \\ & & & b^v \end{pmatrix} \end{aligned}$$

est réducible aux formes ternaires lorsque la déterminante

$$\begin{aligned} \mathcal{D} = & a'bb + aa''b'b' + a'a''b''b'' + aa'''b'''b''' + a'a'''b'''b''' + a''a'''b^vb^v \\ & - (bbb^vb^v + b'b'b'''b''' + b''b''b'''b'') + 2bb''b'''b^v + 2bb'b'''b^v + 2b'b''b'''b''' \\ & - 2(abbb'b''' + a'bb''b''' + a''b'b''b^v + a'''b'''b'''b^v) - aa'a''a''' \end{aligned}$$

est égale à zéro.

Pour le prouver mettons  $\mathcal{D}$  dans la forme:

$$\begin{aligned} & a(a'bb + a''b'b' + a'''b'''b''' - 2bb'b''' - a'a''a''') \\ & - (bb - a''a''')b^vb^v - (b'b' - a'a''')b'''b''' - (b'''b''' - a'a'')b''b'' \\ & - 2(a'''b''' - bb')b^vb''' - 2(a''b' - bb'')b^vb'' - 2(a'b - b'b''')b'''b'', \end{aligned}$$

nous trouverons

$$\begin{aligned} & \mathcal{D}(bb - a''a''') \\ & = (abb - aa''a''')(a'bb + a''b'b' + a'''b'''b''' - 2bb'b''' - a'a''a''') \\ & - \{(bb - a''a''')b^v + (a'''b''' - bb')b''' + (a''b' - bb'')b''\}^2 \\ & - \{(b'b' - a'a''')(bb - a'a''') - (a'''b''' - bb')^2\}b'''b''' \\ & - 2\{(bb - a''a''')(a'b - b'b'''') - (a'''b''' - bb')(a''b' - bb'')\}b'''b'' \\ & - \{(b'''b''' - a'a'')(bb - a'a''') - (a''b' - bb'')\}b''b'' \\ & = (abb - aa''a''')(a'bb + a''b'b' + a'''b'''b''' - 2bb'b''' - a'a''a''') - \{a''a'''b^v - bbb^v \\ & + bb'b''' + bb''b''' - a'''b'''b''' - a''b'b''\}^2 + (a'bb + a''b'b' + a'''b'''b''' \\ & - 2bb'b''' - a'a''a''')(a'''b'''b''' - 2bb'b''' + a''b''b'') \\ & = (a'bb + a''b'b' + a'''b'''b''' - 2bb'b''' - a'a''a''')(abb + a''b''b'' + a'''b'''b''' \\ & - 2bb'b''' + -aa''a''') - (a''a'''b^v - bbb^v + bb'b''' + bb''b''' - a'''b'''b''' \\ & - a''b'b'')^2. \end{aligned}$$

$$\begin{aligned}
& \mathcal{D}(a'''b''' - bb') \\
&= (aa''b''' - abb')(a'bb + a''b'b' + a'''b'''b''' - 2bb'b''' - a'a''a''') \\
&\quad - \{(bb - a''a'')b^v + (a'''b''' - bb')b''' + (a''b' - bb'')b''\}\{(b'b' - a'a'')b''' \\
&\quad + (a'''b''' - bb')b^v + (a'b - b'b'')b''\} \\
&\quad - \{(b'''b''' - a'a'')(a'''b''' - bb') - (a''b' - bb'')(a'b - b'b'')\}b''b'' \\
&\quad - \{(a'''b''' - bb')^2 - (bb - a''a'')(b'b' - a'a'')\}b'''b^v \\
&\quad - \{(a''b' - bb'')(a'''b''' - bb') - (bb - a''a'')(a'b - b'b'')\}b''b^v \\
&\quad - \{(a'b - b'b'')(a'''b''' - bb') - (b'b' - a'a'')(a''b' - bb'')\}b'''b^v \\
&= (aa'''b''' - abb')(a'bb + a''b'b' + a'''b'''b''' - 2bb'b''' - a'a''a''') \\
&\quad - (a''a'''b^v - bbb^v + bb'b''' + bb''b''' - a''b'b' - a'''b'''b''') \\
&\quad \times (a'a'''b''' - b'b'b''' + bb'b^v + b'b'b''' - a'bb'' - a'''b'''b^v) \\
&\quad - (a'bb + a''b'b' + a'''b'''b''' - 2bb'b''' - a'a''a'')(b''b''b''' + a'''b'''b^v \\
&\quad - bb''b^v - b'b''b'''') \\
&= (a'bb + a''b'b' + a'''b'''b''' - 2bb'b''' - a'a''a'')(aa'''b''' \\
&\quad - b''b''b''' + bb''b^v + b'b''b''' - abb' - a'''b'''b^v) \\
&\quad - (a''a'''b^v - bbb^v + bb'b''' + bb''b''' - a''b'b'' - a'''b'''b''')(a'a'''b''' - b'b'b''' \\
&\quad + bb'b^v + b'b''b''' - a'bb'' - a'''b'''b^v),
\end{aligned}$$

ou en faisant

$$\begin{aligned}
& a'bb + a''b'b' + a'''b'''b''' - 2bb'b''' - a'a''a''' = \mathcal{A}, \\
& abb + a''b''b'' + a'''b'''b''' - 2bb''b''' - aa''a''' = \mathcal{A}', \\
& ab'b' + a''b''b'' + a'''b''b^v - 2b'b''b^v - aa'a''' = \mathcal{A}'', \\
& ab'''b''' + a'b'''b''' + a''b''b^v - 2b'''b'''b^v - aa'a'' = \mathcal{A}''', \\
& aa'b - b''b''b + b''b'''b^v + b'b'''b^v - ab'b''' - a'b''b''' = \mathcal{B}, \\
& aa''b' - b'''b'''b' + bb'''b^v + b''b'''b''' - abb''' - a''b''b^v = \mathcal{B}', \\
& a'a''b'' - b'''b'''b'' + bb''b^v + b'b'''b''' - a'bb''' - a''b'b'' = \mathcal{B}'', \\
& aa'''b''' - b''b''b''' + bb''b^v + b'b''b''' - abb' - a'''b'''b^v = \mathcal{B}''', \\
& a'a'''b''' - b'b'b''' + bb'b^v + b'b''b''' - a'bb'' - a'''b'''b^v = \mathcal{B}'''' , \\
& a''a'''b^v - bbb^v + bb''b''' + bb''b''' - a''b'b'' - a'''b'''b''' = \mathcal{B}^{\mathcal{V}}, \\
& \mathcal{D}(bb - a''a''') = \mathcal{A}\mathcal{A}' - \mathcal{B}^{\mathcal{V}}\mathcal{B}^{\mathcal{V}}, \quad \mathcal{D}(a'''b''' - bb') = \mathcal{A}\mathcal{B}''' - \mathcal{B}'''^{\mathcal{V}}\mathcal{B}^{\mathcal{V}},
\end{aligned}$$

et par des calculs semblables

$$\begin{aligned}
& \mathcal{D}(b'b' - a'a'') = \mathcal{A}\mathcal{A}'' - \mathcal{B}''\mathcal{B}''', \\
& \mathcal{D}(b'''b''' - a'a'') = \mathcal{A}\mathcal{A}''' - \mathcal{B}''\mathcal{B}'', \quad \mathcal{D}(a'b - b'b'') = \mathcal{A}\mathcal{B} - \mathcal{B}''\mathcal{B}''' ;
\end{aligned}$$

puis en mettant  $\mathcal{D}$  sous la forme

$$\begin{aligned} a'\mathcal{A}' - (bb - a''a''')b^vb^v - (b''b'' - aa''')b'''b''' - (b''''b'''' - aa'')b'b' \\ - 2(a'''b'''' - bb'')b'''b^v - 2(a''b'' - bb''')b'b^v - 2(ab - b''b''')b'b''' \end{aligned}$$

[on a]

$$\begin{aligned} \mathcal{D}(b''b'' - aa''') &= \mathcal{A}'\mathcal{A}'' - \mathcal{B}''' \mathcal{B}''' , \\ \mathcal{D}(b'''b'''' - aa'') &= \mathcal{A}'\mathcal{A}''' - \mathcal{B}' \mathcal{B}' , \\ \mathcal{D}(a'''b''' - bb'') &= \mathcal{A}' \mathcal{B}''' - \mathcal{B}''' \mathcal{B}^V , \\ \mathcal{D}(a''b'' - bb''') &= \mathcal{A}' \mathcal{B}'' - \mathcal{B}' \mathcal{B}^V , \\ \mathcal{D}(ab - b''b''') &= \mathcal{A}' \mathcal{B} - \mathcal{B}' \mathcal{B}''' ; \end{aligned}$$

[et] sous celle

$$\begin{aligned} a''\mathcal{A}'' - (b''b'' - aa''')b'''b''' - (b'b' - a'a''')b''''b'''' - (b^vb^v - aa')bb \\ - 2(a'''b^v - b'b'')b'''b'''' - 2(a'b'' - b'b^v)bb'''' - 2(ab' - b''b^v)bb''' \end{aligned}$$

[on a]

$$\begin{aligned} \mathcal{D}(b^vb^v - aa') &= \mathcal{A}''\mathcal{A}''' - \mathcal{B}\mathcal{B}, \\ \mathcal{D}(a'''b^v - b'b'') &= \mathcal{A}'' \mathcal{B}^V - \mathcal{B}''' \mathcal{B}''' , \\ \mathcal{D}(a'b'' - b'b^v) &= \mathcal{A}'' \mathcal{B}'' - \mathcal{B}''' \mathcal{B}, \\ \mathcal{D}(ab' - b''b^v) &= \mathcal{A}'' \mathcal{B}' - \mathcal{B}''' \mathcal{B}; \end{aligned}$$

et enfin sous cette-ci

$$\begin{aligned} a'''\mathcal{A}''' - (b'''b''' - a'a'')b''b'' - (b''''b'''' - aa'')b'b' - (b^vb^v - aa')bb \\ - 2(a''b^v - b'''b''')b'b'' - 2(a'b''' - b'''b^v)bb'' - 2(ab''' - b'''b^v)bb' \end{aligned}$$

[on a]

$$\begin{aligned} \mathcal{D}(a''b^v - b'''b''') &= \mathcal{A}''' \mathcal{B}^V - \mathcal{B}' \mathcal{B}'' , \\ \mathcal{D}(a'b''' - b'''b^v) &= \mathcal{A}''' \mathcal{B}''' - \mathcal{B}\mathcal{B}'' , \\ \mathcal{D}(ab''' - b'''b^v) &= \mathcal{A}''' \mathcal{B}''' - \mathcal{B}\mathcal{B}' . \end{aligned}$$

Ainsi, lorsque  $\mathcal{D} = 0$  il faut satisfair aux équations

$$\begin{aligned} \mathcal{A}\mathcal{A}' &= \mathcal{B}^V \mathcal{B}^V, & \mathcal{A}\mathcal{B}''' &= \mathcal{B}''' \mathcal{B}^V, & \mathcal{A}'' \mathcal{B}^V &= \mathcal{B}''' \mathcal{B}''' , \\ \mathcal{A}\mathcal{A}'' &= \mathcal{B}''' \mathcal{B}''' , & \mathcal{A}\mathcal{B}' &= \mathcal{B}'' \mathcal{B}^V, & \mathcal{A}'' \mathcal{B}'' &= \mathcal{B}\mathcal{B}''' , \end{aligned}$$

$$\begin{aligned} \mathcal{A}\mathcal{A}''' &= \mathcal{B}''\mathcal{B}'', & \mathcal{A}\mathcal{B} &= \mathcal{B}''\mathcal{B}''', & \mathcal{A}''\mathcal{B}' &= \mathcal{B}\mathcal{B}''', \\ \mathcal{A}'\mathcal{A}'' &= \mathcal{B}''' \mathcal{B}''', & \mathcal{A}'\mathcal{B}''' &= \mathcal{B}''\mathcal{B}^v, & \mathcal{A}''' \mathcal{B}^v &= \mathcal{B}'\mathcal{B}'', \\ \mathcal{A}'\mathcal{A}''' &= \mathcal{B}'\mathcal{B}', & \mathcal{A}'\mathcal{B}'' &= \mathcal{B}'\mathcal{B}^v, & \mathcal{A}''' \mathcal{B}''' &= \mathcal{B}\mathcal{B}'', \\ \mathcal{A}''\mathcal{A}''' &= \mathcal{B}\mathcal{B}, & \mathcal{A}'\mathcal{B} &= \mathcal{B}'\mathcal{B}'', & \mathcal{A}''' \mathcal{B}''' &= \mathcal{B}\mathcal{B}', \end{aligned}$$

pour cela nous pouvons supposer  $\mathcal{A} = m\delta^2$ ,  $\mathcal{A}' = m\alpha^2$ ,  $\mathcal{A}'' = m\beta^2$ ,  $\mathcal{A}''' = mv^2$ ; d'où il résulte, en se bornant aux valeur positives de  $\mathcal{B}$ ,  $\mathcal{B}'$ , etc.,  $\mathcal{B} = m\beta v$ ,  $\mathcal{B}' = m\alpha v$ ,  $\mathcal{B}'' = m\delta v$ ,  $\mathcal{B}''' = m\alpha\beta$ ,  $\mathcal{B}'''' = m\delta\beta$ ,  $\mathcal{B}^v = m\delta\alpha$ ; et comme la déterminante  $\mathcal{D}$  peut encore être mise sous les quatre formes

$$\begin{aligned} a\mathcal{A} + b^v\mathcal{B}^v + b''''\mathcal{B}'''' + b''\mathcal{B}'', &\quad a'\mathcal{A}' + b^v\mathcal{B}^v + b''''\mathcal{B}'''' + b'\mathcal{B}', \\ a''\mathcal{A}'' + b''''\mathcal{B}'''' + b''\mathcal{B}'' + b\mathcal{B}, &\quad a''' \mathcal{A}''' + b''\mathcal{B}'' + b'\mathcal{B}' + b\mathcal{B}; \end{aligned}$$

nous avons pour le cas présent quatre équations

$$\begin{aligned} a\delta^2 + b^v\delta\alpha + b''''\delta\beta + b''\delta v &= 0, & a'\alpha^2 + b^v\delta\alpha + b''''\alpha\beta + b'\nu\alpha &= 0, \\ a''\beta^2 + b''''\delta\beta + b''''\alpha\beta + b\nu\beta &= 0, & a'''v^2 + b''\delta v + b'\alpha\nu + b\beta\nu &= 0; \end{aligned}$$

ajoutant ensemble les trois premières de ces équations et mettent pour  $a'''v^2$  sa valeur tirée de la dernière nous aurons

$$a\delta^2 + a'\alpha^2 + a''\beta^2 + 2b^v\delta\alpha + 2b''''\delta\beta + 2b''''\beta\alpha = a'''v^2$$

qui étant jointe aux autres équations trouvées par un calcul semblable donne

$$\left. \begin{aligned} a\delta^2 + a'\alpha^2 + a''\beta^2 + 2b^v\delta\alpha + 2b''''\delta\beta + 2b''''\beta\alpha &= a'''v^2 \\ a\delta^2 + a'\alpha^2 + a'''v^2 + 2b^v\delta\alpha + 2b''\delta v + 2b'\nu\alpha &= a''\beta^2 \\ a\delta^2 + a''\beta^2 + a'''v^2 + 2b''''\delta\beta + 2b''\delta v + 2b\nu\beta &= a'\alpha^2 \\ a'\alpha^2 + a''\beta^2 + a'''v^2 + 2b''''\alpha\beta + 2b'\alpha\nu + 2b\nu\beta &= a\delta^2 \end{aligned} \right\} \quad (1)$$

et les quatre premières équations divisées respectivement pour  $\delta$ ,  $\alpha$ ,  $\beta$ ,  $\nu$  se réduisent à

$$\left. \begin{aligned} a\delta + b^v\alpha + b''''\beta + b''\nu &= 0 \\ a'\alpha + b^v\delta + b''''\beta + b'\nu &= 0 \\ a''\beta + b''''\delta + b''''\alpha + b\nu &= 0 \\ a'''v + b''\delta + b'\alpha + b\beta &= 0 \end{aligned} \right\} \quad (2)$$

enfin de ce deux système d'équations nous concluons

$$\delta^2 \begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b''' \end{pmatrix} = \begin{pmatrix} a' & a'' & a''' \\ b & b' & b''' \end{pmatrix},$$

$$\begin{aligned}\alpha^2 \begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b''' \\ & & & b'''' \\ & & & b^v \end{pmatrix} &= \begin{pmatrix} a & a'' & a''' \\ b & b'' & b'''' \\ & & b^v \end{pmatrix}, \\ \beta^2 \begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b''' \\ & & & b'''' \\ & & & b^v \end{pmatrix} &= \begin{pmatrix} a & a' & a''' \\ b' & b'' & b^v \\ & & b^v \end{pmatrix}, \\ v^2 \begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b''' \\ & & & b'''' \\ & & & b^v \end{pmatrix} &= \begin{pmatrix} a & a' & a'' \\ b''' & b'''' & b^v \end{pmatrix}.\end{aligned}$$

*Exemple de calcul*

$$\begin{aligned}a\delta^2xx + a'\delta^2x'x' + a''\delta^2x''x'' + a'''\delta^2x'''x''' + 2b\delta^2x''''x'' + 2b'\delta^2x''''x' \\+ 2b''\delta^2x''''x + 2b'''\delta^2x''x' + 2b''''\delta^2x''x + 2b^v\delta^2x'x \\= (a'\alpha^2 + a''\beta^2 + a'''\nu^2 + 2b''''\alpha\beta + 2b'\alpha\nu + 2b\nu\beta)xx + a'\delta^2x'x' \\+ a''\delta^2x''x'' + a'''\delta^2x'''x''' + 2b\delta^2x''''x'' + 2b'\delta^2x''''x' - 2(a'''\nu + b\beta + b'\alpha)\delta x''x \\+ 2b''\delta^2x''x' - 2(a''\beta + b'''\alpha + b\nu)\delta x''x - 2(a'\alpha + b''''\beta + b'\nu)\delta x'x \\= a'(\alpha^2xx + \delta^2x'x' - 2\alpha\delta xx') + a''(\beta^2xx + \delta^2x''x'' - 2\beta\delta xx'') + a''''(\nu^2xx \\+ \delta^2x''''x''' - 2\nu\delta xx''') + 2b(\nu\beta xx + \delta^2x''''x'' - \beta\delta x''x - \nu\delta x''x) \\+ 2b'(\alpha\nu xx + \delta^2x''''x' - \alpha\delta x''''x - \nu\delta x'x) + 2b''''(\alpha\beta xx + \delta^2x''x'' - \alpha\delta x''x - \beta\delta x'x) \\= a'(\alpha x - \delta x')^2 + a''(\beta x - \delta x'')^2 + a''''(\nu x - \delta x''')^2 + 2b(\beta x - \delta x')(\nu x \\- \delta x''') + 2b'(\alpha x - \delta x')(\nu x - \delta x''') + 2b''''(\alpha x - \delta x')(\beta x - \delta x'').\end{aligned}$$

*Lorsque  $\mathcal{D} = 0$ , l'adjointe*

$$\begin{pmatrix} \mathcal{A} & \mathcal{A}' & \mathcal{A}'' & \mathcal{A}''' \\ \mathcal{B} & \mathcal{B}' & \mathcal{B}'' & \mathcal{B}''' & \mathcal{B}'''' & \mathcal{B}^v \end{pmatrix}$$

*de la forme*

$$\begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b''' \\ & & & b'''' \\ & & & b^v \end{pmatrix},$$

*se réduit à un carré multiplié par m facteur commun des coefficients de ses termes.*

Car

$$\begin{aligned}\mathcal{A}xx + \mathcal{A}'x'x' + \mathcal{A}''x''x'' + \mathcal{A}'''x'''x''' + 2\mathcal{B}x''''x'' + 2\mathcal{B}'x''''x' + 2\mathcal{B}''x''''x \\+ 2\mathcal{B}''''x''x' + 2\mathcal{B}''''''x''x + 2\mathcal{B}^v x'x = m\{\delta^2xx + \alpha^2x'x' + \beta^2x''x'' + \nu^2x''''x''' \\+ 2\beta\nu x''''x'' + 2\alpha\nu x''''x' + 2\delta\nu x''x + 2\alpha\beta x''x' + 2\delta[\beta]x''x + 2\delta\alpha x'x\} \\= m(\delta x + \alpha x' + \beta x'' + \nu x''')^2,\text{ }^{60}\end{aligned}$$

par conséquent  $a, b^v, b''''; b'', b', b''; b''''; b''''', b''''; a'', b;$  et  $b'', b', b, a'''$  sont les valeurs de  $x, x', x'', x'''$  qui, dans ce cas, rendent l'adjointe égale à zéro.

<sup>60</sup> It should be  $2\delta\beta x''x$  instead of  $2\delta\nu x''x$ .

Si on ajoute ensemble les quatre équations (1) on trouve, après la division par 2,

$$\begin{aligned} a\delta^2 + a'\alpha^2 + a''\beta^2 + a'''v^2 + 2b\nu\beta + 2b'\nu\alpha + 2b''\nu\delta \\ + 2b'''\beta\alpha + 2b''''\beta\delta + 2b^v\alpha\delta = 0 \end{aligned}$$

c'est-à-dire que pour le même cas,  $\delta, \alpha, \beta, \nu$  sont les valeurs de  $x, x', x'', x'''$  qui rendent la forme

$$\begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b''' \end{pmatrix}$$

égale à zéro.



L'adjointe de la forme

$$\begin{pmatrix} \mathcal{A} & \mathcal{A}' & \mathcal{A}'' & \mathcal{A}''' \\ \mathcal{B} & \mathcal{B}' & \mathcal{B}'' & \mathcal{B}''' \end{pmatrix}$$

est celle-ci

$$\begin{pmatrix} aD^2 & a'D^2 & a''D^2 & a'''D^2 \\ bD^2 & b'D^2 & b''D^2 & b'''D^2 \end{pmatrix},$$

en effet au moyen des équations, qu'il est aisément de vérifier,

$$\begin{aligned} Ab^v + \mathcal{B}''b' + \mathcal{B}'''b''' + \mathcal{B}^v a' &= 0, \\ Ab''' + \mathcal{B}''b + \mathcal{B}^v b''' + \mathcal{B}'''a'' &= 0, \\ Ab'' + \mathcal{B}'''b + \mathcal{B}^v b' + \mathcal{B}''a''' &= 0, \\ \mathcal{A}b^v + \mathcal{B}'b'' + \mathcal{B}'''b''' + \mathcal{B}^v a &= 0, \end{aligned}$$

on trouve:

$$\begin{aligned} \mathcal{A}'\mathcal{B}\mathcal{B} + \mathcal{A}''\mathcal{B}'\mathcal{B} + \mathcal{A}'''\mathcal{B}''\mathcal{B}''' - 2\mathcal{B}\mathcal{B}'\mathcal{B}''' - \mathcal{A}'\mathcal{A}''\mathcal{A}''' &= D^2a \\ \mathcal{A}\mathcal{B}\mathcal{B} + \mathcal{A}''\mathcal{B}'\mathcal{B}'' + \mathcal{A}'''\mathcal{B}''\mathcal{B}''' - 2\mathcal{B}\mathcal{B}'\mathcal{B}''' - \mathcal{A}\mathcal{A}''\mathcal{A}''' &= D^2a' \\ \mathcal{A}\mathcal{B}'\mathcal{B}' + \mathcal{A}'\mathcal{B}''\mathcal{B}'' + \mathcal{A}''\mathcal{B}^v\mathcal{B}^v - 2\mathcal{B}'\mathcal{B}''\mathcal{B}^v - \mathcal{A}\mathcal{A}'\mathcal{A}''' &= D^2a'' \\ \mathcal{A}\mathcal{B}''' \mathcal{B}''' + \mathcal{A}'\mathcal{B}''' \mathcal{B}''' + \mathcal{A}''\mathcal{B}^v\mathcal{B}^v - 2\mathcal{B}''' \mathcal{B}''' \mathcal{B}^v - \mathcal{A}\mathcal{A}'\mathcal{A}'' &= D^2a''' \\ \mathcal{A}\mathcal{A}'\mathcal{B} - \mathcal{B}^v\mathcal{B}^v\mathcal{B} + \mathcal{B}''\mathcal{B}''\mathcal{B}^v + \mathcal{B}'\mathcal{B}''' \mathcal{B}^v - \mathcal{A}\mathcal{B}'\mathcal{B}''' - \mathcal{A}'\mathcal{B}''\mathcal{B}''' &= D^2b \\ \mathcal{A}\mathcal{A}''\mathcal{B}' - \mathcal{B}''' \mathcal{B}''' \mathcal{B}' + \mathcal{B}\mathcal{B}''' \mathcal{B}^v + \mathcal{B}''\mathcal{B}''' \mathcal{B}''' - \mathcal{A}\mathcal{B}\mathcal{B}''' - \mathcal{A}''\mathcal{B}''\mathcal{B}^v &= D^2b' \\ \mathcal{A}'\mathcal{A}''\mathcal{B}'' - \mathcal{B}''' \mathcal{B}''' \mathcal{B}'' + \mathcal{B}\mathcal{B}''' \mathcal{B}^v + \mathcal{B}'\mathcal{B}''' \mathcal{B}''' - \mathcal{A}'\mathcal{B}\mathcal{B}''' - \mathcal{A}''\mathcal{B}'\mathcal{B}^v &= D^2b'' \\ \mathcal{A}\mathcal{A}''' \mathcal{B}''' - \mathcal{B}'' \mathcal{B}'' \mathcal{B}''' + \mathcal{B}\mathcal{B}'' \mathcal{B}^v + \mathcal{B}'\mathcal{B}'' \mathcal{B}''' - \mathcal{A}\mathcal{B}\mathcal{B}' - \mathcal{A}''' \mathcal{B}''' \mathcal{B}^v &= D^2b''' \\ \mathcal{A}'\mathcal{A}''' \mathcal{B}''' - \mathcal{B}' \mathcal{B}' \mathcal{B}''' + \mathcal{B}\mathcal{B}' \mathcal{B}^v + \mathcal{B}'\mathcal{B}'' \mathcal{B}''' - \mathcal{A}'\mathcal{B}\mathcal{B}'' - \mathcal{A}''' \mathcal{B}''' \mathcal{B}^v &= D^2b'''' \end{aligned}$$

$$\mathcal{A}''\mathcal{A}'''B^V - \mathcal{B}\mathcal{B}\mathcal{B}^V + \mathcal{B}\mathcal{B}''\mathcal{B}''' + \mathcal{B}\mathcal{B}'\mathcal{B}''''' - \mathcal{A}''\mathcal{B}'\mathcal{B}'' - \mathcal{A}'''B'''B''''' = \mathcal{D}^2b^v$$

*Exemple de calcul*

$$\begin{aligned}
 & \mathcal{A}'\mathcal{B}\mathcal{B} + \mathcal{A}''\mathcal{B}'\mathcal{B} + \mathcal{A}'''B'''B''' - 2\mathcal{B}\mathcal{B}'\mathcal{B}''' - \mathcal{A}'\mathcal{A}''\mathcal{A}''' \\
 &= \mathcal{A}'(\mathcal{B}\mathcal{B} - \mathcal{A}''\mathcal{A}''') + \mathcal{B}'(\mathcal{A}'\mathcal{B}' - \mathcal{B}\mathcal{B}''') + \mathcal{B}'''(\mathcal{A}'''B''' - \mathcal{B}\mathcal{B}') \\
 &= \mathcal{D}\mathcal{A}'(aa' - b^vb^v) + \mathcal{D}\mathcal{B}'(b'a - b''b^v) + \mathcal{D}\mathcal{B}'''(b'''a - b^vb''') \\
 &= \mathcal{D}[a(\mathcal{A}'a' + \mathcal{B}'b' + \mathcal{B}'''b''' + \mathcal{B}^Vb^v) - b^v(\mathcal{A}'b^v + \mathcal{B}'b'' + \mathcal{B}'''b''''' + \mathcal{B}^Va)] \\
 &= \mathcal{D}^2a\mathcal{A}'\mathcal{A}''\mathcal{B}^V + \mathcal{B}\mathcal{B}\mathcal{B}^V + \mathcal{B}\mathcal{B}''\mathcal{B}''' + \mathcal{B}\mathcal{B}'\mathcal{B}''''' - \mathcal{A}''\mathcal{B}'\mathcal{B}'' - \mathcal{A}'''B'''B''''' \\
 &= \mathcal{B}^V(\mathcal{A}'\mathcal{A}''' - \mathcal{B}\mathcal{B}) + \mathcal{B}''(\mathcal{B}\mathcal{B}''' - \mathcal{A}''\mathcal{B}') + \mathcal{B}'''(\mathcal{B}\mathcal{B}' - \mathcal{A}'''B'') \\
 &= \mathcal{D}\mathcal{B}^V(b^vb^v - aa') + \mathcal{D}\mathcal{B}''(b''b^v - b'a) + \mathcal{D}\mathcal{B}'''(b'''b^v - b'''a) \\
 &= \mathcal{D}[b^v(\mathcal{B}^Vb^v + \mathcal{B}''b'' + \mathcal{B}'''b''''' + \mathcal{A}a) - a(\mathcal{B}^Va' + \mathcal{B}'b' + \mathcal{B}'''b''' + \mathcal{A}b^v)] \\
 &= \mathcal{D}^2b^v
 \end{aligned}$$

↔

$\mathcal{D}^3$  est la déterminante de l'adjointe  $\begin{pmatrix} \mathcal{A} & \mathcal{A}' & \mathcal{A}'' & \mathcal{A}''' \\ \mathcal{B} & \mathcal{B}' & \mathcal{B}'' & \mathcal{B}''' \\ & & & \mathcal{B}^V \end{pmatrix}$  car

$$\begin{aligned}
 & \mathcal{A}\mathcal{A}'\mathcal{B}\mathcal{B} + \mathcal{A}\mathcal{A}''\mathcal{B}'\mathcal{B}' + \mathcal{A}'\mathcal{A}''\mathcal{B}''\mathcal{B}'' + \mathcal{A}\mathcal{A}'''B'''B''' + \mathcal{A}'\mathcal{A}'''B'''B''''' + \mathcal{A}''\mathcal{A}'''B^VB^V \\
 & - (\mathcal{B}\mathcal{B}\mathcal{B}^V\mathcal{B}^V + \mathcal{B}'\mathcal{B}'\mathcal{B}'''B''' + \mathcal{B}''\mathcal{B}''\mathcal{B}''') + 2\mathcal{B}\mathcal{B}''\mathcal{B}'''B^V \\
 & + 2\mathcal{B}\mathcal{B}'\mathcal{B}'''\mathcal{B}^V + 2\mathcal{B}'\mathcal{B}'\mathcal{B}''\mathcal{B}''' - 2(\mathcal{A}\mathcal{B}\mathcal{B}'\mathcal{B}''' + \mathcal{A}'\mathcal{B}\mathcal{B}''\mathcal{B}''' + \mathcal{A}''\mathcal{B}'\mathcal{B}''\mathcal{B}'' \\
 & + \mathcal{A}'''B'''B'''\mathcal{B}^V) - \mathcal{A}\mathcal{A}'\mathcal{A}''\mathcal{A}''' \\
 &= \mathcal{A}\{\mathcal{A}'\mathcal{B}\mathcal{B} + \mathcal{A}''\mathcal{B}'\mathcal{B}' + \mathcal{A}'''B'''B''''' - 2\mathcal{B}\mathcal{B}'\mathcal{B}''' - \mathcal{A}'\mathcal{A}''\mathcal{A}'''\} \\
 & + \mathcal{B}''\{\mathcal{A}'\mathcal{A}''\mathcal{B}'' - \mathcal{B}''\mathcal{B}''\mathcal{B}'' + \mathcal{B}\mathcal{B}''\mathcal{B}^V + \mathcal{B}'\mathcal{B}'''B''' - \mathcal{A}'\mathcal{B}\mathcal{B}''' - \mathcal{A}''\mathcal{B}'\mathcal{B}^V\} \\
 & + \mathcal{B}'''(\mathcal{A}'\mathcal{A}'''B''' - \mathcal{B}'\mathcal{B}'\mathcal{B}''' + \mathcal{B}\mathcal{B}''\mathcal{B}^V + \mathcal{B}'\mathcal{B}''\mathcal{B}''' - \mathcal{A}'\mathcal{B}\mathcal{B}'' - \mathcal{A}'''B'''B^V) \\
 & + \mathcal{B}^V\{\mathcal{A}''\mathcal{A}'''B^V - \mathcal{B}\mathcal{B}\mathcal{B}^V + \mathcal{B}\mathcal{B}''\mathcal{B}''' + \mathcal{B}\mathcal{B}'\mathcal{B}''''' - \mathcal{A}''\mathcal{B}'\mathcal{B}'' - \mathcal{A}'''B'''B'''''\\
 &= \mathcal{D}^2\{\mathcal{A}a + \mathcal{B}''b'' + \mathcal{B}'''b''''' + \mathcal{B}^Vb^v\} = \mathcal{D}^3
 \end{aligned}$$

↔

La forme quaternaire  $\begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b''' \\ & & & b^v \end{pmatrix}$  est définie lorsque la forme ternaire  $\begin{pmatrix} A^v & A''' & A'' \\ -B & -B' & -B'' \end{pmatrix}$  dans laquelle

$$\begin{aligned}
 b^vb^v - aa' &= A^v, & ba - b''b''''' &= B, \\
 b'''b''''' - aa'' &= A''''' & b'a - b''b^v &= B', \\
 b''b'' - aa''' &= A'', & b'''a - b'''''b^v &= B'',
 \end{aligned}$$

est définie négative; elle est positive ou négative selon que  $a$  est positif ou négatif.

C'est ce qui résulte de la transformation invariante

$$\begin{aligned}
 & a \begin{pmatrix} a & a' & a'' & a''' & b''' & b^v \\ b & b' & b'' & b''' & b''' & b^v \end{pmatrix} \\
 &= aaxx + b^v b^v x' x' + b''' b''' x'' x'' + b'' b'' x''' x''' + 2a(b^v x' + b''' x'' + b'' x''') x \\
 &\quad + 2b^v b''' x'' x' + 2b'' b^v x'' x' + 2b'' b''' x'' x''' - (b^v b^v - aa') x' x' \\
 &\quad - (b''' b''' - aa'') x'' x'' - (b'' b'' - aa''') x''' x''' + 2(ba - b'' b''') x'' x''' \\
 &\quad + 2(b' a - b'' b^v) x' x''' + 2(b''' a - b''' b^v) x' x'' \\
 &= (ax + b^v x' + b''' x'' + b'' x''')^2 - \{A^v x' x' + A''' x'' x'' + A'' x''' x''' \\
 &\quad - 2Bx''' x'' - 2B' x''' x' - 2B'' x'' x'\}.
 \end{aligned}$$

Les conditions nécessaires pour que la forme  $\begin{pmatrix} A^v & A''' & A'' \\ -B & -B' & -B'' \end{pmatrix}$  soit définie négative se réduisent à  $A^v, a\mathcal{A}'''$  et  $\mathcal{D}$  négatifs.

Car d'après l'art. 271, les conditions sont  $B''B'' - A^v A''''$ ,  $A^v \mathcal{D}$  et  $A^v$  négatifs,<sup>61</sup> d'où résulte  $\mathcal{D}$  positif et on trouve

$$\begin{aligned}
 B''B'' - A''''A^v &= (b'''a - b'''b^v)^2 - (b^v b^v - aa')(b'''b''' - aa'') \\
 &= aab'''b''' + aa'b'''b''' + aa''b^v b^v - 2ab'''b'''b^v - aaa'a'' \\
 &= a\mathcal{A}''' \\
 BB'' + B'A'''' &= (ba - b''b''')(b'''a - b''''b^v) + (b'a - b''b^v)(b'''b''' - aa'') \\
 &= aabb''' - ab''b'''b''' - abb'''b^v + ab'''b'''b' - aaa''b' + aa''b''b^v \\
 &= -a\mathcal{B}' \\
 B'B'' + BA^v &= (b'a - b''b^v)(b'''a - b''''b^v) + (ba - b''b''')(b^v b^v - aa') \\
 &= aab'b''' - ab''b'''b^v - ab'b'''b^v + ab^v b^v b - aaa'b + aa'b''b'''' \\
 &= -a\mathcal{B}
 \end{aligned}$$

$$\begin{aligned}
 \mathcal{D} &= A^v BB + A''''B'B' + A''B''B'' + 2BB'B'' - A^v A''''A'' \\
 &= A''(B''B'' - A^v A''') + B(BA^v + B'B'') + B'(A''''B' + BB'') \\
 &= A''a\mathcal{A}''' - Ba\mathcal{B} - B'a\mathcal{B}' \\
 &= a\mathcal{A}'''(b''b'' - aa'') - a\mathcal{B}(ba - b''b''') - a\mathcal{B}'(b'a - b''b^v) \\
 &= (\text{à cause de } \mathcal{A}'''b'' + \mathcal{B}b''' + \mathcal{B}'b^v + \mathcal{B}''a = 0 \text{ et de } \mathcal{A}'''a''' + \mathcal{B}b + \mathcal{B}'b' + \mathcal{B}''b'' = \mathcal{D}) \\
 &\quad - a^2[\mathcal{A}'''a''' + \mathcal{B}b + \mathcal{B}'b' + \mathcal{B}''b''] + ab''[\mathcal{A}'''b'' + \mathcal{B}b''' + \mathcal{B}'b^v + \mathcal{B}''a] = -a^2\mathcal{D},
 \end{aligned}$$

aussi pour que  $\mathcal{D}$  soit positif il faut que  $\mathcal{D}$  soit négatif.

<sup>61</sup> Here Germain wrote  $A$  instead on  $A^v$ , probably forgetting the apex.

On trouve par un calcul semblable

$$\begin{aligned} \mathcal{A}''' \begin{pmatrix} \mathcal{A} & \mathcal{A}' & \mathcal{A}'' & \mathcal{A}''' \\ \mathcal{B} & \mathcal{B}' & \mathcal{B}'' & \mathcal{B}''' \\ & & & \mathcal{B}''' \\ & & & \mathcal{B}^v \end{pmatrix} &= \mathcal{A}''' \mathcal{A}''' x''' x''' + \mathcal{B} \mathcal{B} x'' x'' + \mathcal{B}' \mathcal{B}' x' x' \\ &+ \mathcal{B}'' \mathcal{B}'' x x + 2\mathcal{A}''' (\mathcal{B} x' + \mathcal{B}' x' + \mathcal{B}'' x) x''' + 2\mathcal{B} \mathcal{B}' x'' x' + 2\mathcal{B} \mathcal{B}'' x'' x + 2\mathcal{B}' \mathcal{B}'' x' x \\ &+ (\mathcal{A}'' \mathcal{A} - \mathcal{B}'' \mathcal{B}'') x x + (\mathcal{A}''' \mathcal{A}' - \mathcal{B}' \mathcal{B}') x' x' + (\mathcal{A}''' \mathcal{A}'' - \mathcal{B} \mathcal{B}) x'' x'' \\ &+ 2(\mathcal{B}''' \mathcal{A}''' - \mathcal{B} \mathcal{B}') x'' x' + 2(\mathcal{B}''' \mathcal{A}''' - \mathcal{B} \mathcal{B}'') x'' x + 2(\mathcal{B}^v \mathcal{A}''' - \mathcal{B}' \mathcal{B}'') x' x \\ &= (\mathcal{A}''' x''' + \mathcal{B} x'' + \mathcal{B}' x' + \mathcal{B}'' x)^2 \\ &+ \mathcal{D} \{(b''' b''' - a'a'') x x + (b''' b''' - aa'') x' x' + (b^v b^v - aa') x'' x'' \\ &+ 2(ab''' - b''' b^v) x'' x' + 2(a'b''' - b^v b'') x'' x + 2(a'' b^v - b''' b''' ) x' x\} \end{aligned}$$

et on voit, en conservant les dénominations précédentes et en faisant de plus  $b''' b''' - a'a'' = A'''$ ,  $b''' a' - b''' b^v = B'''$ ,  $b^v a'' - b''' b''' = B'''$ , que la forme

$$\begin{pmatrix} \mathcal{A} & \mathcal{A}' & \mathcal{A}'' & \mathcal{A}''' \\ \mathcal{B} & \mathcal{B}' & \mathcal{B}'' & \mathcal{B}''' \\ & & & \mathcal{B}''' \\ & & & \mathcal{B}^v \end{pmatrix}$$

ne peut être définie au moins que cette

$$\begin{pmatrix} \mathcal{A}''' & \mathcal{A}''' & \mathcal{A}^v \\ \mathcal{B}'' & \mathcal{B}''' & \mathcal{B}''' \end{pmatrix}$$

ne le soit.

Les conditions pour que  $\begin{pmatrix} \mathcal{A}''' & \mathcal{A}''' & \mathcal{A}^v \\ \mathcal{B}'' & \mathcal{B}''' & \mathcal{B}''' \end{pmatrix}$  soit définie sont, d'après l'art. 271,  $B'' B'' - A''' A^v = a \mathcal{A}'''$  et  $A^v \mathcal{D}'$  négatifs. On trouve  $\mathcal{D}'$  positif car

$$\begin{aligned} B''' A''' - B'' B''' &= (b''' a' - b''' b^v)(b''' b''' - aa'') - (ab''' - b''' b^v)(a'' b^v - b''' b''' ) \\ &= a'b''' b''' b''' - b''' aa'a'' - b''' b'' b''' b^v + aa'' b''' b^v - [aa'' b''' b^v - b''' ab''' b''' \\ &\quad - b''' a'' b^v b^v + b''' b''' b''' b^v] \\ &= b''' [ab''' b''' + a'b''' b''' + a'' b^v b^v - 2b''' b''' b^v - aa'a''] = b''' \mathcal{A}''' \\ B''' A^v - B'' B''' &= (b^v a'' - b''' b''' )(b^v b^v - aa') - (b''' a - b''' b^v)(b''' a' - b''' b^v) \\ &= b^v \mathcal{A}''' \\ \mathcal{D}' &= A''' B'' B'' + A''' B''' B''' + A^v B''' B''' - 2B'' B''' B''' - A''' A''' A^v \\ &= A''' (B'' B'' - A''' A^v) + B''' (B''' A''' - B'' B''' ) + B''' (B''' A^v - B'' B''' ) \\ &= \mathcal{A}''' \{a \mathcal{A}''' + b''' B''' + b^v B''' \} = \mathcal{A}'''^2 \end{aligned}$$

par conséquent  $A^v$  est négatif et comme ce cas est celui où la forme

$$\begin{pmatrix} \mathcal{A}''' & \mathcal{A}''' & \mathcal{A}^v \\ \mathcal{B}'' & \mathcal{B}''' & \mathcal{B}''' \end{pmatrix}$$

est définie négatif, il faut pour que

$$(\mathcal{A}'''x''' + \mathcal{B}x'' + \mathcal{B}'x' + \mathcal{B}''x)^2 + \mathcal{D} \begin{pmatrix} \mathcal{A}''' & \mathcal{A}''' & \mathcal{A}^v \\ \mathcal{B}'' & \mathcal{B}''' & \mathcal{B}''' \end{pmatrix}$$

soit toujours positif, que  $\mathcal{D}$  soit négatif: d'où on conclut que les conditions nécessaires pour que l'adjointe quaternaire

$$\begin{pmatrix} \mathcal{A} & \mathcal{A}' & \mathcal{A}'' & \mathcal{A}''' \\ \mathcal{B} & \mathcal{B}' & \mathcal{B}'' & \mathcal{B}''' & \mathcal{B}^v \end{pmatrix}$$

soit définie sont  $\mathcal{A}^v$ ,  $\mathcal{A}'''$  et  $\mathcal{D}$  négatifs; c'est-à-dire que les mêmes que l'on a déjà obtenues pour la forme  $a \begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b''' & b^v \end{pmatrix}$ . Ainsi lorsque cette dernière est définie, son adjointe l'est également mais à cause de  $\mathcal{A}'''$  négatif, si la forme est définie négative, l'adjointe sera définie positive et viceversa.

En supposant que la forme ternaire  $Ass + A'tt + A''uu + 2Btu + 2B'su + 2B''st$ , dont la déterminante est  $\mathfrak{D}$ , soit représentée par la forme quaternaire

$a \begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b''' & b^v \end{pmatrix}$  dont les indéterminées sont  $x = ps + mt + nu$ ,  $x' = p's + m't + n'u$ ,  $x'' = p''s + m''t + n''u$ ,  $x''' = p'''s + m'''t + n'''u$ ; le nombre  $\mathfrak{D}$  sera représenté par la forme  $\begin{pmatrix} \mathcal{A} & \mathcal{A}' & \mathcal{A}'' & \mathcal{A}''' \\ \mathcal{B} & \mathcal{B}' & \mathcal{B}'' & \mathcal{B}''' & \mathcal{B}^v \end{pmatrix}$  adjointe de  $a \begin{pmatrix} a & a' & a'' & a''' \\ b & b' & b'' & b''' & b^v \end{pmatrix}$ , en faisant:

$$\begin{aligned} x &= p''(m'''n' - m'n''') - p'(m'''n'' - m''n''') - p'''(m''n' - m'n'') \\ x' &= p(m'''n'' - m''n''') - p''(m'''n - mn''') - p'''(m'n - mn'') \\ x'' &= p'(m'''n - mn''') - p(m'''n' - m'n''') - p'''(m'n - mn') \\ x''' &= p(m''n' - m'n'') - p'(m'n - mn'') - p''(m'n - mn') \end{aligned}$$

↔

Cette proposition qui est entièrement analogue à celle de l'art. 280 se vérifie également par le calcul. Par exemple dans le cas où  $a = a' = a'' = a''' = 1$ ,  $b = b' = b'' = b''' = b^v = 0$  d'où résulte  $\mathcal{A} = \mathcal{A}' = \mathcal{A}'' = \mathcal{A}''' = -1$ ,  $\mathcal{B} = \mathcal{B}' = \mathcal{B}'' = \mathcal{B}''' = \mathcal{B}^v = 0$ , on trouve

$$\begin{aligned} \mathfrak{D} &= A(BB - A'A'') + B'(A'B' - BB'') + B''(A''B'' - BB') \\ &= (p^2 + p'^2 + p''^2 + p'''^2)\{(mn + m'n' + m''n'' + m'''n''')^2 \\ &\quad - (m^2 + m'^2 + m''^2 + m'''^2)(n^2 + n'^2 + n''^2 + n'''^2)\} \\ &\quad + (pn + p'n' + p''n'' + p'''n''')\{(pn + p'n' + p''n'' + p'''n''')(m^2 + m'^2 \\ &\quad + m''^2 + m'''^2) - (mn + m'n' + m''n'' + m'''n''')(pm + p'm' + p''m'' + p'''m''')\} \end{aligned}$$

$$\begin{aligned}
& + (pm + p'm' + p''m'' + p'''m''') \{(pm + p'm' + p''m'' + p'''m''')(n^2 + n'^2 \\
& + n''^2 + n'''^2) - (mn + m'n' + m''n'' + m'''n''')(pn + p'n' + p''n'' + p'''n''')\} \\
= & (p^2 + p'^2 + p''^2 + p'''^2) \{m^2n^2 + m'^2n'^2 + m''^2n''^2 + m'''^2n'''^2 \\
& + 2m'''m''n'' + 2m''m'n''' + 2m'''mn''n + 2m''m'n''n' \\
& + 2m''mn''n + 2m'mn'n - (m^2n^2 + m^2n'^2 + m^2n''^2 + m^2n'''^2 + m'^2n^2 + m'^2n'^2 \\
& + m'^2n''^2 + m'^2n'''^2 + m''^2n^2 + m''^2n''^2 + m''^2n'''^2 + m'''^2n^2 \\
& + m'''^2n'^2 + m'''^2n''^2 + m'''^2n'''^2)\} \\
& + (pn + p'n' + p''n'' + p'''n''') \{m^2np + m^2n'p' + m^2n''p'' + m^2n'''p''' \\
& + m'^2np + m'^2n'p' + m'^2n''p'' + m'^2n'''p''' \\
& + m''^2np + m''^2n'p' + m''^2n''p'' + m''^2n'''p''' + m'''^2np + m'''^2n'p' + m'''^2n''p'' \\
& + m'''^2n'''p''' - (m^2np + mm'n'p' + mm''n'p'' + mm'''n'p''' + m'mn'p' \\
& + m'^2n'p' + m'm'''n'p''' + m''mn''p + m''m'n''p' + m''^2n''p'' + m'''mn'''p \\
& + m'''m'n'''p' + m'''m''n'''p'' + m'''^2n'''p''')\} \\
& + (pm + p'm' + p''m'' + p'''m''') \{mn^2p + m'n^2p' + m''n^2p'' \\
& + m'''n^2p''' + mn'^2p + m'n'^2p' + m''n'^2p'' + m'''n'^2p''' \\
& + mn''^2p + m'n''^2p' + m''n''^2p'' + m'''n''^2p''' + mn'''^2p + m'n'''^2p' \\
& + m''n'''^2p'' + m'''n'''^2p''' \\
& - (mn^2p + mnn'p' + mnn''p'' + mnn'''p''' + m'n'np + m'n'^2p' + m'n'n''p'' \\
& + m'n'''p''' + m''n''np + m''n''n'p' + m''n''^2p'' \\
& + m''n''n'''p''' + m'''n'''np + m'''n''n'p' \\
& + m'''n''n''p'' + m'''n''^2p''')\} \\
= & ^{62} - (p^2 + p'^2 + p''^2 + p'''^2) \{(m'''n'' - m''n''')^2 + (m'''n' - m'n''')^2 \\
& + (m''n - mn''')^2 + (m''n' - m'n'')^2 + (m''n - mn'')^2 + (m'n - mn')^2\} \\
& + (pn + p'n' + p''n'' + p'''n''') \{mp'(mn' - m'n) + mp''(mn'' - m''n) \\
& + mp'''(mn''' - m'''n) + m'p(m'n - mn') \\
& + m'p''(m'n'' - m''n') + m'p'''(m'n''' - m'''n') + m''p(m''n - mn'') \\
& + m''p'(m''n' - m'n'') + m''p'''(m''n''' - m'''n'') \\
& + m'''p(m'''n - mn''') + m'''p'(m'''n' - m'n''') + m'''p''(m'''n'' - m''n''')\} \\
& + (pm + p'm' + p''m'' + p'''m''') \{np'(m'n - mn') + np''(m''n - mn'') \\
& + np'''(m'''n - mn''') + n'p(mn' - m'n) + n'p''(m'n' - m'n'') \\
& + n'p'''(m'''n' - m'n''') + n''p(mn'' - m''n) + n''p'(m'n'' - m''n') \\
& + n''p'''(m'''n'' - m''n''') + n'''p(mn''' - m'''n) + n'''p'(m'n''' - m''n') \\
& + n'''p''(m''n''' - m'''n'')\}
\end{aligned}$$

<sup>62</sup> S. Germain erroneously wrote  $m'''n'''^2p'''^2$  instead of the right  $m'''n'''^2p'''$ .

$$\begin{aligned}
&= -p'^2(m''''n'' - m'''n''')^2 - p^2(m''''n'' - m'''n''')^2 \\
&\quad - p''^2(m''''n' - m'n''')^2 - p^2(m''''n' - m'n''')^2 - p''^2(m''''n - mn''')^2 \\
&\quad - p'^2(m''''n - mn''')^2 \\
&\quad - p''^2(m''n' - m'n'')^2 - p^2(m''n' - m'n'')^2 - p'''^2(m''n - mn'')^2 \\
&\quad - p'^2(m''n - mn'')^2 - p'''^2(m'n - mn')^2 - p''^2(m'n - mn')^2 \\
&\quad + \{(p''n'' + p'''n''')(m''p'' - m''p''') - (p''m'' + p'''m''')(n''p'' - n''p''') \\
&\quad - (p''^2 + p'''^2)(m''n'' - m'''n''')\}(m''n'' - m'''n''') \\
&\quad + \{(p'n' + p'''n'')(m'''p' - m'p''') - (p'm' + p'''m''')(n'''p' - n'p''') \\
&\quad - (p'^2 + p'''^2)(m'''n' - m'n''')\}(m'''n' - m'n''') \\
&\quad + \{(pn + p''n'')(m'''p - mp''') - (pm + p'''m''')(n'''p - np''') \\
&\quad - (p^2 + p'''^2)(m'''n - mn''')\}(m'''n - mn''') \\
&\quad + \{(p'n' + p''n'')(m''p' - m'p'') - (p'm' + p''m'')(n''p' - n'p'') \\
&\quad - (p''^2 + p''^2)(m''n' - m'n'')\}(m''n' - m'n'') \\
&\quad + \{(pn + p''n'')(m''p - mp'') - (pm + p''m'')(n''p - np'') \\
&\quad - (p^2 + p''^2)(m''n - mn'')\}(m''n - mn'') \\
&\quad + \{(pn + p'n')(m'p - mp') - (pm + p'm')(n'p - np') \\
&\quad - (p^2 + p'^2)(m'n - mn')\}(m'n - mn') \\
&\quad + \{(pn + p'n')(m'''p'' - m''p''') - (pm + p'm')(n'''p'' - n''p''')\}(m'''n'' - m'''n''') \\
&\quad + \{(pn + p''n'')(m'''p' - m'p''') - (pm + p'm')(n'''p' - n'p''')\}(m'''n' - m'n''') \\
&\quad + \{(p'n' + p''n'')(m'''p - mp''') - (p'm' + p''m'')(n'''p - np''')\}(m'''n - mn''') \\
&\quad + \{(pn + p'''n'')(m''p' - m'p'') - (pm + p'''m''')(n''p' - n'p'')\}(m''n' - m'n'') \\
&\quad + \{(p'n' + p'''n'')(m''p - mp'') - (p'm' + p''m'')(n''p - np'')\}(m''n - mn'') \\
&\quad + \{(p''n'' + p'''n'')(m'p - mp') - (p''m'' + p'''m'')(n'p - np')\}(m'n - mn') \\
&= -p'^2(m''''n'' - m'''n''')^2 - p^2(m''''n'' - m'''n''')^2 \\
&\quad - p''^2(m''''n' - m'n''')^2 - p^2(m''''n' - m'n''')^2 - p''^2(m''n - mn''')^2 \\
&\quad - p'^2(m''n - mn''')^2 - p'''^2(m''n' - m'n'')^2 - p^2(m''n' - m'n'')^2 \\
&\quad - p''^2(m''n - mn'')^2 - p'^2(m''n - mn'')^2 - p'''^2(m'n - mn')^2 \\
&\quad - p''^2(m'n - mn')^2 + \{pp''(m''n - mn'') - pp'''(m''n - mn'') \\
&\quad + p'p''(m''n' - m'n'') - p'p'''(m'n' - m'n'')\}(m''n'' - m''n'') \\
&\quad + \{pp'(m'''n - mn''') - pp'''(m'n - mn') + p'p''(m'''n'' - m''n'') \\
&\quad - p'p'''(m'n'' - m''n')\}(m'''n' - m'n''') \\
&\quad + \{pp'(m'''n' - m'n''') - p'p''(mn' - m'n) + pp''(m''n''' - m'''n'') \\
&\quad - p''p'''(mn'' - m''n)\}(m'''n - mn''') \\
&\quad + \{pp'(m''n' - m'n'') - p'p''(mn' - m'n) + pp'''(m''n''' - m'''n'') \\
&\quad - p''p'''(mn''' - m'''n)\}(m''n - mn'')
\end{aligned}$$

$$\begin{aligned}
& + \{pp''(m'n''.m''n') - p'p''(mn'' - m''n) + pp'''(m'n''' - m'''n') \\
& - p'p'''(mn''' - m'''n)(m'n - mn') \\
& = -p'''^2(m''n' - m'n'')^2 - p''^2(m'''n' - m'n'''^2) \\
& - p'^2(m''n'' - m''n''')^2 + 2(m'''n'' - m''n''')(m'''n' - m'n'''^2)p'p'' \\
& - 2(m'''n'' - m''n''')(m''n' - m'n'')p'p''' + 2(m'''n' - m'n'''^2)(m''n' \\
& - m'n'')p''p''' - p'''^2(m''n - mn'')^2 - p''^2(m'''n - mn'''^2) \\
& - p^2(m'''n'' - m''n''')^2 + 2(m'''n'' - m''n''')(m'''n - mn'''^2)pp'' \\
& - 2(m'''n'' - m''n''')(m''n - mn'')pp''' + 2(m'''n - mn'''^2)(m''n - mn'')p''p'' \\
& - p'''^2(m'n - mn')^2 + p'^2(m''n - mn''')^2 \\
& - p^2(m'''n' - m'n''')^2 + 2(m'''n' - m'n''')(m'''n - mn'''^2)pp' \\
& - 2(m'''n' - m'n''')(m'n - mn'')pp''' + 2(m'''n - mn'''^2)(m'n - mn')p'p''' \\
& - p''^2(m'n - mn')^2 - p'^2(m''n - mn'')^2 - p^2(m''n' - m'n'')^2 \\
& + 2(m''n' - m'n'')(m''n - mn'')pp' - 2(m''n' - m'n'')(m'n - mn')pp'' \\
& + 2(m''n - mn'')(m'n - mn')p'p'' \\
& = -\{p''(m'''n' - m'n''') - p'(m'''n'' - m''n''') \\
& - p'''(m''n' - m'n'')^2 - \{p(m'''n'' - m''n''') - p''(m'''n - mn''') \\
& + p'''(m''n - mn'')^2 - \{p'(m'''n - mn''') - p(m'''n' - m'n''') \\
& - p'''(m'n - mn')^2 - \{p(m''n' - m'n'') - p'(m''n - mn'') + p''(m'n - mn')^2 \\
& = -x^2 - x'^2 - x''^2 - x'''^2.
\end{aligned}$$

↔

En réfléchissant sur la nature des formes on est porté à croire qu'en général, lorsque la déterminante est zéro, une forme composée de  $n$  variables est réducible en " $n$ " manières différentes aux formes composées de  $n - 1$  variables.

Par exemple pour la forme quinaire

$$\begin{aligned}
& axx + a'x'x' + a''x''x'' + a'''x'''x''' + a''''x''''x'''' + 2bx''''x'''' + 2b'x''''x'' \\
& + 2b''x''''x' + 2b''''x''''x + 2b'''x''''x'' + 2b^v x''''x' + 2b^{vi} x''''x + 2b^{vii} x''x' \\
& + 2b^{viii} x''x + 2b^{ix} x'x
\end{aligned}$$

on trouve

$$\begin{aligned}
\mathfrak{D} = & a''''[aa'b''''b'''' + aa''b^vb^v + aa'''bb^{vii}b''' + a'a''b^{vi}b^{vi} \\
& + a'a'''b^{viii}b^{viii} + a''a'''b^{ix}b^{ix} - aa'a''a''' \\
& - 2(ab''''b^vb^{vii} + a'b''''b^{vi}b^{viii} + a''b^vb^{vi}b^{ix} + a'''b^{vii}b^{viii}b^{ix}) \\
& - (b^{ix}b^{ix}b''''b'''' + b^vb^vb^{viii}b^{viii} + b^{vi}b^{vi}b^{vii}b^{vii}) + 2b^{ix}b''''b^{vi}b^{vii} \\
& + 2b^{ix}b''''b^vb^{viii} + 2b^{vi}b^{vii}b^{vib}b^{viii}] - (a'b''''b'''' + a''b^vb^v + a'''b^{vii}b^{vii} \\
& - 2b''''b^vb^{vii} - a'a''a''')b''''b'''' - (ab''''b'''' + a''b^{vi}b^{vi} + a'''b^{viii}b^{viii} \\
& - 2b''''b^{vi}b^{viii} - aa''a''')b''''b'' - (ab^vb^v + a'b^{vi}b^{vi} + a'''b^{ix}b^{ix} - 2b^vb^{vi}b^{ix})
\end{aligned}$$

$$\begin{aligned}
& -aa'a''')b'b' - (ab^{vii}b^{vii} + a'b^{viii}b^{viii} + a''b^{ix}b^{ix} - 2b^{vii}b^{viii}b^{ix} - aa'a'')bb \\
& - 2(aa'b''' - b^{ix}b^{ix}b''' + b^{vi}b^{viii}b^{ix} + b^v b^{viii}b^{ix} - ab^v b^{vii} - a'b^{vi}b^{viii})bb' \\
& - 2(aa''b^v - b^{viii}b^{viii}b^v - b'''b^{viii}b^{ix} + b^{vi}b^{viii}b^{viii} - ab'''b^{vii} - a''b^{vi}b^{ix})bb'' \\
& - 2(a'a''b^{vi} - b^{vii}b^{viii}b^{vi} + b'''b^{viii}b^{ix} + b^v b^{viii}b^{viii} - a'b'''b^{viii} - a''b^v b^{ix})bb''' \\
& - 2(aa'''b^{vii} - b^{vi}b^{vi}b^{viii} + b'''b^{vi}b^{ix} + b^v b^{viii}b^{viii} - ab'''b^v - a''b^{viii}b^{ix})b'b'' \\
& - 2(a'a'''b^{viii} - b^v b^v b^{viii} + b'''b^v b^{ix} + b^v b^{vi}b^{viii} - a'b'''b^{vi} - a''b^{viii}b^{ix})b'b''' \\
& - 2(a''a'''b^{ix} - b'''b'''b^{ix} + b'''b^v b^{viii} + b'''b^{vi}b^{viii} - a''b^v b^{vi}) \\
& - a''b^{vii}b^{viii})b''''' + \mathcal{D}(a'b'''b''''' + a''b^v b^v + a'''b^{vii}b^{vii} - 2b'''b^v b^{viii} - a'a''a''') \\
& = [aa'b'''b''''' + aa''b^v b^v + aa'''b^{viii}b^{viii} + a'a''b^{vi}b^{vi} + a'a'''b^{viii}b^{viii} \\
& + a''a'''b^{ix}b^{ix} - aa'a''a''' - 2(ab'''b^v b^{vii} + a'b'''b^{vi}b^{viii} + a''b^v b^{vi}b^{ix} \\
& + a'''b^{vii}b^{viii}b^{ix}) - (b^{ix}b^{ix}b'''b''' + b^v b^v b^{viii}b^{viii} + b^{vi}b^{vi}b^{viii}b^{viii}) \\
& + 2b^{ix}b'''b^{vi}b^{viii} + 2b^{ix}b'''b^v b^{viii} + 2b^{vi}b^{viii}b^v b^{viii}] [a'a''bb + a'a'''b'b' \\
& + a''a'''b'''' + a'a'''b'''b''' + a''a'''b^v b^v + a'''a'''b^{viii}b^{viii} \\
& - a'a''a'''a''' - 2(a'b'b'b''' + a''bb''b^v + a'''b'b''b^{vii} + a'''b^v b^{vi}b^{ix}) \\
& - (bbb^{vii}b^{viii} + b'b'b^v b^v + b''b''b'''b''')] \\
& - [(a'b'''b''''' + a''b^v b^v + a'''b^{viii}b^{viii} - 2b'''b^v b^{viii} - a'a''a''')b''' \\
& + (a''a'''b^{ix} - b'''b'''b^{ix} + b'''b^{vi}b^{viii} + b'''b^v b^{viii} - a''b^v b^{vi} - a'''b^{viii}b^{viii})b'' \\
& + (a'a'''b^{viii} - b^v b^v b^{viii} + b'''b^v b^{ix} + b^v b^{vi}b^{viii} - a'b'''b'' - a'''b^{viii}b^{ix})b' \\
& + (aa'b''' - b^{ix}b^{ix}b''' + b^{vi}b^{viii}b^{ix} + b^v b^{viii}b^{ix} - ab^v b^{viii} - a''b^v b^{ix})b]^2,
\end{aligned}$$

ou en faisant  $aa'b'''b''''' + aa''b^v b^v + \text{etc.} = \mathcal{A}$ ,  $a'a''bb + a'a'''b'b' + \text{etc.} = \mathcal{A}'$ ,  $(a'b'''b''''' + \text{etc.})b''' + \text{etc.} = \mathcal{B}$  et en réservant  $\mathfrak{A}$  pour représenter  $a'b'''b''''' + \text{etc.}$   $\mathfrak{D}\mathfrak{A} = \mathcal{A}\mathcal{A}' - \mathcal{B}^2$ . On trouverait de même autant d'équations analogues qu'il y a de combinaisons possibles des quantités  $\mathcal{A}$ ,  $\mathcal{A}'$ ,  $\mathcal{A}''$  etc. prises deux à deux dans le cas où  $\mathfrak{D}$  égaliserait zéro, on entirerait résultats analogues à ceux que l'on a obtenus pour les formes ternaires et quaternaires.

## IV

A Monsieur le docteur Gauss  
logé chez Ritter, Steinweg n°. 1917  
A Brunswick<sup>63</sup>

Monsieur

L'intérêt du aux hommes supérieurs suffit pour expliquer le soin que j'ai pris, de priere le général Pernety de faire savoir à qui il jugerait convenable, que vous avez droit à l'estime de tout gouvernement éclairé.

<sup>63</sup> Beside the address and inscribed into a rectangle, Gauss wrote "Nro 9 März 9 // Sophie Germain." Gauss likely received the letter on March 9 and this letter was the ninth among those he received in March. Gauss also numbered this letter "Nro 4."

En me rendant compte de l'honorables mission dont je l'avais chargé Mr. Pernetty m'a mandé qu'il vous avait fait connaitre mon nom: cette circonference me détermine à vous avouer que je ne vous suis pas aussi parfaitemment inconnue que vous le croyez: mais que, craignant le ridicule attaché au titre de femme savante, j'ai autrefois emprunté le nom de Mr. Le Blanc pour vous écrire et vous communiquer des notes qui, sans doute, ne méritaient pas l'indulgence avec laquelle vous avez bien voulu y répondre.

La reconnaissance que je vous dois pour l'encouragement que vus m'avez accordé, en me témoignant que vous me comptiez au nombre des amateurs de l'arithmétique sublime dont vous avez développé les mystères, était pour moi un motif particulier de m'informer de vos nouvelles, dans un moment où les troubles de la guerre pouvaient inspirer quelques craintes et j'ai appris avec une véritable satisfaction que vous étés resté dans vos foyes aussi tranquille que les circonstances le permettaient: je crains cependant que les suites de ces grands événements ne nous privent encore longtemps des ouvrages que vous préparez sur l'astronomie et sourtout de la continuation de vos recherches arithmétiques, car cette partie de la science a pour moi un attrait particulier et j'admire toujours avec un nouveau plaisir l'enchainement des vérités exposées dans votre livre: malheureusement la faculté de penser avec force est un attribut réservé à un petit nombre d'esprits privilégiés et je suis bien sure de ne rencontrer aucun des développements qui, pour vous semblent une suite inévitable de ce que vous avez fait connaître.

Je joins à ma lettre une note destinée à vous témoigner que j'ai conservé pour l'analyse le goût qu'a développé en moi la lecture de votre ouvrage et qui m'a autre fois inspiré la confiance de vous adresser mes faibles essais, sans autre recommandation auprès de vous que la bienveillance accordée par les savants aux admirateurs de leurs travaux.

J'espère que la singularité dont je fais aujourd'hui l'aveu ne me privera pas de l'honneur que vous m'avez accordé sous un nom emprunté et que vous ne dédaignerez pas de consacrer quelques instants à me donner directement de vos nouvelles, croyez, Monsieur, à l'intérêt que j'y attache et recevez l'assurance de la sincère admiration avec laquelle j'ai l'honneur d'être

votre très humble servante  
Sophie Germain

Paris, ce 20 fevrier 1807

PS. Mon adresse est: M.elle Germain  
chez son père rue S.te Croix de  
la Bretonnerie n°. 23 à Paris.

### Addendum

*De quelque manière que l'on sépare un nombre quelconque de la forme  $h^2 + nf^2$  en deux parties (n étant un nombre premier de la forme  $4k + 3$ ) la somme des puissances n-ième de chacune de ces parties sera aussi de la même forme  $h^2 + nf^2$ .*

En effet dans l'équation  $4\frac{x^n - 1}{x - 1} = Y^2 + nZ^2$ , Z est fonction invariable de x et 1, et Y est une fonction telle qu'elle change de signe seulement par la permutation de x

en 1 et de 1 en  $x$ ; or, les valeurs de  $Y$  et  $Z$  dans l'équation  $4\frac{x^n+y^n}{x+y} = Y^2 + nZ^2$  sont composées de  $x$  et  $-y$ , comme celles de l'équation précédante le sont de  $x$  et de 1, et il est clair que le nombre des termes de ces valeurs est, en  $y$  comprenant ceux dont les coefficients peuvent être zéro,  $\frac{n-1}{2} + 1 = 2(k+1)$ ; puisque ce nombre exprime combien il y a de puissances paires de  $xy$  dans le premier membre de l'équation, on sait d'ailleurs que le premier et le dernier terme de la valeur de  $Y$  sont multipliées par 2: à l'égard des autres termes de la même valeur, et de ceux de la valeur de  $Z$  ils se réduisent, en prenant séparément les sommes de ceux qui appartiennent à un même coefficient, à  $k$  différences ou sommes de deux puissances semblables, l'une de  $x$  l'autre de  $y$  multipliées par une puissance de  $xy$ : d'où il résulte que, quelques soient  $x$  et  $y$ , ces  $k$  sommes et par conséquent aussi les valeurs de  $Y$  et de  $Z$ , sont divisibles par 2; et qu'ainsi  $Y$  et  $Z$  sont des nombres entiers dans l'équation  $4\frac{x^n+y^n}{x+y} = Y^2 + nZ^2$ , et cela posé, il est évident que si  $x + y = h^2 + nf^2$ ,  $x^n + y^n = H^2 + nF^2$ .

Réciproquement, si la somme des puissances  $n$ -ièmes, de deux nombres quelconques est de la forme  $h^2 + nf^2$  la somme de ces nombres eux-mêmes sera de la même forme.<sup>64</sup>

La proposition ci dessus résulte de celle ci, si l'un des facteurs de la formule  $h^2 \pm nf^2$  ( $n$  étant un nombre premier) est  $(1, \pm n)$  l'autre facteur appartient nécessairement à la même forme.

Cette dernière proposition doit peut-être être admise sans démonstration, cependant, nous la prouverons de la manière suivante: si on suppose que le produit de  $(a, b, c)$  par  $(1, \pm n)$ , soit  $(1, \pm n)$  les neufs équations ( $\Omega$ ) nr. 235 deviennent

$$\left. \begin{array}{l} a = pq'' - p''q, \quad 2b = pq''' - qp''' + p'q'' - p''q', \quad c = p'q''' - p'''q' \\ s = pq' - p'q, \quad 0 = pq''' - qp''' - p'q'' + p''q', \quad \pm n = p''q''' - q''p''' \\ s = q'q'' - qq''', \quad 0 = pq''' + qp''' - p'q'' - q'p'', \quad \pm n = p'p'' - pp''' \end{array} \right\} (\Omega)$$

des cinquième et huitième on tire les deux suivantes  $pq''' - p'q'' = 0$ ,  $qp''' - q'p'' = 0$  pour y satisfaire il faut, à cause  $q'''$  et  $q''$ ,  $q$  et  $q'$  premiers entre eux (conditions résultantes de la septième équation  $\Omega$ ) que l'un des deux systèmes suivants d'équations aient lieu

$$\begin{aligned} p &= q'', & p' &= q''', & p''' &= q', & p'' &= q; \\ pq''' &= 0, & p'q'' &= 0, & qq''' &= 0, & q'p'' &= 0. \end{aligned}$$

La comparaison des septième et neuvième équations ( $\Omega$ ) montre que le premier doit être rejeté puisque il porterait à conclure  $-1 = \pm n$  mais on tire du second  $2b = 0$ ,  $-ac = \pm n$  et parce que  $n$  est un nombre premier on a nécessairement  $a = 1$  ou  $\pm n$ ,  $c = \pm n$  ou 1 donc etc.

<sup>64</sup> On the sheet of Germain's letter, at this point, Gauss wrote down a numerical counterexample to her claim (see Gauss's response).

<sup>65</sup> In Germain's manuscript appears  $pq'''$  instead of  $qp'''$ .

L'équation  $4\frac{x^n+y^n}{x+y} = Y^2 - nZ^2$  ( $n$  étant un nombre premier de la forme  $4k + 1$ ) ne peut se réduire, indépendamment de la valeur de  $n$ , à  $\frac{x^n+y^n}{x+y} = Y^2 - nZ^2$ , que dans le cas où l'un des nombres  $x$  et  $y$  est pair parce que le nombre  $(n-1)/2 + 1 = 2k + 1$  des termes des valeurs de  $Y$  et de  $Z$  est impair; et que  $Y$  et  $Z$  étant ici fonctions invariables de  $x$  et  $-y$ , leurs termes, excepté celui du milieu, appartiennent deux à deux à un même coefficient, de sorte que pour affirmer, que les valeurs de  $Y$  et  $Z$  dans l'équation  $4\frac{x^n+y^n}{x+y} = Y^2 - nZ^2$  sont des nombres impairs il faut être sûr que ce terme du milieu est lui-même un nombre pair: c'est ce qui à toujours lieu lorsque  $x + y$  est un nombre impair: ainsi on peut établir en employant les mêmes raisonnements que pour le cas où  $n$  est de la forme  $4k + 1$ : *que de quelque manière que l'on sépare un nombre impair de la forme  $h^2 - nf^2$  en deux parties (n étant un nombre premier de la forme  $4k + 1$ ) la somme des puissances n-imes de chacune de ces parties sera aussi de la forme  $h^2 - nf^2$ .*

Et réciproquement que, *si la somme des puissances n-ème de deux nombres l'un pair et l'autre impair est de la forme  $h^2 - nf^2$  la somme de ces nombres eux-mêmes sera de la même forme.*

Les différentes propositions que nous venons de démontrer sont susceptibles de la même généralisation que l'équation fondamentale  $4\frac{x^n-1}{x-1} = Y^2 \pm nZ^2$ , c'est-à-dire, qu'elles seraient encore vraies si au lieu des puissances  $n$ -èmes on prenait les puissances  $n^s$ -èmes d'un nombre quelconque.

### Gauss's reply.

Votre lettre du 20 fevrier, mais qui ne m'est parvenue que le 12 Mars, a été pour moi la source d'autant de plaisir que de surprise. Combien l'acquisition d'une amitié aussi flat[t]euse et précieuse est-elle douce à mon coeur. L'intérêt vif, que Vous avez pris à mon sort pendant cette guerre funeste mérite la plus sincère reconnaissance. Assurément, Votre lettre au Général Pernety m'eût été fort utile, si j'avais été dans le cas d'avoir recours à une protection spéciale de la part du gouvernement français. Heureusement les événements et les suites de la guerre ne m'ont pas touché de trop près jusqu'ici, bien que je sois persuadé, qu'elles auront une grande influence sur le plan futur de ma vie. Mais comment Vous décrire mon admiration et mon étonnement, en voiant [voyant] se métamorphoser mon correspondant estimé Mr. Leblanc en cet illustre personnage, qui donne un exemple aussi brillant de ce que j'aurais peine de croire. Le goût pour les sciences abstraites en général et surtout pour les mystères des nombres est fort rare: on ne s'en étonne pas; les charmes enchanteurs de cette sublime science ne se décelent dans toute leur beauté qu'à ceux qui ont le courage de l'approfondir. Mais lorsqu'une personne de ce sexe, qui, par nos moeurs et par nos préjugés, doit rencontrer infiniment plus d'obstacles et de difficultés, que les hommes, à se familiariser avec ces recherches épineuses, sait néanmoins franchir ces entraves et pénétrer ce qu'elles ont de plus caché, il faut sans doute, qu'elle ait le plus noble courage, des talents tout à fait extraordinaires, le génie supérieur. En effet rien ne pourrait me prouver d'une manière plus flat[t]euse et moins équivoque, que les attractions de cette science, qui a embelli ma vie de tant de jouissances, ne sont pas chimériques, que la prédilection, dont Vous l'avez honorée.

Les notes savantes, dont toutes Vos lettres sont si richement remplies, m'ont donné mille plaisirs. Je les ai étudiées avec attention, et j'admire la facilité avec laquelle Vous avez pénétré toutes les branches de l'Arithmétique, et la sagacité avec laquelle Vous les avez su généraliser et perfectionner. Je Vous prie d'envisager comme une preuve de cette attention, si j'ose ajouter une remarque à un endroit de Votre dernière lettre. Il me semble, que la proposition inverse, savoir "si la somme des puissances  $n$ -emes de deux nombres quelconques est de la forme  $hh + nff$ , la somme de ces nombres eux-mêmes sera de la même forme" est énoncée en peu trop généralement. Voici un exemple où cette règle est en défaut :

$$\begin{aligned} 15^{11} + 8^{11} &= 8649755859375 + 8589934592 = 8658345793967 \\ &= 1595826^2 + 11 \cdot 745391^2 \end{aligned}$$

néanmoins  $15 + 8 = 23$  ne peut se réduire sous la forme  $xx + 11yy$ .

Il en est de même de la proposition : "si l'un des facteurs de la formule  $yy + nzz$  ( $n$  étant un nombre premier) est de la forme  $(1, 0, n)$ , l'autre appartient nécessairement à la même forme". Votre démonstration ne prouve que ce, qu'aucune autre forme indéfinie, que telle qu'est équivalente à  $(1, 0, n)$ , multipliée par la forme  $(1, 0, n)$  ne peut donner le produit  $(1, 0, n)$ , mais cette démonstration ne s'étende pas sur le nombres définis. Soit, pour le déterminant  $-n$ ,  $C$  une classe de formes quelconque, mais ni équivalente à la principale ni à une autre classe *anceps*, soit  $D$  la classe résultante de la duplication de  $C$  (qui sera différente de la principale), enfin soit  $D'$  la classe opposée à  $D$ . Il s'ensuit, que de la composition de  $C + C + D'$  résulte la classe principale. Ainsi si les deux nombres  $f, g$  peuvent être représentés par une forme de la classe  $C$ , et le nombre  $h$  par une forme de la classe  $D'$ , le produit  $fg \times h$  peut se réduire à  $(1, 0, n)$ , mais il est facile [de voir] que  $fg$  ne se réduit pas seulement à  $D$  ou  $D'$  mais aussi à  $(1, 0, n)$ . Nous avons donc ici le cas, qu'un facteur  $fg$ , et le produit  $fg \cdot h$  sont de la forme  $(1, 0, n)$  sans que pourtant l'autre facteur y appartienne nécessairement. Au reste on voit facilement que le premier facteur doit être composé, sans cela la proposition serait juste. Dans l'exemple ci dessus le facteur  $\frac{15^{11}+8^{11}}{23}$  enveloppe le diviseur 67.

Depuis cinq ans des travaux astronomiques—au[x]quels pour le dire en passent je dois surtout l'heureuse situation, dont j'ai joui pendant la vie de notre duc,<sup>66</sup> le victime malheureux de son attachement fidèle à la maison de Prusse—m'ont empêché de me délivrer autant qu'auparavant a ma préférence pour l'Arithmétique et les autres branches de l'analyse. Je n'ai pas pourtant négligé celle ci tout à fait. Tout au contraire j'ai rassemblé peu à peu un grand nombre de recherches, qui un jour fourniront un autre volume—si non deux—certainement pas moins intéressant que le premier. Même dans le dernier hiver j'ai réussi à y ajouter une branche entièrement nouvelle. C'est la théorie des résidus cubiques et des résidus biquarrés, portée à un degré de perfection égal à celui, qu'a atteint la théorie des résidus quarrés. Je mets cette théorie, qui répand un nouveaux jour sur les résidus quarrés parmi les recherches les plus curieuses dont je me suis jamais occupé. Je ne saurais Vous en donner une idée sans

<sup>66</sup> Karl Wilhelm Ferdinand [1735–1806] duke of Brunswick, to whom Gauss dedicated the D.A. He died as a consequence of a severe wound received in the war against Napoleon when he was commander-in-chief of the Prussian army.

écrire un Mémoire express. Voici pourtant quelque théorème spécial, qui pourra servir d'un petit échantillon.

- I. Soit  $p$  un nombre premier de la forme  $3n + 1$ . Je dis, que 2 (c.a.d. +2 et -2) est résidu cubique de  $p$ , si  $p$  se réduit à la forme  $xx + 27yy$ ; qui 2 est Non-résidu cubique de  $p$  si  $4p$  se réduit à cette forme. P.E. 7. 13. 19. 31. 37. 43. 61. 67. 73. 79. 97. Vous ne trouverez que  $31 = 4 + 27$ ,  $43 = 16 + 27$ , et  $2 \equiv 4^3 \pmod{31}$ ,  $2 \equiv (-9)^3 \pmod{43}$
- II. <sup>67</sup> Soit  $p$  un nombre premier de la forme  $8n + 1$ . Je dis que +2 et -2 seront résidus ou non-résidus biquarres de  $p$ , suivent ce que  $p$  est ou n'est pas de la forme  $xx + 64yy$ . Par ex. parmi les nombres 17. 41. 73. 89. 97. 113. 137. Vous trouvez que  $73 = 9 + 64$ ,  $89 = 25 + 64$ ,  $113 = 49 + 64$  et  $25^4 \equiv 2 \pmod{73}$ ,  $5^4 \equiv 2 \pmod{89}$ ,  $20^4 \equiv 2 \pmod{113}$ .<sup>68</sup>

Les démonstrations de ces théorèmes et de ceux qui sont plus généraux sont intimement liées à des recherches délicates. Voici une autre proposition relative aux résidus quarrés, dont la démonstration est moins cachée : je ne l'ajoute pas, pour ne pas Vous dérober le plaisir de la développer Vous-même, si Vous la trouverez [trouverait] digne d'occuper quelques moments de Votre loisir.

Soit  $p$  un nombre premier. Soient les  $p - 1$  nombres inférieurs à  $p$  partagés en deux classes

$$\begin{array}{ll} A \dots & 1, 2, 3, 4, \dots, (p-1)/2 \\ B \dots & (p+1)/2, (p+3)/2, (p+5)/2, \dots, p-1 \end{array}$$

Soit  $\alpha$  un nombre quelconque non divisible par  $p$ . Multipliés tous les nombres  $A$  par  $\alpha$ ; prenés [prenaient] en les moindres résidus selon le module  $p$ , soient [soyent], entre ces résidus,  $\alpha$  appartenants à  $A$  et  $\beta$  appartenants à  $B$  de sorte que  $\alpha + \beta = (p-1)/2$ . Je dis que  $\alpha$  est résidu quarré de  $p$  lorsque  $\beta$  est pair, non résidu lorsque  $\beta$  est impair.

On peut tirer de cette proposition plusieurs conséquences très remarquables ; entre autres, elle donne le moyen [moyen] d'étendre l'induction, par laquelle on rassemble des cas spéciaux du théorème fondamental aussi loin qu'on veut, ce qui ne pourrait se faire par les méthodes exposées art. 106–124.

J'ai donné dans mon ouvrage deux démonstrations rigoureuses de ce fameux théorème et j'en possède encore trois autres toutes entièrement différentes entre elles; deux d'entre elles même peuvent être conduites de deux différentes manières chaqu'une [chacune]: ainsi je pourrais soutenir que je peu le démontrer de *sept* manières différentes. Les autres démonstrations que je préférerais pour l'élégance aux deux données dans mon ouvrage, seront publiées aussitôt que j'y trouverai l'occasion. A propos, dans la première démonstration qui se trouve dans la IV section il s'est glissé une faute légère qui je n'ai apercue qu'après que je ne pouvoit plus l'indiquer. Il faut donc faire la correction suivante:

<sup>67</sup> This theorem was communicated to the Royal Society of Göttingen on April 5, 1825, and inserted in the memoir entitled *Theoria residuorum biquadraticorum commentatio prima* (Gauss 1828a).

<sup>68</sup> The last congruence is not correct, in fact we have  $20^4 \equiv -8 \pmod{113}$ , but one has  $27^4 \equiv 2 \pmod{113}$ .

p.146 (cas (4)) l.12, lisés [lisais] comme il suit “Facile vero perspicitur, ex ista aequatione deduci posse haec  $a' pRh \dots (\alpha)$ ,  $\pm ahRa' \dots (\beta)$ ,  $\pm ahRp \dots (\gamma)$ . Ex ( $\alpha$ ) sequitur, perinde ut in (2),  $h$  vel utriunque  $a'$ ,  $p$  vel neutrius residuum esse. Sed casus prior ideo est impossibilis, quod ex  $hRa'$  et ( $\beta$ ) sequeretur  $aRa'$  contra hypoth. Quamobrem necessario est  $hNp$  adeoque, per ( $\gamma$ ),  $aNp$ . Q.E.D”

Au reste à la page 144 il se trouve une faute d'impression non indiquée, savoir art. 139 ligne 3 au lieu de  $\pm aNp$  il faut lire  $\pm aRp$ .

J'aurais répondu plus tôt à Votre lettre, mais la découverte d'une nouvelle planète par Mr. Olbers m'a un peu distrait.<sup>69</sup> Par le premier essai que j'a fait sur son orbite je trouvé, son mouvement considérablement plus vite celui de Cérès, Pallas et Junon, savoir 978'' par jour. L'inclinaison de l'orbite de 7°6'. L'excentricité 0,1. Cette planète a beaucoup plus de clarté que Cérès, Pallas et Junon et j'espère la trouver parmi les observations de l'histoire céleste, peut être même parmi celles de Flamsteed.<sup>70</sup> Je viens d'achever un ouvrage étendu sur les méthodes qui me sont propres, à déterminer les orbites des planètes. Mais quoique je l'aie écrit en allemand, je trouve beaucoup de difficulté d'y engager un libraire. La guerre a suspendu tout commerce, plusieurs de nos plus grands libraires l'ont refusé. Je suis à présent à traiter avec un autre qui se montre un peu plus courageux. S'il trouvera son conte à cette entreprise, peut être il sera encouragé par là à risquer la publication d'un second volume de mes disquisitions.

Continuez, Mademoiselle, de me favoriser de Votre amitié et de Votre correspondance, qui font mon orgueil, et soiès [soyes] persuadée, que je suis et serai toujours avec la plus haute estime.

Votre plus sincère admirateur  
Ch. Fr. Gauss

Bronsvic [Brunswick] ce 30 Avril 1807

Jour de ma naissance

## V

Monsieur

Je vous dois mille remerciements pour les choses flatteuses dont votre dernière lettre est remplie, je ne les prends qu'à titre d'encouragement et certainement, ma plus grande ambition sera toujours de ne pas me montrer indigne de l'honneur que vous me faites en me promettant de continuer une correspondance à laquelle j'ai tout à gagner.

Vous avez pris la peine d'examiner une proposition inverse que je vous ai communiquée et de m'indiquer l'erreur que j'ai commise. Je reconnaiss la justesse de votre observation et vous remercie bien franchement de m'en avoir donné avis; si je ne craignais même d'abuser de votre complaisance je vous priera de me render à l'avenir, le même service que je considérerai toujours comme une marque de votre bienveillance.

<sup>69</sup> On March 27, 1807, the astronomer Heinrich Wilhelm Olbers discovered a new asteroid (at that time called “minor planets”). He allowed Gauss to name it “Vesta”.

<sup>70</sup> John Flamsteed, astronomer [1646–1719]. In 1675 he was appointed Royal Astronomer and for him was built the Greenwich Observatory. His work *Atlas Coelestis*, the largest star atlas that ever had been published, appeared posthumously in 1725.

Combien j'ai eu de plaisir en lisant vos trois théorèmes sur les résidus! J'en ai cherché les démonstrations, je les joins à ma lettre pour les soumettre à votre jugement, car elles ne me paraîtront hors de doute que lorsqu'elles auront votre approbation.

Vous ne pourrez, à l'avenir, me faire de plus grand plaisir qu'en m'envoyant les premières propositions arithmétiques qui vous tomberont sous la main: en essayant de les démontrer j'acquerrai l'habitude d'un genre de considération qui est pour moi plein de charme; mais dont la difficulté serait trop grande si j'étais réduite à mes propres forces car, pour vous dire la vérité, j'avais déjà voulu examiner les résidus des puissances plus élevées que le carré, mais je n'avais pu pénétrer cette théorie qui est restée l'objet de ma curiosité.

Voici pourtant le petit nombre de proposition auxquelles j'étais parvenue et que je n'oserais vous communiquer si je ne comptais sur l'indulgence à laquelle vous m'avez accoutumé:

$p$  étant un nombre premier, si  $q$  est un nombre premier à  $p - 1$ , tous les nombres de la série  $1, 2, \dots, p - 1$  seront résidus puissance  $q$ -ièmes ( $\text{mod. } p$ ).

En effet si il en était autrement il faudrait que plusieurs puissances  $q$ -ièmes fussent congruentes entre elles ( $\text{mod. } p$ ): soit donc, si il était possible,  $a^q \equiv b^q (\text{mod. } p)$ ; quelques soient  $a$  et  $b$ , on aurait, en prenant  $r$  pour racine primitive  $r^n \equiv a, r^m \equiv b, n$  et  $m$  étant des nombres  $< p - 1$ , par conséquent  $r^{nq} \equiv a^q, r^{mq} \equiv b^q, r^{nq} \equiv r^{mq}, r^{(n-m)q} \equiv 1$ ; résultat impossible parce que  $q$  étant premier à  $p - 1$ , il faudrait que  $n - m$ , qui est essentiellement  $<$  que  $p - 1$ , fut égal à ce nombre.

Si on a au contraire  $p - 1 = qs$ , il y aura parmi les  $qs$  nombres  $1, 2, \dots, qs, s$  résidu et  $(q - 1)s$  non résidus puissance  $q$ -ième ( $\text{mod. } p$ ).

En effet, soit  $r^d \equiv a, r^{s+d} \equiv a', r^{2s+d} \equiv a'', \dots, r^{(q-1)s+d} \equiv a^{q-1}$ , on aura évidemment  $a^q \equiv a'^q \equiv a''^q \dots \equiv (a^{q-1})^q$ ; par conséquent, puisqu'il y a  $q$  puissances  $q$ -ièmes congruentes entre elles, l'élévation à la puissance  $q$ -ième des  $qs$  nombres moindres que  $p$  ne fournira que  $s$  nombres résidus puissance  $q$ -ième différents entre eux, et il y aura parmi ces nombres  $(q - 1)s$  non résidus.

Le produit de deux résidus puissance  $q$ -ième ( $\text{mod. } p = sq + 1$ ), est également résidu puissance  $q$ -ième, même modul, et en général le produit de  $a \equiv r^m$  par  $b \equiv r^n$  est ou n'est pas résidu puissance  $q$ -ième ( $\text{mod. } p$ ), suivant que  $m + n$  est ou n'est  $\equiv 0$  ( $\text{mod. } q$ ).

Si on désigne par  $2^m, q, q'$ , ect. les différents facteurs de  $k$  dans  $p = 2k + 1, -1$  sera résidu puissance  $(2^{m-1})$ -ième,  $q$ -ième,  $q'$ -ième, ect. ( $\text{mod. } p$ ); car,  $r$  étant une racine primitive, on aura  $r^k \equiv -1$  et il est clair que  $r^k = (r^{qq'})^{2m} = (r^{2mq'})^q = (r^{2mq'})^{q'} = \text{etc.}$

Pour les nombres premiers  $2^{2^i} + 1, 2$ , est résidus  $(2^{2^i-i-1})$ -ième puissance; car c'est en effet ce qui résulte immédiatement de la congruence  $2^{2^i+1} \equiv 1 (\text{mod. } 2^{2^i} + 1)$ .

Comme les nombres  $2^{2^i} + 1$  peuvent être mis sous la forme  $2^{i+1} \cdot 2^{2^i-i-1} + 1$  on voit qu'il y a  $2^{i+1}$  résidus  $(2^{2^i-i-1})$ -ième puissance et que ces  $2^{i+1}$  résidus sont  $1, 2, 2^2, 2^3, \dots, 2^{2^i-1}, -1, -2, -2^2, -2^3, \dots, -2^{2^i-1}$ .

Il résulte de cette proposition qu'elle ont sait a priori que dans la résolution de l'équation du second degré dont les racines sont les périodes  $(2^i, 1), (2^i, g^{2^{2^i-i-1}})$  ( $g$  étant la racine primitive), le signe + du radical appartient à la première et le signe - à la seconde; car en dernière analyse

$$\begin{aligned}
 & (2^i, 1) \\
 &= 2 \left\{ \cos \frac{P}{n} + \cos \frac{2^2 P}{n} + \cos \frac{2^4 P}{n} + \cos \frac{2^6 P}{n} + \cdots + \cos \frac{2^{2^i-2} P}{n} \right\} \\
 &= 2 \left\{ \cos \frac{2^2 P}{4n} + \cos \frac{2^4 P}{4n} + \cos \frac{2^6 P}{4n} + \cos \frac{2^8 P}{4n} + \cdots + \cos \frac{2^{2^i} P}{4n} \right\}, \\
 & (2^i, g^{2^{2^i-i-1}}) \\
 &= 2 \left\{ \cos \frac{2P}{n} + \cos \frac{2^3 P}{n} + \cos \frac{2^5 P}{n} + \cos \frac{2^7 P}{n} + \cdots + \cos \frac{2^{2^i-1} P}{n} \right\} \\
 &= 2 \left\{ \cos \frac{2^3 P}{4n} + \cos \frac{2^{54} P}{4n} + \cos \frac{2^7 P}{4n} + \cos \frac{2^9 P}{4n} + \cdots + \cos \frac{2^{2^i+1} P}{4n} \right\}
 \end{aligned}$$

et en comparant termes à termes les valeurs de ces deux périodes, on voit que ceux de  $(2^i, 1)$  sont plus grands que leurs correspondants dans  $(2^i, g^{2^{2^i-i-1}})$ , dont le dernier est même négatifs, d'où il résulte  $(2^i, 1) > (2^i, g^{2^{2^i-i-1}})$ . On trouve de même  $(2^{i-1}, 1) > (2^{i-1}, g^{2^{2^{i-1}-i}})$  etc., et plus généralement (en considérant comme plus grandes celles des périodes qui ont une valeur négative moins grande, et employant les différentes puissances de deux à la place des puissances de la racine primitive qui leurs sont congruantes, puissances qui dépendent du choix de cette racine)

$$\begin{aligned}
 & (2^{i-1}, 1) > (2^{i-1}, 2) > (2^{i-1}, 4) > (2^{i-1}, 8) \\
 & (2^{i-2}, 1) > (2^{i-2}, 2) > (2^{i-2}, 4) > (2^{i-2}, 8) > \\
 & (2^{i-2}, 2^4) > (2^{i-2}, 2^5) > (2^{i-2}, 2^6) > (2^{i-2}, 2^7) \\
 & \vdots \\
 & (2, 1) > (2, 2) > (2, 2^2) > (2, 2^3) > \cdots > (2, 2^{2^i-1}).
 \end{aligned}$$

Par exemple pour  $p = 2^{2^2} + 1$ , 2 est simplement résidu quadratique et on trouve  $(4, 1) > (4, g)$  pour  $g = 3$  donne et  $g^{14} \equiv 2, g^{12} \equiv 4, g^{10} \equiv 2^3, (2, 1) > (2, 2) > (2, 2^2) > (2, 2^3)$ , [pour]  $g = 6$  [donne]  $g^2 \equiv 2, g^4 \equiv 2^2, g^6 \equiv g^3$ .

Je vois avec regret que l'ouvrage que vous faites imprimer est écrit en allemand, car cette langue m'est entièrement inconnue, mais je serais tentée de l'apprendre un peu, comme j'ai fait [avec] la latine affin de n'être pas privée de la connaissance de vos méthodes. Je crois aisément que la librairie a beaucoup souffert de cette malheureuse guerre, je fais des voeux pour que ce contrôlé temps ne nuise pas à impression des vos ouvrages et pour que vous restiez toujours à l'abri de ses suites. Croyez, Monsieur, à la sincérité de l'intérêt qui les dicte et agréez l'assurance de la reconnaissance et de l'admiration avec lequelles je suis

votre servante Sophie Germain

Ce 27 juin 1807

## Addendum

*Théorème I* (éxtrait de votre lettre du 30 avril dernier)

“Soit  $p$  un nombre premier de la forme  $3n + 1$ . Je dis que 2 (c.a.d. +2 et -2) est résidu cubique de  $p$  si  $p$  se réduit à la forme  $xx + 27yy$ , que 2 est non résidu cubique de  $p$  si  $4p$  se réduit à cette forme.”

*Démonstration.*

On a toujours (voyez nr. 358)  $4p = (6a - 3b - 3c - 2)^2 + 27(b - c)^2$  et, par conséquent, lorsque  $p = xx + 27yy$ , on a  $6a - 3b - 3c - 2 = 2x$ ,  $b - c = 2y$ ; mais a cause de  $n = a + b + c$  (v. num. I)<sup>71</sup> si  $b + c$  est un nombre pair  $a$  sera également un nombre pair et  $a - 1 = (\mathfrak{K}\mathfrak{K})$  un nombre impair; or, comme en général, lorsque  $h$  et  $h + 1$  sont deux nombres compris dans  $\mathfrak{K}$ ,  $p - h - 1$  et  $p - h$  sont également contenus dans  $\mathfrak{K}$ ; ( $\mathfrak{K}\mathfrak{K}$ ) est toujours un nombre pair, a moins que l'une des valeurs de  $h$  ne soit telle que  $p - h - 1 = h$ ,  $(p - 1)/2 = h$ .

A cause de  $p - 1$  résidu cubique, si  $(p - 1)/2$  est résidu cubique, 2 l'est pareillement; donc 2 est résidu cubique lorsque  $p = xx + 27yy$ , et non résidu lorsque  $4p$ , seulement, appartient à la forme  $x^2 + 27y^2$ . C.Q.E.D.

*Théorème II*

“Soit  $p$  un nombre premier de la forme  $8n + 1$ . Je dis que +2 et -2 seront résidus ou non résidus bi-quarré de  $p$ , suivant que  $p$  est ou n'est pas de la forme  $xx + 64yy$ .”

La démonstration du présent théorème exige beaucoup de calculs préalables parce que le livre ne présente aucun résultat dont on puisse faire un usage direct.

Je considère d'abord, comme pour le cas des nombres  $3n + 1$ , l'ensemble des moindres restes des puissances d'une racine primitive comprise dans les périodes  $(2n, 1) = p$ ,  $(2n, g) = p'$ ,  $(2n, g^2) = p''$ ,  $(2n, g^3) = p'''$ , ensembles que je désigne par  $\mathfrak{K}$ ,  $\mathfrak{K}'$ ,  $\mathfrak{K}''$ ,  $\mathfrak{K}'''$ , et conformément a ce qui a été pratiqué nr. 358, je désigne également par  $(\mathfrak{K}\mathfrak{K})$  le nombre des nombres de la série 1, 2, 3, ...,  $p - 1$  qui tant par eux mêmes qu'étant augmentés de l'unité sont compris dans  $\mathfrak{K}$ . A cause de -1 résidu bi-quarré on démontre comme au nr. cité, que,  $(\mathfrak{K}\mathfrak{K}')$  représentant le nombre des nombres compris dans  $\mathfrak{K}$  qui étant augmentés de l'unité sont compris dans  $\mathfrak{K}'$  et  $(\mathfrak{K}'\mathfrak{K})$  désignant le nombre des nombres compris dans  $\mathfrak{K}'$ , qui étant augmentés de l'unité son compris dans  $\mathfrak{K}$ , on a  $(\mathfrak{K}\mathfrak{K}') = (\mathfrak{K}'\mathfrak{K})$  et de même aussi  $(\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K})$  etc.  $(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}')$  etc.  $\mathfrak{K}$  représente l'ensemble de tous les résidus biquarrés  $(\text{mod } 8n + 1)$  et, en général, si  $h$  et  $h + 1$  sont deux de ces nombres,  $p - h - 1$  et  $p - h$  seront également contenus dans  $\mathfrak{K}$  de sorte que  $(\mathfrak{K}\mathfrak{K})$  sera toujours un nombre pair a moins qu'il n'existe une valeur de  $h$  telle que  $p - h - 1 = h$ ,  $(p - 1)/2 = h$ , c'est-à-dire, a moins que  $(p - 1)/2$  ne soit résidu bi-quarré et comme  $p - 1$  est lui-même résidu bi-quarré, cette condition ne peut avoir lieu que lorsque 2 est aussi résidu biquarré il ne reste plus autre chose a prouver, si ce n'est que  $(\mathfrak{K}\mathfrak{K})$  est toujours un nombre impair lorsque  $8n + 1 = xx + 64yy$  et un nombre pair lorsque  $8n + 1$  n'est pas de cette forme.

<sup>71</sup> She is referring to equation number I, which appears in art. 358 of the D.A.

Soient  $(\mathfrak{K}\mathfrak{K}) = a$ ,  $(\mathfrak{K}\mathfrak{K}') = b$ ,  $(\mathfrak{K}\mathfrak{K}'') = c$ ,  $(\mathfrak{K}\mathfrak{K}''') = d$ ,  $(\mathfrak{K}'\mathfrak{K}'') = e$ ,  $(\mathfrak{K}''\mathfrak{K}'') = f$ ,  $(\mathfrak{K}'\mathfrak{K}') = d'$ ,  $(\mathfrak{K}'\mathfrak{K}''') = e'$ ,  $(\mathfrak{K}''\mathfrak{K}''') = e''$ ,  $(\mathfrak{K}'''\mathfrak{K}''') = b'$ ; on trouve

$$\begin{aligned} pp' &= bp + dp' + ep'' + e' p''', & pp'' &= ep + ep' + fp'' + e'' p''' \\ p' p'' &= bp' + dp'' + ep''' + e' p, & p' p''' &= cp' + ep'' + fp''' + ep \\ p'' p''' &= bp'' + dp''' + ep + e' p', & pp &= 2n + ap + bp' + cp'' + dp''' \\ p''' p &= bp''' + dp + ep' + e' p'', & p' p' &= 2n + ap' + bp'' + cp''' + dp \\ p'' p'' &= 2n + ap'' + bp''' + cp + dp', & p''' p''' &= 2n + ap''' + bp + cp' + dp'' \end{aligned}$$

et en cherchant directement la valeur de  $pp'''$

$$pp''' = dp + e' p' + e'' p'' + b' p'''.$$

La comparaison des deux valeurs du produit  $pp'''$  donne  $e' = e$ ,  $e'' = e'$ ,  $b' = b$ : on a par la nature des quantités  $a$ ,  $b$  etc.

$$\begin{aligned} 2n - 1 &= a + b + c + d \\ 2n &= d' + b + e + e' \quad \text{ou} \quad 2n = d' + b + 2e \\ 2n &= f + c + e + e'' \quad \text{ou} \quad 2n = f + c + 2e \\ 2n &= b' + d + e' + e'' \quad \text{ou} \quad 2n = b + d + 2e \end{aligned}$$

la comparaison des deux dernières valeurs de  $2n$  donne  $f + c = b + d$  celle des 1.re et 3.me donne  $d' = d$  et on tire de la dernière combinée avec la valeur de  $2n - 1$  la condition  $a = 2e - c - 1$ .

En développant le produit

$$\begin{aligned} pp' p'' p''' &= c^2 pp' + ce(p' p' + p''' p') + cfp' p'' + ce(pp'' + pp) \\ &\quad + ee(p' p'' + p' p + p''' p'' + pp''') + ef(p'' p'' + pp'') + fc(pp''') \\ &\quad + ef(p' p''' + p''' p'') + ffp'' p''' \\ &= (c^2 + e^2) pp' + cep' p' + (ce + ef) p''' p' + (cf + ee) p' p'' \\ &\quad + (ce + ef) pp'' + cepp \\ &\quad + (e^2 + f^2) p'' p''' + (ee + fc) pp''' + efp'' p'' + efp''' p''' \\ &= (c^2 + e^2) \{bp + dp' + ep'' + ep'''\} + ce \{2n + ap' + bp'' + cp''' + dp\} \\ &\quad + (ce + ef) \{cp' + ep'' + fp''' + ep\} + (cf + ee) \{bp' + dp'' + ep''' + e' p\} \\ &\quad + (ce + ef) \{cp + ep' + fp'' + ep'''\} + ce \{2n + ap + bp' + cp'' + dp'''\} \\ &\quad + (e^2 + f^2) \{bp'' + dp''' + ep + ep'\} + (cf + ee) \{bp''' + dp + ep' + ep''\} \\ &\quad + ef \{2n + ap'' + bp''' + cp + dp'\} + cf \{2n + ap''' + bp + cp' + dp''\} \\ &= 4n(ce + ef) \\ &\quad + p \{(c^2 + e^2)b + ce(d + a) + (ce + ef)(c + e) + (cf + ee)(e + d) \\ &\quad + (e^2 + f^2)e + ef(b + c)\} \\ &\quad + p' \{(c^2 + e^2)d + ce(a + b) + (ce + ef)(c + e) + (cf + ee)(b + e)\} \end{aligned}$$

$$\begin{aligned}
& + (e^2 + f^2)e + ef(d + c) \\
& + p''\{(c^2 + e^2)e + ce(b + c) + (ce + ef)(e + f) + (cf + ee)(d + e) \\
& + (e^2 + f^2)b + ef(a + d)\} \\
& + p'''\{(c^2 + e^2)e + ce(c + d) + (ce + ef)(f + e) + (cf + ee)(a + b) \\
& + (e^2 + f^2)d + ef(b + a)\}.
\end{aligned}$$

On trouve par la comparaison des coëfficients de  $p$  et  $p'$

$$\begin{aligned}
& (c^2 + e^2)(b - d) + ce(d - b) + (cf + ee)(d - b) + ef(b - d) \\
& = (b - d)\{c^2 + e^2 - ce - cf - e^2 + ef\} \\
& = (b - d)\{c(c - f) + e(f - c)\} = (b - c)(c - e)(c - f) = 0
\end{aligned}$$

d'où il résulte que l'une des trois conditions  $b = c$ ,  $c = e$ ,  $c = f$ , doit avoir lieu.  
La comparaison des coëfficients de  $p''$  et  $p'''$  donne

$$\begin{aligned}
& ce(b - d) + (cf + ee)(d - b) + (ee + ff)(b - d) + ef(d - b) \\
& = (b - d)\{ce - cf - ee + ee + ff - ef\} \\
& = (b - d)\{(c - f)e - f(c - f)\} = (b - d)(c - f)(e - f) = 0
\end{aligned}$$

et conduit ainsi à l'une des trois conditions  $b = d$ ,  $c = f$ ,  $e = f$ ; parmi ces conditions il s'en trouve deux qui ont déjà été données par l'équation précédente et si on supposait que ni l'une ni l'autre de celles-là ne doivent être admises, il faudrait s'en tenir à  $e = f$  qui a cause de la troisième condition  $c = e$  fournie, par la dite équation précédente, ramènerait à conclure  $c = f$  contre l'hypothèse. On a donc plus à choisir qu'entre les deux conditions  $b = d$ ,  $c = f$ .

On tire de la comparaison des coëfficients de  $p$  et  $p''$

$$\begin{aligned}
& \{c^2 + e^2 - e^2 - f^2\}(b - e) + ce(d + a - b - c) + (ce + ef)(c - f) \\
& + ef(c + b - a - d) \\
& = (c - f)\{(c + f)(b - e) + ce + ef + e(d + a - b - c)\} \\
& = (c - f)\{cb + fb + ed + ea - be - ce\} [= 0]
\end{aligned}$$

c'est-à-dire  $c = f$  ou  $(c + f)b + e(d - b) + ea - ec = 0$ . Si on supposait  $d = b$ , cette dernière équation deviendrait, en mettant pour  $c + f$  la valeur  $d + b = 2b$  (v. p. 2)<sup>72</sup>  $2b^2 + ea = ec$ .

Dans la vue de décider si on peut s'en tenir à la supposition  $d = b$  j'ai recours aux développements des produits,

$$\begin{aligned}
pp'p'' &= bpp'' + dp'p'' + ep''p'' + ep''p''' \\
&= b\{cp + ep' + fp'' + ep'''\} + d\{bp' + dp'' + ep'''' + ep\} \\
&\quad + e\{2n + ap'' + bp'''' + cp + dp'\} + e\{bp'' + dp'''' + ep + ep'\}
\end{aligned}$$

<sup>72</sup> S. Germain means page 2 of the *addendum* where the equality  $f + c = b + d$  is obtained.

$$\begin{aligned}
&= 2ne + p\{bc + de + ec + e^2\} + p'\{be + bd + ed + e^2\} \\
&\quad + p''\{bf + d^2 + ea + eb\} + p'''\{be + de + be + de\} \\
p'p''p &= bp'p + dp''p + ep'''p + epp \\
&= b\{bp + dp' + ep'' + ep'''\} + d\{cp + ep' + fp'' + ep'''\} \\
&\quad + e\{bp'' + dp + ep' + ep''\} + e\{2n + ap + bp' + cp'' + dp'''\} \\
&= 2ne + p\{b^2 + dc + de + ea\} + p'\{bd + de + e^2 + be\} \\
&\quad + p''\{be + fd + e^2 + ec\} + p'''\{be + de + be + de\}
\end{aligned}$$

et la comparaison des coefficients de  $p$ ,  $p'$ ,  $p''$  et  $p'''$ , dans ces produits.

La comparaison des coefficients de  $p$  donne  $bc + ec + e^2 + de = b^2 + dc + ea + de$ ,  $ec + e^2 = (b - c)b + dc + ea$ ; celle des coefficients de  $p'$  donne  $bf + d^2 + ea + be = fd + e^2 + ec + be$ ,  $ec + e^2 = (b - d)f + d^2 + ea$ : a l'égard des coefficients de  $p''$  et  $p'''$  ils sont identiques dans l'un et l'autre développement et ne fournissent par conséquent aucune nouvelle condition. En examinant même les deux équations  $ec + e^2 = (b - d)f + d^2 + ea$ ,  $ec + e^2 = (b - c)b + dc + ea$  on voit à cause de  $(b - c)b + dc = (f - d)b + dc$  (on a mis dans le 2-ème membre pour  $b - c$  sa valeur  $f - d$  tirée de  $b + d = f + c$  (p. 2))  $= fb + d(c - b) = fb + d(d - f) = (b - d)f + d^2$  qu'elles se réduisent à une seule savoir  $ec + e^2 = (b - d)f + d^2 + ea$ , laquelle devient  $ec + e^2 = d^2 + ea$  par la supposition  $b = d$ ; et si on compare ce résultat à l'équation  $2b^2 + ea = ec$  qui doit avoir lieu en même temps, on trouve  $ec - b^2 = ec + e^2$  ou  $e^2 + b^2 = 0$  d'où on conclut enfin que l'on doit choisir la condition  $f = c$ .

La valeur de  $2n$  se réduit par là à  $2c + 2e$  et on a  $b + d = 2c$  (p. 2). En reprenant l'équation  $ec + e^2 = (b - d)f + d^2 + ea$  on en tire  $ec + e^2 = (2c - 2d)c + d^2 + e(2e - c - 1)$  (on a mis pour  $a$  sa valeur v.-.2),  $e = 2c^2 - 2dc + d^2 + e^2 - 2ec = (c - d)^2 + (c - e)^2$ ,  $4(8n + 1) = 32(c + e) + 4 = 64(c - e)^2 + 32(c - e) + 4 + 64(c - d)^2$ , on a évidemment  $c - d = 2y$  lorsque  $8n + 1 = xx + 64yy$ ; la question est donc réduite à prouver que  $a$  est un nombre impair lorsque  $c - d$  est un nombre pair. Pour y parvenir il faut encore avoir recours à la réflexion suivante: pour les nombres de la forme  $8n + 1$ , 2 il est toujours résidus quadratiques aussi bien que  $4n$ , et il résulte delà qu'il y a un nombre impair de nombres qui tant par eux mêmes qu'étant augmentés de l'unité sont résidus quadratiques ( $\text{mod } 8n + 1$ ). Supposons en effet qu'il y ait un nombre pair de nombres qui tant par eux mêmes qu'étant augmentés de l'unité soient résidus quadratiques, on ne trouvera aucune valeur de  $h$  qui satisfasse à l'équation  $(p - 1)/2 = h$  ou  $4n = h$ , c'est-à-dire que  $4n$  ne sera pas résidu quadratique contre l'hypothèse donc etc.

Il est clair que les nombres qui tant par eux mêmes qu'étant augmentés de l'unité sont résidu quadratique sont l'un et l'autre contenus dans  $\mathfrak{K}$ , l'un et l'autre contenus dans  $\mathfrak{K}''$ , ou contenus l'un dans  $\mathfrak{K}$  et l'autre dans  $\mathfrak{K}''$ : l'ensemble de ces nombres peut donc être exprimé par  $(\mathfrak{KK}) + (\mathfrak{KK}'') + (\mathfrak{K}'\mathfrak{K}'') = a + c + d$  il résulte delà que  $a$  est pair ou impair suivant que  $c + d$  est lui-même impair ou pair et je crois être parvenue à la démonstration du théorème en question.

### Troisième théorème

“Soit  $p$  un nombre premier. Soient les  $p - 1$  nombres inférieurs à  $p$  partagés en deux classes

$$A \dots 1, 2, 3, \dots, (p-1)/2$$

et

$$B \dots (p+1)/2, (p+3)/2, (p+5)/2, \dots, p-1,$$

soit  $a$  un nombre quelconque non divisible par  $p$ . Multipliez tous les nombres  $A$  par  $a$ , prenez en les moindres résidus selon le modul  $p$ , soient, entre ces résidus,  $\alpha$  appartenans à  $A$  et  $\beta$  appartenans à  $B$  de sorte qui  $\alpha + \beta = (p-1)/2$ . Je dis que  $a$  est résidu quarré de  $p$  lorsque  $\beta$  est pair, non résidus lorsque  $\beta$  est impair."

#### Démonstration

Les  $\beta$  résidus qui appartiennent à la classe  $B$  sont le  $\beta$  nombres, pris avec le signe  $-$ , qui sont contenus dans la classe  $A$  et ni font pas partie des  $\alpha$  résidus compris directement dans cette classe, car il est impossible, quelques soient  $n, r$  et  $r'$  ( $r$  et  $r'$  representant cependant toujours deux nombres de la classe  $A$ ) que l'on ait à la fois  $ar \equiv n, ar' \equiv p-n$ , puis qu'il en résultera  $a(r+r') \equiv 0 \pmod{p}$ : et, par conséquent tous les nombres de la classe  $A$ , se trouvent parmi les moindres résidus en question, soit avec le signe  $+$ , soit avec le signe  $-$ . Je suppose donc que l'on fasse le produit de tous le nombre de la classe  $A$ , par eux mêmes et par  $a^{(p-1)/2}$  et que l'on fasse aussi le produit de tous le moindres résidus: on aura en nommant  $P$  ce produit,  $a^{(p-1)/2}P = \pm P$ : le signe  $+$  du dernière nombre répond au cas où  $\beta$  est pair et le signe  $-$  à celui où  $\beta$  est impair: mais on a  $a^{(p-1)/2} \equiv 1$  ou  $a^{(p-1)/2} \equiv -1$ , suivant que  $a$  est ou non est résidu quarré, donc  $\beta$  est pair dans le premier cas et impair dans le second. C.Q.E.D

On trouve quelque chose d'analogue pur les résidus biquarré. En effet:

*soit  $p = 4k + 1$  un nombre premier, soient les  $2k$  résidus quarré ( $\pmod{p}$ ) partagés en deux classes  $A$  et  $B$ , la première comprenant les résidus qui ne sont pas plus grand que  $2k$  et l'autre des mêmes résidus qui surpassent  $2k$ . Soit  $a$  un résidu quelconque ( $\pmod{p}$ ) soient entre ces résidus  $\alpha$  appartenans à  $A$  et  $\beta$  appartenans à  $B$  de sorte que  $\alpha + \beta = 2k$ . Je dis que  $a$  est résidu biquarré de  $p$  lorsque  $\beta$  est pair et similement résidu quarré lorsque  $\beta$  est impair.*

La démonstration est absolument la même que celle du cas précédent, excepté qu'au lieu de multiplier le produit de tous les nombres de la classe  $A$  par  $a^{(p-1)/2}$ , il faut multiplier ici par  $a^{(p-1)/4}$  parcequ'en effet  $(p-1)/4 = k$  est le nombre des nombres compris dans cette classe; et on conclut  $a^{(p-1)/4} \equiv 1$  ou  $a^{(p-1)/4} \equiv -1$  suivant que  $\beta$  est pair ou impair.

En général si on connoissait tous les résidus  $(2^{m-1})$ -ième puissance ( $\pmod{p}$ ) ( $p = 2^mk + 1$ ) on deciderait si l'un de ces résidu est aussi résidu  $(2^m)$ -ième puissance, en partagent les résidus  $(2^{m-1})$ -ième puissance entre deux classes l'une renfermant ceux qui sont au dessous et l'autre ceux qui sont plus grands que  $2^{m-1}k$  et examinant si parmi les moindres restes des produis du résidu en question par les nombres de la première classe, il s'en trouve un nombre pair au impair compris dans la secondeieme dans le premier cas,  $a^k \equiv 1$  et dans le second  $a^k \equiv -1$ .

### Gauss's reply.

Gottingue, ce 19 janvier 1808

En vous remerciant de tout mon coeur pour votre dernière lettre et les intéressantes communications que vous m'y faites, Mademoiselle, je vous prie mille fois pardon, d'y répondre aussi tard. Cette négligence est pour la plus grande partie une suite de changements qui se sont faits dans ma situation. J'ai changé ma demeure, pour accepter la place de professeur d'astronomie à Gottingue qu'on m'avait offerte depuis longtemps. Je ne vous dis rien des circonstances fâcheuses qui m'ont enfin déterminé à faire ce pas ni des nouvelles tracasseries auxquelles je me trouve exposé ici : j'espère que l'interposition de l'Institut où j'ai eu recours y mettra fin. Ne contemplons à présent que la belle perspective que j'ai de pouvoir avec plus d'aisance, du moins dans la suite, veiller à mes travaux surtout arithmétiques, et de les publier successivement dans les mémoires de la Société de Gottingue. J'ai le plaisir de vous envoyer les prémisses,<sup>73</sup> lesquelles, comme j'espère, vous feront quelque plaisir. Vous me pardonnerez que cette fois je ne puis m'étendre davantage sur la belle démonstration de mes théorèmes arithmétiques. J'admire la sagacité avec laquelle vous avez pu en si peu de temps y parvenir. J'espère de pouvoir bientôt publier toute la théorie dont ces propositions élégantes font partie, avec une foule d'autres choses. Que mes occupations arithmétiques, me rendent heureux dans un temps où je ne vois autour de moi que le malheur et le désespoir! Ce ne sont que les sciences, le sein de la famille et la correspondance avec ses amis chéris où l'on puisse se dédommager et se reposer de l'affliction générale.

L'ouvrage sur le calcul des orbites des planètes, dont je vous ai parlé dans ma dernière lettre, est enfin sous presse. J'espère qu'il sera achevé dans quelques mois. Je n'ai pas redouté la peine de le traduire en Latin, afin qu'il puisse trouver un plus grand nombre de lecteurs.<sup>74</sup>

Soyez toujours aussi heureuse, ma chère amie, que vos rares qualités d'esprit et de coeur le méritent, et continuez de temps en temps de me renouveler la douce assurance que je puis me compter parmi le nombre de vos amis, titre duquel je serai toujours orgueilleux.

Ch. Fr. Gauss

### VI

A Monsieur  
 Monsieur le docteur Gauss Professeur  
 D'Astronomie dans l'Université de Gottingue  
 A Gottingue<sup>75</sup>  
 Monsieur,

<sup>73</sup> The paper in question is *Theorematis aritmetici demonstratio nova* (Gauss 1808).

<sup>74</sup> Gauss is referring to his tract *Theoria motus corporum coelestium in sectionibus conicis solem ambientium* (Gauss 1809), which he wrote in German and the publisher asked for its translation in latin, at that time a more common language among scientists.

<sup>75</sup> Beneath the address and inscribed into a rectangle, Gauss wrote "Nro 31 März 29 // Sophie Germain".

Il est sans doute inutile de vous dire combien je prens de part aux malheurs dont cette funeste guerre est pour vous l'occasion, il est triste pour ceux qui trouvant leurs plus grand plaisirs dans la jouissance des fruits de vos traveaux, de penser que tandis que vos meditations le préparent, vous n'étés environé que de sujet de peine: esperons qu'un mérite si supérieur sera enfin connu des chefs du gouvernement et qu'il sentirons que leur glorie est intéressé à vous faire joir des avantages au quels vous avez droit.

J'ai lu avec le plus grand plaisir la mémoire que vous avez bien voulu m'envoyer,<sup>76</sup> j'admire comment le premier théorème que vous m'avez déjà fait connaître est devenu dans vos mains le source d'une des plus belles démonstrations que présente l'arithmétique; je suis chargée par Mr. Le Gendre vous remercier de l'exemplaire que je lui ai remis de votre part et je m'estime heureuse en vous disant combien il fait de cas de votre démonstration, d'avoir à vous présenter un hommage plus digne que le mien de vous être offert. En effet vous ne pourriez avoir pour juge un savant plus au fait de la difficulté dans cette matière, aussi vous rend-il tout la justice qui vous est due et cela avec un plaisir, qui honore son caractère et dont je ne puis m'empêcher de vous faire part, parce qu'il arrive trop souvent que l'assentement le plus difficile à obtenir est justement celui des gens qui ont traité les mêmes questions où l'on fait des plus grand pas.

Je vois avec plaisir que vous avez pris la peine de faire passer dans la langue latine l'ouvrage sur les orbites,<sup>77</sup> il est de nature à intéresser un grand nombre de lecteur, et je vous assure que je n'aurais pas voulu rénover à l'étudier lors même qu'il eut été écrit en allemand, j'avais même déjà acheté grammaire et dictionnaire à ces effet, mais l'étude des langues n'est pas guéré de mon goût il n'eut fallu moins que la haute extime que j'ai pour vos traveaux pour m'engager à m'y livrer.

En relisant ma démonstration de votre théorème: *2 résidu biquarré des nombres*  $xx + 64yy$ , je me suis aperçu que je me suis trompée dans l'endroit où j'ai voulu prouver que  $a$  est un nombre impair lorsque  $c - d$  est pair, j'ai dit à tort que le nombre des nombres qui tout par eux mêmes qu'étant augmentés de l'unité, sont résidus biquarré est  $(\mathfrak{R}\mathfrak{R}) + (\mathfrak{R}\mathfrak{R}'') + (\mathfrak{R}''\mathfrak{R}'')$  tandis qu'il est  $(\mathfrak{R}\mathfrak{R}) + 2(\mathfrak{R}\mathfrak{R}'') + (\mathfrak{R}''\mathfrak{R}'')$ , par une seconde erreur j'ai écrit  $(\mathfrak{R}\mathfrak{R}) + (\mathfrak{R}\mathfrak{R}'') + (\mathfrak{R}''\mathfrak{R}'') = a + c + d$  au lieu de  $(\mathfrak{R}\mathfrak{R}) + 2(\mathfrak{R}\mathfrak{R}'') + (\mathfrak{R}''\mathfrak{R}'') = a + 3c$  ce qui rend mon raisonnement entièrement défectueuse. Pour y supplier je reprens les 2 équations  $2n - 1 = a + b + c + d$ ,  $2n = b + d + 2e$  et j'observe que parmi les quantités  $a, b, c, d$  trois sont paires et une seulement est impaire, que par conséquent, lorsque  $c - d$  est pair il faut que  $c$  et  $d$  soient également paires et que lorsque  $d$  est paire la seconde équation rapportée montre que  $b$  est pair aussi, d'où il résulte que  $a$  est alors impaire.

Au reste cette démonstration peut être singulièrement abrégée par la considération du système suivant de 6 congruances

$$\begin{aligned} r^{\mathcal{Q}+Y-Y'} - r^Y &\equiv 1 \\ r^{\mathcal{Q}+Y'-Y} - r^{Y'} &\equiv 1 \\ r^{\mathcal{Q}+Y} - r^{Y-Y'} &\equiv 1 \end{aligned}$$

<sup>76</sup> Gauss is referring to *Theorematis aritmetici...* (Gauss 1808).

<sup>77</sup> She is referring to *Theoria motus corporum...* (Gauss 1809).

$$\begin{aligned} r^{Q+Y'} - r^{Y'-Y} &\equiv 1 \\ r^{Q-Y} - r^{2Q-Y'} &\equiv 1 \\ r^{Q-Y'} - r^{2Q-Y} &\equiv 1 \end{aligned}$$

dans lesquelles  $2Q = P - 1$ ,  $r$  représente une racine primitive, et  $Y, Y'$  désignant des nombres quelconques moindres que  $2Q$ . On voit aisément que l'une quelconque de ces 6 congruances peut servir à faire trouver les 5 autres.

Voici à présent le partie que l'on peut tirer:

Si on nomme  $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}'', \mathfrak{K}'''$  etc. les périodes qui contiennent les puissances  $n$ -ième,  $(n+1)$ -ième,  $(n+2)$ -ième,  $(n+3)$ -ième etc. de la racine primitive, que l'on désigne pour  $[\mathfrak{K}\mathfrak{K}']$  etc. le nombre des congruances appartenantes à un même système, et dont les premiers membres sont les différences entre une puissance  $n$ -ième et une puissance  $(n+1)$ -ième etc., que l'on suppose  $-1$  résidu puissance  $n$ -ième, cette-à-dire  $Q$  divisible par  $n$  et que l'on fasse  $Y = yn + \delta, Y' = y'n + \delta$  on trouve  $[\mathfrak{K}\mathfrak{K}^\delta] = [\mathfrak{K}^{n-\delta}\mathfrak{K}^{n-\delta}]$  et comme chaque système contenant la différence des puissances  $n$ -ième et  $(n+\delta)$ -ième fournit la même équation, on en conclut, en désignant par  $(\mathfrak{K}\mathfrak{K}^\delta)$  etc. le nombre des nombres contenus dans  $\mathfrak{K}$  qui étant augmentés de l'unité sont dans  $\mathfrak{K}^\delta$  etc.  $(\mathfrak{K}\mathfrak{K}^\delta) = (\mathfrak{K}^{n-\delta}\mathfrak{K}^{n-\delta})$ .

On voit par cette conditions pourquoi une seulement des quantités  $(\mathfrak{K}\mathfrak{K}^\delta)$  est impair puisque 2 est nécessairement contenu dans l'une des périodes  $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}'', \mathfrak{K}'''$  etc.

Si on fait ensuite  $Y = yn + d, Y' = y'n + \delta$ , on trouve en raisonnant de même  $(\mathfrak{K}^{n+d-\delta}\mathfrak{K}^{n+d}) = (\mathfrak{K}^{n-d}\mathfrak{K}^{n-\delta}) = (\mathfrak{K}^{n+\delta-d}\mathfrak{K}^{n+\delta})$ .

On voit encore par la considération des systèmes de 6 congruences que  $(\mathfrak{K}\mathfrak{K})$  est de l'une des formes  $6h + 3, 6h$  suivant que 2 est résidu ou non résidu puissance  $n$ -ième. Si on fait  $n = 4$ , qui est le cas de la démonstration citée, on a les équations

$$\begin{aligned} (\mathfrak{K}\mathfrak{K}') &= (\mathfrak{K}'''\mathfrak{K}''), & (\mathfrak{K}\mathfrak{K}'') &= (\mathfrak{K}''\mathfrak{K}''), & (\mathfrak{K}\mathfrak{K}''') &= (\mathfrak{K}'\mathfrak{K}'); \\ (\mathfrak{K}'\mathfrak{K}'') &= (\mathfrak{K}''\mathfrak{K}''') = (\mathfrak{K}'''\mathfrak{K}'), \end{aligned}$$

que j'avais deduites de la comparaison entre différentes formes de mêmes produits.

Si on fait ensuite  $n = 2$  on a l'équation  $(\mathfrak{K}'\mathfrak{K}') = (\mathfrak{K}\mathfrak{K}')$ , d'où on peut conclure que 2 est résidu pour les nombres  $8m + 1$  et non résidu pour les nombres  $8m + 5$ .<sup>78</sup>

En effet on a

$$4m = (\mathfrak{K}'\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}') = 2(\mathfrak{K}'\mathfrak{K}'), \quad 4m + 2 = (\mathfrak{K}'\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}') = 2(\mathfrak{K}'\mathfrak{K}')$$

c'est-à-dire  $(\mathfrak{K}'\mathfrak{K}')$  pair dans le premier cas et impair dans le second ou  $(\mathfrak{K}\mathfrak{K})$  impair pour les nombres  $8m + 1$  et pair pour ceux  $8m + 5$ .

Lorsque  $n = 2n'$  et que  $Q$  est seulement divisible par  $n'$ , c'est-à-dire [lorsque]<sup>79</sup>  $-1$  est résidu puissance  $n'$ -ème et non pas puissance  $n$ -ème les équations résultantes

<sup>78</sup> Opening the letter, Gauss probably damaged the sheet of paper and of the word "conclure" only "con" remained readable, over it Gauss wrote the complete word.

<sup>79</sup> See the previous footnote, here Gauss added in his hand "lorsque".

de la]<sup>80</sup> en considération des [du] système de 6 congruances sont:

$$\begin{aligned} (\mathfrak{R}^{n'+d-\delta} \mathfrak{R}^d) &= (\mathfrak{R}^{n'+\delta-d} \mathfrak{R}^\delta) = (\mathfrak{R}^{n'+d} \mathfrak{R}^{d-\delta}) = (\mathfrak{R}^{n'+\delta} \mathfrak{R}^{\delta-d}) \\ &= (\mathfrak{R}^{n'-d} \mathfrak{R}^{n-\delta}) = (\mathfrak{R}^{n'-\delta} \mathfrak{R}^{n-d}) \end{aligned}$$

et en fesant  $\delta = d$

$$(\mathfrak{R}^{n'} \mathfrak{R}^d) = (\mathfrak{R}^{n'+d} \mathfrak{R}) = (\mathfrak{R}^{n'-d} \mathfrak{R}^{n-d}).$$

On a aussi lorsque  $n' = 1$ ,  $(\mathfrak{R}' \mathfrak{R}') = (\mathfrak{R} \mathfrak{R}) = (\mathfrak{R} \mathfrak{R}')$ .

Si on prend un nombre quelconque  $a$  tel que  $a$  soit dans  $\mathfrak{R}'$  et  $a + 1$  dans  $\mathfrak{R}$ ,  $P - a$  sera dans  $\mathfrak{R}$  et  $P - a - 1$  dans  $\mathfrak{R}'$  de sorte que  $(\mathfrak{R} \mathfrak{R}')$  sera un nombre pair, à moins que il n'y ait un valeur de  $a$  telle que  $P - a - 1 = a$  ou  $a = (P - 1)/2$ , si cela arrive 2 sera dans  $\mathfrak{R}$  c'est-à-dire résidu.

On peut conclure delà: 2 résidu pour les nombres  $8m + 7$  et non résidu pour les nombres  $8m + 3$  car on a dans le premier cas  $4m + 3 = (\mathfrak{R}' \mathfrak{R}') + (\mathfrak{R} \mathfrak{R}') + 1 = 2(\mathfrak{R} \mathfrak{R}') + 1$  c'est-à-dire  $(\mathfrak{R} \mathfrak{R}')$  impair et dans le second  $4m + 1 = (\mathfrak{R}' \mathfrak{R}') + (\mathfrak{R} \mathfrak{R}') + 1 = 2(\mathfrak{R} \mathfrak{R}') + 1$  c'est-à-dire  $(\mathfrak{R} \mathfrak{R}')$  pair.

Votre dernier mémoire contient une nouvelle démonstration de ces propositions qui sans doute est bien préférable à cette ci,<sup>81</sup> aussi ne vous la présentez ainsi que comme une témoignage de mon goût pour ce genre de question et de la confiance en votre indulgence que m'inspire la bienveillance dont vous m'honorez, recevez en, Monsieur mes sincères remerciements et croyez que j'aurez toujours pour vous l'admiration et l'intérêt dans votre supériorité

Ce 19 mars 1808

Sophie Germain

## VII

Monsieur

Je vous dois mille et mille remerciements pour le beau mémoire que Mr. Le Genbre m'a remis de votre part il me charge de vous témoigner combien il attache lui-même de pris à ce présent et je me félicite d'avoir à vous transmettre un suffrage plus éclairé que le mien.<sup>82</sup> J'ai lu cet ouvrage avec toute l'attention dont je suis capable, j'admiré la généralité des recherches qui en sont l'objet, elles me paruissent faire suite à celles qui remplissent les prop. 356 et 357 de votre premier livre sur l'arithmétique où vous traitez seulement des nombres premiers. J'ai vu avec le plus grand plaisir la démonstration du théorème fondamental présenté comme un cas particulier d'une proposition beaucoup plus générale.

Vous me mandez d'être occupé dans ce moment de la belle théorie des résidus cubiques et biquadratiques, elle m'inspire le plus grand intérêt et la curiosité la plus vive; je

<sup>80</sup> This was added by Gauss.

<sup>81</sup> *Theorematis arithmeticæ demonstratio nova* (Gauss 1808).

<sup>82</sup> She is referring to *Summatio quarundam serierum singularium commentationes*, which Gauss presented in 1808 to the Göttingen Academy of Sciences (Gauss 1811).

ne crois pas qu'il existe ni pour les uns ni pour les autres de ces résidus aucune loi de réciprocité analogue à celles qui composent le théorème fondamental; il y a sans doute de grandes différences entre ces résidus et les résidus quarrés ainsi, par exemple, quoi qu'il soit vrai que tout nombre, excepté les quarrés, pris positivement, soit non résidu quarré pour quelque nombre premier  $2k + 1$ , il n'est pas vrai que tout nombre, excepté les biquarrés pris positivement soit non résidu biquarré pour quelque nombre premier de la forme  $4k + 1$ , car  $-4$  est résidus biquarré pour tous ces nombres, parce que  $-1$  et  $4$  sont toujours à la fois résidus biquarrés ou simplement résidu quarré; je crois qu'a la vérité  $4$  est le seul quarré, qui pris avec le signe  $-$ , soit résidu biquarré pour tout nombre premier de la forme  $4k + 1$ , vous trouverez, peut être, que cela est assez clair de soi même pour qu'il soit inutile de le démontrer puisque si  $q^2$  par exemple jouissait de cette propriété, il en résultera que sa racine  $q$  devait être résidu quarré pour tous le nombre premiers de la forme  $8k + 1$  et non résidu quarré pour tous les nombres premiers de la forme  $8k + 5$ , au reste je n'ai pas pu réussir à cette démonstration pour les quarrés paires, je suis seulement venu au bout de prouver, comme il suit, que tout quarré impair pris avec le signe  $-$  est non résidu biquarré de quelque nombre premier de la forme  $8k + 5$ .

Soit  $(2h + 1)^2$  un quarré impair quelconque, le nombre  $(2h + 1)^2 + 4$  sera de la forme  $8k + 5$ , par conséquent il sera premier ou il sera le produit de deux facteurs des formes  $8k + 3$  et  $8k + 7$  ou de celles  $8k + 1$  et  $8k + 5$ ; mais  $(2h + 1)^2 + 4$  étant la somme de deux quarrés ne peut avoir pour facteurs que des nombres qui soient pareillement la somme de deux quarrés, or les nombres des formes  $8k + 3$ ,  $8k + 7$  ne jouissent pas de cette propriété ainsi le nombre  $(2h + 1)^2 + 4$  a nécessairement un facteur premier de la forme  $8k + 5$ , soit  $p$  ce facteur, on aura  $(2h + 1)^2 \equiv -4 \pmod{p}$  et à cause de  $-4$  résidu biquarré  $\pmod{p}$   $(2h + 1)^2$  sera aussi résidu biquarré même modul donc, enfin,  $-(2h + 1)^2$  sera simplement résidu quarré, c'est-à-dire non résidu biquarré  $\pmod{p}$ .

De  $-4$  résidu biquarré pour tout nombre premier  $p = 4k + 1$  il résulte qu'en prenant [prennent]  $n^2$  pour le plus grand quarré contenu dans  $k$  et  $q$  pour le quotient de la division de  $k$  par  $n^2$ ,  $q$  est résidu biquarré  $\pmod{p}$  à cause de  $-4qn^2 \equiv 1 \pmod{p}$ , car tous les facteurs premiers de  $n$  sont résidus quarrés et par conséquent  $n^2$  résidu biquarré  $\pmod{p}$  cela est clair si  $n$  ne contient que des facteurs impairs et la même chose a lieu lorsque  $n$  est multiple de 2, parce que 2 est dans ce cas résidu quarré  $\pmod{p}$  puis que ce nombre et alors de la forme  $8k + 1$ . Si on fait  $q = 2$  on trouve que 2 est résidu biquarré pour les nombres premiers de la forme  $8n^2 + 1$  et il en résulte qu'un nombre de cette forme  $8n^2 + 1$  ne peut être premier à moins que  $n^2$  ne satisfasse à l'équation  $n^2 = \frac{y^2+y}{2} + 8x^2$ .

En étudiant votre mémoire du 15 Janvier 1808,<sup>83</sup> qui m'a inspiré tant d'admiration et d'étonnement par la simplicité des formules qu'il contient et par les belles conclusions que vous en avez deduites, je me suis avisée de chercher ce qu'elles donneraient si on les appliquaient aux résidus biquarrés; pour cela, au lieu des nombres  $1, 2, \dots, (p - 1)/2$  je prends les résidus quarrés  $<$  de  $(p + 1)/2$  que je désigne par les

<sup>83</sup> Germain is probably referring to *Theorematis arithmetici demonstratio nova* which Gauss presented to the Göttingen Academy of Sciences on January 15, 1808, (Gauss 1808).

lettres  $r, r'r''$  etc. et je represente par  $(k, p)$  le nombre des produits  $kr, kr', kr''$  etc. dont les moindres restes selon le modul  $p$  sont  $>$  de  $(p - 1)/2$ .

L'équation f.VI devient

$$(k, p) = \left[ \frac{2kr}{p} \right] + \left[ \frac{2kr'}{p} \right] + \left[ \frac{2kr''}{p} \right] + \cdots - 2 \left[ \frac{kr}{p} \right] - 2 \left[ \frac{kr'}{p} \right] - 2 \left[ \frac{kr''}{p} \right] - \cdots$$

puisque  $-1$  est résidu quarré mod  $(p = 4n + 1)$ , il est clair qu'il-y-a  $n$  résidus quarrés  $r, r', r''$  etc. moindres que  $(p + 1)/2$  par conséquent

$$\begin{aligned} (-k, p) &= \left[ \frac{2r(p - k)}{p} \right] + \left[ \frac{2r'(p - k)}{p} \right] + \left[ \frac{2r''(p - k)}{p} \right] + \cdots \\ &\quad - 2 \left[ \frac{r(p - k)}{p} \right] - 2 \left[ \frac{r'(p - k)}{p} \right] - 2 \left[ \frac{r''(p - k)}{p} \right] - \cdots \\ &= 2r + 2r' + \cdots - n - \left[ \frac{2kr}{p} \right] - \left[ \frac{2kr'}{p} \right] - \left[ \frac{2kr''}{p} \right] - \cdots \\ &\quad - 2(r + r' + \cdots) + 2n + 2 \left[ \frac{kr}{p} \right] + 2 \left[ \frac{kr'}{p} \right] + 2 \left[ \frac{kr''}{p} \right] + \cdots \end{aligned}$$

et  $(k, p) + (-k, p) = (p - 1)/4$ , d'où il résulte comme f.VII que  $k$  et  $-k$  sont à la fois résidus ou non résidus biquarres lorsque  $p = 8n' + 1$  et au contraire l'un résidu et l'autre non résidu biquarré lorsque  $p$  est de la forme  $8n' + 5$ .

Si on prend  $p = 8n' + 1$  et  $k = 2$  on aura

$$(2, p) = \left[ \frac{4r}{p} \right] + \left[ \frac{4r'}{p} \right] + \left[ \frac{4r''}{p} \right] + \cdots - 2 \left[ \frac{2r}{p} \right] - 2 \left[ \frac{2r'}{p} \right] - 2 \left[ \frac{2r''}{p} \right] - \cdots$$

et comme  $4$  n'est la plus grande des quantités  $r, r', r''$  etc. la seconde ligne disparaîtra et  $(2, p)$  sera égal au nombre des résidus quarrés compris entre  $2n'$  exclusivement et  $4n'$  inclusivement, c'est en effet ce à quoi se réduit la première ligne dont tous les termes sont nuls, jusqu'et y compris  $r^n = 2n'$ . Ainsi  $2$  est résidu ou non résidu biquarré (mod  $p = 8n' + 1$ ) suivant qu'il y a un nombre pair ou impair de résidus quarrés compris entre l'unité et  $2n'$  inclusivement. Cette proposition est analogue a celle-ci qui a lieu pour les nombres premiers  $4n + 1$ :  $2$  est résidu ou non résidu quarré suivant que  $n$  est pair ou impair.

On voit que la suite des résidus quarrés remplace, pour les résidus biquarres celle des nombres naturels pour les résidus quarrés.

Je ne m'étonne pas, Monsieur, de l'attrait que vous porte vers les recherches arithmétiques, lorsque je vois chaque jour vos travaux couronnés par de nouveaux succès: combien je vous remercie de l'honneur que vous me faites en me les faisant connaître et en accueillant avec indulgence le petit nombre d'idées que je prends la liberté de vous communiquer, elles doivent vous paraître, en quelque sorte, pueriles, si vous les comparez à celles qui se présentent en foule à votre génie créateur devant lequel il s'ouvre à chaque instant de nouvelles routes! Ce que vous me dites touchant une

équation analogue, pour le cube, à ce que l'équation  $xx - Dy = 1$  est pour le carré, présenterait sans doute des difficultés inespugnables, à tout autre qu'a vous, il semble en effet que les deux facteurs dans lesquels on peut séparer une pareille équation n'étant plus du même ordre l'un que l'autre il doive être difficile, par exemple, d'en trouver toutes les solutions au moyen d'une seule. Au reste je ne prétends nullement sonder la profondeur de vos recherches, je sens que mon esprit est trop loin du vôtre quoique nos goûts soient semblables, car j'ai comme vous une grande prédisposition pour les questions arithmétiques, je trouve que cette partie de la science est susceptible d'un genre particulier d'elegance que les sciences physico-mathématiques ne peuvent atteindre, il semble qu'en toutes choses l'intérêt des idées soit en raison inverse de l'utilité qu'elles présentent pour la pratique, on ne s'en étonne pas lorsque l'on considère que l'esprit humain travaillant pour son unique satisfaction doit renoncer de plus grandes beautés intellectuelles que lorsqu'il est dirigée par un motif étranger. Cependant quelque soit l'objet auquel vous consacrerez vos veilles je régarderai toujours le temps que je mettrai à en étudier les produits comme celui que j'aurai le mieux employé pour ma satisfaction et mon instruction.

J'ai tant de remerciements à vous faire que je ne puis les épouser; vous m'avez déjà envoyé plusieurs beaux mémoires, vous me promettez un ouvrage plus étendu sur l'astronomie, vous me faites espérer, pour un avenir plus éloigné la belle théorie des résidus cubiques et biquadrats enfin vous daignez prendre la peine de me rendre compte de vos travaux et d'encourager un goût qui fait mon bonheur. Je vous prie, Monsieur, d'agrémenter à tous de titres l'expression de ma reconnaissance de mon admiration et de tous les sentiments distingués dus à vos talents et à l'intérêt que vous voulez bien me témoigner.

Ce 22 mai 1809

Sophie Germain

## VIII

A Monsieur

Monsieur Le docteur Gauss

Professeur d'Astronomie à l'Université de Gottingue

Gottingue

Monsieur,

L'empressement que je mets à connaître vos ouvrages m'avait engagée à faire demander à Lipsie votre livre sur la détermination des orbites dans un temps où je ne prévoyais pas que vous me feriez l'honneur de me l'offrir.<sup>84</sup> J'ai été servie avec tant de promptitude que je viens de le recevoir: je croirais abuser de votre générosité si en vous remerciant de tout mon coeur de la promesse que vous m'avez faite de m'envoyer, je ne vous faisais savoir que je l'ai déjà entre les mains.

Je n'avais pas voulu differer plus longtemps de répondre à la lettre et au présent dont vous m'avez honorée et cependant j'ai cru vous témoigner d'avantage le cas que je fais de vos ouvrages et de la généreuse bonté avec laquelle vous voulez bien me

<sup>84</sup> She is referring to *Theoria motus corporum coelestium...*(Gauss 1809)

les envoyer en attendant que j’usse le livre pour vous dire que je réserve votre bonne volonté pour les mémoires dont je n’aurais aucune connaissance si vous ne preniez la peine de me les faire passer, j’ajoute dans la sincérité de ma reconnaissance qu’ils ont un prix de plus à mes yeux lorsqu’ils me sont offerts par vous.

J’ai parcouru l’ouvrage dont il s’agit avec une attention suffisante pour remarquer la simplicité et la clarté qui y règne, j’admire comment un auteur habitué à des recherches si élevées soit pourtant se rendre, pour ainsi dire, élémentaire lorsque les besoins de la pratique l’exige. J’ai vu dans la première partie avec quel ordre vous avez rangé les matériaux qui doivent servir dans celles qui suivent, les calculs pour les différentes sections coniques sont d’une grande simplicité vous employé les mêmes quantités sous des formes appropriés à chaque cas. Je n’avais pas encore vu l’emploi de quatre observations, au reste je me réserve d’établir toutes les parties de l’ouvrage avec le soin que mérite tout ce qui sorte de votre savante plume. Mais je n’ai pas voulu attendre que j’en ai eu le temps pour vous mander que ce livre est venu jusqu’à moi c’est cette circonstance qui m’engage à vous écrire à un si court interval[le] j’espère, Monsieur, que vous excuserez mon importunité et que vous accueillerez avec bienveillance l’assurance répétée de mon admiration et de mon respect

Ce 26 mai 1809

Sophie Germain

PS. Quelqu’occupée que je suis à lire l’ouvrage sur les orbites et à relire encore votre dernier mémoire je soupire toujours après votre théorie des résidus biquarrés et je ne crains pas de vous témoigner pour cette partie un goût que je ne puis, comme vous, justifier par des succès.

## IX

Paris (Rue de Braque n.4) ce 12 mai 1819

Monsieur,

Je regrette infiniment que vous n’ayez pas accompagné Monsieur votre ami; j’aurais eu le plus grand plaisir à vous entendre parler des belles théories qui sont l’objet de vos études favorites et pour lequelles j’ai moi même une véritable passion.

Les démonstrations nouvelles que contient votre mémoire m’ont enchantée.<sup>85</sup> Vous paraissiez préférer la dernière à cause de la liaison qu’elle établit entre des vérités qui au premier coup d’œil semblent être indépendants. J’ai sans doute été fort sensible à ce genre de surprise que déjà plusieurs endroits des *disquisitiones* m’avoient fait éprouver. Cependant je vous avourez que l’énoncé du théorème nr. 2 m’a plu encore d’avantage. Cette phrase qui le termine: *Tunc tres numeri n, N, 1/4(m – 1)(N – 1), vel omnes simul pares erunt, vel unus par duoque reliqui impares* m’a frappé d’un genre d’admiration en quelque sorte contraire à celui dont je viens de parler car on y sent la démonstration toute entière et par cette raison elle me semble avoir atteint le plus haut degré d’elegance que l’on puisse imaginer.

<sup>85</sup> The paper in question is *Theorematis fundamentalis in doctrina de residuis quadraticis, demonstrationes et ampliationes novae* (Gauss 1818).

C'est toujours avec un nouvel intérêt que l'on considère des points de vue différents d'une même vérité: l'applications entièrement neuve que vous faites du théorème fondamental à la détermination de la question de résidu ou non résidu présent un autre genre de jouissance: c'est une véritable acquisition qui peut être d'un grand usage.

Je regrette que vous différiez depuis si longtem[p]s de nous donner vos recherches sur les résidus cubiques et biquarres en traitant ces questions il est probable que vous auriez le moyen d'aller encore plus loin, je veux dire d'étendre la théorie aux résidus puissance quelconque.

Je n'ai pas encore eu le tem[p]s de lire le mémoire sur les attractions,<sup>86</sup> je me propose de l'étudier car cet objet m'est beaucoup moins familier que la théorie des résidus. J'ai voulu me réserver avant le départ de Monsieur votre ami, le tem[p]s de vous faire les remerciements que je vous dois et aussi de vous communiquer les recherches que m'ont occupées depuis l'époque à laquelle j'ai eu l'honneur de vous écrire.

Quoique j'ai travaillé pendant quelque tem[p]s à la théorie des surfaces vibrantes (à laquelle j'aurais beaucoup de choses à ajouter si j'avais la raison de faire les expériences que j'ai imaginées concernant les surfaces cylindriques) je n'ai jamais cessé de penser à la théorie des nombres. Je vous donnerai une idée de ma préoccupation pour ce genre de recherches en vous avouant que même sans aucune expérance de succès je la préfère à un travail qui me donnerait nécessairement un résultat et qui pourtant m'intéresse... quand j'y pense.

Longtem[p]s avant que notre académie ait proposé pour sujet de prix la démonstration de l'impossibilité de l'équation de Fermat, cet[te] espèce de défi porté aux théories modernes par un géomètre qui fuit privé des res[s]ources que nous possédons aujourd'hui, me tourmentait souvent. J'entre-voyais *vaguement* une liaison entre la théorie des résidus et la fameuse équation, je crois même vous avez parlé anciennement de cette idée car elle m'a frappée aussitôt que j'ai connu votre livre.

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  $p$ -ième puissance placés de suite dans la série des nombres naturels divisera nécessairement l'un des nombres  $x$ ,  $y$  et  $z$ .

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

On sait que l'équation a une infinité de solutions lorsque  $p = 2$ . Et en effet tous les nombres, exceptés 3 et 5 ont au moins deux résidus quarrés dont la différence est l'unité. Aussi dans ce cas la forme connue savoir  $h^2 + f^2$ ,  $2fh$ ,  $h^2 - f^2$  des nombres

<sup>86</sup> The paper in question is probably *Theoria attractionis corporum sphaeroidicorum ellipticorum homogeneorum methodo nova tractata* (Gauss 1813).

$z$  [ $x$ ],  $y$  et  $z$  montre-t-elle que l'un de ces nombres est multiple de 3 et aussi que l'un des mêmes nombres est multiple de 5.

Il est ais  de voir que si un nombre quelconque  $k$  est r sida puissance  $p$ -i me mod  $2Np + 1$  et qu'il y ait deux r sida puissance  $p$ -i me m me mod. dont la diff rence soit l'unit , il y aura aussi deux r sida puissances  $p$ -i me dont la diff rence sera  $k$ .

Mais il peut arriver qu'on ait deux r sida  $p$ -i me dont la diff rence soit  $k$ , sans que  $k$  soit r sida  $p$ -i me.

Cela pos  voici l' quation g n rale dont la solution me semble d pendre comme celle de Fermat de l'ordre des r sida:

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

car d'apr s ce que vient d' tre dit on voit que tous nombre premier de la forme  $2Np + 1$  pour lequel deux r sida  $p$ -i mes n'ont pas le nombre  $k$  pour diff rence divise le nombre  $z$  [l'un des nombres  $x$ ,  $y$ ,  $z$ ]. Il suit del  que s'il y avait un nombre infini de tels nombres l' quation serait impossible.

Je n'ai jamais p  [pu] arriver   l'infini quoique j'ai recul  bien loin les limites par un m thode de t tonnement trop longue pour qu'il me soit possible de l'exposer ici. Je n'oserais m me pas affirmer que pour chaque valeur de  $p$  il n'existe pas une limite au-del  de laquelle tous les nombres de la forme  $2Np + 1$  auraient deux r sida  $p$ -i mes plac s de suite dans la s rie des nombres naturels. C'est le cas qui int resse l' quation de Fermat.

Vous concevrez ais ment, Monsieur, que j'ai d  parvenir   prouver que cette  quation ne serait possible qu'en nombres dont la grandeur effraye l'imagination; car elle est encore assujettie   bien d'autres conditions que je n'ai pas le tem[ps] d'examiner   cause des d tails n cessaires pour [en] ´tablir la r alit . Mais tout ce la n'est encore rien, il faut l'infini et non pas le tr s grand.

Chemin f sent [faisant] je me suis aid e d'un syst me de six congruances [congruences] dont une quelconque redonne les cinq autres. Lorsque pour un nombre de la forme  $2Np + 1$ , 2 est non r sida puissance  $p$ -i me et qu'en m me tem[ps]  $N$  est premier   3 les six congruances [congruences] ne sont pas r ductibles   un moindre nombre. On peut  tre s r alors ( $n$  ¯tant un nombre entier diff rent pour chaque valeur de  $2Np + 1$ ) qu'il y a toujours  $6n$  r sida  $p$ -i mes (mod  $2Np + 1$ ) plac s deux   deux pr s l'un de l'autre dans la s rie des nombres naturels. J'ai fait beaucoup d'efforts pour trouver les cas dans laquelles  $n = 0$ . La m thode que j'ai employ  [employ e] montre que le nombre des conditions   remplir pour que  $n$  ne soit pas z ro d pend de la valeur de  $N$  dans le nombre  $2Np + 1$  que l'on prend pour modul[e]: elle est parfaitement ind pendante de celle de  $p$  (par cons quent [dans] tout [ce] qui suit  $p$  ne repr sente plus exclusi[ve]ment les nombres premiers mais des entiers quelconques c'est ce qui est  vident par les exemples que je citerai dans la suite) en sorte que toute les fois que je calculais des valeur de  $N$  pour lesquelles  $2N + 1$  ou  $4N + 1$  ¯taient premiers je trouvais toujours moyen de remplir les conditions exig es. Cela doit  tre en effet puisqu'il y a toujours deux r sida puissance plac s de suite dans la s rie des nombres naturels et qu'except  pour 3 et pour 5 il y a toujours aussi deux r sida quarr s plac s de suite.

Lorsque  $N$  n'est pas trop grand on n'a qu'un petit nombre de conditions   essayer et si on ne trouve aucun nombre qui y satisfasse on peut  tre s r que quelque soit  $p$

on n'a jamais deux résidus  $p$ -ièmes ( $\text{mod } 2Np + 1$ ) placés de suite dans la série des nombres naturels.

La méthode donne toutes les valeurs de  $p$  pour lesquelles il y a deux résidus qui se suivent, elle donne aussi pour chaque valeur de  $p$  la totalité des cas où un résidu  $p$ -ième est suivi d'un semblable résidu. Elle donne avec un égale facilité les cas où l'intervalle qui sépare deux résidus  $p$ -ièmes est  $k$  mais si  $k$  est  $> 1$  le système des six congruences n'a plus lieu. Cette méthode n'a d'autre inconvénient que la longueur lorsque  $N$  est un peu grand. À la vérité certains artifices de calcul qui se présentent naturellement peuvent l'abréger un peu. Au reste les calculs qu'elle exige sont extrêmement simples et faciles.

Voici quelques exemples extraits d'une note déjà ancienne que je n'ai pas le tem[ps] de vérifier:

En excluant  $p = 1$  et  $p = 2$  on trouve qu'aucun nombre premier des formes  $4p + 1$ ,  $8p + 1$  ne peuvent avoir deux résidus  $p$ -ièmes dont la différence soit l'unité: que le seul nombre premier de la forme  $10p + 1$  qui ait deux résidus de suite est  $10 \cdot 3 + 1$ : Que les seuls nombres de la forme  $14p + 1$  qui aient [ayant] deux résidus de suite sont  $14 \cdot 3 + 1$  et  $14 \cdot 9 + 1$ : que le seul nombre de la forme  $16p + 1$  qui ait deux résidus de suite est  $16 \cdot 16 + 1$ : que le seul nombre de la forme  $20p + 1$  qui ait deux résidus de suite est  $20 \cdot 16 + 1$ .

Je suppose que vous avez sous les yeux le mémoire ou plutôt le projet de mémoire de Mr. Poinsot car il faut faire soi-même le travail que l'auteur s'est épargné.<sup>87</sup> Quoi qu'il en est soit son idée m'a parue fort heureuse. J'ai admiré comment étant partis de principes si différents, il m'avait fourni en quelque sorte la méthaphysique de ma méthode. En effet en faisant [faisant] usage de la remarque de cet auteur on voit comment j'ai dû arriver aux résultats que je viens d'exposer car il s'agit ici de traiter les racines de l'équation binome du degré  $2N$ , et quoique les quantités résultantes de la combinaison de ces racines (ou ce qui revient au même, et est plus conforme à la méthode que j'ai employée de la combinaison de leurs puissances) ne puisse devenir réelles que pour certaines valeurs de  $2Np + 1$  et par conséquent aussi de  $p$ , leurs rapports entr'elles [entre-elles] sont indépendants des valeurs de  $p$ .

J'ai cherché aussi à appliquer les idées de Mr. Poinsot aux nombres de la forme  $2^s p + 1$  qui donnent à résoudre une équation binome de l'ordre  $2^s$ .

J'aurais voulu établir un rapport entre les valeurs des racines de cette équation et celle de l'équation du degré  $2^{s'}$  qui donne les résidus  $p$ -ièmes puissances ( $\text{mod } 2^{s'} p + 1$ ). Si on pouvait trouver dans quels cas le nombre  $2^s p + 1$  se trouve parmi les racines de l'équation de l'ordre  $2^{s'}$  et vice-versa dans quels cas  $2^{s'} p + 1$  se trouve parmi les racines de l'équation de l'ordre  $2^s$  cela serait fort jolie et tout à fait analogue au théorème fondamental, mais je n'y suis pas.

La notation de Mr. Poinsot m'a encore fourni une nouvelle manière de prouver que 2 est résidu quarré des nombres de la forme  $8n + 1$  et non résidu quarré de ceux de la forme  $8n + 5$ : je ne sais pourquoi cette vérité se montre sous tant de faces différentes. Voici ce que c'est:  $2\sqrt{-1} = (1 + \sqrt{-1})^2$  par conséquent  $2\sqrt{-1}$  est résidu quarré: si

<sup>87</sup> She is referring to the memoir of Louis Poinsot [1777–1859], *Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres* (Poinsot 1818).

le modul[e] est  $8n + 1$ ,  $\sqrt{-1}$  est résidu quarré: si le modul est  $8n + 5$ ,  $\sqrt{-1}$  est non résidu quarré donc etc.

On voit aussi au moyen de cette notation que si 2 est résidu  $p$ -ième ( $\text{mod } 2Np + 1$ ),  $p$  étant toute fois un nombre impair, on aura trois résidus  $p$ -ièmes qui se suivront dans la série des nombres naturels. Ces trois résidus seront  $\sqrt{-1} - 1$ ,  $\sqrt{-1}$ ,  $\sqrt{-1} + 1$ . En effet si 2 est résidus  $p$ -ième  $\pm 2\sqrt{-1}$  et par conséquent aussi  $(\sqrt{-1} \pm 1)^2$  et  $\sqrt{-1} \pm 1$  seront également résidus  $p$ -ième donc etc.

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

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

Il faut avoir manié le calcul pour sentir ces choses-là. À la vérité avec ce secours je n'ai pas encore été bien loin.

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

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

votre très humble servante  
Sophie Germain

## X

Monsieur,

je profite du retour auprès de vous, de votre savant disciple, Monsieur Bader, pour vous remercier de votre bon souvenir et aussi pour vous envoyer de nouveaux exemplaires de mes mémoires.

J'ai lu avec un grand plaisir, votre mémoire sur les résidus biquarrés que ce jeune savant m'a remis de votre part.<sup>88</sup>

<sup>88</sup> She is referring to *Theoria residuorum biquadraticorum commentatio prima*, which was presented to the Göttingen Academy of Sciences in 1825 (Gauss 1828a).

Il suffirait pour entréténir en moi le goût des recherches arithmétiques, de me rappeler qu'il m'a procure l'honneur de recevoir autrefois, plusieurs lettres des vous Monsieur, croyez que je regrette vivement d'être privée depuis longtem[p]s de ces savantes communications auxquelles je n'ai jamais cessé d'attacher le plus haut prix.

En causant, avec Mr. Bader, de l'objet actuelle de mes études, je lui ai donné occasion de me parler, et par suite, de me communiquer, le savant mémoire dans lequel vous comparez la courbure des surfaces à celle de la sphère (j'aurais bien désiré pouvoir me procurer ce mémoire; je l'ai rendu à regret et par pure discréption, car je ne sais où le retrouver).<sup>89</sup>

Je ne puis vous dire, Monsieur, combien j'ai été à la fois étonnée et satisfaite en apprenant qu'un grand géomètre avait eu, presqu'en même tem[p]s que moi-même, l'idée d'une comparaison qui me semble tellement rationnelle que je ne conçois [concevais] ni comment on ne s'en est pas avisé plutôt, ni comment on a voulu faire aucune attention, ici, à ce que j'ai déjà publié à cet égard.

Indépendamment de la supériorité qui caractérise tout ce qui sort de votre savante plume, il existe une différence essentielle entre vos recherches et les miennes. Les vôtres, Monsieur, sont tout à fait géométriques: les miennes au contraire sont en quelque sorte méchaniques et n'empruntent à la géométrie que ce qui est nécessaire pour établir dans les cas où il y a lieu, l'identité des forces dont l'expression est depuis longtem[p]s l'objet presqu'exclusif de mes recherches.

Je vais essayer de vous donner un aperçu de la manière dont j'ai été conduite à comparer la courbure d'une surface à celle d'une certaine sphère: vous savez, Monsieur, qu'en nommant  $r$  et  $r'$  les deux rayons de principales courbures d'une surface *élastique*, naturellement plane, qui aurait changé de figure par l'effet d'une cause extérieure, j'ai soutenu que la force avec laquelle la surface tend à reprendre sa figure naturelle est proportionnelle à  $1/r + 1/r'$ . J'ai [seu] (car pour le dire en passant je n'ai obtenu la connaissance des objections de Mr. Poisson contre ma théorie que d'une manière détournée et plus ou moins incertaine) qu'un des commissaires, se fondant sur ce que dit Euler touchant le nombre infini des courbures différentes qui résultent des intersections des divers plans qu'on peut faire passer par le point donné de la surface, avait pensé que je n'avais pas justifié le choix des courbures principales et que je n'étais pas autorisée à dire qu'elles donnent la nature de la courbure de cette surface dans le point choisi.

En cherchant à combattre l'objection j'ai remarqué qu'en prenant la somme des raisons inverses des rayons de courbure de deux des courbes d'intersections normales, il suffisait de choisir celles qui sont contenues dans deux plans perpendiculaires entr'eux pour obtenir une quantité constante et égale à la somme des raisons inverses des deux rayons de courbures principales. J'ai encore remarqué que si les deux plans d'intersections choisis font l'angle de  $45^\circ$  avec ceux qui contiennent les lignes de courbures principales, les rayons de courbures des courbes contenues dans les plans choisis sont égaux entr'eux et au rayon d'une sphère qui couperait la surface de telle manière que deux des quadrants seraient au dessus et les deux autres au dessous de la surface. Cette sphère est celle que j'ai nommé *de moyenne courbure*.

<sup>89</sup> She is referring to *Disquisitiones generales circa superficies curvas*, which was presented to the Göttingen Academy of Sciences in 1827 (Gauss 1828b).

Je suis en état de démontrer, par des considérations qui se sont présentées à moi dans ces derniers temps et qui sont sans comparaison préférables à ce que j'ai dit à cet égard dans les mémoires que j'ai publiée, que quelque soit la figure de l'élément de la surface, c'est-à-dire, quelque soit la manière dont la courbure de l'élément est repartie autour du point de tangence, la force qui serait employée à détruire la courbure de cette élément demeurerait constante tant que le rayon de la sphère de moyenne courbure demeurerait lui-même constant.

Ces remarques trouveront leur place dans des questions que je n'avais pas en vue lorsque je me suis livrée à leur premier examen: ainsi par exemple elles pourront servir à comparer la force de l'élément d'une voûte en dôme à celle de l'élément d'une voûte en berceau et en effet on voit que la courbure moyenne peut être la même et dans une surface courbe en tous sens et dans une surface où la courbure n'existerait que dans un seul sens.

Cette dernière observation m'a donné lieu d'établir la proposition suivante qui résulterait également de vos formules, Monsieur, et qui, par cette raison, me devient plus précieuse:

“Si on compare la superficie courbe d'un cylindre à celle du quart de la sphère décrite d'un rayon double du rayon de la sphère inscrite au cylindre on trouvera que ces deux surfaces, qui ont pourtant des figures fort différentes, ont en même tem[ps] qu'une entendue égale, une *quantité* égale de courbure: leurs parties aliquotes jouissent aussi de cette double égalité”.

Je regrette d'être privée de l'avantage que je trouverais à jouir comme Monsieur Bader, de votre savante conversation: ce qu'il m'en rapporte ne m'étonne pas mais est pour moi un objet d'envie. Independamment de ce que je pourrais apprendre de vous, je regrette encore de ne pouvoir soumettre à votre jugement une foule d'idées que je n'ai pas publiée et qu'il serait trop long d'écrire.

Veuillez au moins Monsieur, me conserver une place dans votre souvenir et agreez l'assurance de mon profond respect

votre servante  
Sophie Germain

Paris ce 28 mars 1829

### Consistency and editions of the correspondence

Letters of Sophie Germain

1. Mr. Le Blanc to Gauss, Paris 21 Novembre 1804 (Stupuy 1879, pp. 298–302; Boncompagni 1880);  
*Addendum*, partially published in Del Centina (2008, pp. 373–375).
2. Mr. Le Blanc a Gauss, Paris 21 Julliet 1805 (Boncompagni 1880);  
*Addendum*, unpublished.
3. Mr. Le Blanc to Gauss, Paris 16 Novembre 1805 (Stupuy 1879, pp. 308–311; Boncompagni 1880);  
*Addendum*, unpublished.

4. Sophie Germain to Gauss, Paris 20 Fevrier 1807 (Schering 1877; Boncompagni 1880);  
*Addendum*, unpublished.
5. Sophie Germain to Gauss, Paris 27 Juin 1807 (Boncompagni 1880);  
*Addendum*, unpublished.
6. Sophie Germain to Gauss, Paris 19 Mars 1808, unpublished.
7. Sophie Germain to Gauss, Paris 22 Mai 1809, unpublished.
8. Sophie Germain to Gauss, Paris 26 Mai 1809, unpublished.
9. Sophie Germain to Gauss, Paris 12 Mai 1819 (Del Centina 2008, pp. 356–362).
10. Sophie Germain to Gauss, Paris 28 Mars 1829, partially published in English in Buccarelli and Dworsky (1980, pp. 114–115).

All letters and mathematical notes are held at the Niedersächsische Staats- und Universitätsbibliothek in Göttingen: Cod. ms. Gauss Briefe A: Germain, n. 9. Abteilung Handschriften und Selten Drucke.

### Letters of Gauss

- A. Gauss to Mr. Le Blanc, Brunswick 16 Juin 1805 (Stupuy 1879, pp. 302–306).
- B. Gauss to Mr. Le Blanc, Brunswick 20 Août 1805 (Stupuy 1879, pp. 306–307).
- C. Gauss to Sophie Germain, Brunswick 30 April 1807 (Boncompagni 1879) and (Gauss 1917, pp. 70–74).
- D. Gauss to Sophie Germain, Gottingue 19 Janvier 1808 (Stupuy 1879, pp. 318–320).

Letters A, B and D are held at the Bibliothèque National, Fonds Français n. 9118. Letter C is dispersed.

### References

- Babbage, C. 1989. Science and reform. In: *Selected works of Charles Babbage*, ed. A. Hyman: 11–34. Cambridge: Cambridge University Press.
- Babbage, C., and Herschel, J. 1813. Preface. *Memoirs of the Analytical Society* 1: 1–22.
- Barlow, P. 1811. *An elementary investigation of the theory of numbers, with its application to the indeterminate and diophantine analysis, the analytical and geometrical division of the circle and several other curious algebraical and arithmetical problems*. London: Johnson.
- Bertrand, J. 1859. Correspondance. *Comptes Rendus hebdomadaires des Séances de l'Académie des Sciences* 49: 45.
- Bertrand, J. 1877. Correspondance. *Comptes Rendus hebdomadaires des Séances de l'Académie des Sciences* 84: 1017.
- Bertrand, J. 1879. Oeuvres de Sophie Germain. *Journal des Savants* Mai: 307–314.
- Boncompagni, B. 1879. Lettera inedita di Carlo Federico Gauss a Sofia Germain pubblicata da B. Boncompagni, Calcografia e autografia Achille Paris, Firenze. Printed version in: *Archiv der Mathematik und Physik* 63 (1880), Litterarischer Bericht 259: 27–31.
- Boncompagni, B. 1879–1880. Presentazione di opere. *Atti dell'Accademia Pontificia de' Nuovi Lincei* 33: 427.
- Boncompagni, B. 1880. Cinq lettres de Sophie Germain à Charles Frédéric Gauss publiées par B. Boncompagni d'après les originaux possédés par la Société Royale des Sciences de Göttingen, Berlin, Institut de photolithographie des frères Burchard, imprimerie de Gustave Schade. Printed version in: *Archiv der Mathematik und Physik* 65, Litterarischer Bericht 257: 5–9 and *Archiv der Mathematik und Physik* 66, Litterarischer Bericht 256: 4–10.

- Boncompagni, B. 1883. Lettre de Charles-Frédéric Gauss au Dr Henri-Guillaume-Mathias Olbers en date de Braunschweig den 3 September 1805, publiée par B. Boncompagni d'après l'original possédé par la Société Royale des Sciences de Göttingen, Berlin, Institut de photolithographie des frères Burchard, imprimerie de Gustave Schade (the letter and its Italian translation by A. Sparagna, were printed in *Bullettino di Bibliografia e Storia delle Scienze Matematiche e Fisiche* 16: 215–220).
- Boncompagni, B. 1884. Intorno ad una lettera di Carlo Federico Gauss al Dr. Enrico Guglielmo Mattia Olbers. *Atti dell'Accademia Pontificia de' Nuovi Lincei* 36: 201–295.
- Boncompagni, B. 1895. *Catalogo della insigne biblioteca appartenuta alla chiara memoria del Principe Baldassarre Boncompagni, Parte I.* Roma, Cecchini.
- Bucciarelli, L.L., and Dworsky, N. 1980. *Sophie Germain: An essay in the history of the theory of elasticity.* Studies in the History of Modern Science, 6. Dordrecht: Reidel.
- Cauchy, A. 1815. Mémoire sur les fonctions qui ne peuvent obtenir que deux valeurs égales et de signes contraires par suite des transpositions opérées entre les variables qu'elles renferment. *Jour. École polytechnique* 10. Also in: *Oeuvres complètes* (2) 1: 91–169.
- Cauchy, A. 1829. *Exercices de mathématique* 4: 253–299. Also in: *Oeuvres complètes* (2) 9: 298–341.
- Chasles, M. 1879. *Comptes Rendus hebdomadiers des Séances de l'Académie des Sciences* 89: 800.
- Collison, M.J. 1977. The origins of the cubic and biquadratic reciprocity laws. *The Archive for History of Exact Sciences* 17: 63–69.
- Comte, A. 1864. *Cours de philosophie positive.* Paris: Bachelier.
- Dahan-Dalmédico, A. 1987. Mécanique et théorie des surfaces: les travaux de Sophie Germain. *Historia Mathematica* 14: 347–365.
- De Jonquières, E. 1896. Sur une lettre de Gauss du moi de Juin 1805. *Comptes Rendus hebdomadiers des Séances de l'Académie des Sciences* 122: 829.
- Del Centina, A. 2005. Letters of Sophie Germain preserved in Florence. *Historia Mathematica* 32: 60–75.
- Del Centina, A. 2008. Unpublished manuscripts of Sophie Germain and a revaluation of her work on Fermat's last theorem. *The Archive for History of Exact Sciences* 62: 349–392.
- Del Centina, A., and Fiocca, A. 2004. *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.* Firenze: Olschki.
- Del Centina, A., and Fiocca, A. 2010. *Guglielmo Libri matematico e storico della matematica.* Firenze: Olschki.
- Dickson, L.E. 1971. *History of the theory of numbers*, 3 vols. New York: Chelsea.
- Dunnington, G.W. 1955. *Gauss, titan of science.* New York: Hafner. Reprinted by The Mathematical Association of America in 2004.
- Edwards, H.M. 1977. *Fermat's last theorem: A genetic introduction to algebraic number theory.* New York: Springer.
- Eisenstein, G. 1844a. Beweis des Reciprocitätsatzes für die cubischen Reste in der Theorie der aus dreitzen Wurzeln der Einheit zusammengesetzten complexen Zahlen. *Journal für die reine und angewandte Mathematik* 27: 289–310.
- Eisenstein, G. 1844b. Lois de réciprocité. *Journal für die reine und angewandte Mathematik* 28: 53–67.
- Folkerts, M. 2003. The fate of the manuscripts in the Boncompagni collection. In *Il Sogno di Galois. Scritti sulla storia della matematica dedicati a Laura Toti Rigatelli per il suo 60mo compleanno*, 229–267. Siena: Centro Studi della Matematica Medievale.
- Gandhi, J.M. 1966. A note on Fermat's last theorem. *The American Mathematical Monthly* 73: 1106–1107.
- Gauss, C.F. 1799. Demonstratio nova theorematis omnem functionem algebraicam rationalem integrum unius variabilis in factores reales primi vel secundi gradus resolvi posse. Also in: *Werke*, dritter Band, herausgegeben von der Königlichen Gesellschaft 1866: 1–56.
- Gauss, C.F. 1801. *Disquisitiones Arithmeticae, Lipsia apud Gerh. Fleischer.* Also in: *Werke*, erster Band, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen 1863: 1–474.
- Gauss, C.F. 1808. Theorematis arithmeticici demonstratio nova. *Commentationes S.R. Scientiarum Gottingensis* 16. Also in: *Werke*, zweiter Band, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen 1863: 1–8.
- Gauss, C.F. 1809. *Theoria motus corporum caelestium in sectionibus conicis solem ambientium.* Hamburgi: Perthes et I.H. Besser. Also in: *Werke*, siebenter Band, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen 1906: 1–280.

- Gauss, C.F. 1811. Summatio quarumdam serierum singularium. *Commentationes S.R. Scientiarum Gottingensis recentiores* 1. Also in: *Werke*, zweiter Band, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen 1876: 9–45.
- Gauss, C.F. 1813. Theoria attractionis corporum sphaeroidorum ellipticorum homogeneorum methodo nova tractata. *Commentationes S.R. Scientiarum Gottingensis recentiores* 2. Also in: *Werke*, fünfter Band, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen 1867: 1–22.
- Gauss, C.F. 1818. Theorematis fundamentalis in doctrina de residuis quadratrici demonstrationes et ampliations novae. *Commentationes S.R. Scientiarum Gottingensis recentiores* 4. Also in: *Werke*, zweiter Band, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen 1863: 47–64.
- Gauss, C.F. 1828a. Theoria residuum biquadraticorum commentatio prima, *Commentationes S.R. Scientiarum Gottingensis recentiores*, IV. Also in: *Werke*, zweiter Band, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen 1863, pp. 65–92.
- Gauss, C.F. 1828b. Disquisitiones generales circa superficies curvas. *Commentationes S.R. Scientiarum Gottingensis recentiores* 6. Also in: *Werke*, vierter Band, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen 1873: 217–258.
- Gauss, C.F. 1832. Theoria residuum biquadraticorum commentatio secunda. *Commentationes S.R. Scientiarum Gottingensis recentiores* 7. Also in: *Werke*, zweiter Band, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen 1863: 93–148.
- Gauss, C.F. 1863a. *Werke*, erster Band, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen.
- Gauss, C.F. 1863b. *Werke*, zweiter Band, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen.
- Gauss, C.F. 1900. *Werke*, achter Band, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen.
- Gauss, C.F. 1917. *Werke*, zehnten Bandes, Erste Abteilung, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen.
- Genocchi, A. 1852. Note sur la théorie des résidus quadratiques. *Mémoires couronnés et mémoires des savants étrangers publ. par l'Académie royale des sciences, des lettres et des beaux-arts de Belgique* 25: 1–54.
- Genocchi, A. 1880. Il carteggio di Sofia Germain e Carlo Federico Gauss. *Atti della Accademia delle Scienze di Torino* 15: 795–808.
- Genocchi, A. 1884a. Alcune asserzioni di C.F. Gauss circa le forme quadratiche  $YY \pm nZZ$ . *Bullettino di Bibliografia e di Storia delle Scienze Matematiche e Fisiche* 17: 245–247.
- Genocchi, A. 1884b. Teoremi di Sofia Germain intorno ai residui biquadratici. *Bullettino di Bibliografia e di Storia delle Scienze Matematiche e Fisiche* 17: 248–251.
- Genocchi, A. 1885. Ancora un cenno sui residui cubici e biquadratici. *Bullettino di Bibliografia e di Storia delle Scienze Matematiche e Fisiche* 18: 231–234.
- Genocchi, A., and Realis, S. 1884. Intorno ad una proposizione inesatta di Sofia Germain. *Bullettino di Bibliografia e di Storia delle Scienze Matematiche e Fisiche* 17: 315–316.
- Germain, S. 1821. *Recherches sur la théorie des surfaces élastiques*. Paris: Courcier.
- Germain, S. 1826. *Remarques sur la nature, les bornes et l'étendue de la question des surfaces élastiques*. Paris: Huzard et Courcier.
- Germain, S. 1828. Examen des principes qui peuvent conduire à la connaissance des lois de l'équilibre et du mouvement des solides élastiques. *Annales de Chimie* 38: 123–131.
- Germain, S. 1831a. Mémoire sur la courbure des surfaces. *Journal für die reine und angewandte Mathematik* 7: 1–29.
- Germain, S. 1831b. Note sur la manière dont se composent les valeurs de  $y$  et  $z$  dans l'équation  $\frac{4(x^p-1)}{x-1} = y^2 \pm z^2$ , et celles de  $Y'$  et de  $Z'$  dans l'équation  $\frac{4(x^p-1)}{x-1} = Y'^2 \pm Z'^2$ . *Journal für die reine und angewandte Mathematik* 7: 201–204.
- Germain, S. 1833. *Considérations générales sur l'état des sciences et des letters*, éd. M. Lherbette. Paris: Lachevardière.
- Germain, S. 1880. Mémoire sur l'emploi de l'épaisseur dans la théorie des surfaces élastiques. *Journal de Mathématiques Pures et Appliquées* (3) 6: Appendice.
- Goldstein C., Schappacher N., Schwermer J. (eds.) 2007. *The Shaping of Arithmetic after C.F. Gauss's *Disquisitiones Arithmeticae**. New York, Springer.
- Günther, S. 1881. Die Briefwechsel zwischen Gauss und Sophie Germain. *Historisch-literarische Abteilung der Zeitschrift für Mathematik und Physik* 26: 19–25.

- Günther, S. 1882. Il carteggio tra Gauss e Sofia Germain (Italian translation by Alfonso Sparagna). *Bullettino di Bibliografia e di Storia delle Scienze Matematiche e Fisiche* 15: 174–179.
- Henry, C. 1879. Les manuscrits de Sophie Germain et leur récent éditeur, Documents nouveaux. *Revised Philosophy* 8: 619–641.
- Henry, C. 1880. Bulletin des Sciences Mathématiques et Astronomiques. *Comptes Rendus et Analyses* (2) 4: 273–276 [Review of the five letters by Sophie Germain to Gauss edited by Boncompagni].
- Jacobi, C.G.J. 1827. De residuis cubicis commentatio numerosa. *Journal für die Reine und Angewandte Mathematik* 2: 66–69.
- Jacobi, C.G.J. 1841. De determinantibus functionalibus. *Journal für die reine und angewandte Mathematik* 22: 319–360.
- Jacobi, C.G.J. 1846. Über die Kreistreilung und ihre Anwendung auf die Zahlentheorie. *Journal für die reine und angewandte Mathematik* 30: 166–184.
- Klein, F. 1826. *Vorlesungen über die entwicklung der Mathematik im 19.jahrhundert*, Band I, Berlin.
- Lacroix, S.F. 1804. *Complément des Éléments d'algèbre à l'usage de l'École Centrale des Quatre-Nations*, 3-eme édition revue et augmentée. Paris: Courcier.
- Lagrange, J.-L. 1808. *Traité de la résolution des équations numériques de tous les degrés, nouvelle édition revue et augmentée par l'auteur*. Paris: Courcier.
- Lagrange, J.-L. 1867–1892. *Oeuvres*, 14 vols. Paris: Gauthier–Villars.
- Laubenbacher, R., and Pengelley, D., 2010. Voici ce que j'ai trouvé: Sophie Germain's grand plan to prove Fermat's Last Theorem. *Historia Mathematica* 37: 641–692.
- Legendre, A.-M. 1785. Recherches d'analyse indéterminée, Histoire de l'Académie Royal des Sciences année MDCCLXXXV, avec les Mémoire de Mathématiques et de Physique pour la même année (1788): 465–559.
- Legendre, A.-M. 1798. *Essai sur la théorie des nombres*. Paris: Duprat.
- Legendre, A.-M. 1806. *Nouvelles méthodes pour la détermination des orbites des comètes*. Paris: Courcier.
- Legendre, A.-M. 1808. *Essai sur la théorie des nombres*, 2-ème édition. Paris: Courcier.
- Legendre, A.-M. 1827. Recherches sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat. *Mémoires Ac. des Sc. de l'Ins. de France* (2) 6: 1–60.
- Lejeune-Dirichlet, M.G. 1828. Recherches sur les diviseurs premiers d'une classe de formules du quatrième degré. *Journal für die reine und angewandte Mathematik* 3: 35–69.
- Lemmermeyer, F. 2000. *Reciprocity law, from Euler to Eisenstein*. New York: Springer.
- Libri, G. 1832. Notice sur M.Ile Sophie Germain. *Journal des Débats* 18 mai 1832. Also in: *Considérations générales sur l'état des sciences et des lettres*, éd. M. Lherbette. Paris: Lachevardière.
- Libri, G. 1829. *Mémoires de Mathématique et de Physique*. Firenze: Ciardetti.
- Maccioni Ruju, A., and Monstert, M. 1995. *The life and time of Guglielmo Libri (1802–1869): Scientist, patriot, scholar, journalist and thief: A nineteenth-century story*. Hilversum: Verloren.
- MacKinnon, N. 1990. Sophie Germain, or, was Gauss a Feminist? *The Mathematical Gazette* 74: 346–351.
- Mansion, P. 1880a. *Nouvelle Correspondance Mathématique* 6: 217–219 [Review of Gauss's letter to Sophie Germain edited by Boncompagni].
- Mansion, P. 1880b. *Nouvelle Correspondance Mathématique* 6: 315–317 [Review of the five letters by Sophie Germain to Gauss edited by Boncompagni].
- Mansion, P. 1880c. Sur les lettres de Sophie Germain à Gauss publiées par B. Boncompagni. *Nouvelle Correspondance Mathématique* 6: 407–408.
- Peters, C.A.F., Ed. 1860. *Briefwechsel zwischen C.F. Gauss und H.C. Schumacher*, erster Band. Altona, Esch.
- Plackett, R.L. 1972. The discovery of the method of least squares. *Biometrika* 59: 239–251.
- Poincaré, L. 1818. Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres. *Mémoires Ac. des Sc. de l'Institut de France* 14 (1813–1815): 381–392.
- Poincaré, L. 1820. Mémoire sur l'application de l'algèbre à la théorie des nombres. *Jour. Éc. polytechnique* 11: 342–410. Also in: *Mémoires Ac. des Sc. de l'Institut de France* (2) 4 (1824): 99–184.
- Raina, B.L. 1969. On Fermat's last theorem. *American Mathematical Monthly* 76: 49–51.
- Ribenboim, P. 1999. *Fermat's last theorem for amateurs*. New York: Springer.
- Sampson, J.H. 1990. Sophie Germain and the theory of numbers. *The Archive for History of Exact Sciences* 41: 157–161.
- Schering, E. 1877. Carl Friedrich Gauss' Geburtstag nach Hundertjähriger Wiederkehr Festrede, Abhandlungen der Mathematischen Classe der K. Gesellschaft der Wissenschaften in Göttingen, Band 22. Italian translation in: *Annali di Matematica pura e Applicata* 9: 210–239.

- Schering, E. 1879. Bemerkungen über Gauss' Brief vom 30 April 1807 an Sophie Germain, Nachrichten von der K. Gesellschaft der Wissenschaften und der G.A. Universität zu Göttingen: 381–384.
- Schering, E. 1880. Briefe der Sophie Germain an Gauss in Photographie veröffentlicht von B. Boncompagni, Nachrichten von der K. Gesellschaft der Wissenschaften und der G. A. Universität zu Göttingen: 367–369.
- Schilling, C., Ed. 1900. *Wilhelm Olbers sein Leben und seine Werke*, zweiter Band, Briefwechsel zwischen Olbers und Gauss erste Abtheilung. Berlin: Julius Springer.
- Schmidt, F., and Stäckel, P. 1899. *Briefwechsel zwischen Carl Friedrich Gauss und Wolfgang Bolyai*. Leipzig: Teubner.
- Sierpiński, W. 1964. *Elementary theory of numbers*. Warszawa: Pergamon Press.
- Smith, H.J.S. 1965. Report on the theory of numbers. In *The collected mathematical papers by Henry John Stephen Smith*, 38–366. New York: Chelsea.
- Stupuy, H. 1879. *Oeuvres Philosophiques de Sophie Germain*. Paris: Ritti.
- Stupuy, H. 1896. *Oeuvres Philosophiques de Sophie Germain*, Nouv. ed. Paris: Ritti.
- Truesdell, C. 1991. Sophie Germain: Fame earned by a stubborn error. *Bollettino di Storia delle Scienze Matematiche* 11(2): 3–24.
- Waterhouse, W.C. 1994. A counterexample for Germain. *The American Mathematical Monthly* 101: 140–150.