Exercise 4.22: Show that if a and b are relatively prime numbers and ab is a square, then both a and b are squares. Hint: Use the Fundamental Theorem of Arithmetic, which says that any positive integer can be factored into a product of prime numbers, and the prime factors are unique up to their order in the product.

Exercise 4.23: Read about Christian Goldbach and discuss his influence on Euler's number-theoretic work.

Exercise 4.24: Lagrange wrote an appendix to Euler's *Elements of Algebra*. Look up the appendix in Euler's *Opera Omnia* and discuss its contents.

Exercise 4.25: Use [47] to complete the details of Euler's proof for exponent three.

4.4 Germain's General Approach

Sophie Germain was the first mathematician to make progress with a general approach toward proving Fermat's Last Theorem. Born in Paris into a family of the French middle class, she was able to overcome the obstacles to her education from society, and the disapproval of her parents, by using her father's extensive library, sometimes even clandestinely, to educate herself at home.

Higher education in mathematics was virtually nonexistent in France until the founding of the Ecole Polytechnique in 1795 as part of educational reforms after the Revolution, with its primary mission the education of military engineers and civil servants. It was more ambitious than the institutions that preceded it, eventually setting the standard for technical education throughout the Western world and making Paris the world center of mathematical research. The United States Military Academy at West Point, for instance, is modeled after it. The Ecole Polytechnique was a model for the modern university, in classroom instruction and examination, and in having active researchers as instructors. Teachers developed textbooks out of course lectures; such texts are the immediate ancestors of our modern college textbooks. Unfortunately, Germain could not avail herself of this splendid new institution, which barred women from attending, but she did obtain lecture notes. Using the name of an acquaintance registered as a student at the Ecole Polytechnique, Antoine-August Le Blanc, Germain submitted a report on analysis to Lagrange. Lagrange was impressed with the originality and insight of "M. Le Blanc," and wished to meet him. Discovering the true identity of the report's author did not diminish Lagrange's opinion of the work; he provided Germain with support and encouragement for many years.

PHOTO 4.11. Germain.

Germain continued her studies in mathematics, and began to make original contributions to research. She is best known for her work on the theory of elasticity, in particular the theory of vibrating surfaces, for which she was awarded a prize of the Academy of Sciences in 1816. An excellent account of Sophie Germain's life and work is [23]. Shorter accounts can be found in [35, 42, 79].

Despite her accomplishments in elasticity theory, her major work was in number theory. In fact, it was number theory that was her true love, which occupied her throughout her life. Early on, she began studying Legendre's *Theory of Numbers*, published in 1789, and wrote to him about it, thereby initiating an extensive correspondence. Germain's interest in number theory coincided with the 1801 publication of Gauss's *Disquisitiones Arithmeticae*, the groundbreaking work that propelled number theory into the very center of nineteenth-century mathematics. After carefully studying the *Disquisitiones*, Germain initiated a correspondence with Gauss, again using the name Le Blanc, praising the *Arithmeticae* and enclosing some of her own results for his evaluation. Gauss was impressed with her efforts, going so far as to mention Monsieur LeBlanc very favorably to other scientists.

When, in 1807, Germain revealed her true identity to Gauss, he responded:

> But how can I describe my astonishment and admiration on seeing my esteemed correspondent Monsieur LeBlanc metamorphosed into this celebrated person, yielding a copy so brilliant it is hard to believe? The taste for the abstract sciences in general and, above all, for the mysteries of numbers, is very rare: this is not surprising, since the charms of this sublime science in all their beauty reveal themselves only to those who have the courage to fathom them. But when a woman, because of her sex, our customs and prejudices, encounters infinitely more obstacles than men, in familiarizing herself with their knotty problems, yet overcomes these fetters and penetrates that which is most hidden, she doubtless has the most noble courage, extraordinary talent, and superior genius. Nothing could prove to me in a more flattering and less equivocal way that the attractions of that science, which have added so much joy to my life, are not chimerical, than the favor with which you have honored it.
>
> The scientific notes with which your letters are so richly filled have given me a thousand pleasures. I have studied them with attention and I admire the ease with which you penetrate all branches of arithmetic, and the wisdom with which you generalize and perfect [23, p. 25].

Germain outlined her strategy for a general proof of FLT in a long letter to Gauss, written on May 12, 1819, after a ten-year hiatus in their correspondence. Before delving into an explanation of her work she expresses her long-term devotion to the study of number theory:

> Although I have worked for some time on the theory of vibrating surfaces... I have never ceased thinking about the theory of numbers. I will give you a sense of my absorption with this area of research by admitting to you that even without any hope of success, I still prefer it to other work which might interest me while I think about it, and is sure to yield results.
>
> Long before our Academy proposed a prize for a proof of the impossibility of the Fermat equation, this type of challenge, which was brought to modern theories by a geometer who was deprived of the resources we possess today, tormented me often. I have a vague inkling of a connection between the theory of residues and the famous equation; I believe I spoke to you of this idea a long time ago, because it struck me as soon as I read your book.
>
> Here is what I have found [69]:

She then goes on to make a simple but very important observation that is central to her method. Let p be an odd prime.

Basic Lemma:

PHOTO 4.12. Germain's 1819 letter to Gauss.

> If the Fermat equation for exponent p has a solution, and if θ is a prime number with no nonzero consecutive pth power residues modulo θ, then θ necessarily divides one of the numbers x, y, or z.

To see why this is true, first note that what is meant by a pth power residue modulo θ is simply the remainder, modulo θ, of a pth power. (See the Appendix for a brief introduction to congruence arithmetic.) So now suppose the Fermat equation $x^p + y^p = z^p$ has a solution, and suppose that none of x, y, or z is divisible by θ. Thus, modulo θ, we can divide by any of x, y, z (see Proposition 4 of the Appendix). Letting a be a multiplicative inverse for x modulo θ we obtain the congruence

$$(ax)^p + (ay)^p \equiv (az)^p \pmod{\theta},$$

and thus $1 + (ay)^p \equiv (az)^p$. Thus the residues of $(ay)^p$ and $(az)^p$ will be consecutive. Notice that they are also nonzero, since θ does not divide a, y, or z. This contradicts the assumption on θ, proving the assertion.

Germain then concludes that if for a fixed p one could find infinitely many primes θ satisfying the condition that θ has no nonzero consecutive pth power residues modulo θ, then, by the previous observation, each of these would have to divide one of x, y, z, and thus one of these three numbers would be divisible by infinitely many primes, which is absurd. This would prove FLT for that exponent.

Despite much effort, she never succeeded in proving FLT by this approach for even a single exponent. However, she invented a method for producing many primes θ satisfying the above condition. For any particular exponent, her method may then show that any solutions to the Fermat equation would have to be quite large. She made many such applications of her method in her manuscripts [70]. For instance, for $p = 5$, she showed that any solutions

to the Fermat equation would have to be at least 30 decimal digits in size! As she says in her letter to Gauss, "You can easily imagine, Monsieur, that I must have been able to prove that this equation is only possible for numbers whose size frightens the imagination. . . . But all this is still nothing; it requires the infinite and not just the very large."

Sophie Germain never published her work on FLT. One might speculate that her experience with the establishment at the Paris Academy of Sciences played an important role in this decision. During her time, it was common to publish papers as memoirs of the Academy. After several disputes relating to the publication of her prize-winning work on elasticity theory, she ended up publishing that work at her own expense. A renewed battle over the publication of her number-theoretic work might have been too unpleasant for her to contemplate. It should be noted that a few years before her death she did publish a short paper on number theory in the recently founded *Journal für die reine und angewandte Mathematik*, a private German scientific journal.

The only commonly known result of Germain's appeared in 1825, as part of a supplement to the second edition of Legendre's *Theory of Numbers*. The supplement also appeared as a *Memoir* of the Royal Academy of Sciences of the Institut de France in 1827 [107]. In this supplement, Legendre presents his own proof (the first) for the $p = 5$ case of FLT, along with part of Germain's work, explicitly credited to her in a footnote. The reference in this footnote is commonly considered to be her only contribution to FLT and is known as "Sophie Germain's Theorem." In fact, her work is considerably more extensive than this result [102].

In order to state her theorem, first observe that it is enough to consider Fermat's equation for odd prime exponents (see Exercise 4.10 of the Introduction). Recall from the Introduction that we may furthermore assume that x, y, and z are relatively prime. Germain's theorem addresses the existence of solutions in which none of the three numbers x, y, z is divisible by the prime exponent p. Today this is called Case I of FLT. We state her result in modern terminology.

Sophie Germain's Theorem: *If p is an odd prime, and if there exists an auxiliary prime θ with the properties that*

1. *p is not a pth power modulo θ, and*
2. *the equation $r' \equiv r + 1$ modulo θ cannot be satisfied for any two pth power residues,*

then Case I of Fermat's Last Theorem is true for p.

Note that Condition 2 is identical to the condition she mentions in her letter to Gauss, that there should not exist any nonzero consecutive pth power residues modulo θ.

Germain also developed methods to verify the hypotheses of her theorem and applied them to do so for all primes less than 100.

PHOTO 4.13. Germain's manuscript.

Her result is implicit in a theorem from a handwritten manuscript in the *Manuscrits de Sophie Germain*, MS. FR 9114, in the Bibliothèque Nationale in Paris, beginning on page 92.

Germain, from a manuscript entitled

Demonstration of the impossibility to satisfy in integers the equation $z^{2(8n\pm3)} = y^{2(8n\pm3)} + x^{2(8n\pm3)}$

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

To prove this theorem it suffices to suppose that there exists at least one prime number θ of the form $2Np+1$ for which at the same time one cannot find two pth power residues whose difference is one, and p is not a pth power residue. Not only does there always exist a number θ satisfying these two conditions, but the course of calculation indicates that there must be an infinite number of them. For example, if $p = 5$, then $\theta = 2 \cdot 5 + 1 = 11$, $2 \cdot 4 \cdot 5 + 1 = 41$, $2 \cdot 7 \cdot 5 + 1 = 71$, $2 \cdot 10 \cdot 5 + 1 = 101$, etc.

Let therefore $z = lr,\ x = hn,\ y = \nu m$. If one assumes that p is [relatively] prime to $z,\ x$, and y, then one will have that

$$\begin{aligned} x + y = l^p \qquad & x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + \text{ etc} \quad = r^p, \\ z - y = h^p \qquad & z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 + \text{ etc} \quad = n^p, \\ z - x = \nu^p \qquad & z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 + \text{ etc} \quad = m^p. \end{aligned}$$

Since we have assumed that there are no two pth power residues modulo θ whose difference is one, it follows that in the equation $z^p = x^p + y^p$ one of the numbers $x,\ y,\ z$ is necessarily a multiple of θ. To make a choice, let us take $z \equiv 0 \pmod{\theta}$. Thus one has $l^p + h^p + \nu^p \equiv 0 \pmod{\theta}$. It is therefore necessary, again, that one of the numbers $l,\ h,\ \nu$ be a multiple of θ; because $z = lr \equiv 0$ it can only be l. And as a result $x \equiv -\nu^p$, $y \equiv -h^p$, $x + y \equiv 0 \pmod{\theta}$. Consequently $px^{p-1} \equiv p\nu^{p(p-1)} \equiv r^p$. That is to say, p is a pth power residue, contrary to the hypothesis.

The first sentence after the statement of the theorem must actually be considered a hypothesis. While Germain believed that an auxiliary prime θ satisfying the assumed conditions exists for any prime number p, she never succeeded in showing this. Also, she assumes that x, y, and z are relatively prime, since any solution of the Fermat equation in which x, y, and z are not relatively prime can be used to find a solution x', y', z' such that x', y', and z' are relatively prime.

Germain's reasoning is very terse and requires substantial work on the part of the reader. In order to follow her argument in the second paragraph, let us first derive the displayed equations, which are to follow from her additional assumption that p does not divide x, y, or z. From this assumption, she will derive a contradiction; i.e., she will show that it is impossible for p not to divide one of $x,\ y$, or z. We note that in the portion of the manuscript quoted above, Germain shows only that one of $x,\ y$, or z must be divisible by p rather than p^2 as in the statement of the theorem. Begin by factoring:

$$x^p + y^p = (x + y)\varphi(x, y),$$

where

$$\varphi(x, y) = x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + \cdots + y^{p-1}.$$

Observe that this factorization holds because p is odd. We next show that $x + y$ and $\varphi(x, y)$ are relatively prime. If not, let q be a prime dividing

both. Then $y = -x +$ some multiple of q, and substitution yields $\varphi(x, y) = px^{p-1} +$ a multiple of q. From this we see that either p or x must be divisible by q. If p is divisible by q, then it equals q, since both are prime. Thus $p = q$ divides $x + y$, hence also z. But this contradicts Germain's assumption that p is prime to x, y, and z. If, on the other hand, x were divisible by q, then x and $x + y$ would both have q as common factor, contradicting the assumption that x and y are relatively prime.

Now, since the product of the relatively prime numbers $x + y$ and $\varphi(x, y)$ is the pth power z^p, it must be that each of them is itself a pth power (see Appendix). Thus, we may write them as l^p and r^p respectively, as shown in the displayed equations. Multiplying these two together yields $z^p = (x + y)\varphi(x, y) = l^p r^p = (lr)^p$, and so $z = lr$, as Germain claims at the beginning of her argument. The other equations follow similarly from $z^p - y^p = x^p$ and $z^p - x^p = y^p$.

Her next assertion, that one of x, y, z is a multiple of θ, follows from the Basic Lemma. The argument continues by assuming that it is z. The reader may check that if in fact it were x or y, everything that follows could be carried out in a similar manner. Adding the left displayed equations, we obtain

$$l^p + h^p + \nu^p = 2z \equiv 0 \pmod{\theta}.$$

Imitating the proof of the Basic Lemma, the hypothesis on θ insures that one of l, h, or ν is a multiple of θ. Her next assertion implicitly assumes that we are dealing only with primitive solutions to the Fermat equation, that is, x, y, and z are relatively prime. If either h or ν were divisible by θ, then y or x would have the factor θ in common with z, violating primitivity.

From the congruence $x + y = l^p \equiv 0 \pmod{\theta}$ she obtains, by substituting $y \equiv -x$ in the top right equation, that

$$r^p \equiv px^{p-1} \equiv p(-\nu^p)^{p-1} = p\nu^{p(p-1)}.$$

Since ν is not divisible by θ we may divide by $\nu^{p(p-1)}$ (see Appendix), obtaining

$$p \equiv \left(\frac{r}{\nu^{p-1}}\right)^p.$$

As Germain observes, this contradicts one of the hypotheses of the theorem.

Notice again that at this point Germain has only proven that one of the numbers x, y, z is divisible by p rather than p^2. It is this weaker version of the theorem that is called Sophie Germain's Theorem in the literature [47, p. 64]. Moreover, this result is responsible for the division of possible solutions into two types: Case I solutions are those where x, y, z are all prime to the exponent p, whereas Case II solutions are those where p divides one of x, y, z. Thus, Germain's Theorem proves the nonexistence of Case I solutions whenever an auxiliary prime θ can be found satisfying the required conditions, and she succeeded in doing this up to exponent 97.

Much of Germain's other work on Fermat's Last Theorem was directed toward developing methods for finding such auxiliary primes θ. For instance, she developed a method for proving that for any odd prime p, if $\theta = 2Np + 1$ is also prime and N is not a multiple of 3, then it satisfies the condition that there are no consecutive pth power residues modulo θ. She made a detailed study for $N \leq 10$, however without verifying that her method worked in general [70, pp. 198 ff.],[102].

An extension of her method was used as late as 1985 to prove that Case I holds for infinitely many prime exponents [2], testifying to the importance and depth of her ideas. Germain's ideas have not lost their relevance after almost two hundred years.

Exercise 4.26: Read about Germain's work on elasticity theory and why she became interested in it.

Exercise 4.27: Read about the work of other female mathematicians before and after Germain.

Exercise 4.28: Find all quadratic residues modulo 3. Find all 7th power residues modulo 29.

Exercise 4.29: Use Germain's Theorem to show that there are no Case I solutions to the Fermat equation for exponent 3 by showing that 3 is not a cube modulo 7, and that no two nonzero third power residues differ by 1.

Exercise 4.30: Use Germain's Theorem to show that there are no Case I solutions to the Fermat equation for exponent 7.

Exercise 4.31: Can a prime θ of the form $2Np + 1$ satisfy Germain's nonconsecutivity condition if N is a multiple of 3?

Exercise 4.32: Verify the hypothesis of Germain's Theorem for the first prime larger than 100.

4.5 Kummer and the Dawn of Algebraic Number Theory

Germain's general approach notwithstanding, progress on the problem continued only very slowly, with proofs for specific exponents. Credit for exponent 5 was shared between Legendre and Dirichlet. By the time Dirichlet succeeded in producing a proof for exponent 14 in 1832, and the French mathematician Gabriel Lamé for exponent 7 in 1839, it had become clear that their methods seemed unlikely to lead further. A whole new approach was needed, based on different principles.