Sophie Germain and Special Cases of Fermat's Last Theorem

Colleen Alkalay-Houlihan

1 Sophie Germain

1.1 A Passion for Mathematics

Marie-Sophie Germain was a self-taught mathematician with an exceptional desire to learn mathematics. Born April 1, 1776 in Paris, France, revolution surrounded Germain's childhood. She came from a relatively prosperous family; her father was a silk merchant and was elected a member of the Constituent Assembly in 1789, when Germain was 13 years old. Escaping the chaos of revolution, Germain retreated into her father's library, where she discovered mathematics.

The first books to enrapture her were Etienne Bézout's standard mathematical textbooks and Jean-Etienne Montucla's "Histoire des mathématiques."[2] Here she read the legend telling of how Archimedes, circa 212 B.C., was examining a geometric figure in the sand with such concentration that he did not respond to an enemy soldier's questions, and was speared to death. Germain began to realize that mathematics must be a fascinating subject, to inspire such absolute focus in a person, and henceforth she dedicated her time to studying math from the books in her father's study.

In this time, however, women were not known to study mathematics; some aristocratic women were expected to have a basic understanding, but just enough to sustain a social conversation.[5] Germain, on the other hand, studied late into the night, absorbed in her attempts to understand, unguided, Bézout's texts. As her friend Guglielmo Libri recounted in her obituary, Germain's parents disapproved of her mathematical obsession. For this reason, they put out the fire in her room at night, and also took away her candles and clothing after nightfall, so that she would be unable to study. Even this did not deter her. She would study "at night in a room so cold that the ink often froze in its well, working enveloped with covers by the light of a lamp."[2]

In 1794, when Germain was 22, the Ecole Polytechnique was founded in Paris, with the purpose of training exceptional young mathematicians and scientists. It was open only to male students, and so Germain was unable to attend classes, given by mathematicians such as Joseph-Louis Lagrange. However, she was able to obtain weekly lecture notes by using the alias "Antoine-August Le Blanc," and she completed and submitted assignments under this same name. Her answers to these problem sets were "ingenious," and she also submitted written "observations" that so impressed Lagrange that he expressed an interest in meeting his student. Germain was forced to reveal her true identity, and Lagrange became her friend and mathematical mentor. Amazingly, she had taught her self mathematics all the way to the undergraduate level, and despite this weak background, her work was impressive enough to merit the praise of one of the foremost mathematicians of her time.[5, 3]

1.2 Sophie Germain's Interest in Number Theory

Germain became interested in number theory after reading Adrien-Marie Legendre's *Essai sur la théorie des nombres* (1789) and Carl Friedrich Gauss's *Disquisitiones Arithmeticae* (1801).[1] She

began work on Fermat's Last Theorem, which I will discuss in this text. She worked on original research for several years, until she had accomplished and understood a great deal, and she decided she needed to discuss her work with a number theorist. Boldly, she wrote directly to Gauss, again using her pseudonym, sharing her new, more general approach to proving Fermat's Last Theorem. Gauss was impressed by her progress, and he began to correspond with her.[5, 1]

Upon learning that his correspondent was not, in fact, M. Le Blanc, but rather Sophie Germain, a woman, Gauss responded,

> "But how to describe to you my admiration and astonishment at seeing my esteemed correspondent Monsieur Le Blanc metamorphose himself into this illustrious personage who gives such a brilliant example of what I would find it difficult to believe. A taste for the abstract sciences in general and above all the mysteries of numbers is excessively rare: one is not astonished at it: the enchanting charms of this sublime science reveal only to those who have the courage to go deeply into it. But when a person of the sex which, according to our customs and prejudices, must encounter infinitely more difficulties than men to familiarize herself with these thorny researches, succeeds nevertheless in surmounting these obstacles and penetrating the most obscure parts of them, then without doubt she must have the noblest courage, quite extraordinary talents and superior genius."[5]

After her correspondence with Gauss petered off, and she no longer was supported in her mathematical endeavours, Germain turned to the study of physics.

Sophie Germain died June 27, 1831 in Paris.[1] On her death certificate, she was recorded as having been a "rentière," not a mathematician.[5]

2 A Special Case of Fermat's Last Theorem

2.1 An Introduction to Fermat's Last Theorem

Originally posed by Pierre de Fermat in the late 1630's, Fermat's Last Theorem states that

> $x^n + y^n = z^n$ has no positive integer solutions for all $n > 2$.

The original Latin statement, famously written by Fermat in the margin of his copy of Diophantus' *Arithmetica*, was

> "Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."(As quoted in [6])

This translates to "It is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or in general any power higher than the second into two powers of like degree. I have discovered a truly remarkable proof which this margin is too small to contain."[4]

The proof of this mathematical conjecture, deceptively easy to state, eluded mathematicians for over three hundred and fifty years. Finally, in 1995, Andrew Wiles published a proof of a conjecture which had been previously shown to imply Fermat's Last Theorem. (This also relied on a related paper co-authored with his former doctoral student, Richard Taylor.)

2.2 Past Work on Fermat's Last Theorem

Countless mathematicians have worked on Fermat's Last Theorem (FLT), including Euler, Legendre, Gauss, Abel, Dirichlet, Kummer, and Cauchy. Germain was in fact on of the first people to have a "grand plan" for proving the theorem for all primes p, rather than a more patchwork attempt to prove special cases.[4]

Fermat himself proved the case $n = 4$. Using his method of infinite descent, he showed that the area of a right triangle with rational sides cannot be a perfect square. This is equivalent to the statement that there are no integer solutions to $x^4 + y^4 = z^2$, which then implies that there are no solutions to $x^4 + y^4 = z^4$. If there were integer solutions $a, b, c \in \mathbb{Z}$ such that $a^4 + b^4 = c^4$, then letting $d = c^2$ would give $a^4 + b^4 = d^2$, which is a contradiction.

Any integer > 2 is either a multiple of 4 or has an odd prime factor. Thus, it now suffices to prove FLT for all odd prime exponents. If $n = pm$ where p is a prime, then $x^n + y^n = z^n$ has a solution implies $(x^m)^p + (y^m)^p = (z^m)^p$, which gives a solution for the exponent p.

In 1770, Euler published a proof for the case $p = 3$, although some subtle points were not rigorously justified in his proof. At the time Germain began working on FLT, only the proofs for the cases $n = 3$ and $n = 4$ were known.[4]

2.3 Sophie Germain's "Grand Plan"

In around 1816, the Academy of Sciences in Paris announced a competition with a prize for a proof of Fermat's Last Theorem. Germain neither submitted to this competition nor published any work on FLT, despite the fact that she worked a great deal on the problem and made notable progress. Due to the unpublished nature of her manuscripts, the extent of her work on FLT was not known until very recently. (See [3] for a detailed examination of her original manuscripts and her various efforts relating to FLT.)

Germain's grand plan did not work out as desired, but she proved some other interesting results along the way. Historically, she has not been given credit for many of her results, some of which were later proven by Legendre, presumably independently.[3]

In a letter to Gauss, dated May 12, 1819, she explained her idea for a general proof. She aimed to show that for all odd primes p, there are infinitely many *auxiliary primes* of the form $2np + 1$, where $n \in \mathbb{Z}_{\geq 1}$, such that the set of non-zero residues $x^p \bmod (2np + 1)$ for $1 \leq x \leq 2np$ does not contain any consecutive integer residue classes $\bmod (2np + 1)$. For example, if $a^p \equiv m \bmod (2np + 1)$ and $b^p \equiv (m + 1) \bmod (2np + 1)$ for some $a, b \neq 0$, then this condition would not be satisfied, since m and $m + 1$ belong to consecutive integer residue classes. She then showed that given an integer solution to $x^p + y^p = z^p$, all auxiliary primes satisfying the non-consecutive pth power residue condition necessarily divide either x, y, or z. I will prove this second statement after a brief example of auxiliary primes. Germain analysed the auxiliary primes with $1 \leq n \leq 10$ for all primes less than 100.

What is important about Germain's technique is that she was the first person we know of who attempted to prove FLT for infinitely many prime exponents, rather than just on a case-by-case basis.[4] This philosophy reflects modern attempts to prove the theorem for infinitely many primes at once.

The following is an example of auxiliary primes for the case $p = 5$, as shown in [4], with additional explanations.

First look at $n = 1$. Then $2np + 1 = 2 \cdot 5 + 1 = 11$, so we look at all of the residue classes of the

integers $1 \leq k \leq 10$ to the power 5.

$$\begin{aligned} & \{1^5,\ 2^5,\ 3^5,\ 4^5,\ 5^5,\ 6^5,\ 7^5,\ 8^5,\ 9^5,\ 10^5\} \\ = \ & \{1,\ 32,\ 243,\ 1024,\ 3125,\ 7776,\ 16807,\ 32768,\ 59049,\ 100000\} \bmod 11 \\ = \ & \{1,\ 10,\ 1,\ 1,\ 1,\ 10,\ 10,\ 10,\ 1,\ 10\} \bmod 11 \\ = \ & \{1,\ 10\} \end{aligned}$$

Since 1 and 10 are not consecutive integers $\bmod 11$, we see that 11 is an auxiliary prime for 5.

For $n = 2$, $2np + 1 = 21$, which is not a prime, so $n = 2$ certainly does not yield an auxiliary prime.

$n = 3$ gives $2np + 1 = 31$, and the fifth power residues $\bmod 31$ are $\{1, 5, 6, 25, 26, 30\} \bmod 31$. This fails the non-consecutive residues condition, since 25 and 26 are consecutive residues. In fact, as I will prove below, the non-consecutive residues condition fails whenever n is a multiple of 3.

$n = 4$ yields fifth power residues $\{1, 3, 9, 14, 27, 32, 38, 40\} \bmod 41$. This has no consecutive residues, so 41 is an auxiliary prime.

$n = 5$ gives $2np + 1 = 51 = 3 \cdot 17$, so this is not a prime.

$n = 6$ is a multiple of 3, so this will not work either.

$n = 7$ satisfies that there are no consecutive fifth power residues $\bmod 71$.

$n = 8$ gives that $2np + 1 = 81$ which is not a prime.

$n = 9$ is a multiple of 3.

$n = 10$ satisfies that there are no consecutive fifth power residues $\bmod 101$.

Thus, we see that for $p = 5$ and $1 \leq n \leq 10$, it is true that 11, 41, 71, and 101 are all auxiliary primes. We now need the following proposition, based on that shown in [3].

Proposition 1. *Let p be an odd prime. Given a non-trivial integer solution to $x^p + y^p = z^p$, all auxiliary primes that satisfy the non-consecutivity condition of p^{th} power residues necessarily divide either $x, y,$ or z.*

Proof. Let q be such an auxiliary prime. Assume for a contradiction that q divides neither x, y, nor z. Then, since q is a prime, x, y, and z all have inverses $\bmod q$. Let $a = x^{-1} \bmod q$. Multiplying both sides of the equation by a^p gives $(ax)^p + (ay)^p = (az)^p \Rightarrow 1 + (ay)^p \equiv (az)^p \bmod q$. Thus, ay and $az \in \mathbb{Z}/q\mathbb{Z}$ satisfy that their p^{th} power residues $\bmod q$ are consecutive, which is a contradiction. □

Using the above proposition, we have that if there is a solution of FLT for $p = 5$, then one of x, y, or z must be a multiple of 11, one of 41, one of 71, and one of 101. Thus, one of x, y, and z must be a multiple of at least two of these auxiliary primes.

This brings us back to Sophie Germain's original grand plan to solve FLT. She aimed to prove that every odd prime p has infinitely many auxiliary primes satisfying the non-consecutive p^{th} power residues criterion. If this were true, then any integer solution to $x^p + y^p = z^p$ would satisfy that infinitely many auxiliary primes must divide one of x, y, or z. Since the set of primes that must divide either x, y, or z is infinite, this implies that infinitely many primes must divide at least one of x, y, or z. This gives a contradiction to the existence of a solution to FLT with the exponent p. It was later shown, however, that for each odd prime p, there are only finitely many auxiliary primes satisfying the non-consecutivity condition. Thus, this ambitious approach does not work.

In particular, Germain herself proved, in a letter to Legendre, that for $p = 3$, the only auxiliary primes that work are 7 and 13, and so there certainly cannot be infinitely many auxiliary primes for

this specific case. This shows that she was aware that her grand plan would not work, at least not for all primes.[3] Below, the proof Germain provided to Legendre is explained. It appears that she formulated the proof overnight, since in her letter she thanks Legendre for telling her "yesterday" something that implies there are only finitely many solutions for $p = 3$. She then proceeds to write out a fully formulated proof.[3] I think that this is evidence that her work, in both mathematics and physics, would have been more significant had she enjoyed the benefit of her peers' collaborations and suggestions. Her work suffered from many errors, some rather subtle, that would have been noticed had another mathematician looked over her proofs, especially a mathematician with formal training, which she lacked.

Before proceeding to Germain's proof that the grand plan does not work for $p = 3$, here are a theorem and a lemma to make the proof clearer.

Euler's Theorem, special case: *Let $q = 2np+1$ be a prime and let $0 < a < q$. Then $x^p \equiv a \bmod q$ has a solution if and only if $a^{2n} \equiv 1 \bmod q$.*

Proof. Since $q = 2np$, we have that $\varphi(q) = 2np$. To see the "only if" implication, note that $x^p \equiv a \bmod q$ has a solution implies that $a^{2n} \equiv 1 \bmod q$. This is by Fermat's Little Theorem, since $a^{2n} = (x^p)^{2n} = x^{2pn}$, where x is some solution to $x^p \equiv a$ here. For the "if" implication, let $a^{2n} \equiv 1 \bmod q$. If $a = 1$, then the theorem holds, choosing $x = 1$. So we can assume $a \neq 1$, and therefore $a = g^p$ is a solution, for g some primitive root modulo q, since $g^k = 1$ implies $k = 2pn$. □

Lemma 2. *There are $2n$ different non-zero p^{th} power residues modulo $q = 2np + 1$.*

Proof. By the case of Euler's theorem proven above, we know that there is a bijection between the non-zero p^{th} power residues mod q and solutions to $a^{2n} \equiv 1 \bmod q$.
Let g be a primitive root modulo q. (q is prime, so there must be a primitive root.) Then g^p, g^{2p}, g^{3p}, ..., $g^{(2n-1)p}$, g^{2np} are all unique elements of $\mathbb{Z}/q\mathbb{Z}$ that are $\equiv 1 \bmod q$ when taken to the $2n^{th}$ power. The cardinality of $\{p, 2p, ..., 2np\}$ is $2n$. □

We can now show Germain's proposition.

Proposition 3. *The grand plan cannot work for $p = 3$. For any prime q of the form $6a + 1$, with $q > 13$, there are non-zero consecutive cubic residues. That is, the non-consecutive p^{th} power residues condition fails for $q = 2np + 1$ for $p = 3$ and $n > 2$, so the only valid auxiliary primes for $p = 3$ are $q = 7$ and 13.*

Proof. We only consider the non-zero residue classes $1, ..., 6a$. Suppose for a contradiction that the non-consecutive power residues condition holds true; i.e., that there are no consecutive cubic residues. Note that we are looking at cubic residues because $p = 3$, so the p^{th} power residues are the cubic residues. Further suppose that there are no pairs of cubic residues whose difference is 2. The term "residues" here refers to the residue classes, not congruence classes, and so all residues r that we examine are such that $1 \leq r \leq 6a$; we do not look at 0. In particular, -1 and 1 are cubic congruence classes, but their difference in *residue* classes that we look at is not 2.

$q = 2a \cdot 3 + 1$ here, so there are $2a$ cubic residues, as shown above. These are distributed amongst the $6a$ residues, and differences of 1 or 2 between these residues are not permitted, by assumption. To separate these $2a$ cubic residues, there must be $2a - 1$ "gaps" between them, each containing at least 2 non-cubic residues (n.c.r.'s), and all of the gaps together containing the $4a$ n.c.r.'s. Since each of $2a - 1$ gaps requires at least 2 n.c.r.'s, this uses $4a - 2$ of the n.c.r.'s, and leaves 2 that can

be distributed anywhere. Thus, it is either the case that all but two gaps contain exactly 2 n.c.r.'s and two contain 3 n.c.r.'s each, or all but one contain 2 n.c.r.'s and one gap contains 4 n.c.r.'s.

Since $q > 13$, we know that 1 and 8 must be cubic residues, since $1^3 = 1$ and $2^3 = 8 \bmod q$. By our assumptions on the gap between cubic residues, 2 and 3 cannot be cubic residues. If 4 were a cubic residue, then taking $8 \cdot 4^{-1} = 8/2 = 2$ would also give a cubic residue $\bmod q$, but we just said that 2 cannot be a cubic residue. So 4 is also not a cubic residue. Thus, we must have that 5 is a cubic residue, since otherwise there cannot be a sufficient gap between the residue and 8, and the size of the gap cannot be greater than 4 n.c.r.'s, either. Furthermore, we have now distributed one of the two extra n.c.r.'s. This implies that only one other pair of cubic residues can have a gap between them of exactly 3 n.c.r.'s.

The sequence of cubic residues must therefore be 1, 5, 8, 11, ..., $6a-10$, $6a-7$, $6a-4$, $6a$, since the cubic residues are symmetric about $6a/2$. This is because $b \equiv x^3$ for some $x \bmod q \Leftrightarrow -b \equiv -x^3$, and $-b \equiv (q-b) \bmod q$. Therefore, the two exceptional gaps of size 3 are located and the beginning and the end of the sequence. We now show that this cannot be the pattern of cubic residues, and thus one of our assumptions must be false.

We are concerned only with primes of the form $6a + 1 > 13$. The first case to look at is 19. $4^3 = 64 \equiv 7 \bmod 19$, which is not on the list. So 19 is not an auxiliary prime to 3. The next possible auxiliary prime is $31 = 6 \cdot 5 + 1$, so we see that for all possible auxiliary primes for 3 that are greater than 19, $3^3 = 27$ gives a cubic residue modulo q. This contradicts the pattern that the cubic residues must follow under our assumptions, since 27 is less than $6a \geq 30$, and $27 \equiv 0 \bmod 3$. In the pattern we found, all cubic residues, with the exceptions of 1 and $6a$, must be $\equiv 2 \bmod 3$.

Therefore, one of the two initial assumptions must be false. If the non-consecutivity condition on 3^{rd} power residues is false, then the proposition holds.

So we may assume that the failure is due to the second assumption. This means that there are some cubic residues with only a single n.c.r. between them. Let r and r' be such that $r - r' = 2$; i.e., the gap between r and r' is a single n.c.r. Let g be a primitive rood modulo q. 2 is not a cubic residue, since we are still assuming there is at least one n.c.r. between each pair of cubic residues, and 1 must be a cubic residue. This implies that $g^{3k\pm1} = 2$, where $k \in \mathbb{Z}$, since the power of g representing 2 cannot be divisible by 3.

Consider $r + r'$. We claim that $r + r' \not\equiv 0 \bmod q$. If $r + r' \equiv 0$, then $r \equiv -r'$, so $2 = r - r' \equiv 2r$ $\Rightarrow r \equiv 1 \Rightarrow r = 1 \in \mathbb{Z}$. This last fact uses that we are looking are residues $1 \leq r \leq q - 1$. It cannot be that $2 = 1 - r'$, because $1 \leq r' \leq q - 1$. Thus, $r + r' \not\equiv 0 \bmod q$.

This in turn implies that $r + r'$ is in $(\mathbb{Z}/q\mathbb{Z})^\times$, and so $r + r' = g^m$ for some $1 \leq m \leq q - 1$. If m were divisible by 3, then $1 + r'r^{-1} = g^m r^{-1}$, with both $r'r^{-1}$ and $g^m r^{-1}$ cubic residues. This contradicts the non-consecutivity condition. So 3 does not divide m, and thus $r + r' \equiv g^{3j\pm1}$, $j \in \mathbb{Z}$. Now we claim that the sign in $r + r'$ must agree with that in $r - r'$, i.e. the sign in $3k \pm 1$ agrees with that in $3j \pm 1$. If not, letting $r + r' = g^{3j\mp1}$ gives that $r^2 - r'^2 = (r - r')(r + r') \equiv g^{3k\pm1} g^{3j\mp1} = g^{3k+3j\pm1\mp1} = g^{3(k+j)}$, $(k + j) \in \mathbb{Z}$, so $r^2 - r'^2$ is a cubic residue. As above, this contradicts the non-consecutivity condition on cubic residues.

Finally, we add together $r - r' = g^{3k\pm1}$ and $r + r' = g^{3j\pm1}$ to obtain $2r = g^{3k\pm1} + g^{3j\pm1}$. Recall that $2 = g^{3k\pm1}$, as originally defined. Thus, $g^{3k\pm1} r = g^{3k\pm1} + g^{3j\pm1} \Rightarrow r = 1 + g^{3(j-k)}$. This again contradicts the non-consecutivity assumption, and this is all that we have assumed.

Therefore, the original assumption that there were no two consecutive cubic residues $\bmod q$ must have been false. □

2.4 Two Cases for Fermat's Last Theorem

As a result of Sophie Germain's work, Fermat's Last Theorem was divided into two cases for examination.[4]

FLT Case 1: $x^p + y^p = z^p$ has no integer solutions for which none of x, y, and z are divisible by p.

FLT Case 2: $x^p + y^p = z^p$ has no integer solutions for which one and only one of x, y, and z is divisible by p.

Note that if any two of x, y, and z are divisible by p, then so too is the third number. Let all three integers be divisible by p^k but not p^{k+1}, $k \in \mathbb{Z}_{\geq 1}$. Then, dividing each integer by p^k gives a solution satisfying either case 1 or 2.

3 Sophie Germain's Theorem

The original statement of Sophie Germain's theorem is stronger than the theorem for which she is usually given credit.

Sophie Germain's Theorem (Original)
If p is an odd prime and there exists an auxiliary prime $q = 2np + 1$ satisfying:

1. *there are no consecutive p^{th} power residues* mod q
2. *p is not a p^{th} power residue* mod q

then in any solution to the Fermat equation $x^p + y^p = z^p$, p^2 must divide one of x, y, or z. In particular, Case 1 of Fermat's Last Theorem is true for p.

This theorem is usually stated in a weaker form, as follows:

Sophie Germain's Theorem
If p is an odd prime and $q = 2p + 1$ is also prime, then p must divide one of x, y, or z, and therefore Case 1 of Fermat's Last Theorem is true for p.

A prime p satisfying that $2p + 1$ is also prime is called a *Sophie Germain prime*.

Credit is in fact often given to Legendre for proving that p^2, and not just p, must divide one of these integers, even though this was part of Germain's proof. Legendre explicitly credits Germain for this result, but later authors have often understated her contributions.[3]

I will now show that if $q = 2p + 1$ is a prime, then conditions 1 and 2 of Germain's original theorem are necessarily satisfied.

Claim 4. *There are no consecutive p^{th} power residues* mod q *if and only if $x^p + y^p + z^p \equiv 0 \bmod q$ implies that x, y, or $z \equiv 0 \bmod q$.*

Proof. This proof is essentially the same as that of Proposition 1. Assume there is an integral solution $x^p + y^p + z^p \equiv 0 \bmod q$ but x, y, and $z \not\equiv 0 \bmod q$. $\Leftrightarrow x^p + y^p \equiv -z^p = (-z)^p \bmod q$, none of these integers congruent to $0 \bmod q$. Multiplying both sides by $(x^{-1})^p$ gives $1 + y^p =$

$(-z)^p$. This gives consecutive power residues mod q. This proof actually shows both directions by contrapositives, since given $z^p = y^p + 1$, none of these elements $\equiv 0$ of course, we can multiply both sides by g^p for g some primitive root mod q to find a non-trivial solution to $x^p + y^p + z^p \equiv 0 \mod q$. □

Claim 5. *Suppose $q = 2p + 1$; that is, p is an odd Sophie Germain prime. Then conditions 1 and 2 of Sophie Germain's original theorem are satisfied.*

Proof. $\varphi(q) = 2p$. So for any $a \in (\mathbb{Z}/q\mathbb{Z})^\times$, $a^{2p} = (a^p)^2 \equiv 1 \mod q$, by Fermat's Little Theorem. $\Rightarrow a^{2p} - 1 \equiv 0 \mod q \Rightarrow (a^p - 1)(a^p + 1) \equiv 0 \mod q \Rightarrow a^p \equiv 1 \mod q$ or $a^p \equiv -1 \mod q$, since q is prime. If x, y, and $z \not\equiv 0 \mod q$ then $x^p + y^p + z^p \equiv \pm 1 \pm 1 \pm 1 \not\equiv 0 \mod q$. In order to have $x^p + y^p + z^p \equiv 0 \mod q$, one of these integers must be congruent to $0 \mod q$. Thus, condition 1 is satisfied.

Furthermore, since $x^p = \pm 1 \mod q$, it is impossible for $x^p \equiv p$ for any x, and so condition 2 is also satisfied. □

As mentioned in the example given for $p = 5$, the non-consecutive residues condition fails for $q = 2np + 1$ whenever n is a multiple of 3, as Germain herself showed.[4]

Proposition 6. *If p is a prime and $q = 2 \cdot 3kp + 1$ is also prime, then there exist x, y, and z each non-zero mod q such that $x^p + y^p + z^p \equiv 0 \mod q$. Therefore, condition 1 of Sophie Germain's (original) theorem does not hold for this q.*

Proof. $\varphi(q) = 2 \cdot 3kp$. Let g be a primitive root modulo q. $g^n \not\equiv 0 \mod q$ for all $n \in \mathbb{Z}$. Let $m = g^{2kp} \not\equiv 1$, since $|g| = \varphi(q) = 6kp$. Moreover, $m^3 = g^{6kp} \equiv 1 \mod q \Rightarrow m^3 - 1 = (m - 1)(m^2 + m + 1) \equiv 0$. $m \not\equiv 1 \Rightarrow m^2 + m + 1 \equiv 0 \mod q \Leftrightarrow g^{4kp} + g^{2kp} + 1 \equiv 0 \mod q$. None of these elements are $\equiv 0$, and so, by Claim 4, condition 1 of Sophie Germain's theorem cannot be satisfied. □

Germain actually proved much more than Claim 5. She showed that if $x^p \not\equiv 2 \mod q$ for all x and the auxiliary prime q is of the form $4p+1$, $8p+1$, $10p+1$, $14p+1$, or $16p+1$, then condition 1 of her theorem holds. She then examined the exceptional cases where there is some $a^p \equiv 2 \mod q$, and found the auxiliary primes of the form $2np + 1$ satisfying condition 1 for all n such that $1 \leq n \leq 10$ and all odd prime exponents $p \leq 100$. She also showed that all of these auxiliary primes found satisfy condition 2.

Legendre is usually credited with finding this, as his results were published in an 1823 paper, and Germain never published her results.[4] It appears that the two of them found their results independently, given that they used very different techniques.[3]

Germain and Legendre collectively showed that all odd prime exponents $p < 197$ satisfy Case 1 of Fermat's Last Theorem, by explicitly finding an auxiliary prime $q = 2np + 1$ that satisfies Sophie Germain's theorem. See [4] for a table listing these auxiliary primes. This result was a large leap forward, even if it only showed that one of two cases holds true. Recall that previously, proofs had only been known for the exponents 3 and 4. Even a partial result relating to so many different primes was impressive.

I will now show the proof of the strong version of Sophie Germain's theorem, which is restated below.

Sophie Germain's Theorem (Original)
If p is an odd prime and there exists an auxiliary prime $q = 2np + 1$ satisfying:

1. *there are no consecutive p^{th} power residues* $\bmod q$
2. *$x^p \not\equiv p \bmod q$ for all $1 \leq x \leq q-1$*

then in any solution to the Fermat equation $x^p + y^p = z^p$, p^2 must divide one of $x, y,$ or z.

Proof. We assume, without loss of generality, that x, y and z are all coprime. (See the remark after the introduction of the two cases of FLT for details.)

First, we claim that the pairs of numbers below can have no common divisors other than p.

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

Let $\varphi(x, y)$ denote the right-hand expression on the first line. If some prime $q \neq p$ divides both $x + y$ and $\varphi(x, y)$, then $y \equiv -x \bmod q$, by definition of $q \mid (x + y)$. Then, substituting this into $\varphi(x, y)$ immediately gives $\varphi(x, y) \equiv px^{p-1} \bmod q$, which is divisible by q by assumption. x must be divisible by q, since q does not divide p. This gives that both x and $x + y$ are divisible by q, which implies that y is divisible by q as well, contradicting the assumption that x and y are relatively prime. Thus, no primes other than p can divide both $x + y$ and $\varphi(x, y)$.

The same can be seen for the second and third pairs of numbers, using that if q divides $z - y$ then $z \equiv y \bmod q$, and similarly for x.

We now need the following subclaim.

Claim 7. *p must divide one of $x, y,$ or z.*

Proof of Subclaim: Now, we assume for contradiction that x, y, and z are all coprime with p. Then, letting $z = lr$, $x = hn$, and $y = vm$, we have that:

$$\begin{aligned} x+y = l^p \quad &\text{and} \quad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - ... + ... + y^{p-1} = r^p \\ z-y = h^p \quad &\text{and} \quad z^{p-1} + z^{p-2}y + z^{p-3}y^2 + ... + y^{p-1} = n^p \qquad (1) \\ z-x = v^p \quad &\text{and} \quad z^{p-1} + z^{p-2}x + z^{p-3}x^2 + ... + x^{p-1} = m^p. \qquad (2) \end{aligned}$$

These equations were given by Barlow around 1810, and also stated by Abel in 1823.[3] We are assuming that each pair of numbers is coprime with p, and we just showed that the only common factor each pair can have is p. Thus, we are essentially assuming that each pair of numbers is coprime. Looking at the first line, for example, this explains why $x + y = l^p$, with no r factors, and $\varphi(x, y) = r^p$, with no l factors; otherwise, the left and right numbers would not be coprime. Then, note that $(x+y) \cdot \varphi(x, y) = x^p + y^p = z^p$, this last equality coming from the statement of the theorem. Therefore, we see that $x + y \neq l^k$ for any $k \neq p$, and similarly we must have $\varphi(x, y) = r^p$. The second and third equations follow analogously.

As shown in Proposition 1, the auxiliary prime q, which is assumed to exist and satisfy conditions 1 and 2, must divide either x, y, or z. Without loss of generality, assume that q divides z. (If q divided x or y, the following equations would simply have a sign change in them.)

$q|z \Rightarrow q|2z$, so $2z = (z - y) + (z - x) + (x + y) = l^p + h^p + v^p \equiv 0 \bmod q$. Now, as shown in Claim 4, $l^p + h^p + v^p \equiv 0 \bmod q \Leftrightarrow$ either l, h, or v is divisible by q. If either h or v were divisible

by q, using that $y = z - h^p$ and $x = z - v^p$ from equations 1 and 2, and that $q|z$, then either y or x, respectively, would be divisible by q as well. This contradicts the assumption that x, y, and z are all coprime. Thus, it must be that $q|l$.

$x + y = l^p$, so this implies that $y \equiv -x \bmod q$. We also have that $\varphi(x, y) \equiv px^{p-1} \equiv r^p \bmod q$, as shown.

Since $z \equiv 0 \bmod q$ by assumption, $z - x = v^p \equiv -x \bmod q$. So x must be a p^{th} power residue mod q, by definition. Now use that $px^{p-1} \equiv r^p \bmod q$. Substituting in v^p for x, this yields $p(v^{p-1})^p \equiv r^p$. Recall that q does not divide x, since $q|z$ by assumption and x and z are coprime. This therefore implies that p is also a p^{th} residue mod q. This contradicts condition 2. Thus, we see that it cannot be that p does not divide either x, y, or z. So p divides one of these integers. $\triangle$

Now we no longer assume that it is z that q divides. We instead assume, without loss of generality, that $p|z$; it is not necessarily true that $q|z$ with this assumption.

Note that the above subclaim is enough to establish the weaker version of Sophie Germain's theorem, as it is usually stated.

Now set $z = lrp$. We claim that $x+y = l^p p^{p-1}$ and $x^{p-1} - x^{p-2}y + x^{p-3}y^2 - ... + ... + y^{p-1} = pr^p$. The remaining equations are the same, because x and y are still coprime to p, so $x = hn$ and $y = vm$. Since $z^p = (x + y) \cdot \varphi(x, y)$ must be divisible by p^p, it suffices to show that $\varphi(x, y)$ is divisible by p but not by p^k for all $k > 1$. $\varphi(x, y) = \frac{y^p + x^p}{x+y}$. Let $s = x + y$. This gives:

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

Every term but the last in the above sum is divisible by p^2. $s = x + y \equiv x^p + y^p \equiv z^p \bmod p$, by Fermat's Little Theorem, and so p divides s. The last term is divisible by exactly p because $\gcd(x, p) = 1$. So $\varphi(x, y)$ is divisible by exactly the first power of p.

Using equations 1 and 2 given above, $2z - (x + y) = 2z - x - y = h^p + v^p$; this implies that p divides $h^p + v^p$, since p divides both z and $x + y$. Moreover, p divides $h + v$, by Fermat's Little Theorem. $\Rightarrow h \equiv -v \bmod p$, which implies that $h^p \equiv -v^p \bmod p^2$. To see this, write $h = -v + mp$, where $m \in \mathbb{Z}$. $h^p = (-v + mp)^p = -v^p + v^{p-1}p^2m - ... + (mp)^p \equiv -v^p \bmod p^2$, since p^2 divides all terms except for $-v^p$.

$x + y = l^p p^{p-1}$ was shown, so $p^2 | (x + y)$, and we just showed above that $p^2 | h^p + v^p$. We also know that $2z = h^p + v^p + (x + y)$, and therefore p^2 divides z. $\square$

This concludes my exposition of Sophie Germain's work relating to Fermat's Last Theorem. It is my hope that the reader now has a greater understanding of the significant progress she made on this problem, progress for which she historically has not been given sufficient credit.

References

[1] "Sophie Germain." Encyclopaedia Britannica Online. Encyclopaedia Britannica Inc., 2013. Web. http://www.britannica.com/EBchecked/topic/230626/Sophie-Germain/2647/Additional-Reading.

[2] L. L. Bucciarelli and N. Dworsky, "Sophie Germain," *Studies in the History of Modern Science*, Volume 6, pp. 9-19, 1980.

[3] R.Laubenbacherand D. Pengelley, "'Voici ce que jai trouvé:' Sophie Germain's grand plan to prove Fermat's Last Theorem," pre-print, 2010.

[4] L. Riddle, "Sophie Germain and Fermat's Last Theorem," Agnes Scott College, 2009. http://www.agnesscott.edu/Lriddle/women/germain-FLT/SGandFLT.htm

[5] S. Singh, excerpt from "Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem," October 1997, http://www.pbs.org/wgbh/nova/physics/sophie-germain.html.

[6] A. Wiles, "Modular Elliptic Curves and Fermat's Last Theorem," *Annals of Mathematics*, Second Series, Vol. 141, No. 3, pp. 443-551, May, 1995.