Fall 2018

The Role of Sophie Germain in Solving Fermat's Last Theorem

Amal Yaqoub Yosef

The Role of Sophie Germain in Solving Fermat's Last Theorem

By

Amal Yosef

A.S., Moraine Valley Community College, 2001

B.A., Saint Xavier University,2005

THESIS

Submitted in partial fulfillment of the requirements

For the Degree of Master of Science,

With a Major in Mathematics

Governors State University

University Park, IL, 60484

2018

Abstract

Fermat's Last Theorem sat unproven for more than 300 years. It all started around 1637, when Pierre de Fermat stated the theorem: $x^p+y^p = z^p$ has no positive integer solutions for x, y, z when $p > 2$. He wrote a note in the margin saying that he has the proof but it was bigger than the margin. Sophie Germain, a French mathematician tried her hand in proving Fermat's Last Theorem. She came up with a theorem that was later referenced to as Germain Theorem. She took Fermat's Last Theorem $x^p + y^p = z^p$ and suggested that if p is a prime number greater than 2 and $2p + 1$ is a prime also, then p must divide x, y, or z. Germain's theory and proof changed the approach to proving Fermat's Last Theorem and divided it into two cases where the first case states that none of the three valuesx, y, or z is divisible by p. and the second case states that the exponent p divides at least one of the three values x, y,or z. The main concept of this paper is to explore Germain's approach to solving Fermat's Last Theeorem for the exponent $p > 2$ and how her idea led to solving the problem by introducing a new and fresh approach.

Dedication

In the first place, I would like to give thanks to all mathematicians out there who loved Mathematics and tried their hands to proving Fermat's Last Theorem (FLT). Bigger thanks will have to go to all the people who wrote the books or journals or blogs or even the You-Tubers who made it easier for me to see the beauty of this project and opened my eyes to the intricate parts of the proofs.

Secondly, I would like to thank my most flexible and helpful supervisor Professor Andrius Tamulis. You put up with so much of my nonsense and always encouraged me to pop in as you called it at any time to discuss my findings and anything that needed explaining. You were also a big help with returning my emails in a timely manner. I would like to thank Professor Dianna Galante and Professor Chris Tweddle for being readers on my thesis committee and being there for the much needed support.

Last, but not least, I would love to dedicate this thesis to my family: my father (God rest his soul) he would have been so proud, my mother, my sisters and brothers, my husband Rashad and my children: (Lama, Rami, Loreen and Sami Hourani) who had to put up with any shortcomings from me and encouraged me all through this illuminating educational process. We did it guys!

Contents

1 Introduction:

> Cubem 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 caparet. [7]

In the late 1630s, Pierre de Fermat (1601-1665) wrote this note in the margin of his copy of Claude Bachet's Latin translation of Diophantus's *Arithmetica* which got the attention of great mathematicians for over 300 years. In English, ”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.” [5]

Fermat's Last Theorem which will be abbreviated to (FLT) from now on in this paper is converted in modern terms into:

$$x^p + y^p = z^p \quad \text{has no positive integer solutions,}$$
$$\text{for } x, y, z \text{ when} \quad p > 2. \text{ [6]}$$

It looks like a simple conjecture, but it took a great number of mathematicians over three centuries to prove it, until Sir Andrew Wiles who worked on it secretly for most of his life, proved it in a three inspiring lectures in June 1995, at the Isaac Newton Institute in Cambridge. [4] Wiles used techniques far beyond what was available to Fermat, and it is therefore believed that Fermat thought he had a proof that was in fact false.

Figure 1: Pierre-De-Fermat (1601-1665)
[12]

The journey to prove FLT led to the numerous discoveries of modern Mathematics and the additions to existing mathematics. In short, proving Fermat's Last Theorem over the centuries was very beneficial to the mathematical fields to bring it to the 20th century mathematics. Fermat might not have proved the theorem as he stated in Diaphanous book margin, because he later published his proof of the special case $p = 4$.

The phenomenon of Fermat's last theorem started when Fermat died in (1665). His son, Samuel, published his copy of Diophantous because he was afraid that his father's work would be lost and forgotten. From then on, Fermat's Last Theorem became a major mathematical challenge to great mathematicians everywhere. Mathematicians of the highest abilities, including Euler, Legendre, Gauss, Sophie Germain, Dirichlet, Kummer and Cauchy worked on it. Sophie Germain, like a lot of mathematicians, was fascinated with FLT for some time, but lack of communication with peers to bounce ideas off and get feedback was a hindrance. Despite her lack of formal education, she was the first mathematician to make progress with a general approach toward proving Fermat's Last Theorem [3]. Fermat's Last Theorem was named such, not because it was the last theorem Fermat proposed or worked with, but because it was the last of his theorems to be proven. Germain was one of the first to provide a different plan for proving Fermat's Last Theorem and to give a partial solution for a large class of exponents instead of working on one prime number case at a time [8].

Germain was born in Paris on April 1, 1776. Her family was middle-class wealthy. She had two other sisters. Her father, Ambroise-Franois Germain, a silk merchant, was a member of the third estate to the Constituent Assembly convened in 1789 [6].

She wasn't educated formally, because in the 18th century France, girls were not permitted to go to school. She was not of the elite class where she could have gotten some education by a special tutor, so she taught herself the basics. The French Revolution broke out when Germin was only thirteen years of age. She started spending a great deal of time in the library because her family was afraid for her safety and would not let her leave the house. She was facinated by the story she read of how Archimedes died. He was speared to death by a Roman soldier who asked him a question during the invasion of the city by the Romans. Archimedes was so engrossed in the study of a geometric figure in the sand that he failed to respond and thus was killed.

Germain thought if geometry could hold such fascination for Archimedes, then it was a subject worthy of attention and studying. This interested her in mathematics. One of the amazing things about her was that she taught herself Latin and Greek using her family's library so she could read the works of Sir Isaac Newton and Leonhard Euler.

2 Germain's work on number theory prior to FLT:

In 1794, when Sophie Germain was 18 years old, the Ecole Polytechnique was founded in Paris. It was an academy founded to train mathematicians and scientists for their country [3]. Women were not allowed to enroll in the academy, but Germain was able to get the lecture notes for several of the courses for her studies. This opened the door for her to learn from prominent mathematicians of her day by writing to them using the pseudonym of Monsieur Antoine-August LeBlanc who was a former student of the Academy that died prior to this. She contacted Joseph-Louis Lagrange at the end of a term in the academy to submit a report on analysis. He was very impressed with her work and wanted to meet the student who had written it.

3 Sophie Germain's life and Education:

Lagrange was amazed that the work was actually done by a female, but he recognized her abilities and became her mentor and he encouraged and supported her for several years. Germain became a part of the circles of scientists and mathematicians that she was not allowed in before because she was introduced by a male mathematician (Lagrange).

Germain contributed to acoustics, a branch of physics that deals with sounds and sound

Figure 2: Sophie Germain (1776-1831)
[14]

waves, elasticity, the ability of a substance to change form or shape responding to a force exerted, and also the Theory of Numbers. The most famous number theory topic she worked on was Fermat's Last Theorem. Number theory was of a special interest to her; it occupied her throughout her life. When Adrien-Marie Legendre published his book of *Théorie des Nombres* in 1789, she began corresponding with him incognito after studying his work closely. Germain sent him some of her own ideas on the subject of number theory and elasticity. Her work on number theory eventually made significant results.

More than a decade later, she started a correspondance with the German mathematician Carl Friedrich Gauss after he published his book in Number Theory, *Disquisitiones Arithmeticae* in 1801. According to Germain's friend the Italian mathematician, Guglielmo Libri, she was amazed by the originality of this famous professor's work and experienced another incentive to engage in this kind of analysis. She sent Gauss some of her work in number theory using her pseudonym. In one correspondance in the year 1807, she claimed that: if $x^p + y^p$ is of the form of $h^2 + pf^2$ then $x + y$ is also of the same form. Gauss replied: $15^{11} + 8^{11}$ can be written as $h^2 + 11f^2$, but $15 + 8$ cannot [**?**, p-49]. In the same year, Gauss found out that he was corresponding with a gifted woman. He was so excited that he wrote to her:

> 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... 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 [6, p-7].

She correspondened with Lagrange, Lagendre and Gauss for long periods of time and her work was respected by the three highly regarded mathematicians and later by others who knew of her work.

4 Germain's early theorems regarding FLT:

When the academy Ecole Polytechnique established a prize to proving FLT, it interested Germain and she started working on a proof. She never published any of her work and findings while she was alive, but Legendre credited her in 1825 a footnote in of his second edition memoires that he published on FLT. After years of research and hard work on her own on FLT, she decided she needed to discuss her work with a number theorist to share her new, more general approach to proving Fermat's Last Theorem, so she wrote to Gauss about her discoveries of Fermat's Last Theorem:

> I add to this art some other considerations which relate to the famous equation of Fermat $x^n + y^n = z^n$ whose impossibility in integers has still only been proved for $n = 3$ and $n = 4$; I think I have been able to prove it for $n = p - 1$, p being a prime number of the form $8k + 7$. I shall take the liberty of submitting this attempt to your judgment, persuaded that you will not disdain to help with your advice an enthusiastic amateur in the science which you have cultivated with such brilliant success [8].

This propopsition did not work out because it was missing some elements to complete the proof. This letter of hers shows that she already knew of the proof for the exponents 3 and 4. The case for the exponent 3 was proven by Euler earlier, but it was discovered later that it had some flaws. The case for exponent 4 was proven by Fermat himself using the method of infinite decent [8].

As a direct result of Germain's work on FLT, Fermat's Last Theorem got divided into two cases:

Case one: $x^p + y^p = z^p$ has no integer solutions where x, y, and z are relatively prime to p meaning that p doesn't divide x, y, or z.

Case two: $x^p + y^p = z^p$ has no integer solutions to which one and only one of the relatively prime integers x, y, and z is divisible by p. This means that p divides only one of x, y, or z.

For the purpose of this paper, we'll use the notation for case one of FLT as
FLT_1, which states: There does not exist nonzero, pairwise relatively prime integers x, y and z such that: $x^p + y^p + z^p = 0$ and $p \nmid xyz$. and
FLT_2 that states: There does not exist nonzero, pairwise relatively prime integers x, y and z such that: $x^p + y^p + z^p = 0$ and $p \mid$ only one of x, y or z. [9] In this paper, I will be focusing on FLT_1 because that is what Germain did. Germain worked with primes to tackle FLT, then she came up with her own theorem regarding the exponent p, later she started to involve p^2 in her theorems which is a little bit more broad than that of p. Another one of her theorems was her key theorem to work with large-sized solutions and her grand plan.

I will state a few simple mathematical theorems to help explain the proofs of the theorems. The following fact is used in the proof of Sophie Germain's theorem, it also relies on the Fundamental Theorem of Arithmetic.

Theorem 1. *Let r and s be relatively prime integers. If rs is a p^{th} power, then r and s must both be p^{th} powers.*

Fermat's Little Theorem (FLT_l) states: If p is prime, and a is a natural integer where $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Lemma 1. *Let x, y be coprime integers and p be an odd prime. Then, the Greatest*

Common Divisor $GCD(x, y) = (x + y, \frac{x^p+y^p}{x+y}) = 1$ *or* p

5 Sophie Germain's letter to Gauss in 1819:

Germain outlined her strategy for a general proof of FLT in a long letter to Gauss, written on May 12, 1819, presenting her ideas on FLT, and explaining that she had never stopped thinking about number theory and that she had been thinking on FLT long before the Academy established this new prize [6].

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

> clear, since the equation: $x^p + y^p = z^p$ yields the congruence $1 \equiv r^{sp} - r^{tp}$ in which r represents a primitive root and s and t are integers. It follows that if there are infintely many such numbers, the equation would be impossible [6, p-20].

Germain is utilizing some facts about the residues modulo the prime and another fact that for a prime modulus, there is always a primitive root for the prime modulus, such that any number with nonzero residue is congruent to a power of the primitive root. For the above examples, $r = 2$ is a primitive root of $p = 7$ and of $p = 13$ [6].

5.1 Sophie Germain's Auxiliary primes:

Germain's main idea was to prove FLT prime exponents in general. She started with the idea: if there exist a prime p where $2p + 1$, is also a prime, then they are auxiliary primes. These were later called Germain's primes. The first few Germain primes are: $2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113$, and 131. A list of a few sets of Germain primes are in Table 1 below:

Germain proved FLT for the prime p and its relative prime $2p + 1$. This is also known by some mathematicians as the weaker version of Germain's theorem.

5.2 Sophie Germain's theorem and proof to solve FLT for p:

Trying to prove FLT, Sophie Germaine came up with a theorem stating that:

Table 1: Sophie Germain's primes

prime p	$2p+1$
2	5
3	7
5	11
11	23
23	47
29	59
41	83
53	107

Theorem 2. *Let p be an odd prime. If there is an auxiliary prime θ with the properties:*

1. $x^p + y^p + z^p = 0 \pmod{\theta}$ *implies* $x = 0$ *or* $y = 0$ *or* $z = 0 \pmod{\theta}$*, and*

2. $a^p \equiv p \pmod{\theta}$ *is impossible for any integer* a*,*

   then the equation $x^p + y^p = -z^p$ has no solutions for which x, y, and z are relatively prime to p, where $p \nmid x, y, z$.

Proof. Suppose that there is a solution x, y, z to the equation, $-x^p = y^p + z^p$ such that $p \nmid x, y$, or z and assume that x, y, and z are relatively prime. Now we can factor $-x^p = y^p + z^p$ as follows:

$$y^p + z^p = (y+z)(y^{p-1} - y^{p-2}z + y^{p-3}z^2 - ... + z^{p-1})$$

Let $(y^{p-1} - y^{p-2}z + y^{p-3}z^2 - ... + z^{p-1})$ be referred to as $f(x, y)$. To prove that both factors $(y + z)$ and $f(x, y)$ are relatively prime, we introduce a prime n that is common to both factors, $(y + z)$ and $f(x, y)$, then $y \equiv -z \pmod{n}$ and by substituting in $f(x, y)$, we get: $py^{p-1} \equiv 0 \pmod{n}$. So either $n \mid p$ or $n \mid y^{p-1}$. If $n \mid p$, then

$n = p$ since they are both primes. This would contradict the assumption that none of x, y, or z is divisible by p and if $p \mid (y^p + z^p)$, then $(-x)^p$ and so $p \mid x$. Thus the second statement should be true. But if $y \equiv 0 \pmod{n}$, then n would divide both y and $y + z$, but y and z have no common factors. As neither of these can be true, there is no prime factor that divides both $y + z$ and $f(x, y)$ which makes them relatively prime, and consequently they are both p th powers by Theorem 1 above. The equations $(-y)^p = (x^p + z^p)$ and $(-z)^p = (x^p + y^p)$ can be factored the same way. From this, it follows that there must be integers a, b, c, m, j, and k in the following equations that the British mathematician Peter Barlow introduced in 1810 and stated by the Norwegian mathematician Niels Henrik Abel in 1823:

$$y + z = m^p \qquad y^{p-1} - y^{p-2}z + ... + z^{p-1} = a^p \qquad x = -ma \tag{1}$$

$$z + x = j^p \qquad z^{p-1} - z^{p-2}x + ... + x^{p-1} = b^p \qquad y = -jb, \tag{2}$$

$$x + y = k^p \qquad x^{p-1} - x^{p-2}y + ... + y^{p-1} = c^p \qquad z = -kc. \tag{3}$$

the above equations were introduced by the British mathematician Barlow in 1812 and stated again by Abel in 1823. Now, since: $x^p + y^p + z^p = 0 \pmod{\theta}$, implying by the first condition of the theorem that x, y, or z must be zero mod θ, then lets assume without loss of generality that $x \equiv 0 \pmod{\theta}$, then: $2x = x + x = j^p + k^p + -(y + z) = j^p + k^p + (-m)^p \equiv 0 \pmod{\theta}$. Now, θ must divide either m, j, or k according to the first condition of the theorem. If j or k is $0 \pmod{\theta}$, then $y = -jb \equiv 0 \pmod{\theta}$, or $z = -kc \equiv 0 \pmod{\theta}$. This together with the fact that $x \equiv 0 \pmod{\theta}$ implies that at least two of x, y, and z are divisible by θ, which contradicts the assumption that x, y, and z are pairwise relatively prime. Therefore, as neither j nor k is congruent to $0 \pmod{\theta}$, then $m \equiv 0 \pmod{\theta}$ and since $y + z = m^p$, this implies that $y = -z$

$\pmod{\theta}$. So $a^p = y^{p-1} - y^{p-2}z + ... + z^{p-1} \equiv py^{p-1} \equiv 0 \pmod{\theta}$ as before and, since $x \equiv 0 \pmod{\theta}$, $c^p = x^{p-1} - x^{p-2}y + x^{p-3}y^2 - ... + y^{p-1} \equiv y^{p-1} \pmod{\theta}$. Putting these together gives, $a^p \equiv pc^p \pmod{\theta}$. Since c is not congruent to $0 \pmod{\theta}$, there is an integer g such that $cg \equiv 1 \pmod{\theta}$, as every element not congruent to zero must have a multiplicative inverse $\pmod{\theta}$. We can thus insert a factor of $(cg)^p$ on the left side of $a^p \equiv pc^p \pmod{\theta}$ without changing the result, so $(acg)^p \equiv pc^p \pmod{\theta}$. By canceling the factor of c^p, we reach $(ag)^p \equiv p \pmod{\theta}$, which is contrary to the second assumption on θ which proves Sophie Germain's theorem. □

5.2.1 Sophie Germain's first condition on her theorem for p:

In her work to find suitable primes, she worked with primes $p < 100$ and the auxiliary primes $\theta = Np + 1$ with N ranging from 1 to 10. The combined efforts of Germain and Lagendre, made it up to 197 of auxiliary primes discovered. Below is a table of such auxiliary prime θ where N is a positive integer.

Table 2: Auxiliary Primes $\theta = Np + 1$ to primes p

N	p	θ	N	p	θ	N	p	θ	N	p	θ
2	3	7	2	5	11	4	7	29	2	11	23
4	13	53	8	17	137	10	19	191	2	23	47
2	29	59	10	31	311	4	37	149	2	41	83
4	43	173	14	47	659	2	53	107	14	59	827
16	61	977	4	67	269	8	71	569	4	73	293
4	79	317	2	83	167	2	89	179	4	97	389
8	101	809	10	103	1031	8	107	857	10	109	1091
2	113	227	4	127	509	2	131	263	8	137	1097
4	139	557	8	149	1193	10	151	1511	10	157	1571
4	163	653	14	167	2339	2	173	347	2	179	359
10	181	1811	2	191	383	4	193	773	38	197	7487

In the table above, the values $N = 6$ and $N = 12$ are not shown because a prime of the form $\theta = 6p + 1$ would not satisfy condition one, For example, suppose $p = 5$ and $\theta = 31$, let $x = 1$, $y = 9$, and $z = 81$. None of these three integers is equal to $0 \pmod{31}$, but, $1^5 + 9^5 + 81^5 = 3486843451 = 112478821 \cdot 31 \equiv 0 \pmod{31}$ Meaning that integers x, y, z with $p = 5$ and $N = 6$ violate Germain's first condition which states: $x^p + y^p + z^p = 0 \pmod{\theta}$ implying that $x = 0$ or $y = 0$ or $z = 0 \pmod{\theta}$. The table and the argument were taken from [8].

5.2.2 Demonstarting the proof for p by using an example:

for Fermat's Equation: $x^p + y^p + z^p = 0 \pmod{11}$, if we factorize $(-x^5) = (y^5 + z^5) = (y + z)(y^4 - y^3z + y^2z^2 - ... + z^4)$ as before, the two factors are relatively prime because we assumed that x, y, z are pairwise coprime and none of them are divisible by 5, then both factors must be individually 5^{th} power residues by unique factorization. The same argument applies to the factorization of $-y^5$ and $-z^5$, and so we have integers m, j, k and a,b,c such that:

$$\begin{array}{ll} y + z = m^5 & y^4 - y^3z + y^2z^2 - yz^3 + z^4 = a^5 \\ z + x = j^5 & z^4 - z^3x + z^2x^2 - zx^3 + x^4 = b^5 \\ x + y = k^5 & x^4 - x^3y + x^2z^2 - xy^3 + y^4 = c^5 \end{array}$$

and we have $-x^5 = m^5a^5$ which implies that $-x = ma$. Similarly we have, $-y = jb$ and $-z = kc$. Now if we look at the 5^{th} power integers $\pmod{11}$ for $x = 0, 1, 2, ..., 10$, we find the 5^{th} power residues $\pmod{11} = 0, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1$, so the 5^{th} power of an integer must be $0, \pm 1 \pmod{11}$ by using an alternate proof without the assumption from theorem 2 about θ, and according to the condition of the proof we can only have a solution of $x^p + y^p + z^p = 0$ if one of the numbers x, y, z is a multiple of 11, because if not, then all three of these will be $\pm 1 \pmod{11}$, and adding the three such values up to zero is impossible. There fore, 11 divides only one of x, y, z. Since the three variables are symmetrical, we can assume that one of them, let's say $x \equiv 0 \pmod{11}$, but we have:

$$2z = (z - y) + (z - x) + (x + y) = m^p + j^p + k^p \equiv 0 \pmod{q} \equiv 0 \pmod{11}.$$

We have three 5^{th} powers adding up to $0 \pmod{11}$ and again as before, one of the three numbers m, j, k must be a multiple of 11. Since $z = ma \equiv 0$, then 11 doesn't divide j nor k because that would imply that x or y are divisible by 11 which contradicts the assumption that x, y, z are realatively prime. This leads us to conclude that it can only be m. But, if we say $11 \mid m$, then that also contradicts the assumption because if $m = x + y \equiv 0 \pmod{11}$ then we get $x \equiv -y \pmod{11}$ and substituting in the first equation, yeilds $a^5 \equiv 5y^4 \pmod{11}$, and $c^5 \equiv y^4 \pmod{11}$. If we combine the two preceeding equations, we get: $a^5 \equiv 5c^5 \pmod{11}$ and this is impossible because all $5^t h$ powers modulo 11 are $0, \pm 1$. We can also rule out $a = c \equiv 0 \pmod{11}$ because $z = -kc$, and we know that $11 \nmid z$, which completes the example [8].

5.3 Sophie Germain's Theorem and proof to solve FLT for p^2:

The following results are from [1], some from [2], and some from [6]

Germain later extended her proof to include p^2 instead of just p using the theorem:

Theorem 3. *for an odd prime exponent p, if there exists an auxiliary prime q such that:*

1. *there are no two nonzero consecutive p^{th} powers mod q and,*

2. $x^p \neq p \pmod{q}$ *for all* $1 \leq x \leq q-1$, *then in any solution to the Fermat equation* $z^p = x^p + y^p$, *one of* x, y, *or* z *must be divisible by* p^2 *, and* FLT_1 *is true for p [6, p-9].*

The nonconsecutivity condition, will be referred to as C_1 and for the second condition, p not being a p^{th} power residue will be reffered to as C_2.

Lemma 2. *There are no consecutive* p^{th} *power residues* $\pmod{q}$ *if and only if* $x^p + y^p + z^p \equiv 0 \pmod{q}$, *then* x, y, *or* $z \equiv 0 \pmod{q}$.

Proof. To see that this lemma is true, we construct the following short proof: Suppose that: $x^p + y^p + z^p \equiv 0 \pmod{q}$ has a solution and suppose that none of x, y, z are divisible by q. Equivilantly, $x^p + y^p \equiv -z^p \equiv -z^p \pmod{q}$, and suppose that none of the integers are congruent to $0 \pmod{q}$. Multiplying both sides by $(x^{-1})^p$ gives the congruence:

$$1 + (y/x)^p = (z/x)^p$$

Thus the residues of $(y/x)^p$ and $(z/x)^p$ are consecutive non-zero p^{th} power. This proof shows both directions by contraposition. Assume that we have consecutive p^{th} powers, $1 + h^p \equiv o^p \pmod{q}$ where none of the elements is equal to zero. This shows that the residues of h^p and o^p will be consecutive which contradicts C_1. If we multiply both sides by g^p for g some primitive root $\pmod{q}$, we find a nontrivial solution to $g^p + (hg)^p + (og)^p \equiv 0 \pmod{q}$. None of them are equal to zero and all are p^{th} powers which contradicts C_2. □

Now to prove Theorem 3 above:

Proof. Let's assume that x, y and z are all coprime and that $x^p + y^p = z^p$ and that p does not divide xyz, then we have:

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

Now let $f(x, y)$ represent the right-hand expression on the first line. If some prime $q \neq p$ divides both $(y+x)$ and $f(x, y)$, then $y \equiv -x \pmod q$, by definition of $q \mid x + y$ and by substituting in $f(x, y)$, we get: $px^{p-1} \pmod q$, which is divisible by q by assumption. x must be divisible by q, since q doesn't divide p. This means that x and $x + y$ are divisible by q which implies that y is divisible by q contradicting the assumption that x and y are relatively prime. Thus no prime other than p can divide both $x+y$ and $f(x, y)$. The same can be seen for the second and third pairs of numbers, using; if q divides $z-y$ then, $z \equiv y \pmod q$, and similarly for x where $z \equiv x \pmod q$. Now we use the claim from the theorem that p must divide one of x, y, or z. Under the assumption that x, y, and z are all coprime with p, we let $z = ma$, $x = jb$, and $y = kc$, and now we have the following equations:

$$x + y = m^p \text{ and } x^{p-1} - x^{p-2}y + x^{p-3}y^2 - ... + y^{p-1} = a^p$$

$$z - y = j^p \text{ and } z^{p-1} + z^{p-2}y + z^{p-3}y^2 + ... + y^{p-1} = b^p$$

$$z - x = k^p \text{ and } z^{p-1} + z^{p-2}x + z^{p-3}x^2 + ... + x^{p-1} = c^p$$

We show that for each pair of numbers above, p is the only prime divisor they have in common. Looking at line (8) explains why $x + y = m^p$, with no a factors, and $f(x, y) = a^p$, with no m factors because if otherwise, the left and right numbers would not be coprime. We can see that $(x+y) \neq m^k$ for any $k \neq p$, and we have $f(x, y) = a^p$. The other two equations follow suit. Now from the lemma 2 above, we assume that $q \mid z$ then $q \mid 2z$, so $2z = (z - y) + (z - x) + (x + y) = j^p + k^p + m^p \equiv 0 \pmod q$. Now: $m^p + j^p + k^p \equiv 0 \pmod q$ then either m, j, or k is divisible by q by the Lemma above. If either j or k were divisible by q , using that $y = z - j^p$ and $x = z - k^p$ from equations 5 and 6, and that $q \mid z$, then either y or x, respectively, would be divisible by q too. This is a contradiction to the assumption that x, y, and z are all coprime. Thus, it must be that $q \mid m$. $x + y = m^p$, so this implies that $y \equiv -x \pmod q$. We also have that $f(x, y) \equiv px^{p-1} \equiv a^p \pmod q$, as shown above. Since $z \equiv 0 \pmod q$ by assumption, $z - x = k^p \equiv -x \pmod q$. So x must be a p^{th} power residue $\pmod q$. Now to use $px^{p-1} \equiv a^p \pmod q$ to substitute it in k^p for x, yields $p(k^{p-1})^p \equiv a^p$. Recalling that $q \nmid x$, and since $q \mid z$ by assumption and x and z are coprime implies that p is also a p^{th} power residue $\pmod q$. This contradicts C_2, hence $p \mid x, y$, or z.

We now assume that $p \mid z$ and setting $z = map$. Now, $x + y = m^p p^{p-1}$ and $f(x, y) = pa^p$, $x = jb$ and $y = kc$ because x and y are still coprime to p, and since $z^p = (x + y)f(x, y)$ must be divisible by p^p, it suffices to show that $f(x, y)$ is divisible by p but not by p^k for all $k > 1$. $f(x, y) = \frac{y^p + x^p}{x+y}$. Let $s = x + y$ yielding:

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

Every term but the last in the above sum is divisible by p^2. Since p divides $s = x + y \equiv x^p + y^p \equiv z^p \pmod p$, by FLT_l. The last term is divisible by p, since x is relatively prime to p. So $f(x, y)$ is divisible by p too. Using the equations above, $2z - (x + y) = 2z - x - y = m^p + j^p$; implies that $p \mid (m^p + j^p)$, since p divides both z and $x + y$. Moreover, $p \mid (m + j)$, by FLT_l, $m \equiv -k \pmod{p}$, which implies that $m^p \equiv j^p \pmod{p^2}$. To clarify this, we write $m = -j + tp$, where $t \in Z$. $m^p = (-j + mp)^p = -j^p + j^{p-1}p^2t - ... + (tp)^p \equiv -j^p \pmod{p^2}$, since p^2 divides all terms except for $-j^p$. $x+y = m^p p^{p-1}$ was shown, so $p^2 \mid (x+y)$, and we just showed above that $p^2 \mid j^p + k^p$. We also know that $2z = j^p + k^p + (x + y)$, and therefore $p^2 \mid z$ proving the theorem on exponent p^2. □

5.3.1 An example where C_1 works:

> If a solution of FLT with $p = 5$ existed, then x, y, z have to be divisible by 5. The theorem was generalized to other powers, and Sophie Germain gave a general theorem which helped proving FLT for all prime numbers, $p < 100$ in case 1. [10]

Germain's work on FLT took years of research, most of it was solo, but she discussed her results mostly with Gauss sporadically. We are back to the example $p = 5$ that we discussed briefly earlier, but with a little more depth. So let's take a look at case $p = 5$, $N = 1$, and $\theta = 2Np + 1 = 2 \cdot 1 \cdot 5 + 1 = 11$ and $1 \leq N \leq 10$. The non-zero 5^th

power residues $\pmod{11}$ are: $1^5, 2^5, 3^5, 4^5, 5^5, 6^5, 7^5, 8^5, 9^5, 10^5$

$$= 15, 25, 35, 45, 55, 65, 75, 85, 95, 105 \pmod{11}$$
$$= 1, 32, 243, 1024, 3125, 7776, 16807, 32768, 59049, 100000 \pmod{11}$$
$$= 1, 10, 1, 1, 1, 10, 10, 10, 1, 10 \pmod{11}$$
$$= 1, 10 \pmod{11}$$

We see that the only 5^{th} power residues modulo 11 are 1 and 10, and these two integers are not consecutive. Hence $\theta = 2Np + 1 = 11$ satisfies the C_1 relative to 5. If we try the same method for $N = 2, 3, ..., 10$, we get:

$N = 2$ involves $\pmod{21}$, but 21 is not prime.

$N = 3$ has 5^{th} power residues $1, 5, 6, 25, 26, 30 \pmod{31}$ and this set fails the non-consecutive residue condition. In fact, it can be shown that the condition for non-consecutive power residues will fail whenever N is a multiple of 3.

$N = 4$ has 5^{th} power residues $1, 3, 9, 14, 27, 32, 38, 40 \pmod{41}$ and this set has no consecutive elements.

$N = 5$ involves $\pmod{51}$, but 51 is not prime.

$N = 6$ is a multiple of 3.

$N = 7$ has residues $1, 20, 23, 26, 30, 32, 34, 37, 39, 41, 45, 48, 51, 70 \pmod{71}$ and this set has no consecutive elements.

$N = 8$ involves $\pmod{81}$, but 81 is not prime.

$N = 9$ is a multiple of 3.

$N = 10$ has residues $1, 6, 10, 14, 17, 32, 36, 39, 41, 44, 57, 60, 62, 65, 69, 84, 91, 95, 100 \pmod{101}$ and this set has non-consecutive elements.

According to this example, the auxiliary primes that satisfy C_1 for the 5^{th} power residues are: $11, 41, 71$, and 101, corresponding to $N = 1, 4, 7$, and 10 and if 5 is not one of the p^{th} powers residues, then C_2 is also satisfied. Germain stated in her theorem that if C_1 and C_2 are satisfied, then each one of $11, 41, 71$, and 101 would have to divide either x, y, or z. In other words, x, y, or z would have to each be multiples of at least one of these auxiliary primes [8].

5.3.2 An example where C_1 does not work:

We will still consider the prime $p = 5$, but now we are going to demonstrate the result by choosing $\theta = 7$. The $5^t h$ power residues $\pmod 7$ are:

Table 3: 5^{th} power Residues modulo 7

N	N^5	$N^5 \pmod 7$
1	1	1
2	32	4
3	243	5
4	1024	2
5	3125	3
6	7776	6

In table 3, the 5^{th} power residues modulo 7 are $1, 2, 3, 4, 5, 6$. These integers are consecutive, hence $\theta = 7$ does not satisfy C_1 relative to 5 [2].

5.4 Sophie Germain's p^{th} power condition C_2:

The second condition of Sophie Germain's theorem is about whether the prime exponent p itself is a p^{th} power $\pmod \theta$ or not. We already discussed it's implication as C_2.

5.4.1 Cubic Residues for $p = 3$ where $\theta = 13$ and $\theta = 7$:

The cubic residues where $p = 3$, is a special case where the only auxiliary primes (θ) that satisfy the two conditions in Sophie Germain's theorem are 7 and 13 according to a letter that Germain sent Lagendre and it seems that she sent a short proof to Legendre. They will be demonstrated by the example in the table below: [6]

Table 4: Cubic Residues

N	N^3	$N^3 \pmod{13}$
1	1	1
2	8	8
3	27	1
4	64	12
5	125	8
6	216	8
7	343	5
8	512	5
9	729	1
10	1000	12
11	1331	5
12	1728	12

If we look for the cubic residues $\pmod{13}$ from table 4 above, we get:

$$8^3 \equiv 512 \pmod{13} \equiv 5 \pmod{13}$$

C_1 and C_2 of Sophie Germain's Theorem are met; the nonzero cubic residues $1, 5, 8, 12$ modulo 13 are not consecutive, and 3 is not one of the residues, meaning that the equation $x^p + y^p = -z^p$ has no solutions for which x, y, and z are relatively prime to p, where p does not divide x, y, or z. According to Germain, 7 and 13 are the only auxiliary primes θ where FLT_1 works for $p = 3$. Now for the auxiliary prime $\theta = 7$ dividing x, y, or z. Assume that $7 \nmid x, y$, or z:

$$\begin{aligned} x^3 + y^3 \equiv z^3 \pmod 7, a^3 \equiv \pm 1 \pmod 7, \\ 1^3 \equiv 1 \pmod 7, 2^3 \equiv 1 \pmod 7, \\ 3^3 \equiv -1 \pmod 7, 4^3 \equiv 1 \pmod 7, \\ 5^3 \equiv -1 \pmod 7, 6^3 \equiv -1 \pmod 7, \\ \pm 1 + \pm 1 \equiv \pm 1 \pmod 7 \end{aligned}$$

Which is impossible and FLT_1 holds for the auxiliary prime $\theta = 7$ relative to $p = 3$ [6].

6 Theorem on large-sized solutions:

A theorem that she worked on to prove that any possible solution was infinite, ”so large it frightens the imagination” [6,]:

Theorem 4. *For an odd prime p, if the equation $x^p + y^p = z^p$ is satified in integers, then one of the numbers $x + y$, $z - x$, or $z - y$ must be divisible by p^{2p-1} and by the p^{th} power of all primes of the form $2Np - 1$ which satisfy the two conditions: That there aren't two consecutive non-zero p^{th} power residues $\pmod{2Np + 1}$ and p is not a p^{th} power residue $\pmod{2Np + 1}$ [6, p-42].*

Germain's claim in her key theorem would therefore suggest that for any solution to $x^5 + y^5 = z^5$, then the numbers $x + y, z - x$, or $z - y$ must be divisible by $5^9 (whichisp^{2p-1})$ as well as by $115, 415, 715$, and 1015 (which are the auxiliary primes of $p = 5$ raised to the 5^{th} power). In other words, the numbers $x + y, z - x$, or $z - y$ must be divisible by the product

$59{\cdot}115{\cdot}415{\cdot}715{\cdot}1015 = 691, 053, 006, 763, 356, 095, 514, 121, 490, 614, 455, 078, 125.$

This 39 digit number is a number whose size can frighten anyone [2]

6.1 Grand plan to solve FLT for the ∞:

Germain went on to say in her letter to Gauss,

> ...I have never been able to arrive at the ∞, although I have pushed back the limits quite far by a method of trials too long to describe here. I still dare not to assert that for each value of p, there is no limit beyond which all numbers of the form $2Np + 1$ have two consecutive p^{th} power residues in the sequence of the natural numbers. This ... which concerns the equation of Fermat.You can easily imagine, Monsieur, that I have been able to prove that this equation is not possible except for numbers whose size ... because it is also subject to many other conditions which I do not have the time to list because of the details necessary for establishing its success. But all that is still not enough; it takes the infinite and not just the very large. [6, p-23]

Here, Germain explained her grand plan to prove FLT. It requires finding an infinitely many auxiliary primes each satisfying C_1 for a given exponent p. She illustrated that the existence of infinitely many auxiliary primes θ would make the Fermat's equation impossible.

6.2 Failure of Germain's Grand Plan:

Germain's most desired grand plan and goal was to prove that for each odd prime exponent p, there is an infinte number of auxiliary primes of the form $2Np + 1$ such that the set of nonzero p^{th} power residues satisfies C_1 of her theorem. As mentioned above, Germain observed that if there was such a solution to FLT, then any auxiliary prime would have to divide x, y, or z. If that was the case and if x, y, and z were solutions to Fermat's equation for that exponent p, then each of the infinitely many auxiliary primes must divide one of x, y, or z. Looking at the three subsets of auxiliary primes consisting of those that divide x, those that divide y, and those that divide z, at least one of these subsets must itself be infinite. But that would mean that one of the integers x, y, or z would be a multiple of an infinite number of primes, which is impossible, and hence Fermat's equation could have no solutions for that exponent p. However, as Germain admitted to Gauss, she was unable to establish the existence of an infinite number of auxiliary primes.

"...I have never been able to arrive at the ∞..." [6, p-23]

It was proven later that for each odd prime p there are only a finite number of auxiliary primes that satisfy C_1 which showed how Germain's grand plan failed. On the other hand, it appears that Germain knew of the reason for her grand plan failure because at some point, she sent a letter to Legendre proving that for $p = 3$, there exists a finite number of auxiliary primes not an infinite number of them that satisfy C_1. The same results were acheived in this paper, some of auxiliary primes for a specific prime exponents satisfied C_1 and some ot them did not. Also, for the other examples, there are many auxiliary primes, but only two of those could satisfy Germain's conditions as when $p = 3$, only $\theta = 7$, and $\theta = 13$ satisfied Germain's conditions.

This attempt to prove FLT for infinitely many prime exponents rather than on a case by case basis was a brand new approach which revolutionalized the approach to proving FLT. Germain's work and efforts made it possible for other mathematicians to keep going and build the proof all through history after her all the way to Wiles.

7 Conclusion:

The subject of Sophie Germain's contribution to mathematics is a vast one. The only commonly known result of Germain's approach appeared in 1825, as part of a supplement to the 2^{nd} edition of Legendre's $Theory\ of\ Numbers$ presenting his own proof for $p = 5$ case along with part of Germain's work, which he credited to her in a footnote. This anonymity changed when manuscripts detailing her corespondence with other mathematicians were discovered later. She was not a recognized mathematician and even after her death, the epithet on her tombstone did not recognize her as a mathematician. She died in 1831 at the age of 55 of breast cancer. She died shortly before she was to receive an honorary doctor's degree from the University of Gottingen under the insistence of Gauss. The Italian mathmetician Libre wrote an intimate obituary for her that also served as a biography. Germain taught herself everything she needed to be able to correspond with the well-known mathematicians of her day. Determined, she battled against the barriers created against women in her day. We know most of her proofs from letters she sent her contemporary mathematicians like Lagrange, Legendre, and Gauss. Legendre was the one who started her on the path of being recognized when he credited to her what we now know as Sophie Germain Theorem which led to solving Fermat's

Last Theorem. The world of Cryptography benefited from what was discovered along the journey to prove FLT building on Germain's discoveries until Wiles in 1995 [11]. I chose her work to focus on because she was a fighter and she did what she felt was right even though the odds were against her, but she presisted and prevailed. Sophie Germain became better known after her death as the case was with many brilliant people who passed on unrecognized.

References

[1] Colleen Alkalay-Houlihan, *Sophie Germain and Special Cases of Fermat's Last Theorem./* `http://www.math.mcgill.ca/darmon/courses/12-13/nt/projects/Colleen-Alkalay-Houlihan.pdf` on Tuesday 3/27/18 at 4:53pm.

[2] Lene-Lise Daniloff. *The Work of Sophie Germain and Niels Henrik Abel on Fermat's Last Theorem* Master's Thesis, Spring 2017, University of Oslo downloaded on Wednesday June 14th, 2018 from: `https://www.duo.uio.no/handle/10852/57807`

[3] Perl, Teri. *Math Equals:Biographies of Women Mathematicians + Related Activities*. Menlo Park: Addison-Wesley Publishing, 1978

[4] Ribenboim, Paulo. *Fermat's Last Theorem for Amateurs,* Springer-Verlag, 1999. (Chapter 4 is about Germain's Theorem)

[5] Nagell, T. *Fermat's Last Theorem* §*68 in Introduction to Number Theory.* New York: Wiley, pp. 251-253, 1951.

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

[7] Weisstein, Eric W. *Fermat's Last Theorem.* From MathWorld.

[8] L. Riddle, *Sophie Germain and Fermat's Last Theorem,* Agnes Scott College, 2009.

http://www.agnesscott.edu/Lriddle/women/germain-FLT/SGandFLT.htm on Tuesday 3/27/18

[9] A. Ganville and M. Monogan,*Transactions of the American Mathematical Society* , Vol 36, No. 1, March, 1988. http://www.ams.org/journals/tran/1988-306-01/S0002-9947-1988-0927694-5/S0002-99 Friday 4/13/18

[10] A. D. Aczel, *Fermat's Last Theorem, Unlocking the Secret of An Ancient Mathematical Proble* Dell Publishing, (p-56), New York, 1996

[11] Professor Raymond Flood, *Gauss and Germain Transcript.* http://www.gresham.ac.uk/lecture/transcript/download/gauss-and-germain/ Date: Tuesday, 16 February 2016 - 1:00PM, Location: Museum of London

[12] Fermat's Image. https://en.wikipedia.org/wiki/Pierre de Fermat. Date:12/7/2018

[13] Hill, Amy Marie(1995), *Sophie Germain: A Mathematical Biography* https://core.ac.uk/download/pdf/36683994.pdf on Tuesday 3/27/18

[14] Sophie Germain's Image. https://en.wikipedia.org/wiki/Sophie Germain. December 8th, 2018