On the proof of Sophie Germain's theorem

An extended essay in mathematics

RQ: What is the proof of Sophie Germain's theorem?

Word count: 2883

Redacted version (pg. 1 -11 only)

Contents

1 Introduction

1.1 Overview of the essay

> *"It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."* -Pierre de Fermat, (Heath, 1910)

This extended essay in mathematics is a proof of Sophie Germain's theorem. This essay will prove, analyze, and evaluate the statement of the divisibility of solutions to the equation $\boldsymbol{x^p + y^p = z^p}$, also known as Fermat's Last Theorem, for all odd prime integers $\boldsymbol{p}$.

The proof of Sophie Germaine's theorem proved to be a seminal event in mathematical research, bringing mathematicians one step closer to the proof of what came to be known as Fermat's Last Theorem. Sophie Germain, using her cleverness and ingenuity, proved herself to be a great mathematician in an era where professional woman mathematicians were practically nonexistent.

After the introduction, the key terminology and concepts are introduced and defined. The two most important theorems covered in this essay, Sophie Germain's theorem and Fermat's last theorem, are defined and explained in the next section of the essay, whilst the main body contains the proof of Sophie Germain's theorem, building from propositions and proving them. Following the proof, the problem will be restated and the resulting conclusions drawn, along with further investigation ideas. In this essay, a historical perspective will also be outlined in respective sections to provide the context of the theorems and the people involved, for a deeper understanding.

While Fermat's last theorem has never ceased to fascinate me, I found it to be beyond my mathematical capabilities to fully comprehend or prove. After a lot of careful research, I found recluse in Sophie Germain's theorem, as it was an equally fascinating slice of mathematics and mathematical history. From there it all began.

For simpler navigation, terms Fermat's Last Theorem and Sophie Germain's theorem will hereafter be found in their respective abbreviated forms, FLT and SGT.

1.2 Definition of key terms

Auxiliary primes are prime numbers which satisfy the form $\theta = 2Np + 1$, where $N \in \mathbb{Z}^+$, and p is a prime number.

Germain primes are primes (of the same form) where p is a prime, but without the factor N, $\theta_G = 2p + 1$.

Greatest common denominator, *gcd*, of any two or more positive integers is the highest integer which evenly divides into every of the two or more positive integers.

Fermat's Little Theorem states that, if p is a prime and a an integer, then $a^p \equiv a \mod p$. This will not be proved in the essay, but will be used as such. (*Fermat's Little Theorem*, 1999).

Modular arithmetic is a type of integer arithmetic where numbers "wrap around" upon reaching a given fixed quantity, called the *modulus*. For a positive integer n, two integers x and y are congruent modulo n if their difference is a whole-number multiple of n. The notation used to represent this will be $a = b \pmod{n}$.

Table 1: Table showing the aforementioned primes

Auxiliary and Germain primes			
p	Auxiliary primes ($\theta = 2Np{+}1$)	p	Germain prime ($\theta = 2p + 1$)
3	7, 13, 19...	3	7
5	11, 31, 41...	5	11
7	29, 43, 71...	7	15
13	53, 79, 131...	13	$\xcancel{27} \implies$ not a prime!

2 Overview of the main theorems

2.1 Fermat's Last Theorem and its relevance

FLT is a mathematical theorem first proposed by *Pierre de Fermat* (1607-1665), an eminent French lawyer and mathematician.

While Fermat is best known for his work on light propagation, number theory, and calculus, he rose to fame posthumously with a conjecture he had scribbled on the book he was studying at the time - Diophantus's *Arithmetica*. Fermat, in the margin of his copy of the book, claimed that he had a proof of his conjecture which was too big to contain in the margin and named it a theorem, giving rise to the popular misnomer. Being one of the most notable and sought-after problems in mathematics, it officially became a theorem in 1994, three and a half centuries after Fermat conjectured it, when the British mathematician Andrew Wiles proved it. The proof of the theorem took almost all of the developments of the 20th-century mathematics, which were unavailable to Fermat, rendering his claim to have proven the theorem very unlikely.

If we let x, y, and z be distinct positive non-zero integers, FLT states that there are no integers n greater than 2 that can satisfy the equality relation of the equation:

$$x^n + y^n = z^n \tag{1}$$

How does one go about solving this theorem for all positive integers $n > 2$? Well, perhaps by proving individual cases n cases. For example, it is known that equation (1) has a working form for $n = 2$, namely the Pythagorean equation with Pythagorean triples (eg. $3^2 + 4^2 = 5^2$). These are called homogeneous Diophantine equations.

FLT proved to be a very lucrative, yet seemingly impossible, problem for successive generations of mathematicians, each knowing that the proof would engrave their name into

the annals of mathematics. One of those budding mathematicians was Sophie Germain, who became indulged in number theory and FLT. Not germane to her main research, she worked on FTL for years, failing to make progress. But that did not discourage Germain, who saw progress by developing a new approach where the exponent n is a specific prime number. Her research led to SGT, and it instigated new research on those specific prime numbers, which were later dubbed Germain primes.

2.2 Sophie Germain's theorem

Let p be an odd prime ($p > 2$), such that $2p + 1$ is also a prime, and let x, y, and z be integers which are non-divisible by p (leaving a remainder when divided by p). Sophie Germain's theorem then asserts that $x^p + y^p$ cannot equal z^p.

This theorem has been proved using many ways and techniques, most of which require knowledge of graduate-level mathematics. Adrien-Marie Legendre, a French contemporary mathematician, demonstrated her proof more concisely in 2 parts, which was more rigorous and understandable, thus this work will focus on this proof. He split the problem into two parts:

- **Part I:** $x^p + y^p \neq z^p$ if x, y, and z are non-divisible by p
- **Part II:** $x^p + y^p \neq z^p$ if one, and only one of x, y, or z is divisible by p (leaving no remainder)

These parts are an equivalent way of saying (*Sophie Germain and Fermat's Last Theorem*, 2009):

- **Part I:** $x^p + y^p + z^p = 0 \pmod{\theta} \implies$ either $x = 0 \pmod{\theta}$, $y = 0 \pmod{\theta}$ or $z = 0 \pmod{\theta}$
- **Part II:** $x^p \neq p \pmod{\theta}$

The original statement was first conjectured by Sophie Germain, in a letter to Gauss in 1819 (Singh, 1997). In 1825 her lengthy proof was confirmed by Dirichlet and Legendre, making this her greatest contribution to mathematics.

Although her "grand plan" to prove FLT bore no fruits, using her ingenuity, she proved this theorem along the way.

3 A historical perspective

3.1 Sophie Germain

Sophie Germain (1776-1831) was a French mathematician and scientist (Hill, 1995).

Germain was born into a wealthy family. The daughter of a politically active merchant father, she had a social status right from the start. Although little is known about her early childhood, she was most likely educated at home when her interest in mathematics had sparked. During the French revolution, she kept to herself in her father's expansive library, reading mathematics books and self-educating. Destined to become bourgeois, she resented everyone's disapproval of her allegedly useless career path plan - professional (female) mathematician, in an era of when chauvinism was prevalent. After going as far as to learn Latin just to read the historical mathematical texts, she quickly exhausted her father's library and was ready for a bigger challenge. Coming as her great disappointment, she was not able to enroll in newly opened *École Polytechnique* in Paris purely on the basis of her gender. But nothing was able to stop this budding mathematician, who signed up under the pseudonym of *Antoine-August Le Blanc*, thereby bypassing the arbitrary rule. She prospered in her studies, and quickly became praised because of her talents, but felt that she needed to prove herself in her major fields of interest - number theory and FLT.

3.2 The development of Sophie Germain's theorem

It is known that countless mathematicians worked on FLT, including the brightest minds of generations, but most of their work was futile. Moreover, many have made small progress, but no one could prove it in whole.

Fermat, still under the ruse of having a complete proof, published a proof for $n = 4$

using infinite descent (a type of proof by contradiction) to show that there are no whole-number solutions to the area of a right triangle with whole-number side lengths. Other proofs showing FLT cannot be true for $n = 4$ were later developed as well.

Leonhard Euler, the brilliant Swiss mathematician and scientist, gave a complete proof of FLT for $n = 3$ in a letter to Christian Goldbach. In it, he as well used the method of infinite descent.

By the time Germain came into the scene, proofs for $n = 3$ and $n = 4$ had been known. In her brilliance, Germain had a sophisticated plan, "grand plan", which she outlined to Gauss of how to tackle FLT (Laubenbacher & Pengelley, 2010). She had a plan to prove FLT for a whole set of numbers, and not just a fixed exponent.

Her plan was as follows: prove that for every odd prime exponent p, there has to be an infinite amount of auxiliary primes of form $\theta = 2Np + 1$, such that the set of positive p-th power residues $x^p \pmod{2Np+1}$ does not contain any consecutive integers (*Sophie Germain and Fermat's Last Theorem*, 2009). This statement has a very powerful implication; if there are integers solution p to $x^p + y^p = z^p$, then all of auxiliary primes of p-th power residue condition would have to divide in either one of x, y or z.

For example, let us consider the case when $p = 3$. For the first case, N will be set to 1. The set of 3-rd powers is as follows: $\{1^3, 2^3, 3^3, 4^3, 5^3, 6^3, 7^3, 8^3, 9^3, 10^3\}$. Calculating the numbers, the set looks like this: $\{1, 8, 27, 64, 125, 216, 343, 512, 729, 1000\}$.

Now we take a look at the 3-rd power residues of mod 7 ($\theta = 2Np + 1 = 2 \times 1 \times 3 + 1 = 7$) of this set: $\{1, 8, 27, 64, 125, 216, 343, 512, 729, 1000\} \pmod 7$ and get a new set $\{1, 1, 6, 1, 6, 6, 0, 1, 1, 1, 6\}$. The unique elements of this set can be seen here: $\{0, 1, 6\}$. Even though 7 is a prime, 7 cannot be an auxiliary prime when $p = 3$ because this set contains consecutive residues (0 and 1).

Keeping $p = 3$ and enumerating N from 1 to 10, we arrive at different residue sets:

- **$N = 2$**, $\{1, ..., 1000\} \pmod{13}$ has unique residues $\{1, 5, 8, 12\} \implies$ 13 is an auxiliary prime for $p = 3$
- $N = 3$, $\{1, ..., 1000\} \pmod{19}$ has unique residues 8 and 7 which fail the consecutive condition
- $N = 4$, $\{1, ..., 1000\} \pmod{25}$, but 25 is not a prime
- $N = 5$, $\{1, ..., 1000\} \pmod{31}$ has unique residues 1 and 2
- $N = 6$, $\{1, ..., 1000\} \pmod{37}$ has unique residues 26 and 27
- $N = 7$, $\{1, ..., 1000\} \pmod{43}$ has unique residues 41 and 42
- $N = 8$, $\{1, ..., 1000\} \pmod{49}$, but 49 is not a prime
- $N = 9$, $\{1, ..., 1000\} \pmod{55}$ but 55 is not a prime
- **$N = 10$**, $\{1, ..., 1000\} \pmod{61}$ has unique residues $\{1, 8, 27, 3, 33, 38, 24, 58, 24\} \implies$ 61 is an auxiliary prime for $p = 3$

From this example we can observe that primes 13 ($N = 2$) and 61 ($N = 10$) are auxiliary primes for when $p = 3$. According to Sophie Germain, if there are any solutions to $x^3 + y^3 = z^3$, either one of x, y or z has to be a multiple of 13 or 61. Germain asserted that there are infinitely many auxiliary primes for every odd prime p such that there are no consecutive p-th power residues.

Although her "grand plan" was later shown to be unable to prove FLT by Guglielmo Libri, her breakthroughs formed the principles of SGT.

4 The proof of Sophie Germain's Theorem

4.1 Proposition 1

Suppose x and y are co-primes (the only positive integer that divides both x and y is 1) and suppose p is an odd prime (*Sophie Germain and Fermat's Last Theorem*, 2019). This would imply the following:

$$gcd\Big(x+y, \frac{x^p+y^p}{x+y}\Big) = p = 1 \tag{2}$$

Proof: We can observe that $\frac{x^p+y^p}{x+y} = \frac{(x+y-y)^p+y^p}{x+y}$, and we can see that, if we rearrange the numerator, we can get $x^p+y^p = (x+y-y)^p+y^p$.

Using binomial expansion on $(x+y-y)^p$ we get:

$\binom{p}{0}(-y)^p(x+y)^0 + \binom{p}{1}y^{p-1}(x+y)^1 - \binom{p}{2}y^{p-2}(x+y)^2 - \binom{p}{3}y^{p-3}(x+y)^3 + \cdots + \binom{p}{p}(x+y)^p$

Putting the expansion into the original equation, we get the following:

$= \dfrac{\binom{p}{0}(-y)^p(x+y)^0 + \binom{p}{1}y^{p-1}(x+y) - \binom{p}{2}y^{p-2}(x+y)^2 - \binom{p}{3}y^{p-3}(x+y)^3 + \cdots + (x+y)^p + y^p}{x+y}$

$= \dfrac{-y^p + py^{p-1}(x+y)^1 - \binom{p}{2}y^{p-2}(x+y)^2 - \binom{p}{3}y^{p-3}(x+y)^3 + \cdots + (x+y)^p + y^p}{x+y}$

$= py^{p-1} - \binom{p}{2}y^{p-2}(x+y) - \binom{p}{3}y^{p-3}(x+y)^2 + \cdots + (x+y)^{p-1}$

which implies that $gcd\Big(x+y, \frac{x^p+y^p}{x+y}\Big)$ divided by py^{p-1} is an integer. Because x and y are co-primes, we can see that both $x+y$ and py^{p-1} are co-prime, therefore the gdc has to be 1.