2013

Fermat's Last Theorem

Rozalyn N. Miner
University of Redlands

Fermat's Last Theorem

Rozalyn N. Miner
Advisor: Tamara Veenstra
Committee:
Janet Beery
Rick Cornez
Steven Morics

University of Redlands
Mathematics Department
Spring 2013

Fermat's Life and His Last Theorem

Throughout history, math has been transformed, theorems have been proven, and great people have become known through their discoveries. One of these great people was Pierre Fermat, who studied law at the University in Orleans [11]. Through his work as a government official and the office he held there, he was able to change his name to Pierre de Fermat. There is controversy as to when Fermat was actually born. Most historians say that he was born in 1601, but through research Klaus Barner, a professor at University of Kassel, Germany, found that Fermat was most likely born in 1607. This comes from documents showing that a boy with the name of Pierre with one 'r' was born to Fermat's father in 1601. Other documents show that this son died a few years after his mother. After Fermat's father remarried his wife had five children and one of them was the Pierre Fermat that we know of today. Through Fermat's death records we know he died in 1665 at the age of 57, it can be shown that "he was born between January 13, 1607, and January 12, 1608, and most probably in 1607" [8]. Now that the matter of Fermat's birth is addressed, let us focus on his life.

Fermat had many people he was in contact with in the world of mathematics. Some of these people were friends and others became enemies of his work. Some of his many contacts in the math field were Jean Beaugrand, who is known for his works in geostatics; Pierre de Carcavi, who is known more for his correspondence with other mathematicians; Marin Mersenne, who is known for his work in number theory; Gilles Roberval, who is known for his early work in integration; Etienne Pascal, the father of Blaise Pascal; Rene Descartes, who is known for his application of algebra to geometry; and Blaise Pascal, who is known for his theory of probability [11]. That is a long and prestigious list of men in the math, science and philosophical areas of study.

Fermat was not very interested in the "physical applications of mathematics," but he liked proving geometrical theorems much more [11]. He also would look at other mathematicians' works and would comment on them. Even in the world of mathematics there is drama and sabotage. One of the mathematicians that Fermat upset was Rene Descartes. Fermat was asked to give his opinion on Descartes' *La Dioptrique*, and he said that Descartes was "groping about in the shadows" [11]. Fermat said that Descartes did not deduce his law of refraction correctly because it was inherent in his assumptions, and to say that Descartes was upset is a huge understatement [11]. In retaliation, "Descartes attacked Fermat's method of maxima, minima and tangents" and there were other mathematicians involved in the argument. This included Roberval and Etienne Pascal. Also, Girard Desargues, a geometer, was asked to participate in the role of referee [11]. Eventually Fermat proved that his method was correct and Descartes finally admitted that "... seeing the last method that you use for finding tangents to curved lines, I can reply to it in no other way than to say that it is very good and that, if you had explained it in this manner at the outset, I would have not contradicted it at all" [11]. Descartes had a lot of sway in the mathematical world in his time, and because of that he was able to damage Fermat's reputation [11].

We have come to the end of our brief history on this mathematician, and all that is left to say is an assessment that describes the type of person that Pierre de Fermat was known as, "Secretive and taciturn, he did not like to talk about himself and was loath to reveal too much

about his thinking... His thought, however original or novel, operated within a range of possibilities limited by that [1600-1650] time and that [France] place" [11].

An Introduction to Fermat's Last Theorem

We will now talk about Fermat's Last Theorem. Fermat was a different sort of mathematician because he was thought of as an amateur mathematician. This is because he was first a lawyer and then a mathematician [12]. When Fermat was not "sentencing priests to be burnt at the stake," he was using his spare time to work on his passion, mathematics [15]. In fact, Fermat is known as the prince of amateur mathematicians [15].

With that is mind, it is interesting that Fermat is thought of as one of the most famous number theorists who ever lived. Not only that, Fermat's Last Theorem is one that has a long and intense history because Fermat merely stated it without any proof. Fermat would not publish any of his work and because of this his friends became worried that his work would be forgotten forever [12].

After Fermat's death in 1665, his son Samuel collected everything that he could to make a publication of his father's work. This included letters, mathematical papers, and notes in the margins of books. This is how Fermat's Last Theorem became known and how eventually it became famous. Samuel found the note in the margins of Diophantus's *Arithmetica* next to Proposition II.8, and the note said,

> "But it is impossible to divide a cube into two cubes, or a fourth power [*quadratoquadratum*] into two fourth powers, or generally any power beyond the square into two like powers; of this I have found a remarkable demonstration. This margin in too narrow to contain it" [5].

The way that we denote this in modern terms is as follows:

$$x^n + y^n = z^n$$

has no non-zero integer solutions for x, y, and z when $n > 2$.

Even though Fermat stated that he had a proof to this conjecture, nobody has ever found his proof. In the study of mathematics the proof of a conjecture is everything. Even if a person is able to find a million cases in which a mathematical conjecture is true this does not prove all the cases therefore the conjecture could still be proven false. In the book Fermat's Enigma by Simon Sighn, the author states that "The search for a mathematical proof is the search for a knowledge that is more absolute than the knowledge accumulated by any other discipline" [15]. This is why Fermat's Last Theorem was attempted by so many mathematicians. The list includes people like Leonhard Euler, Sophie Germain, Adrien-Marie Legendre, Lejeune Dirichlet, Gabriel Lamé, Gerd Faltings, and finally Andrew Wiles.

The theorem was not proven until the 1990s by Wiles, and this was a major event in the history of math [12]. Wiles was able to give the mathematical community the knowledge that

they had wanted for so long. Through all of this history we will be able to see how Fermat's Last Theorem helped to develop Algebraic Number Theory. This puzzle of his Last Theorem took over three hundred years to prove. In the following pages we will specifically look at the n=4 and n=3 cases of Fermat's Last Theorem. This will bring in Pythagorean triples and Fermat's Method of infinite decent. We will also look to Euler for the proof of the n=3 case where there turns out to be a hole in his logic. This gap will have us take a look into Abstract Algebra, specifically rings. There will also be a look into the work that Sophie Germain with her theorem that proves Case I of Fermat's Last Theorem. We will also look at what recent research has shown about Germain's work with Fermat's Last Theorem. Lastly we will see where all of these components fall in the bigger picture of the mathematicians and concepts that finally proved Fermat's Last Theorem.

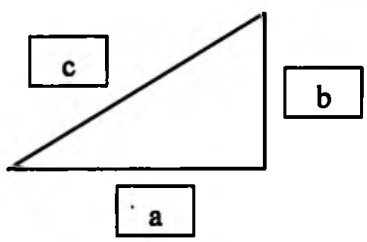
Pythagoras and Pythagorean Triples

To start proving the $n = 4$ case of Fermat's Last Theorem we must first look at Pythagorean Triples and the method to constructing them. This is because the $n = 4$ case is an extension of the equation, $a^2 + b^2 = c^2$. We know this to be the Pythagorean Theorem, and it is from here that we will look at who Pythagoras was and a proof of the Pythagorean Triples Theorem.

Pythagoras was born in Samos around 572 B.C. [4] where he was raised by his father Mnesachus, who came from Tyre as a merchant and his mother Pythais, who was a native of Samos [13]. Pythagoras created a secret society which had an inner circle of followers. These followers lived permanently within the Society, had no personal possessions, and were vegetarians. The followers were taught by Pythagoras and obeyed his rules. The Beliefs of Pythagoras were: "at its deepest level, reality is mathematical in nature, that philosophy can be used for spiritual purification, that the soul can raise to union with the divine, that certain symbols have a mystical significance, and that all brothers of the order should observe strict loyalty and secrecy" [13]. Pythagoras allowed men and women into his secret society. Members of the outer circle though, could live in their own houses, have possessions and did not have to be vegetarians. These members only came to the Society during the day [13].

In general we do not know very much about the work of Pythagoras, because his Society practiced secrecy and communalism which makes it difficult to determine which work is only that of Pythagoras. What is attributed to him are the following: The sum of the angles of a triangle is equal to two right angles, the Pythagorean Theorem, constructing figures of a given area and geometrical algebra, the discovery of irrationals, and the five regular solids. In astronomy Pythagoras thought that the Earth was a sphere at the center of the Universe [13].

As mentioned, Pythagoras is given credit for the Pythagorean Theorem which says that the square of the two sides of a right triangle equals the square of the hypotenuse and is written as $a^2 + b^2 = c^2$. This is shown in the following diagram of a right triangle.



One of the most basic triangles where the Pythagorean Theorem works is the one with sides 3-4-5. The following are examples:

$$3^2 + 4^2 = 5^2, \qquad 5^2 + 12^2 = 13^2, \text{and } 8^2 + 15^2 = 17^2$$

These triples of numbers 3-4-5, 5-12-13, and 8-15-17 are known as Pythagorean triples [14].

What is truly fascinating about triples is that they were around long before Pythagoras. In fact, 2500 years before Pythagoras the Babylonians knew that a triangle with sides 120, 119, and 169 was a right triangle. They also knew that the following are sides of right triangles and were most likely used as a table of trigonometric values [4].

4800	4601	6649
360	319	481
6480	4961	8161
2400	1679	2929
2700	1771	3229

It is important to mention that there are infinitely many integer solutions to Pythagorean triples. This is because if we take any Pythagorean triple (a, b, c) and multiply it by any number d then we have a new Pythagorean triple (da, db, dc) [14]. This comes from

$$(da)^2 + (db)^2 = d^2(a^2 + b^2) = d^2c^2 = (dc)^2.$$

Instead of focusing on all Pythagorean triples, we will only use what are called primitive Pythagorean triples. These are Pythagorean triples where (a, b, c) are pairwise relatively prime. A list of integers is known as pairwise relatively prime if *every pair* of the items in the list are relatively prime. Therefore, not only will the greatest common divisor of $(a, b, c) = 1$, but the $\gcd(a, b) = 1$, $\gcd(a, c) = 1$, and the $\gcd(b, c) = 1$ [3]. From this, at most one of (a, b, c) can be even in a Pythagorean triple. We will show below that exactly one of a or b must be even.

Pythagorean Triples Theorem: You will get every primitive Pythagorean triple (a,b,c) with a odd and b even by using the formulas:

$$a = s \cdot t, \qquad b = \frac{s^2 - t^2}{2}, \qquad c = \frac{s^2 + t^2}{2}$$

where, s and t are any odd integers with no common factors such that $s > t \geq 1$ [14]

We know that the formulas

$$b = \frac{s^2 - t^2}{2}, \qquad c = \frac{s^2 + t^2}{2}$$

are still integers. This is because s and t are both odd and when we add or subtract two odd numbers we get an even number. Therefore dividing an even integer by 2 will still result in an integer.

This is a simple theorem to state and it can be seen at work with a short example. First let us make $s = 3$ and $t = 1$:

$$a = 3 \cdot 1 = 3$$

$$b = \frac{3^2 - 1^2}{2} = \frac{9 - 1}{2} = \frac{8}{2} = 4$$

$$c = \frac{3^2 + 1^2}{2} = \frac{9 + 1}{2} = \frac{10}{2} = 5$$

So, in general we have,

$$a^2 + b^2 = c^2$$

where *a, b,* c are integers. We will use the following construction to produce Pythagorean triples,

$$(s \cdot t)^2 + \left(\frac{s^2 - t^2}{2}\right)^2 = \left(\frac{s^2 + t^2}{2}\right)^2$$

Proof of Pythagorean Triples Theorem

For the proof of the Pythagorean triple formulas we must use two lemmas.

Lemma 1: If *a, b, c* is a primitive Pythagorean triple, then one of the integers *a* and *b* is even while the other is odd.

We will use two cases to show that this is true [2].

Case 1: Let both *a* and *b* be even, then that would mean the gcd(*a, b*) ≥ 2, thus, gcd(*a, b*) > 1. Since we are working with primitive Pythagorean triples the gcd(*a, b*) = 1. This shows that *a* and *b* cannot both be even.

Case 2: Both *a* and *b* are odd. When an odd number is squared it results in another odd number. Also when an odd number is added to another odd number it equals an even number. Therefore, we get that $a^2$and b^2 would both be odd numbers and result in $a^2 + b^2$ equaling an even number. This means that c^2 would be an even number.

An example of what is meant above is as follows:

Let a=3 and b=5 then we get,

$$a^2 = 3^2 = 9 \text{ and } b^2 = 5^2 = 25$$

and we can see both odd numbers when squared resulted in two more odd numbers. Now when we add these two results together we get,

$$9 + 25 = 34$$

This shows that when the two odd numbers are added together that the result is an even number.

Since we have seen an example we can now show how Case 2 works.

Since *a, b* are odd and *c* is even, there must exist integers *x, y, z* such that,

$$a = 2x + 1, \quad b = 2y + 1, \text{ and } \quad c = 2z.$$

From here we substitute these into our Pythagorean equation $a^2 + b^2 = c^2$:

$$(2x + 1)^2 + (2y + 1)^2 = (2z)^2,$$

$$4x^2 + 4x + 4y^2 + 4y + 2 = 4z^2$$

Then if we divide by 2 we get:

$$2x^2 + 2x + 2y^2 + 2y + 1 = 2z^2.$$

This gives us an equation where an odd number equals an even which is impossible. This means that a and b cannot both be odd. From checking that both a and b cannot be even and cannot both be odd then it shows that one of them is even and one of them is odd [14]. Without loss of generality we can make a odd, b even and a, b, c with no common factors. Now lemma 1 is proved

QED

Now that we have looked at and proved lemma 1 we can make the observation that if (a, b, c) is a primitive Pythagorean triple, we can factor

$$a^2 = c^2 - b^2 = (c - b)(c + b)$$

Here are a few examples to show how this works and we will always assume a odd and b even. Let us start with our dearly beloved 3-4-5 triangle where a=3, b=4 and c=5.

$$3^2 = 5^2 - 4^2 = (5 - 4)(5 + 4) = 1 \cdot 9 .$$

Another example is one that is not so loved by us but we will use our 35-12-37 triangle where we make a=35, b=12, and c=37.

$$35^2 = 37^2 - 12^2 = (37 - 12)(37 + 12) = 25 \cdot 49.$$

This makes it look like as if $(c - b)$ and $(c + b)$ are always squares and that they do not have any common factors. Therefore for Lemma 2, we want to prove that gcd$(c - b, c + b) = 1$, and $(c - b)$ and $(c + b)$ are both squares.

Lemma 2: if a, b, c are pairwise relatively prime, and $a^2 = c^2 - b^2 = (c - b)(c + b)$, then $(c - b)$ and $(c + b)$ have no common factors, and $(c - b)$ and $(c + b)$ are both squares.

Before we prove this lemma we need to look at the Unique Factorization Theorem.

The Unique Factorization Theorem: Any integer greater than 1 can be expressed in one way, apart from rearrangement, as a product of primes [17].

So, for the proof of Lemma 2 let us first assume that $(c - b)$ and $(c + b)$ have a common factor d.

Therefore, d, divides both $(c - b)$ and $(c + b)$.We then have that d also divides:

$$(c + b) + (c - b) = 2c, \text{and } (c + b) - (c - b) = 2b$$

This means that d needs to divide $2b$ and $2c$, but since we are assuming that (a, b, c) is a primitive Pythagorean triple, b and c have no common factors. Because of this d must be equal to 1 or 2. Since $(c - b)(c + b) = a^2$, then d would also divide a^2. Thus,

$$d|(c - b)$$

implies,

$$c - b = dm$$

Similarly we have,

$$c + b = dn$$

So,

$$(c - b)(c + b) = d^2mn = a^2$$

This implies,

$$d^2|a^2 \text{ and } d|a$$

Thus, d would divide all three numbers, and we already know that a is an odd integer, therefore, d must be 1. That means that the only number that can divide both $c - b$ and $c + b$ is 1, therefore $c - b$ and $c + b$ do not have any common factors [14].

Now that we know that $(c - b)$ and $(c + b)$ have no common factors, and their product is a square, we will show that both $(c - b)$ and $(c + b)$ must be squares. We use the prime factorizations of $(c - b)$ and $(c + b)$. Since these are relatively prime they will not have the same primes in their prime factorizations p_m, q_n. Thus,

$$(c - b) = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$$

$$(c + b) = q_1^{j_1} \cdot q_2^{j_2} \cdots q_n^{j_n}$$

where $q_l \neq p_j$ for any i, j.

We can then write the prime factorization of the product of $(c - b)$ and $(c + b)$ as

$$(c - b)(c + b) = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m} q_1^{j_1} \cdot q_2^{j_2} \cdots q_n^{j_n}$$

We are also able to write a into its own prime factorization as

$$a = u_1^{l_1} \cdot u_2^{l_2} \cdots u_r^{l_r}$$

Then for $(c - b)(c + b) = a^2$ we can write,

$$p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m} q_1^{j_1} \cdot q_2^{j_2} \cdots q_n^{j_n} = u_1^{2l_1} \cdot u_2^{2l_2} \cdots u_r^{2l_r}$$

We will now call upon the Unique Factorization theorem that was stated before this proof by looking at this prime factorization of a^2 we can see that it is the prime factorization of (c-b)(c+b) in some order. Also the exponents $2l_1, \ldots, 2l_r$ correspond with the exponents $k_1, \ldots, k_m, j_1, \ldots, j_n$. For this to be true then each of the integers k_m and j_n must be divisible by 2. We can write

$$c - b = \left(p_1^{k_1/2} \cdots p_m^{k_m/2}\right)^2$$

$$c + b = \left(q_1^{j_1/2} \cdots q_n^{j_n/2}\right)^2$$

which shows us that c - b and c + b are both squares [2], and lemma 2 is now proved.

QED

Now that we have proved lemma 2, we can see that there are no common factors to (c - b) and (c + b). The product of (c - b)(c + b) equals a square, $a^2 = (c - b)(c + b)$, where from lemma 1 we assumed that a is odd.

If we have s and t where $s > t \geq 1$ are both odd integers and relatively prime and since (c + b) and (c - b) are relatively prime. then we can write

$$c + b = s^2$$
$$c - b = t^2$$

. If we solve for both b and c we get

$$b = s^2 - c$$
$$c = t^2 + b$$

Now through substitution we have,

$$c = t^2 + s^2 - c$$
$$2c = t^2 + s^2$$
$$c = \frac{s^2 + t^2}{2}$$

We also have,

$$b = s^2 - (t^2 + b)$$
$$b = s^2 - t^2 - b$$
$$2b = s^2 - t^2$$
$$b = \frac{s^2 - t^2}{2}$$

Then we have the following equations

$$b = \frac{s^2 - t^2}{2} \qquad \text{and} \qquad c = \frac{s^2 + t^2}{2}$$

Therefore,

$$a = \sqrt{(c-b)(c+b)} = \sqrt{t^2 s^2} = st.$$

By combining the work above, we have concluded our proof of the Pythagorean Triples Theorem. The theorem is restated as follows:

Pythagorean Triples Theorem: You will get every primitive Pythagorean triple (a, b, c) with a odd and b even using the formulas:

$$a = s \cdot t \qquad b = \frac{s^2 - t^2}{2} \quad \text{and} \quad c = \frac{s^2 + t^2}{2}$$

where $s > t \geq 1$ are chosen to be any odd integers with no common factors [14].

The following is a table of all the Pythagorean triples that have s less than or equal to nine.

s	t	$a = s \cdot t$	$b = \frac{s^2 - t^2}{2}$	$c = \frac{s^2 + t^2}{2}$
3	1	3	4	5
5	1	5	12	13
7	1	7	24	25
9	1	9	40	41
5	3	25	8	17
7	3	21	20	29
7	5	35	12	37
9	5	45	28	53
9	7	63	16	65

[14].

Fermat's Method of Infinite Descent

The second method that we must look at for the $n = 4$ case is Fermat's method of infinite descent. Fermat was very proud of this method and towards the end of his life he wrote in a letter that he used his method of infinite descent in each of his proofs. In that same letter, Fermat stated that this method of infinite descent was to be used to show contradictions [6].

To use Fermat's method of infinite descent it must first be assumed that there is a solution in positive integers (X, Y, Z) to the problem at hand. Next, we must show that from this solution there is a smaller solution of positive integers (x, y, z). This would then lead to another smaller solution of positive integers, (x_1, y_1, z_1) and so on. There comes a contradiction from this method of getting smaller and smaller solutions that are positive integers because the positive integers do not get smaller infinitely. Therefore, we know that the original assumption of there being a solution to the problem is false [2].

By combining the method of infinite descent with Pythagorean triples we are able to prove the $n = 4$ case of Fermat's Last Theorem.

The $n = 4$ Case

Fermat proved the $n = 4$ case of his last theorem himself, but Leonhard Euler reproved this case, so before we prove the $n = 4$ case we will look at who Euler was. Throughout Euler's career he made many contributions to mathematics including the subjects of analysis, mechanics, and number theory. Euler was born in Switzerland in 1707 and entered the University of Basel when he was fourteen years old. At the University Euler studied under Johann Bernoulli who denied Euler private lessons, but "he was willing to help Euler with difficulties in the mathematical texts that Euler studied on his own" [9]. Euler worked at the St. Petersburg Academy of Sciences where during his time there he published fifty-five works. After his work in St. Petersburg he went to the Berlin Academy of Sciences in 1740. Then in 1766 Euler returned to St. Petersburg where he stayed for the rest of his life. After he returned he went blind but was still able to work with the help of an aid [9]. As stated before Euler worked in number theory and he worked with the $n = 4$ and $n = 3$ cases of Fermat's Last Theorem. Euler wrote a letter to Christian Goldbach in 1753 that said "I have now indeed found proofs that $a^3 + b^3 \neq c^3$ and $a^4 + b^4 \neq c^4$... But the proofs of these cases are so different from each other, that I do not see any possibility of deriving therefrom a general proof for $a^n + b^n \neq c^n$ for $n > 2$" [9]. Euler used Fermat's method of infinite descent, Pythagorean triples, and the stronger equation of $a^4 + b^4 = c^2$ to prove the
$n = 4$ case.

When we use the Diophantine equation $x^4 + y^4 = z^2$ along with Pythagorean Triples and Fermat's Method of Infinite Descent then as corollary we will be able to prove the $n = 4$ case [2]. Now let us look at the theorem at hand and then prove it.

The Theorem and the Proof

Theorem 1: The equation $x^4 + y^4 = z^2$ has no positive integer solutions x, y, z.

Now to prove this theorem we will first assume that there is a solution (x, y, z) to the equation $x^4 + y^4 = z^2$, and we want to find a smaller solution of positive integers. Now, we can assume that the greatest common divisor of x, y, z is 1, and that each pair is relatively prime. This is because if there was a common factor, other than 1, to x, y, z then we could factor it out and cancel it. Now we want to be able to use what we know from Pythagorean triples, so we can let

$$a = x^2,\ b = y^2,\ c = z \qquad (1)$$

This can then be written as

$$a^2 + b^2 = c^2 \qquad (2)$$

We know that x, y, z are pairwise relatively prime so we have a, b, c as pairwise relatively prime. This is because if a, b, c had any common factors that would mean that x, y, z would also have common factors which we know is not the case here. So we have $a^2 + b^2 = c^2$ which is a primitive Pythagorean triple. We can now bring in our Pythagorean triples formulas where we said that a was odd and b was even. So, we might have to interchanging x and y so that it follows

that x is odd and y is even. There exists relatively prime odd integers s and t where

$$x^2 = a = st \qquad y^2 = b = \frac{s^2 - t^2}{2} \qquad z = c = \frac{s^2 + t^2}{2} \qquad (3)$$

We can observe that st is odd and equal to a square. Because we have specific even and odd options we will refer to the squares modulo 4. For this case the only squares in modulo 4 are 0 and 1. This is shown in the following:

$$0^2 \equiv 0(mod4)$$
$$1^2 \equiv 1(mod4)$$
$$2^2 = 4 \equiv 0(mod4)$$
$$3^2 = 9 \equiv 1(mod4)$$

From $st = x^2$ we must have either

$$st \equiv 0(mod\ 4) \text{ or } st \equiv 1(mod\ 4)$$

We have to remember that st is an odd number and since we are working with mod 4 it implies that $st \equiv 0(mod\ 4)$ is not possible. This is because the only way to have st be congruent to 0 modulo 4 it would have to be a multiple of 4. This is not possible because all multiples of 4 are even and as stated before st is odd. This implies that,

$$st \equiv 1(mod\ 4) \qquad (4)$$

Since st are both odd then s and t are either both $1\ mod\ 4$ or both $3\ mod\ 4$. We can show this by having

$$s \equiv 1(mod\ 4)$$

and

$$t \equiv 3(mod\ 4)$$

When we multiply s and t together we get

$$st \equiv 3(mod\ 4)$$

which contradicts our statement in (4). So we will need both s and t as both $1\ mod\ 4$ or both $3\ mod\ 4$

We can say that

$$s \equiv t\ mod\ 4$$

Now, we refer back to our y^2 formula in (3) we have

$$y^2 = b = \frac{s^2 - t^2}{2} \qquad (5)$$

Where we are able to rewrite it as

$$2y^2 = s^2 - t^2 = (s - t)(s + t) \qquad (6)$$

As stated before, s and t are both odd and relatively prime and as a consequence of gcd(s, t) = 1 we can see that the greatest common factor of (s - t) and (s + t) is 2. This is because if

$$d|(s - t) \text{ and } d|(s + t)$$

then this implies that

$$d|(s - t) + (s + t)$$
$$d|2s$$

Similarly we have

$$d|(s + t) - (s - t)$$
$$d|2t$$

From this we can say that d is less than or equal to two. Since s and t are both odd and $(s - t)$ and $(s + t)$ are even we can say that $d = 2$.

Now, because $s \equiv t \ mod\ 4$ we know that (s - t) is divisible by 4. This is due to the definition of congruence which is as follows:

modular arithmetic has two integers a and b and a positive integer n. We write

$$a \equiv b \bmod n$$

Which is read as a is congruent to b modulo n, if n divides $a - b$.

So for the common factor of (s - t) and (s + t) to be two we need (s + t) to be 2 times an odd integer.

At this point we have that x, y, z are pairwise relatively prime and the product $(s - t)(s + t)$ is twice a square, $2y^2$. We would like to use lemma 2 at this point in time, but as stated before the gcd($s - t$, $s + t$) = 2. We want to be able to use the concept that if you divide two numbers, a and b, by their greatest common divisor, d, then the result is a new greatest common divisor, 1.

$$\gcd(a, b) = d$$

$$\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$$

So, for lemma 2 to apply we need to find two integers that are relatively prime. So, we will start by working with

$$2y^2=(s-t)(s+t)$$

To start we have

$$2y^2=(s-t)(s+t)$$

And from our work above we know that $(s-t)$ is divisible by 4 so we can write $(s-t)=4k$. We also know that $(s+t)$ twice an odd integer so we can write $(s+t)=2j$. From this we are able to say that

$$2y^2=(4k)(2j)$$

Or we can write this as

$$\frac{2y^2}{8}=\left(\frac{s-t}{4}\right)\left(\frac{s+t}{2}\right)$$

We now have

$$\frac{y^2}{4}=\left(\frac{y}{2}\right)^2=\left(\frac{s-t}{4}\right)\left(\frac{s+t}{2}\right)$$

where $\left(\frac{s-t}{4}\right)$ and $\left(\frac{s+t}{2}\right)$ are both integers.

As stated before the

$$\gcd(s-t,s+t)=2$$

by dividing by 2 we have

$$\gcd\left(\frac{s-t}{2},\frac{s+t}{2}\right)=1$$

We are also able to say that

$$\gcd\left(\frac{s-t}{4},\frac{s+t}{2}\right)=1$$

We are now able to use lemma 2. So we have x, y, z are pairwise relatively prime and we know that $\left(\frac{y}{2}\right)^2=\left(\frac{s-t}{4}\right)\left(\frac{s+t}{2}\right)$. We know that $\left(\frac{s-t}{4}\right)$ and $\left(\frac{s+t}{2}\right)$ have no common factors so by lemma 2

we can say that $\left(\frac{s-t}{4}\right)$ and $\left(\frac{s+t}{2}\right)$ both equal squares. We will denote this as

$$\left(\frac{s-t}{4}\right) = v^2 \quad \text{and} \quad \left(\frac{s+t}{2}\right) = u^2 \qquad (7)$$

where u and v are relatively prime integers because we know that $\left(\frac{s-t}{4}\right)$ and $\left(\frac{s+t}{2}\right)$ are relatively prime.

By doing some algebra we are able to rewrite (7) as

$$s - t = 4v^2 \qquad \text{and} \qquad s + t = 2u^2 \qquad (8)$$

Now we solve for s and t in terms of u and v

$$s = 2u^2 - t \qquad (9)$$

Now substitute this into $s - t = 4v^2$, and we have,

$$\begin{gathered} 2u^2 - t - t = 4v^2 \\ 2u^2 - 2t = 4v^2 \\ -2t = 4v^2 - 2u^2 \\ t = u^2 - 2v^2 \end{gathered}$$

We now substitute back into the $s = 2u^2 - t$ equation from (9) and we have

$$s = u^2 + 2v^2$$

So we now have,

$$s = u^2 + 2v^2 \text{ and } t = u^2 - 2v^2 \qquad (10)$$

We can then substitute these equations into the x^2 formula from (3)

$$\begin{gathered} x^2 = st \\ x^2 = (u^2 + 2v^2)(u^2 - 2v^2) \\ x^2 = u^4 - 4v^4 \end{gathered}$$

which can be rewritten as,

$$x^2 + 4v^4 = u^4 \qquad (11)$$

From this we almost have the equation that we want. We can now let

$$A = x \qquad B = 2v^2 \qquad \text{and} \qquad C = u^2 \qquad (12)$$

and we have

$$A^2 + B^2 = C^2$$

which is a primitive Pythagorean triple by the same logic that made (2) relatively prime. Let us now remember what the goal of this proof is and recap. We want to be able to find a smaller solution in the same form of the equation

$$x^4 + y^4 = z^2.$$

We want a smaller solution in the same form so that we can set Fermat's Method of Infinite Descent into motion. We said that the solution to $x^4 + y^4 = z^2$ was (x, y, z). So far we have found a new equation, $A^2 + B^2 = C^2$ with a different solution $(x, 2v^2, u^2)$, but these equations and solutions are not in the same form. So we will now work with what we have found above to find a smaller solution with the same form as $x^4 + y^4 = z^2$ which means that we will go through the process we did above one more time to get a smaller solution in the correct form.

So we have

$$A^2 + B^2 = C^2$$

where

$$x^2 + (2v^2)^2 = u^2$$

We will now use our Pythagorean triples formulas again where there exists S and T such that

$$x = A = ST \quad 2v^2 = B = \frac{S^2 - T^2}{2} \quad u^2 = C = \frac{S^2 + T^2}{2} \tag{13}$$

where S and T are both odd and relatively prime integers. We can then look at the formula

$$4v^2 = S^2 - T^2 = (S - T)(S + T) \tag{14}$$

By the same logic as before, S and T are relatively prime and odd. So the greatest common divisor of $(S - T)$ and $(S + T)$ is 2. We also know that the product of $(S - T)(S + T)$ is a square. We would like to use lemma 2 again, but in this case we need to do some work to find two integers that are relatively prime. We have

$$4v^2 = (S - T)(S + T)$$

We will divide both sides by 4 to have

$$v^2 = \left(\frac{S - T}{2}\right)\left(\frac{S + T}{2}\right)$$

As stated before when you divide two numbers by their greatest common divisor the result is that the new greatest common divisor is 1. We have

$$\gcd(S - T, S + T) = 2$$

So, when we divide by two we have

$$\gcd\left(\frac{S-T}{2}, \frac{S+T}{2}\right) = 1$$

We are now able to use lemma 2. We know that $v^2 = \left(\frac{S-T}{2}\right)\left(\frac{S+T}{2}\right)$. We know that $\left(\frac{S-T}{2}\right)$ and $\left(\frac{S+T}{2}\right)$ have no common factors so by lemma 2 we can say that $\left(\frac{S-T}{2}\right)$ and $\left(\frac{S+T}{2}\right)$ both equal squares. We will denote this as

$$\left(\frac{S-T}{2}\right) = Y^2 \text{ and } \left(\frac{S+T}{2}\right) = X^2$$

By some algebra we can then write that

$$S + T = 2X^2 \qquad \text{and} \qquad S - T = 2Y^2 \tag{15}$$

for some integers X and Y. We then solve for S and T in terms of X and Y so that

$$S = X^2 + Y^2 \qquad \text{and} \qquad T = X^2 - Y^2 \tag{16}$$

We now substitute these equations into the u^2 formula from (13)

$$u^2 = \frac{S^2 + T^2}{2}$$

$$u^2 = \frac{(X^2 + Y^2)^2 + (X^2 - Y^2)^2}{2}$$

After we do some algebra we see that

$$u^2 = X^4 + Y^4$$

which is a new solution (u, X, Y) to our original equation $x^4 + y^4 = z^2$. We must now confirm that this is a smaller solution than our original solution (x, y, z) So we substitute the equations from (10)

$$s = u^2 + 2v^2 \text{ and } t = u^2 - 2v^2$$

Back into the z formula from (3)

$$z = \frac{s^2 + t^2}{2} = \frac{(u^2 + 2v^2)^2 + (u^2 - 2v^2)^2}{2} = u^4 + 4v^4$$

Thus,

$$z = u^4 + 4v^4$$

which shows that u is smaller than z. By applying Fermat's method of infinite descent and by repeating the above argument with (u, X, Y) we would find a positive integer solution such that

$$z > u > u_1$$

And if we continue to repeat this process infinitely we would have

$$z > u > u_1 > u_2 \ldots$$

But there is only a finite amount of positive integer solutions less than z. Therefore a contradiction has occurred and our assumption of having a solution to the equation $x^4 + y^4 = z^2$ is false. We can say that there are no positive integer solutions to $x^4 + y^4 = z^2$.

QED

We can now look at the following corollary that comes from this previous proof.

Corollary: The equation $x^4 + y^4 = z^4$ has no integer solution in the positive integers.

Proof: If a positive solution to the equation $x^4 + y^4 = z^4$ was (x, y, z) then if we were to square the z term then the solution (x, y, z^2) would work as a solution for the equation $x^4 + y^4 = z^2$. But this contradicts what we proved in Theorem 1. Therefore, $x^4 + y^4 = z^4$ has no positive integer solutions.

QED

The n = 3 Case

In the previous section we looked at the $n = 4$ case of Fermat's last theorem and as stated then Euler also proved the $n = 3$ case. Within his proof though was a hole that can be corrected with a lemma that we will address later in this section. So from here we will go through Euler's proof and then look at what is incorrect about Euler's proof. We can then look at what Euler could have been basing this gap off of and then look at the lemma that finishes the proof.

As in the n = 4 case, Euler again used Fermat's method of infinite descent. So we need to show that a positive integer solution x, y, z exists for $x^3 + y^3 = z^3$. From here we need to then find another positive integer solution that is smaller than the original solution. We would then do this an infinite amount of times with an infinite amount of smaller positive integer solutions. Just like in the n = 4 case, finding an infinite amount of positive integer solutions is impossible. We could then say that the original solution x, y, z does not exist.

The Theorem and the Proof

Theorem 2: The equation $x^3 + y^3 = z^3$ has no positive integer solutions x, y, z.

To start our proof we must first assume that $x^3 + y^3 = z^3$ has a solution x, y, z. We will also assume that x, y, z are pairwise relatively prime, in other words, our common divisor of each pair (x, y), (x, z), and (y, z) is 1. From this we can say that there can only be one even number and the other two must be odd. There are two ways to assign the even and odd options. One is where x and y are both odd and the other is where only one of x and y is odd. We will look at both of these. So to start off we will have x and y be odd and z be even. We know that z would be even because when we add the two odd numbers together an even number is the result. Since x and y are both odd, we can assume that $x > y$ without loss of generality. We can now write:

$$x + y = 2p \quad \text{and} \quad x - y = 2q \tag{1}$$

This uses the same concept as above that when you add or subtract two odd numbers the result is an even number.

We are also able to write:

$$x = \tfrac{1}{2}(2p + 2q) = p + q \quad \text{and} \quad y = \tfrac{1}{2}(2p - 2q) = p - q \tag{2}$$

Note that since x is odd we know that p + q is odd and since y is odd p – q is also odd. We will now factor

$$z^3 = x^3 + y^3 = (x + y)(x^2 - xy + y^2) \tag{3}$$

We will now write this factorization in terms of p and q that were found in (1) and (2)

$$z^3 = 2p[(p+q)^2 - (p-q)(p+q) + (p-q)^2] \quad (4)$$

Once we expand what we found in (4) we have

$$z^3 = 2p(p^2 + 3q^2) \quad (5)$$

Which shows that the product of $2p(p^2 + 3q^2)$ equals a cube. We know that p + q and p – q are both odd, therefore, p and q have opposite parity. This is because if an odd and an even number are added or subtracted together the result is an odd number. An example follows:

$$2 + 3 = 5$$
$$7 - 4 = 3$$

We also know that p, q are relatively prime because if there was any common factor, other than 1, it would divide x and y from (2). We already know that x and y are relatively prime, therefore, $p + q$ and $p - q$ are also relatively prime. Since we are working with positive integers it can also be assumed that p and q are both positive integers. Thus, if x and y are both odd we have

$$z^3 = 2p(p^2 + 3q^2)$$

where p and q are relatively prime positive integers with opposite parity.

As stated before, there are two possible ways to assign the even and odd options. Therefore, we can show a similar result if we have one of x and y as odd and the other even. So, we can have x be even and y, z be odd. Since y and z are both odd, we can assume that $z > y$ without loss of generality. From this we will get the same result as before.

$$x^3 = z^3 - y^3 = (z-y)(z^2 + zy + y^2) \quad (7)$$

Then we let

$$z - y = 2p, \quad z + y = 2q, \; z = q + p, \text{ and } y = q - p \quad (8)$$

When we substitute what we have in (8) into the equation from (7) we get:

$$x^3 = 2p((q+p)^2 + (q+p)(q-p) + (q-p)^2 \quad (9)$$

As in (5) once expand this equation we get

$$x^3 = 2p(p^2 + 3q^2) \qquad (10)$$

Which again shows that the product of $2p(p^2 + 3q^2)$ equals a cube. A similar argument to the previous case shows that, p and q are relatively prime integers with opposite parity. So in either case if there is a solution to $x^3 + y^3 = z^3$ we are able to factor and if x and y are both odd we have

$$z^3 = 2p(p^2 + 3q^2)$$

where p and q are relatively prime positive integers with opposite parity.

We must now recall our work with Pythagorean triples, specifically lemma 2. This lemma says If a,b,c are pairwise relatively prime and $a^2 = c^2 - b^2 = (c - b)(c + b)$ then (c – b) and (c + b) have no common factors and are both squares. In this case we will modify this lemma so that it is stated as follows:

Lemma 3: If $stu = w^3$ and s,t,u are all pairwise relatively prime then $s = {s_1}^3$, $t = {t_1}^3$, and $u = {u_1}^3$.

We want to show that the numbers 2p and $p^2 + 3q^2$ from (5) are relatively prime and for their products to be a cube both of these number must be cubes separately.

We will now explore 2p and $p^2 + 3q^2$ to see if they are relatively prime. We know that p and q are of opposite parity therefore, $p^2 + 3q^2$ is odd. Therefore, any common factor of $2p$, $p^2 + 3q^2$ would also be a common factor of p, $p^2 + 3q^2$ which is then a common factor of p, $3q^2$. We know that p and q are relatively prime so the only possible common factors of p, $3q^2$ are 1 and 3. Now, if 3 divides p then 3 also divides $p^2 + 3q^2$ and then $2p$, $p^2 + 3q^2$ are not relatively prime. From here we split the proof into two cases. The first case is when 3 does not divide p which would then mean that $2p$, $p^2 + 3q^2$ are relatively prime. The second case is when 3 does divide p which will be modeled after the proof for the first case.

Case 1: Assume that 3 does not divide p and we will show that $2p$ and $p^2 + 3q^2$ are both cubes by lemma 3.

We are able to use the formula which we will call lemma 4

Lemma 4: $(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2 \qquad (11)$

to find cubes that are in the form $p^2 + 3q^2$.

The following is the expansion of lemma 4 in (11):

$$(a^2 + 3b^2)(c^2 + 3d^2) = a^2c^2 + 3a^2d^2 + 3b^2c^2 + 9b^2d^2$$

So now we rearrange the terms and have:

$$= (a^2c^2 + 9b^2d^2) + (3a^2d^2 + 3b^2c^2)$$

We will now plug in the terms $\pm 6acbd$ into the formula to get:

$$= (a^2c^2 - 6acbd + 9b^2d^2) + (3a^2d^2 + 6acbd + 3b^2c^2)$$

Now we will factor these into

$$= (ac - 3bd)(ac - 3bd) + 3(ad + bc)(ad + bc)$$

$$= (ac - 3bd)^2 + 3(ad + bc)^2$$

Which is the result that we wanted to get for lemma 4 in (11).

We are able to use this formula for the case where $a = c$ and $b = d$ so that we now have

$$(a^2 + 3b^2)^3 = (a^2 + 3b^2)[(a^2 - 3b^2)^2 + 3(2ab)^2] \quad (12)$$

After we expand the equation in (12) we have the following result

$$(a^2 + 3b^2)^3 = (a^3 - 9ab^2)^2 + 3(3a^2b - 3b^3)^2 \quad (13)$$

We are able to write this as,

$$(a^2 + 3b^2)^3 = (a^2 + 3b^2)[(a^2 + 3b^2)(a^2 + 3b^2)]$$

Using what we proved for lemma 4 we have:

$$(a^2 + 3b^2)^3 = (a^2 + 3b^2)[(a^2 - 3b^2)^2 + 3(2ab)^2]$$

Which is the result in line (12).

We need to get to the result in line (13) so we will continue to expansion as follows:

$$= (a^2 + 3b^2)(a^2 - 3b^2)^2 + (a^2 + 3b^2)3(2ab)^2$$

$$= (a^2 + 3b^2)(a^2 - 3b^2)(a^2 - 3b^2) + (a^2 + 3b^2)12a^2b^2$$

$$= (a^2 + 3b^2)(a^4 - 6a^2b^2 + 9b^4) + 12a^4b^2 + 36a^2b^4$$

$$= a^6 - 6a^4b^2 + 9a^2b^4 + 3a^4b^2 - 18a^2b^4 + 27b^6 + 12a^4b^2 + 36a^2b^4$$

All of the steps above were expanding each term and now we must combine and rearrange the terms above to get:

$$= a^6 + 9a^4b^2 + 27a^2b^4 + 27b^6 \qquad (14)$$

We need to become a little creative here to get the result that we want. So we will rewrite the $9a^4b^2$ and the $27a^2b^4$ terms of this equation as:

$$9a^4b^2 = -18a^4b^2 + 27a^4b^2 \text{ and } 27a^2b^4 = 81a^2b^4 - 54a^2b^4$$

We will now replace $9a^4b^2$ and the $27a^2b^4$ from line (14) and we have:

$$= a^6 - 18a^4b^2 + 81a^2b^4 + 27a^4b^2 - 54a^2b^4 + 27b^6$$

$$= (a^6 - 18a^4b^2 + 81a^2b^4) + 3(9a^4b^2 - 18a^2b^4 + 9b^6)$$

$$= (a^3 - 9ab^2)^2 + 3(3a^2b - 3b^3)^2$$

which is the result in line (13).

The work above shows that for any integers a and b then one way to find cubes of the form $p^2 + 3q^2$ is to set

$$p = a^3 - 9ab^2 \text{ and } q = 3a^2b - 3b^3 \qquad (15)$$

We then need to have $p^2 + 3q^2 = (a^2 + 3b^2)^3$.

According to Fermat's Last Theorem by Harold Edwards, "The major gap to be filled in Euler's proof is the proof that this is the *only* way that $p^2 + 3q^2$ can be a cube; that is, if $p^2 + 3q^2$ is a cube then there must be a, b such that p and q are given by the above equations [(15)]" [6].

The way that we can fill in this gap is by using the following lemma:

Lemma 5: Let a and b be relatively prime numbers such that if $z^3 = p^2 + 3q^2$ then there exists integers p and q such that

$$p = a^3 - 9ab^2 \text{ and } q = 3a^2b - 3b^3$$

We will not prove lemma 5 and will assume that that only way for $p^2 + 3q^2 = z^3$ is for $z = a^2 + 3b^2$.

We now refer back to our expressions for p and q in (14) and factor

$$p = a(a - 3b)(a + 3b) \tag{16}$$

$$q = 3b(a - b)(a + b) \tag{17}$$

Where a and b are relatively prime because any common factor of a and b would also divide both p and q.

We need to remember that for case 1 we assumed that 3 does not divide p and we are showing that $2p$ and $p^2 + 3q^2$ are both cubes by lemma 3.

We can now look at the factorization found in (16) for when we have $2p$.

$$2p = 2a(a - 3b)(a + 3b) = \text{cube} \tag{18}$$

We need for the parities of a and b to be opposite or we would have both p and q being even. From this we know that $a - 3b$ and $a + 3b$ from (18) are both odd. A consequence of the previous statement is that the only common factor of $2a$, $a \pm 3b$ would also be a common factor of a, $a \pm 3b$. From this, if $a - 3b$ and $a + 3b$ had any common factors it would also be a common factor of a and $3b$. This would lead to 3 being the only possibly common factor other than one. This is not possible though because if 3 divided a then it would also divide p. We know this because of (15) $p = a^3 - 9ab^2$ which would lead to 3 being a factor of each term. This contradicts our assumption that 3 does not divide p. This shows that $2a$, $a - 3b$, $a + 3b$, are all relatively prime and each are cubes. This comes from lemma 3 which we stated earlier, but we will recall it here.

Lemma 3: If $stu = w^3$ and s, t, u are all pairwise relatively prime then $s = {s_1}^3$, $t = {t_1}^3$, and $u = {u_1}^3$.

Lemma 3 could be proved similar to lemma 2 by using unique factorization theorem.

To continue our proof we can write

$$2a = \alpha^3,\ \ a - 3b = \beta^3,\ \ a + 3b = \gamma^3 \tag{19}$$

Then,

$$\beta^3 + \gamma^3 = 2a = \alpha^3 \tag{20}$$

And this is a solution to our equation $x^3 + y^3 = z^3$ and turns out to be a smaller than the original solution. We can look at

$$\alpha^3\beta^3\gamma^3 = 2a(a - 3b)(a + 3b) = 2p \tag{21}$$

Which is positive and a divisor of z^3 if z is even as in $z^3 = 2p(p^2 + 3q^2)$ or is a divisor of x^3 if x is even as in $x^3 = 2p(p^2 + 3q^2)$. We are able to have α, β, γ be negative because when we have $(-\alpha)^3 = -\alpha^3$we can move the negative cube to the other side of the equation to become a positive cube. The equation that we now have is one of the form $X^3 + Y^3 = Z^3$ where X, Y, Z are all positive and $Z^3 < z^3$ or in the other case $X^3 > x^3$. This then sets Fermat's Method of Infinite Descent into motion and case one is proved.

We will now look at case 2 which is a modification of case 1 and follows much of what we have done above.

Case 2: Consider the case where 3 divides p. Then, p=3s and 3 does not divide q.
Also,

$$z^3 = 2p(p^2 + 3q^2) = 3^2(2s)(3s^2 + q^2) \tag{22}$$

where the numbers $3^2(2s)$ and $3s^2 + q^2$ are relatively prime and cubes.
By the lemma that was mentioned before and to be proved later, $3s^2 + q^2$ can be a cube only if

$$q = a(a - 3b)(a + 3b) \text{ and } s = 3b(a - b)(a + b) \tag{23}$$

for some integers a, b. Since $3^2(2s)$ is a cube then $3^3 2b(a - b)(a + b)$ is a cube and from here we can say that $2b(a - b)(a + b)$ is a cube with each of these factors being relatively prime.
Like in case one we write

$$2b = \alpha^3,\ \ a - b = \beta^3,\ \ a + b = \gamma^3 \tag{24}$$

Then we have,

$$\alpha^3 = 2b = \gamma^3 - \beta^3 \tag{25}$$

and as in case 1, we have an equation $X^3 + Y^3 = Z^3$ with $Z^3 < z^3$.

From here since there is a smaller solution that is a cube which is the result of the sum of two cubes this would imply that there is another smaller cube that is also a solution. Fermat's Method of Infinite Descent is then set into motion and therefore the existence of a solution is impossible. To finish this proof we must show that if p and q are relatively prime integers such that $p^2 + 3q^2$ is a cube then there must be integers a and b such that $p = a^3 - 9ab^2$ and $q = 3a^2b - 3b^3$, which will be accomplished when we talk about the lemma that fills in the gap of this proof.

How to Fill in the Gap

Before we talk about the lemma that will fill in the gap we will look at numbers that are of the form

$$a + b\sqrt{-3} \tag{25}$$

where a and b are integers. Euler needed to find cubes in the form $p^2 + 3q^2$ and shows that for any a and b if we have $p = a^3 - 9ab^2$ and $q = 3a^2b - 3b^3$ as in (15) then $p^2 + 3q^2 = (a^2 + 3b^2)^3$.

Euler uses this and then tries to show that if p and q exist then a and b are in the form

$$p = a^3 - 9ab^2 \text{ and } q = 3a^2b - 3b^3.$$

His method is to calculate with numbers in the form $a + b\sqrt{-3}$. The problem with using numbers in this form is that they do not act the same way that the integers do [12]. We will need to look at definitions from abstract algebra such as, ring, integral domain, and unique factorization domain.

A ring, R, is a non empty set with two binary operations, addition and multiplication, such that for all a,b,c in R

- $a+b=b+a$
- $(a+b)+c=a+(b+c)$
- Additive identity 0. There exists $0 \in R$, s.t. a+0=a
- There is an element $-a$ in R s.t. $a+(-a) = 0$
- $a(bc)=(ab)c$
- $a(b+c)= ab+ac$ and $(b+c)a=ba+ca$ [7]

An Integral domain is a commutative ring with unity and no zero-divisors. In other words, a product is 0 only when one of the factors is 0; $ab = 0$ only when $a = 0$ or $b = 0$ [7]

And finally, an integral domain D is a unique factorization domain if:

- Every nonzero element of D that is not a unit can be written as a product of irreducibles of D, and

- The factorization into irreducibles is unique up to associates and the order in which the factors appear [7].

Now that we have those three definitions we can look at the integers. It turns out that the integers are a type of ring that is both an integral domain and an unique factorization ring. Euler was using numbers in the form $a + b\sqrt{-3}$ which is also a ring, but does not necessarily have the same properties as the integers do. The problem that Euler's n=3 proof has is that he, like many other mathematicians, assumed that the properties of integers carry over to integral domains in general [7].

Now that we know why there is a problem in the proof we can look at how to fix it. Euler calculates with numbers in the form $a + b\sqrt{-3}$ and his work is related to the formula

$$(x^2 + cy^2)(u^2 + cv^2) = (xu - cyv)^2 + c(xv + yu)^2$$

which is a general form of the formula from (11). According to Edwards this formula says that,

> "if the integer A is a product of integers B and C, and if B and C can both be written in the form $a^2 + cb^2$, say $B = x^2 + cy^2$, $C = u^2 + cv^2$, then A can also be written in this form by using the formula $a + b\sqrt{-c} = (x + y\sqrt{-c})(u + v\sqrt{-c})$ to define a and b" [6].

The lemma that we need uses four steps that when put together prove what we need and finishes the n=3 case. We will not actually prove any of these steps so the following is an outline of what needs to be done to finish the n=3 case. These steps are basically Euler's from his work with proving that every prime in the form $4n + 1$ is a sum of two squares, but is taken one step further to factor $a + b\sqrt{-3}$. According to Edwards, the steps are as follow:

(I) If a and b are relatively prime and if $a^2 + 3b^2$ is even then $a + b\sqrt{-3}$ can be written in the form

$$a + b\sqrt{-3} = (1 \pm \sqrt{-3})(u + v\sqrt{-3})$$

Where the sign is appropriately chosen and where u and v are integers.

(II) If a and b are relatively prime and if $a^2 + 3b^2$ is divisible by the odd prime P then P can be written in the form

$$P = p^2 + 3q^2$$

with p and q positive integers and $a + b\sqrt{-3}$ can be written in the form

$$a + b\sqrt{-3} = (p \pm q\sqrt{-3})(u + v\sqrt{-3})$$

where the sign is appropriately chosen and where u and v are integers.

(III) Let a and b be relatively prime. Then $a + b\sqrt{-3}$ can be written in the form

$$a + b\sqrt{-3} = \pm(p_1 \pm q_1\sqrt{-3})\,(p_2 \pm q_2\sqrt{-3}) \cdots (p_n \pm q_n\sqrt{-3})$$

Where the p's and q's are positive integers and ${p_l}^2 + 3{q_l}^2$ is either 4 or an odd prime.

(IV) Let a and b be relatively prime. Then the factors in the above factorization of $a + b\sqrt{-3}$ are completely determined, except for the choice of signs as indicated, by the fact that

$$({p_1}^2 + 3{q_1}^2)({p_2}^2 + 3{q_2}^2) \cdots ({p_n}^2 + 3{q_n}^2) = a^2 + 3b^2$$

is a factorization of $a^2 + 3b^2$ into odd primes and 4's. Moreover, if the factor $p + q\sqrt{-3}$ occurs then the factor $p - q\sqrt{-3}$ does not, and conversely [6].

When these four steps are combined we have the lemma that is needed to finish the n=3 case of Fermat's Last Theorem.

Lemma 5: Let a and b be relatively prime numbers such that $a^2 + 3b^2$ is a cube. Then there exist integers p and q such that

$$a + b\sqrt{-3} = (p + q\sqrt{-3})^3.$$

A proof of this lemma can be found in Fermat's Last Theorem by Harold Edwards. By applying Lemma 5 to the $n = 3$ proof it made it possible to show that $p = a^3 - 9ab^2$ and $q = 3a^2b - 3b^3$are the only way to find cubes in the form $p^2 + 3q^2$. Now, with all of this put together the proof of the n=3 case is finished.

As said in the previous section Euler wrote a letter to Goldbach about how he had a proof for the n=3 case for Fermat's Last Theorem. Euler also said that his proof of the n=3 case seemed to be very different from the proof of the n=4 case. He also stated that because of this he thought that a general proof was still long off. Euler turned out to be right because it would be another ninety years until in the 1840s Kummer developed his theory of ideal factors which lead to some insights about Fermat's Last Theorem and gave hope to a general case being possible [6]. Before Kummer could get to that result though , there was a French mathematician named Sophie Germain who made it possible to prove Case 1 of Fermat's Last Theorem for every prime less than 100 [6]. Our next section is about the work of Germain and how her work helped with eventually proving Fermat's Last Theorem.

Sophie Germain

Sophie Germain is best known for her work with Fermat's Last Theorem. In fact, she was the first person to make progress with a general approach to prove Fermat's Last Theorem. Germain was born in France in 1776 and lived in Paris with her parents and sisters during the French Revolution. She had to overcome the prejudice and discrimination that kept women of that time from learning higher level mathematics. Germain's family tried to keep her from working in mathematics, but she was persistent in learning all she could. She would use a small lamp and practice math wrapped in her bed covers. Many nights it got cold enough to where the ink would freeze in its well. Nothing stopped Germain from studying her passion and because of this her family eventually stopped opposing her [10].

Germain corresponded, under a pseudonym, with Gauss and Legendre. Eventually both men discovered that the brilliant mathematician known as Mr. Leblanc was actually Sophie Germain. Both mathematicians encouraged her to continue her work, and it was Legendre who made Germain famous [6]. Legendre attributed Germain with an important result for Fermat's Last Theorem. This result is known as Sophie Germain's Theorem. Before we look at Sophie Germain's Theorem we will look at another theorem that splits Fermat's Last Theorem into two different cases. We will then look at Sophie Germain's Theorem and some basic modular arithmetic. Lastly we will look at how Germain's Theorem was significant in the pursuit of proving Fermat's Last Theorem.

Fermat's Last Theorem made into Two Cases

The following is a theorem that splits Fermat's Last Theorem into two different cases.

Theorem A: If n is an odd prime and if $2n+1$ is prime then $x^n + y^n = z^n$ implies that x, y, or z is divisible by n.

So, to prove the cases where $n=5$ or $n=11$ or many other prime n's, then one can prove that $x^n + y^n - z^n = 0$ is impossible with the assumption that x, y, or z is divisible by n [6].

The case where none of x, y, or z is divisible by n is left out of this theorem. Fermat's Last Theorem is typically split into two different cases, mostly because of this theorem. The cases are as follows:

Case I: None of x, y, z is divisible by n

Case II: One and only one of x, y, z is divisible by n [12].

Also, Theorem A above is often written in the following form:

"*If n is an odd prime such that* $2n+1$ *is prime, then Case I of Fermat's Last Theorem is true for nth powers*" [6].

It turns out that Case I was more attainable than Case II. Case I of Fermat's Last Theorem is a part of Sophie Germain's Theorem, which follows.

Sophie Germain's Theorem

Sophie Germain's Theorem: Let n be an odd prime. If there is a prime p with the properties that

(1) $x^n + y^n + z^n \equiv 0 \bmod p$ implies that $x^n \equiv 0$ or $y^n \equiv 0$ or $z^n \equiv 0 \bmod p$
(2) $x^n \equiv n \bmod p$ is impossible

Then Case I of Fermat's Last Theorem is true for n [6].

We will not prove this theorem but we will talk about its significance and what having this proof lead to. Before we do that though, we will look at some basics about modular arithmetic because Sophie Germain's Theorem uses modular arithmetic.

Recall that the definition of congruence, modular arithmetic has two integers a and $b$and a positive integer n. we write

$$a \equiv b \bmod n$$

Which is read as a is congruent to b modulo n, if n divides $a - b$, which can also be written as

$$a \equiv kn + b$$

where k is an integer.

The Significance of Sophie Germain's Theorem

Sophie Germain's Theorem made great progress in the pursuit of proving Fermat's Last Theorem. Using her theorem made it possible to prove Case I of Fermat's Last Theorem for all primes less than 100. According to Edwards this means that "for each odd prime n less than 100 she was able to find another prime p which satisfied the conditions of the theorem" [6]. Legendre was able to expand this to all primes less than 197 and for many other primes. From these results mathematicians stopped focusing on Case I of Fermat's Last Theorem and began to focus on Case II which turned out to be the more difficult of the two cases to prove.

Sophie Germain: Beyond Her Theorem

For almost two hundred years it was thought that Sophie Germain's theorem was the only work that she did with Fermat's Last Theorem. Recently it has been discovered that Germain did more than just dabble with Fermat's Last Theorem but had a full fledged plan of attack to prove this theorem. Germain's work is organized into Manuscripts that are full of work that she never published and was recently studied by Rienhard Laubenbacher and David Pengelley. There are five different manuscripts that Laubenbacher and Pengelley write about and there is also a letter from Germain to Legendre as well as a letter from Germain to Gauss. We will focus on what was found in Manuscripts A, B and C to show how much Germain worked with Fermat's Last Theorem.

Germain's work that is compiled into Manuscript A has her "grand plan for proving Fermat's Last Theorem for any prime exponent $p > 2$ based on satisfying a modular non-consecutivity (N-C) condition for infinitely many auxiliary primes" [10]. Legendre also worked on (N-C) verification and his and Germain's techniques are completely different. Legendre was using this to try and prove Case I of Fermat's Last Theorem and it is thought that Germain abandoned her work on this grand plan when Legendre mentioned to her that it would not work for the $n = 3$ case. It turns out that Germain sent Legendre a proof showing that there are a finite amount of valid N-C auxiliaries, thus confirming what Legendre had told her about the $n = 3$ case [10]. Manuscript A also includes a theorem and application to make large minimal sizes solutions to Fermat's Last Theorem based on N-C and p is not a p-th power mod θ conditions (p-N-p conditions). The proof she was working on had a flaw, but the valid part is what we now know as Sophie Germain's Theorem [10].

Germain also worked to prove Fermat's Last Theorem for all exponents $2p$ where $p = 8n \pm 3$ is prime, which is in Manuscript B. This manuscript also provides the best original source of Sophie Germain's Theorem. She uses this to start an argument for Case I and then uses biquadratic residues to argue for Case II. This argument turns out to be flawed because what Germain thought would be relatively prime turned out to be false, so relative primality of her terms does not hold [10].

In Manuscript C, Germain worked with even exponents. In this section she used two theorems and their proofs to start Fermat's Last Theorem for all even exponents. Germain uses a slightly different family of Diophantine equations to attempt to prove Fermat's Last Theorem. Her goal is to prove that the "near-Fermat" equations in the form

$$2z^{2n} = y^{2n} + x^{2n}$$

have no positive solutions for $n > 1$. According to Laubenbacher, Germain's work with these "near-Fermat" equations is correct except for the same flaw from Manuscript B for Case II. This flaw is because of relative primality again [10].

So from all of this we can see that Germain did more than develop a theorem that proved Case I of Fermat's Last Theorem. She attempted to fully prove Fermat's Theorem but was never successful. Through her work with Fermat, she developed theories, techniques, and used a modern point of view on number theory that was also used by Gauss. This look into Germain's manuscripts shows that she was not an amateur at number theory and happened to come across a theorem that would then be named after her. She came to that theorem after an extensive plan to prove Fermat's Last Theorem. [10]. We can also see that Germain worked in isolation for the most part because even those who she had correspondence with did not know of her grand plan to prove Fermat's Theorem. It is easy to see that Germain was a strategist with her work in number theory and was more than just a footnote in the work that Legendre published. Sophie Germain is not the end of the story of Fermat and his theorem, but she is one part in the bigger picture of Fermat's Last Theorem and number theory.

The Bigger Picture

Pythagorean triples, Fermat's Method of Infinite Descent, the $n = 4$ and $n = 3$ cases and Sophie Germain are each a small part of a much bigger picture. Each of these were important components to Fermat's Last Theorem, but the time line of this theorem spans three centuries. Around the year 1637, early in Fermat's career, he made the famous marginal note. This note said,

> "But it is impossible to divide a cube into two cubes, or a fourth power [*quadratoquadratum*] into two fourth powers, or generally any power beyond the square into two like powers; of this I have found a remarkable demonstration. This margin in too narrow to contain it" [5].

In modern mathematics we denote this as

$$x^n + y^n = z^n$$

has no non-zero integer solutions for x, y, and z when $n > 2$.

Fermat's Last Theorem helped the development of Algebraic Number Theory which we will see in the following pages of mathematicians and their work with Fermat's problem. Before we see that though we should see what Algebraic Number Theory is.

Algebraic Number Theory is a part of Number Theory that deals with algebraic numbers and more specifically is used as a way to study Diophantine equations. This study of Algebraic Number Theory is related to the work that is done in Abstract Algebra today.

We should also look at how Algebraic Number Theory is different from Number Theory. In the study of Number Theory it deals with whole number and integers and working with prime numbers. The study of Algebraic Number Theory works with algebraic numbers which can be either complex or real. Examples of algebraic numbers are i, which is complex, and $\sqrt{2}$, which is real. Both i, and $\sqrt{2}$ are not integers, so by working on Fermat's Last Theorem mathematicians were able to develop the study of numbers that are not integers. We will now take a look at some of the major events in proving Fermat's Last Theorem.

Fermat proved the n=4 case using his method of infinite descent. He showed that for

$$x^4 + y^4 = z^4$$

there was no integer solution. Also, if there is a solution for one exponent, then any multiple of that exponent has a solution [7]. Therefore, mathematicians started focusing only on primes.

Euler proved the n=3 case and also proved the n=4 case independently from Fermat's work. Euler, like many others, assumed that all properties of the integers carried over to integral domains in general. Specifically they assumed that unique factorization carried over [7].

Sophie Germain worked with Fermat's Last Theorem and was able to prove Case I of the said theorem for primes under 100. Recent discoveries showed that Germain did more than the theorem that is named for her and had developed a system to prove Fermat's Last Theorem. Even though her plan failed it shows that Germain did not just stumble across a theorem that would prove Case I of Fermat's Last Theorem. Once Case I was proved it was time to focus on Case II.

The case where n=5 of Fermat's Last Theorem was split into two parts. The first part was proved by Dirichlet and the second half was proved by Legendre [6]. The n=7 case was proved by Lamé. He thought that he had finished the problem of Fermat's Last Theorem but he used a factorization that took place in a ring where factorization into the product of irreducibles is not unique [7]

The next mathematician in the Fermat story is Ernst Kummer who worked with ideal numbers that helped prove Fermat's Last Theorem for all primes of a special type. This made it possible for Fermat's Last Theorem to be proved for all exponents less than 100 except for 37, 59, 67, and 74. Kummer's work helped develop the theory of ideals that is used in Abstract Algebra today [7]. We will now look at Niels Henrick Able who gave the proof for the insolubility of the quintic in 1824. A crucial element of how Fermat's Last Theorem was treated came from an Abelian group. Abelian groups are groups where you can reverse the order of operations and not affect the outcome [7]. Richard Dedkend is also a part of the Fermat story because his work with ideals inspired Barry Mazur in the 1900s. Mazur's work was eventually utilized by Andrew Wiles for the proof of Fermat's Last Theorem.

The mathematicians that we have covered in this bigger picture so far worked in the 1800s. We will now look at 20th Century mathematicians and their contributions to the story of Fermat's Last Theorem. In the early 1960s, Goro Shimura and Yataka Taniyama conjectured that modular forms and elliptic curves are related. This became known as the Taniyama – Shimura conjecture. Barry Mazur, who worked with elliptic curves, is thought of as the mathematician whose work inspired at least two of the mathematicians who helped with finishing the proof of Fermat's Last Theorem. Those mathematicians were Gerhard Frey and Kenneth Ribet [1].

Gerhard Frey conjectured that if the Taniyama-Shimura conjecture were true then Fermat's Last Theorem could be proved. He did this by essentially turning Fermat's Last

Theorem into an elliptic equation which then tied Fermat's Last Theorem and the Taniyama-Shimura conjecture together. With Frey's elliptic equation it seemed that it would be impossible to find a modular form that would be related to it. Remember that the Taniyama-Shimura conjecture says that every elliptic equation is related to a modular form. So, if Frey's elliptic equation exists then it would disprove the Taniyama-Shimura conjecture. In Fermat's Enigma, by Simon Singh, Frey's argument is as follows:

(1) If Fermat's Last Theorem is wrong, then Frey's elliptic equation exists.
(2) Frey's elliptic equation is so weird that it can never be modular.
(3) The Taniyama-Shimura conjecture claims that every elliptic equation must be modular.
(4) Therefore the Taniyama-Shimura conjecture must be false [15].

What is really interesting is that this argument works backwards. This is as follows:

(1) If the Taniyama-Shimura conjecture can be proved to be true, then every elliptic equation must be modular.
(2) If every elliptic equation must be modular, then the Frey elliptic equation cannot exist.
(3) If the Frey elliptic equation does not exist, then there are no solutions to Fermat's equation.
(4) Therefore, Fermat's Last Theorem is true [15].

In Frey's argument he had a mistake that he did not see himself, but that many of the mathematicians that he presented to saw. Frey called his elliptic equation weird, but did not prove the absolute weirdness of his elliptic equation. So there became a race to prove the absolute weirdness of Frey's equation because the first person to prove it would be the one known for linking Fermat's Last Theorem to the Taniyama-Shimura conjecture [15].

In 1985 Kenneth Ribet proved that if Shimura-Taniyama conjecture was true then it would follow that Fermat's Last Theorem is also true. Ribet was the mathematician who was finally able to show that Frey's elliptic equation was absolutely weird. He was able to make it so that Fermat's Last Theorem was no longer an isolated problem, but that it was now linked to a significant conjecture of the 21st century [15].

With all of these mathematicians that are a part of the Fermat story we finally come to Andrew Wiles who attempted to prove the Shimura-Taniyama conjecture. So Wiles set out to prove that every elliptic equation is related to a modular form. He started this work in 1986, and then in 1993 Wiles had a proof that was up to 200 pages for Fermat's Last Theorem. He gave a series of three talks at the Isaac Newton Institute at Cambridge England and by the end of his talks he stated that he had a proof of Fermat's Last Theorem [15]. When his proof went into

review though, it was discovered by Nick Katz that there was an error. Wiles teamed up with a former student of his named Richard Taylor and together they were able correct the mistake and in the 1995 May issue of *Annals of Mathematics* Wiles' proof of Fermat's Last Theorem was published.

The story of Fermat's Last Theorem is long and caused many discoveries to be made in the field of Number Theory. Once the theorem was proved it was a major victory for the mathematical community. For so long this theorem was a puzzle that no one could solve until Andrew Wiles was able to piece together all the different parts that would make it possible to prove Fermat's Last Theorem. His proof is one that uses mathematics that was not discovered during the time that Fermat lived which makes most people believe that Fermat did not have a correct proof of his theorem. We will not look at the proof that Andrew Wiles gave because the margins of this research are too narrow to contain it.

Works Cited

1. Aczel, Amir D. *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem.* New York: Four Walls Eight Windows, 1996. Print.
2. Burton, David M. "The Fermat Conjecture." *Elementary Number Theory.* New York [u.a.: McGraw Hill, 1997. 227-41. Print.
3. Caldwell, Chris K. "The Prime Glossary: Pairwise Relatively Prime." *The Prime Pages (prime Number Research, Records and Resources).* 1999-2012. Web. 09 Apr. 2012.
4. Dudley, Underwood. "Pythagorean Triangles." *Elementary Number Theory.* 2nd ed. Mineola, NY: Dover Publications, 2008. 127-34. Print
5. Dunham, William. "A Gem From Isaac Newton." *Journey through Genius: The Great Theorems of Mathematics.* New York: Penguin, 1991. 155-83. Print.
6. Edwards, Harold M. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory.* New York: Springer-Verlag, 1977. Print.
7. Gallian, Joseph A. *Contemporary Abstract Algebra.* Boston: Houghton Mifflin, 2002. Print.
8. Katscher, Friedrich. "Extracting Square Roots Made Easy: A Little Known Medieval Method" ("Appendix: When Was Fermat Born?") *Loci: Convergence* (June 2010). DOI: 10.4169/loci003494 Accessed Feb. 19, 2012
9. Laubenbacher, Reinhard, and David Pengelley. "Chapter 4: Number Theory: Fermat's Last Theorem." *Mathematical Expeditions: Chronicles by the Explorers.* New York [etc.: Springer, 2000. 156-203. Print.
10. Laubenbacher, Reinhard, David Pengelley, "Voici ce que j'ai trouvé:" Sophie Germain's grand plan to prove Fermat's Last Theorem, Historia Mathematica, Volume 37, Issue 4, November 2010, Pages 641-692, ISSN 0315-0860, 10.1016/j.hm.2009.12.002.
11. (1) O'Connor, J. J. and E. F. Robertson, "Pierre de Fermat." In *MacTutor History of Mathematics Archive*, University of St Andrews, Scotland, 1996. Accessed Feb. 19, 2012
12. (2) O'Connor, J. J. and E. F. Robertson, "Fermat's Last Theorem." In *MacTutor History of Mathematics Archive*, University of St Andrews, Scotland, 1996. Accessed Mar. 4, 2012
13. (3) O'Connor, J. J. and E. F. Robertson, "Pythagoras of Samos." In *MacTutor History of Mathematics Archive*, University of St Andrews, Scotland, 1996. Accessed April. 6, 2012
14. Silverman, Joseph H. "Pythagorean Triples." *A Friendly Introduction to Number Theory.* 3rd ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2006. 13-19. Print.
15. Singh, Simon. *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem.* New York: Anchor, 1998. Print.
16. "Timeline of Fermat's Last Theorem." *Timeline of Fermat's Last Theorem.* N.p., n.d. Web. 26 Feb. 2013.
17. Wolfram Alpha. "Algebraic Number Theory." *Wolfram Alpha.* Wolfram Alpha, 2012. Web. 8 April. 2013.

Annotated Bibliography

Aczel, Amir D. *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem*. New York: Four Walls Eight Windows, 1996. Print. – Aczel's book was used to check facts for the bigger picture section of this research.

Burton, David M. "The Fermat Conjecture." *Elementary Number Theory*. New York [u.a.: McGraw Hill, 1997. 227-41. Print. – Burton's book was used to study Pythagorean triples and the n=4 case of Fermat's Last Theorem

Caldwell, Chris K. "The Prime Glossary: Pairwise Relatively Prime." *The Prime Pages (prime Number Research, Records and Resources)*. 1999-2012. Web. 09 Apr. 2012. – Caldwell was used to understand the term relatively prime.

Dudley, Underwood. "Pythagorean Triangles." *Elementary Number Theory*. 2nd ed. Mineola, NY: Dover Publications, 2008. 127-34. Print – Dudley was able to provide information about Pythagorean triples and the Unique Factorization Theorem

Dunham, William. "A Gem From Isaac Newton." *Journey through Genius: The Great Theorems of Mathematics*. New York: Penguin, 1991. 155-83. Print. – Dunham was used for historical context of Fermat

Edwards, Harold M. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*. New York: Springer-Verlag, 1977. Print. – Edwards was used throughout this research. This book gave insight to Pythagorean triples, the n=3 and n=4 cases, and the work of Sophie Germain. This book also covers the mathematicians covered in the conclusion of this research.

Gallian, Joseph A. *Contemporary Abstract Algebra*. Boston: Houghton Mifflin, 2002. Print. Gallian's Abstract Algebra book gave insight to what the definitions of rings, unique factorization domains, and integral domains. This book also had a section on Fermat's Last Theorem.

Katscher, Friedrich. "Extracting Square Roots Made Easy: A Little Known Medieval Method" ("Appendix: When Was Fermat Born?") *Loci: Convergence* (June 2010). DOI: 10.4169/loci003494 Accessed Feb. 19, 2012 - Katscher was used to clear up what the actual birth date of Fermat was.

Laubenbacher, Reinhard, and David Pengelley. "Chapter 4: Number Theory: Fermat's Last Theorem." *Mathematical Expeditions: Chronicles by the Explorers*. New York [etc.: Springer, 2000. 156-203. Print. – Laubenbacher and Pengelley gave insight to the n=3,n=4 cases of Fermat's Last Theorem, and Sophie Germain's work.

Laubenbacher, Reinhard, David Pengelley, "Voici ce que j'ai trouvé:" Sophie Germain's grand plan to prove Fermat's Last Theorem, Historia Mathematica, Volume 37, Issue 4, November 2010, Pages 641-692, ISSN 0315-0860, 10.1016/j.hm.2009.12.002. – Laubenbacher and Pengelley did research that showed that Sophie Germain did more with Fermat's Last Theorem than what was thought.

(1) O'Connor, J. J. and E. F. Robertson, "Pierre de Fermat." In *MacTutor History of Mathematics Archive*, University of St Andrews, Scotland, 1996. Accessed Feb. 19,

2012 - Mactutor gives historical biographies of mathematicians. This source was used to study Fermat.

(2) O'Connor, J. J. and E. F. Robertson, "Fermat's Last Theorem." In *MacTutor History of Mathematics Archive*, University of St Andrews, Scotland, 1996. Accessed Mar. 4, 2012 - Mactutor gives historical biographies of mathematicians. This source was used to study the history of Fermat's Last Theorem.

(3) O'Connor, J. J. and E. F. Robertson, "Pythagoras of Samos." In *MacTutor History of Mathematics Archive*, University of St Andrews, Scotland, 1996. Accessed April. 6, 2012 – Mactutor gives historical biographies of mathematicians. This source was used to study Pythagoras

Silverman, Joseph H. "Pythagorean Triples." *A Friendly Introduction to Number Theory*. 3rd ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2006. 13-19. Print. – Silverman's book was used to help understand the proofs of both Pythagorean Triples, Fermat's Method of Infinite Descent, and the n=4 case of Fermat's Last Theorem.

Singh, Simon. *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem*. New York: Anchor, 1998. Print. – Singh's book was used as a way to understand the history of Fermat's Last Theorem. Some of the mathematical concepts were explained in this book, but it was mostly used for historical context.

"Timeline of Fermat's Last Theorem." *Timeline of Fermat's Last Theorem*. N.p., n.d. Web. 26 Feb. 2013. – This timeline was used to see where each piece of this research fit into the bigger picture of Fermat's Last Theorem

Wolfram Alpha. "Primitive Pythagorean Triples." *Wolfram Alpha*. Wolfram Alpha, 2012. Web. 31 Mar. 2012. – This website provided a definition of Primitive Pythagorean Triples

Wolfram Alpha. "Algebraic Number Theory." *Wolfram Alpha*. Wolfram Alpha, 2012. Web. 8 April. 2013. – This website provided a definition of Algebraic Number Theory and the basic overview of what it is.