Applications of Number Theory to Fermat's Last Theorem

Cameron Byerley

May 14, 2006

Abstract This paper is in the form of the fifth and sixth chapters of lecture notes designed for an introductory number theory class. It uses a number of basic number theory concepts to prove three cases of Fermat's Last Theorem. Fermat's Last Theorem states there are no integral solutions to the equation $x^n + y^n = z^n$ for $n > 2$. We begin with a proof of $n = 4$ and use similar but more computationally and theoretically complicated ideas to prove the cases $n = 3$ and $n = 14$. In addition to providing mathematical details for each proof, the paper places the proofs in a historical context. Although providing a complete proof of Fermat's Last Theorem is far beyond the scope of this paper, examining three cases gives an understanding of the difficulties in generalizing the theorem and the contributions of many well-known mathematicians.

Chapter 1

Special Cases of Fermat's Last Theorem

1.1 Historical Overview

Number Theory is a unique mathematical discipline because many of its most difficult problems can be explained to an average person without delving into esoteric background information. Fermat's Last Theorem(1.1.1) is perhaps one of the best known theorems because it is so simple to state but remained unsolved for hundreds of years despite the efforts of the world's best mathematicians. Andrew Wiles, the man who would eventually prove the theorem, discovered the problem in the book *The Last Problem* by Eric Temple Bell while perusing his local library. He says of reading the Theorem, "It looked so simple, and yet all the great mathematicians in history couldn't solve it. Here was a problem that I, a ten-year-old, could understand and I knew from that moment I would never let it go. I had to solve it." Fermat's Last Theorem is so easy to understand because of its similarity to the Pythagorean Theorem. The Theorem originated with Pierre de Fermat who was born in France in 1601 and was employed as a judge and considered the Prince of Amateur mathematicians. In the margin of Diophantine's *Arithmetica*, next to a discussion of Pythagorean triples, Fermat wrote "It is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as the sum of two fourth powers or, in general, for any number which is a power greater than the second to be written as a sum of two like powers." We restate the theorem in more modern mathematical notation.

Theorem 1.1.1. Fermat's Last Theorem *The equation $x^n + y^n = z^n$ has no solution in positive whole numbers when $n > 2$.*

From 1637 to the point when Wiles finished his proof in 1994 the world of mathematicians were taunted by Fermat's note "I have a truly marvelous demonstration of this proposition which the margin is too small to contain." The book *Fermat's Enigma*[3] gives a more in depth portrait of the history of the problem. Many doubt Fermat's claim of possessing a general proof because generations of the most brilliant and dedicated mathematicians failed to prove it using elementary methods, and Wiles' proof contained over 100 pages and depended on modern techniques unavailable to Fermat. Fermat did have a proof for the case $n = 4$, however, which utilized the idea of infinite descent that he invented. He likely thought that this method could be generalized to higher powers. After giving the proof of the case $n = 4$ in detail we will provide Euler's proof for $n = 3$ and show why a simple modification of the case $n = 4$ was unsuccessful in an attempt to give some idea of how difficult it is to extend a proof from one case to another. Even the brilliant Euler made a fundamental error in his proof which invalidated it and had to be corrected by other mathematicians. When Euler wrote to Goldbach about proving the case $n = 3$ in 1753, he observed that the proofs seemed very different than the case $n = 4$ and that a general proof seemed very remote[1]. Finally we will provide a long and computationally inventive proof of the case $n = 14$ which effectively demonstrates that new and creative thinking is required for each new proof and shows the difficulty in finding a general solution to Fermat's Last Theorem. The proofs all rely heavily on ideas of divisibility and relative primality discussed earlier in these notes. They also provide a historically relevant example of the difference between prime and irreducible and unique factorization. The proofs are historically valuable in themselves, but also motivate the practice of important ideas from Number Theory.

1.2 Infinite Descent and the Case $n = 4$

We begin with the case where $n = 4$ because it was the first case to be proved, most likely because it was the easiest. This proof is also similar to the longer proofs of case $n = 3$ and $n = 14$ and gives the basic idea of how all three proofs work. These proof were all found in *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory* by Harold Edwards [1].

The case where $n = 4$ uses the method of infinite descent and a representation of Pythagorean triples. The idea of a proof by infinite descent is simple. First assume that there is a positive integral solution to your problem. Then through algebraic manipulation, show that given this solution you can find a smaller positive integral solution. This is absurd because you can not have an infinitely decreasing sequence of positive integers. Before showing the details of the infinite descent for the case $n = 4$, we will prove a helpful Lemma about Pythagorean triples. Although we are not using this fact explicitly in our proof, it is interesting to note that we are finding a construction for infinitely many Pythagorean triples. In other words, for the case $n = 2$, the equation given by Fermat's Last Theorem has infinitely many solutions.

Lemma 1.2.1. Pythagorean Triples *For any integers x, y and z that are relatively prime and satisfy $x^2 + y^2 = z^2$, we can find integers p and q such that*

$$x = 2pq$$
$$y = p^2 - q^2$$
$$z = p^2 + q^2$$

where p and q are relatively prime, of opposite parity and $p > q > 0$. The x and y values are interchangeble.

Proof. In this proof we only deal with primitive Pythagorean triples which have no common divisor. Once we find the solution for all primitive Pythagorean triples we can use those formulas to find a solution for all Pythagorean triples. This is unnecessary to prove Fermat's Last Theorem. If k is a common divisor of x, y and z we can replace p with kp and q with kq in our fomulas for x, y and z to find the solutions to all possible Pythagorean triples. Because our Pythagorean triple is primitive, no two numbers can be even because two would be a common divisor. But all three cannot be odd because our equation would say the sum of two odd numbers is odd. Therefore, exactly one is even. Now we want to prove that z is odd and x and y are of opposite parity. If z is even it can be written as $2n$ for some integer n. Then x and y are odd and can be written in the form $2n' + 1$ for another integer n'. Using the ideas of modular arithmetic we see that $x^2 = 4n^2 + 4n + 1 \equiv 1 (\text{mod } 4)$ and $z^2 = 4n^2 \equiv 0 (\text{mod } 4)$. If $x^2 + y^2 = z^2$ and z is even this implies $1 + 1 \equiv 0 (\text{mod } 4)$. This contradiction proves that z is odd. Assume that y is the other odd number; if it is not simply switch it with x.

We can rewrite our equation $x^2 + y^2 = z^2$ as $x^2 = z^2 - y^2$. Factor it as $x^2 = (z-y)(y+z)$ and notice that $x, z-y, y+z$ are all even numbers. Because they are all even we can find positive integers u, v, w such that $x = 2u, z+y = 2v, z-y = 2w$. Plug these new values into $x^2 = (z-y)(y+z)$ to get $(2u)^2 = (2v)(2w)$ or $u^2 = vw$. We can see that v and w are relatively prime because any number that divides them both would divide $v + w = \frac{1}{2}(z+y) + \frac{1}{2}(z-y) = \frac{1}{2}2z = z$ and $u - w = \frac{1}{2}(z+y)\frac{1}{2}(z-y) = y$. Since z and y are relatively prime we know that v and w are also relatively prime. Since $vw = u^2$ we know that v and w must each be squares since they are relatively prime. This implies there exist integers p and q such that

$$z = v + w = p^2 + q^2$$

$$y = v - w = p^2 - q^2.$$

The fact that y is positive implies p is bigger than q. Since z and y are odd, p and q must be of opposite parity. We can use the equation $x^2 = z^2 - y^2$ to find x in terms of p and q.

$$\begin{aligned} x^2 &= z^2 - y^2 = p^4 + 2p^2q^2 + q^4 - p^4 + 2p^2q^2 - q^4 \\ &= 4p^2q^2 \\ &= (2pq)^2 \\ x &= 2pq \end{aligned}$$

We have proven that given any primitive Pythagorean triple with x even we can always find values of p and q that satisfy these equations.

It is easy to finish the analysis of Pythagorean triples by showing that for any p and q such that p and q are relatively prime, of opposite parity and $p > q$ the numbers $2pq, p^2 - q^2, p^2 + q^2$ form a primitive Pythagorean triple. It is easy to verify that

$$(2pq)^2 + (p^2 - q^2)^2 = (p^2 + q^2)^2$$

by noticing that after multiplying and simplifying the terms involving $2pq$ cancel out. Now we only have to show it is a primitive Pythagorean triple. We will use the fact that p and q are relatively prime to show that $2pq$ and $p^2 - q^2$ are relatively prime. Assume that d divides $2pq$ and $p^2 - q^2$. Since $p^2 - q^2$ is odd the common divisor is not even. Thus it must divide p or q

but not both. If $d \mid p^2 - q^2$ and $d \mid p^2$ then we know that $d \mid q^2$. This is a contradiction of our assumption because it implies p and q have a common divisor. □

Applying triples to $n = 4$ To prove the case $n = 4$ we will prove a slightly more general theorem, from which we can easily conclude that there are no integral solutions to $x^4 + y^4 = z^4$.

Theorem 1.2.2. Case $n = 4$ *There are no integral solutions to the equation $x^4 + y^4 = z^2$.*

Proof. First we suppose that there exists postive integers x, y, z such that $x^4 + y^4 = z^2$ and proceed by contradiction. We can assume that they are pairwise relatively pfile:///usr/share/doc/HTML/index.htmlrime because otherwise we could divide out a common factor. Therefore x^2, y^2 and z are a primitive Pythagorean triple. We use the representation of y^2 to begin the infinite descent. We can rewrite the equation as $y^2 + q^2 = p^2$ where p and q are as in Lemma 1.2.1. Since p and q are relatively prime, we know y, p and q form a primitive Pythagorean triple by Lemma 1.2.1. As was shown earlier p must be odd and because q has opposite parity it must be even. We can use our formulas again to write

$$q = 2ab$$
$$y = a^2 - b^2$$
$$p = a^2 + b^2$$

where a and b are relatively prime of opposite parity and $a > b > 0$. Now we use our equation for x^2 to find

$$x^2 = 2pq = 4ab(a^2 + b^2).$$

This tells us that $ab(a^2+b^2)$ must be a square. Since a and b are relatively prime we know that ab and a^2+b^2 are also relatively prime. If ab has a prime divisor it must divide a or b by the definition of prime, but it can not divide both. If it does not divide both it cannot divide $a^2 + b^2$. This tells us that ab and $a^2 + b^2$ must both be squares. Since ab is a square and a and b are relatively prime a and b must be squares. We can find new integers X and Y such that $a = X^2$ and $b = Y^2$. But notice that $X^4 + Y^4 = a^2 + b^2$ and we know that $a^2 + b^2$ is a square. We have shown that if $x^4 + y^4 = z^2$ then we

can find new integers such that $X^4 + Y^4 = Z^2$. Notice that our new square is smaller because $X^4 + Y^4 = a^2 + b^2 = p < p^2 + q^2 = z^2 = x^4 + y^4$. We have established an infinite descending sequence of positive integers. We have found a method to always find a smaller integral solution, which is absurd. Therefore the sum of two fourth powers cannot be a square. □

Corollary 1.2.3. *There are no integral solutions to the equation* $x^4+y^4 = z^4$.

Proof. Every fourth power is also a square so this follows immediately from Theorem 1.2.2. □

1.3 The Case $n = 3$

In our proof of the case $n = 4$ we take advantage of the fact that a $4th$ power is also a square and apply ideas related to Pythagorean triples. Even though three is a smaller number, the proof of the case $n = 3$ is quite a bit more complicated than the proof of $n = 4$. This proof was first published by Leonard Euler (1707-1783), but it was incomplete in an important respect. We will discuss Euler's proof and correct his mistake. Euler's proof also uses the method of infinite descent. He shows that if positive whole numbers x, y and z can be found such that $x^3 + y^3 = z^3$ then we can find smaller positive integers for which the equation is also true.

Overview First I will outline the main flow of the proof to provide an overview without the messy details. After we assume that there exist solutions to the equation $x^3 + y^3 = z^3$, we make some basic observations about the numbers x, y and z. We show why we can assume they are relatively prime and that z is even while x and y are odd. We use some ingenuity to rewrite x and y in terms of new integers p and q. If we substitute $x = p + q$ and $y = p - q$ into the equation $x^3 + y^3$, we end up with the expression $2p(p^2 + 3q^2) = z^3$. If we know that these numbers are relatively prime then they both must be cubes. However there is a possibility that they are both divisible by three so we split our proof into two cases. In the case where $2p$ and $p^2 + 3q^2$ are relatively prime we use a formula that is easily verified with basic algebra to rewrite p and q in terms of new numbers a and b. This is the point in the proof where Euler makes the mistake because of a confusion about calculations in rings of imaginary numbers. By again showing that more numbers are relatively prime, we end up proving that $2a$, $a - 3b$ and

$a+3b$ are all relatively prime and $2p = 2a(a-3b)(a+3b)$. Since $2p$ is a cube all three smaller numbers must be cubes too. Notice that $(a-3b)+(a+3b) = 2a$. We have found three cubes that satisfy $\alpha^3 + \beta^3 = \gamma^3$. After this we must deal with the second case which ends up being very similar. Finally we make sure that the new solution we have found is indeed smaller.

Theorem 1.3.1. Case $n = 3$ There are no integral solutions to the equation $x^3 + y^3 = z^3$.

Proof. Assume that $x^3 + y^3 = z^3$. First we make a few statements about x, y and z. We can assume that x, y and z are pairwise relatively prime and positive. If a factor divides all three we can divide it out. If a factor divides two, it must also divide the third. This can be shown by factoring the equation. This means that at most one is even. We cannot have three odd numbers because if x and y are odd then z is even. Thus we have exactly one even number. Assume that x and y are odd and z is even. If this is not the case we can rearrange our equation to put the even number by itself. For example if we know x is even in the equation $x^3 + y^3 = z^3$ then we know $x^3 = z^3 + (-y)^3$. We know that the numbers $x + y$ and $x - y$ are both even and thus can be written in the form $2p$ and $2q$, respectively. By rewriting x and y creatively we see:

$$x = \frac{1}{2}((x + y) + (x - y)) = \frac{1}{2}(2p + 2q) = p + q$$

$$y = \frac{1}{2}((x + y) - (x - y)) = \frac{1}{2}(2p - 2q) = p - q.$$

We can rewrite $x^3 + y^3 = (x+y)(x^2 - xy + y^2)$ using our new expressions for x and y as

$$2p[(p + q)^2 - (p + q)(p - q) + (p - q)^2] = 2p(p^2 + 3q^2).$$

We can draw a number of conclusions about p and q. Since $p+q$ and $p-q$ are both odd, p and q must be of opposite parity. They must also be relatively prime because if p and q had a factor in common then that factor would divide $x = p + q$ and $y = p - q$. We can assume they are positive because we could change the order of x and y if $x - y$ was negative. We know that neither p nor q is zero because the case where $x = y$ is impossible. Since they are relatively prime this would imply $x = y = 1$ and thus $z^3 = 2$. Thus

given our assumptions that x and y are positive solutions to the equation we see that

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

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

Two Cases: Relatively Prime or Divisible by Three In the next part of the proof we will show that either $2p$ and $p^2 + 3q^2$ are divisible by 3 or are relatively prime and thus must be perfect cubes as well. The only case in which they are not relatively prime is if 3 is a divisor. Since p and q have opposite parity we know that $p^2 + 3q^2$ is odd. This is easy to see by considering what happens when we let p be even and q be odd and when q is even and p is odd. If $2p$ and $p^2 + 3q^2$ have a common factor, p and $p^2 + 3q^2$ must have the same common factor. If $d \mid p$ and $d \mid p^2 + 3q^2$, then we know $d \mid 3q^2$ since $p \mid p^2$. Thus if $2p$ and $p^2 + 3q^2$ have a common factor, it must also be a common factor of p and $3q^2$. We know that p and q are relatively prime so the only possible common factor is 3. If $3 \mid p$ and $3 \mid 3q^2$ then we know that $3 \mid 2p$ and $3 \mid p^2 + 3q^2$. Thus $2p$ and $p^2 + 3q^2$ are either relatively prime or have a greatest common divisor of three. We will break the proof into two cases.

1.3.1 Case One: Relatively Prime

First we consider the case when $2p$ and p^2+3q^2 are not divisible by three and therefore are relatively prime. Using a number of algebraic manipulations we will show that if $p = a^3 - 9ab^2$ and $q = 3a^2b - 3b^2$ then $p^2 + 3q^2$ is a cube. We use the following formula which is easily verified by using commutative, associative and distributive laws. The formula

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

shows that if two numbers are a sum of two squares then their product is a sum of two squares. We modify the formula slightly to fit our numbers by adding a three to one side and modifying the other side accordingly as follows

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2.$$

The proof requires only basic algebraic manipulations that are more tedious than difficult. Instead of using the four variables a, b, c and d just consider

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

$$\begin{aligned}(a^2 + 3b^2)^3 &= (a^2 + 3b^2)[(a^2 - 3b^2)^2 + 3(2ab)^2] \\ &= [a(a^2 - 3b^2) - 3b(2ab)]^2 + 3[a(2ab) + b(a^2 - 3br)]^2 \\ &= (a^3 - 9ab^2)^2 + 3(3a^2b - 3b^3)^2.\end{aligned}$$

Using this we can find cubes of the form $p^2 + 3q^2$ by choosing a and b at random and letting

$$p = a^3 - 9ab^2$$

$$q = 3a^2b - 3b^3.$$

We find that $p^2 + 3q^2 = (a^2 + 3b^2)^3$.

Euler's Mistake Euler proved that the only way $p^2 + 3q^2$ can be a cube is if there are numbers a and b such that p and q are given by the above equations. His proof was wrong because he used ideas from the arithmetic of whole numbers when considering numbers of the form $a+b\sqrt{-3}$. He assumed unique factorization simply because it is true in the integers without verifying it for the new ring where unique factorization does not exist. However, it is possible to fix his proof by using ideas that he published in other articles. The proof of the following Lemma is given by Edwards [1]. We will use it without proof.

Lemma 1.3.2. *Let p and q be relatively prime numbers such that p^2+3q^2 is a cube. Then there exist integers a and b such that $p+q\sqrt{-3} = (a+b\sqrt{-3})^3$.*

The form in the lemma is slightly different than what appears in the proof but it is easy to modify it. By multiplying out the expression and regrouping terms that contain $\sqrt{-3}$ we find, if $p^2 + 3q^2$ is a cube, then there exists integers a and b such that $p = a^3 - 9ab^2$ and $q = 3a^2b - 3b^2$.

The Infinite Descent We can factor the expressions for p and q as

$$p = a(a - 3b)(a + 3b)$$

$$q = 3b(a - b)(a + b).$$

If a and b have a factor in common, then the factor would divide the sum of a and b and thus divide p and q. Since p and q are relatively prime we know

that a and b must be relatively prime. Simply multiplying by 2 we see that there exists an integer n such that

$$2p = 2a(a - 3b)(a + 3b) = n^3.$$

We know that a and b cannot have the same parity because otherwise p and q would both be even. This follows easily from examining the equations and noticing that $a + b$ and $a + 3b$ will be even if a and b have the same parity. Therefore $a - 3b$ and $a + 3b$ are both odd. If there is a common factor of $2a$ and $a \pm 3b$ it is also a common factor of a and $a \pm 3b$. Since a divides a it must also be a common factor of a and $\pm 3b$. If the numbers $a+3b$ and $a-3b$ have a common factor it would divide their sum and difference. Thus any common factor would be a factor of a and $3b$. Three is the only possible common factor of a and $3b$ because a and b are relatively prime. But we know that $3 \nmid a$ because $a \mid p$ and by assumption $3 \nmid p$. This shows that $2a, a - 3b$ and $a + 3b$ are relatively prime and since $2p$ is a cube, all of them must be cubes. Thus there must exists values, α, β, γ, such that $2a = \alpha^3, a - 3b = \beta^3$ and $a + 3b = \gamma^3$. Consider adding together our terms to get $a - 3b + a + 3b = 2a$. Substitute in our new values for these terms to find $\beta^3 + \gamma^3 = \alpha^3$. This is a solution to Fermat's Equation when $n = 3$ with smaller integers than x, y, z. We must actually prove that the new solution uses smaller integers and that these integers are positive before our proof is complete.

Proving that new integers are smaller Notice that

$$\alpha^3\beta^3\gamma^3 = 2a(a - 3b)(a + 3b) = 2p.$$

Remember that we defined $z^3 = 2p(p^2 + 3q^2)$. Thus $2p$ divides z^3. It might still be the case that $2p = z^3$, but if not it must be smaller. We know $2p$ is positive. Since $2p$ is even it is a divisor of z^3 if z is even and a divisor of x^3 if x is even. In any case, then, α^3, β^3 and γ^3 are less than z^3. We must also consider what would happen if α, β or γ were negative. Since $(-\alpha)^3 = -\alpha^3$ we can just move negative cubes to the other side of the equation. The resulting equation will still have all cubes less than z^3. Thus we have really created an infinite descent of positive integers, but only in the case where $3 \nmid p$. To finish the proof assume that $3 \mid p$.

1.3.2 Case $3 \mid p$

Since we are assuming that p is divisible by 3 we can write $p = 3s$. We also know that $3 \nmid q$. Thus we can write $2p(p^2 + 3q^2) = 3^2 2s(3s^2 + q^2)$. Note that $2p(p^2 + 3q^2)$ is a cube so the next logical step is to show that $3^2 2s$ and $3s^2 + q^2$ are relatively prime. This step is similar to what we have already done. Assume that m is a prime numbers such that $m \mid 3^2 2s$. This means that $m \mid 3$, $m \mid 2$ or $m \mid s$. If $m \mid 3$ then we know that $m = 3$ and therefore that $3 \mid q$. We already know this is not true. If $m \mid 2$ then $m = 2$. However $3s^2 + q^2$ is not even because q and s are of opposite parity. This follows from the fact that p and q are opposite parity and factoring the 3 out of p to get s does not change the parity. Finally if $m \mid s$ then $m \nmid 3s^2 + q^2$ because s and q are relatively prime. Since $3^2 2s$ and $3s^2 + q^2$ are relatively prime they must both be cubes.

Lemma 1.3.3. *The number $3s^2+q^2$ can only be a cube if $q = a(a-3b)(a+3b)$ and $s = 3b(a-b)(a+b)$ for some integers a and b.*

This Lemma is equivalent to Lemma 1.3.2 with minor changes in algebra and variable names. Substitute our expression for s given in Lemma 1.3.3 and note that $3^3 2b(a-b)(a+b)$ is a cube. Therefore $2b(a-b)(a+b)$ is a cube. If a and b are relatively prime it is easy to see that each of the factors is relatively prime. We can tell that a and b are relatively prime because $(s, q) = 1$ so $(a(a-3b)(a+3b), 3b(a-b)(a+b)) = 1$. If $(a, b) = k$ then s and q would also have the common factor k.

Since the factors are relatively prime they must each be a cube. Therefore $2b = \alpha^3$, $a - b = \beta^3, a + b = \gamma^2$. Notice $\alpha^3 = 2b = \gamma^3 - \beta^3$. We show that $\gamma < z$ in a similar way as our other case. Notice that $\gamma^3 \mid 3^2 2s$ and $3^2 2s \mid 2p(p^2 + 3q^2) = z^3$. Thus we have found a solution in smaller integers and proven that $x^3 + y^3 = z^3$ is impossible in both cases. □

Chapter 2

Fermat's Last Theorem for case $n = 14$.

2.1 Historical Introduction

In 1832, seven years after Dirichlet and Legendre proved the case $n = 5$, Dirichlet published a proof of the case $n = 14$. It would have been more desirable to prove the case $n = 7$ because every $14th$ power is a $7th$ power but every $7th$ power is not a $14th$ power. Dirichlet was in effect admitting his failure to prove the $n = 7$ case with the publication of $n = 14$. Eventually in 1839 Lamè was able to prove the case $n = 7$, but the argument was "difficult, unmotivated, and, worst of all, seem[ed] hopelessly tied to the case $n = 7$"(Edwards 74). This proof did not provide hope for a general solution because it depended heavily of properties of the number 7. The proof of the case $n = 14$ depends on a similar technique to the proofs of $n = 5$ and $n = 3$ but requires considerable creativity in algebraic manipulation. The crux of the argument is again infinite descent, but in a slightly more complicated form.

2.2 Outline of Key Steps in Proof

Assume there exist pairwise relatively prime integers x, y and z that satisfy the equation $x^{14} + y^{14} = z^{14}$. We use tools from number theory to show that z is not divisible by 7 but either x or y must be divisible by 7. We define new smaller integers a and b that are also relatively prime. By creatively

choosing our values for a and b we can rewrite $y^{14} = 7c^2(7^5c^6 + b^2)$ where $c = 7a$. Keeping in mind that rings of imaginary numbers do not have unique factorization like normal integers we can factor $b^2+7^5c^6$ as $(b-7^2c^3\sqrt{-7})(b+7^2c^3\sqrt{-7})$ and show that these are relatively prime $14th$ powers. Subtract these $14th$ powers to arrive at an equation similar to $z^{14}-x^{14}$ and define a new a and b just as we did before. Using more creative algebraic manipulation of our $14th$ powers of the form $d \pm e\sqrt{-7}$ eventually yields and equation of the form $Z^{14} - X^{14} = 2^4Y^{14}$ where Y is divisible by 7. Now we start from the beginning again, paying attention to the 2^4 which only affects a few of the computations. We prove that the if $Z^{14} - X^{14} = 2^kY^{14}$ has a solution then $Z_1^{14} - X_1^{14} = 2^{4+9k}Y_1^{14}$ where Z_1, X_1 and Y_1 are smaller integers where Y is divisible by 7. After three repititions we arrive at another equation of the form $Z_2^{14} - X_2^{14} = Y_2^{14}$ This sets infinite descent into motion and we have reached a contradiction. Thus the equation $x^{14} + y^{14} = z^{14}$ does not have a solution.

2.3 The Proof

The details of each step will be included in order unless otherwise noted. Some calculations were pushed to the end because they were tedious and unnecessary to understand the proof.

2.3.1 Divisors of x, y and z

We assume there is a solution to $x^{14} + y^{14} = z^{14}$. Assume that x, y and z are pairwise relatively prime and positive. If they are not, we can divide out the common divisor. We identify properties of x, y and z that will be useful later in the proof.

Lemma 2.3.1. *The number z is not divisible by 7.*

Proof. We will proceed by contradiction. Assume $7 \mid z$. This implies $7 \mid x^{14} + y^{14}$. Since 14 is even we can write $7 \mid (x^7)^2 + (y^7)^2$. Let $a = x^7$ and $b = y^7$, then $7 \nmid a$ and $7 \nmid b$ but $7 \mid a^2 + b^2$ or $a^2 + b^2 \equiv 0 (\text{mod } 7)$. It is easy to see that the sum of two squares is not equivalent to 0 modulo 7 by looking at all the possibilities. All numbers not divisible by 7 are equivalent

to $1, 2, 3, 4, 5, 6$ modulo 7. Modulo 7:

$$\begin{aligned} 1^2 &\equiv 1 \\ 2^2 &\equiv 4 \\ 3^2 &\equiv 2 \\ 4^2 &\equiv 2 \\ 5^2 &\equiv 4 \\ 6^2 &\equiv 1. \end{aligned}$$

We can quickly check in our head that the sum of none of these numbers equals 7. Thus $7 \nmid z$. □

We now prove another property of x, y and z.

Lemma 2.3.2. *If x, y and z are pairwise relatively prime positive integers that satisfy $z^{14} - x^{14} = y^{14}$ then one of them must be divisible by 7.*

To prove this we can use a Theorem from Ireland and Rosen's *A Classical Introduction to Modern Number Theory*[2].

Theorem 2.3.3. *If Fermat's equation for an odd prime p*

$$x^p + y^p + z^p = 0$$

has a solution with $p \nmid xyz$ then

$$2^{p-1} \equiv 1(\ mod\ p^2).$$

In our case the prime is 7. It is easy to see that $2^6 \not\equiv 1(\text{ mod } 49)$ so 7 must divide either x, y or z. Without loss of generality assume 7 divides y.

2.3.2 Rewriting our equation

After determining some preliminary facts about the solution, we will substitute and factor creatively to rewrite our solution with a similar intention as in the cases where $n = 4$ and $n = 3$.

Lemma 2.3.4. *The equation $z^{14} - x^{14} = a(a^6 + 7b^2)$ where $a = z^2 - x^2$ and $b = zx(z^4 - z^2x^2 + x^4)$.*

This lemma can be verified using Maple, but the computation not important to the problem except perhaps that it is historically interesting to note how much time mathematicians spent making calculations. The only math required to prove the lemma is the ability to substitute and multiply polynomials. Once we have verified the expressions for a and b, we show they are relatively prime. To prove two numbers are relatively prime we assume they have a prime divisor and use this fact to reach a contradiction. The concept of relative primality is important in many places in this proof and will be proven using similar strategies each time.

Lemma 2.3.5. *The integers a and b are relatively prime and of opposite parity.*

Proof. We will prove that they are relatively prime by contradiction. Assume there is a prime number p, such that $p \mid a$ and $p \mid b$. Since $p \mid zx(z^4-z^2x^2+x^4)$ we know that $p \mid z$, $p \mid x$ or $p \mid z^4 - z^2x^2 + x^4$. If $p \mid z$ we can use the fact that $p \mid z^2 - x^2$ to conclude that $p \mid x$. This is a contradiction because by original assumption, x and z are relatively prime. If $p \mid x$ then using the same idea we can show that $p \mid z$ for a contradiction. Thus we can assume that $p \mid z^4 - z^2x^2 + x^4$ and $p \nmid x$ and $p \nmid z$. We will proceed to prove directly that if $p \mid b$ then $p \nmid a$. Since we know that $p \nmid x^4$ we know that $p \nmid z^4 - z^2x^2$. Thus we can factor to see that $p \nmid z^2(z^2 - x^2)$. This means that $p \nmid z^2$ and $p \nmid z^2 - x^2$, our expression for a. Thus if $p \mid b$ then $p \nmid a$. We have shown that a and b have no common factor p.

We will prove that they have opposite parity by contradiction. We know that a and b cannot both be even since they have no common divisors. Assume that a and b are both odd. We know that $z^{14} - x^{14} = a(a^6 + 7b^2)$. If a and b are both odd then $z^{14} - x^{14}$ is even. This means that y^{14} is even and both x^{14} and z^{14} are odd. If x^{14} is odd then we know that x is odd. If x and z are both odd then $z^2 - x^2$ is even. But $a = z^2 - x^2$ and by assumption a is odd. By contradiction we have shown that a and b cannot both be odd. Thus they have opposite parity. □

Lemma 2.3.6. *The number a is divisible by 7.*

Proof. Since $y^{14} = a(a^6+7b^2)$ and $7 \mid y$ we know that $7 \mid a(a^6+7b^2)$. Because 7 is prime, $7 \mid a$ or $7 \mid a^6 + 7b^2$. Since $7 \mid 7b^2$, if $7 \mid a^6 + 7b^2$ then $7 \mid a^6$. In any case we see that $7 \mid a$. Since a and b are relatively prime we know that $7 \nmid b$. □

We can substitute the value $a = 7c$ into our equation to get $y^{14} = 7c(7^6c^6 + 7b^2)$.

2.3.3 Finding new $14th$ powers

In this section we will show that we can write y^{14} as the product of two $14th$ powers. Factor to get $y^{14} = 7^2c(7^5c^6 + b^2)$. Rewrite this as $y^{14} = 7^2c(7(7^2c^3)^2 + b^2)$. If the product of 2 relatively prime integers is a $14th$ power then each of them is also a $14th$ power. We must show that 7^2c and $b^2 + 7(7^2c^3)^2$ are relatively prime.

Lemma 2.3.7. *The values 7^2c and $b^2 + 7(7^2c^3)^2$ are relatively prime and from this we conclude they are $14th$ powers.*

We will prove this by contradiction.

Proof. Assume p is a prime number such that $p \mid 7^2c$ and $p \mid b^2 + 7(7^2c^3)^2)$. Also note that since $(a, b) = 1$ we know that $(7c, b) = 1$ and therefore $(c, b) = 1$. We also know that $7 \nmid b$. Since $p \mid 7^2c$ we know that $p \mid 7$ or $p \mid c$. If $p \mid c$ then $p \mid 7(7^2c^3)^2$. By assumption $p \mid b^2 + 7(7^2c^3)^2$. This proves that $p \mid b^2$. This is a contradiction because b and c are relatively prime. In the other case $p = 7$. If $7 \mid b^2 + 7(7^2c^3)^2$ then $7 \mid b^2$ because it is easy to see that $7 \mid 7(7^2c^3)^2$. This is a contradiction because we know that $7 \nmid b$.

Thus $(7^2c, b^2 + 7(7^2c^3)^2) = 1$, and we conclude that both are $14th$ powers. □

2.3.4 Calculations in $\mathbf{Z}[\sqrt{-7}]$

The following lemma is necessary for the proof of $n = 14$ but its proof is beyond the scope of these notes. This is similar to Lemma 1.3.2 which is left unproven in the case $n = 3$. It is important to note that it is not a trivial conclusion because we are dealing with a ring with different properties than the integers. For example we can not assume unique factorization.

Lemma 2.3.8. *If $A^2 + 7B^2$ is a $14th$ power and if $7 \mid B$ then $A + B\sqrt{-7} = (a + b\sqrt{-7})^{14}$ for some integers a and b.*

In Lemma 2.3.7 we concluded that $b^2+7(7^2c^3)^2$ was a $14th$ power. We can rewrite this as $b^2 - (-7)(7^2c^3)^2$ so that we can factor it using the difference

of squares. We get,

$$b^2 - (-7)(7^2c^3)^2 = (b - 7^2c^3\sqrt{-7})(b + 7^2c^3\sqrt{-7}).$$

Let $b = A$ and $7^2c^3 = B$. By Lemma 2.3.8 we know that $b + 7^2c^3\sqrt{-7} = (d + e\sqrt{-7})^{14}$.

2.3.5 Finding new $14th$ powers(continued)

Because we have found new $14th$ powers we know that

$$b + 7^2c^3\sqrt{-7} = (d + e\sqrt{-7})^{14}$$

and

$$b - 7^2c^3\sqrt{-7} = (d - e\sqrt{-7})^{14}.$$

Subtract these two equations to yield $2 \cdot 7^2c^3\sqrt{-7} = (d + e\sqrt{-7})^{14} - (d - e\sqrt{-7})^{14}$. We can now rewrite $(d + e\sqrt{-7})^{14} - (d - e\sqrt{-7})^{14}$ as $z^{14} - x^{14}$ was rewritten earlier in our proof. We follow the same steps but replace $z = d + e\sqrt{-7}$ and $x = d - e\sqrt{-7}$. As before define $a = z^2 - x^2$ and $b = zx(z^4 - z^2x^2 + x^4)$ but with d and e instead. We must now do a fair amount of algebra to rewrite our equation once again. By manipulating it again we are getting closer to the goal of finding an equation with three $14th$ powers.

Lemma 2.3.9. *The equation* $2 \cdot 7^2c^3\sqrt{-7} = (d + e\sqrt{-7})^{14} - (d - e\sqrt{-7})^{14}$ *can be rewritten as*

$$7^2c^3 = 2 \cdot de[2^{12}(-7)^3d^6e^6 + 7f^2]$$

where $f = (d^2 + 7e^2)(d^4 - 98d^2e^2 + 49e^4)$.

Proving this lemma requires a fair amount of algebraic details. They are not inherently difficult but do take awhile to read though. They are included in Section 2.4 for completeness but understanding each step is not essential to understanding the proof. One part of the details that is essential to understanding later steps is the fact that $f = b$.

Lemma 2.3.10. *The integers* d *and* e *and* f *are relatively prime.*

Proof. Assume that there exists a prime number k such that $k \mid d$ and $k \mid e$. By looking at Lemma 2.3.9 we see that $k \mid 7^2c^3$. Since $k \mid d$ and $k \mid e$ we know that $k \mid d + e\sqrt{-7}$ as long as we are working in the ring $Z[\sqrt{-7}]$. This means that $k \mid (d + e\sqrt{-7})^{14} = b + 7^2c^3\sqrt{-7}$. Using the idea of a norm we find that $k^2 \mid b^2 + 7^5c^6$. Since $k \mid 7c^2$ we know that $k^2 \mid 7^5c^6$ and thus $k^2 \mid b^2$. This means that $k \mid b^2$ and since k is prime $k \mid b$. Since $7 \nmid b$ we know that $k \neq 7$ so $k^2 \mid 7^5c^6$ implies that $k \mid c$. This is a contradiction because b and c are relatively prime. Thus d and e must also be relatively prime. Now we will prove that f is relatively prime to d and e as well. Assume there exists and integer k such that $k \mid d$ and $k \mid f$. This implies that $k \mid d^2 + 7e^2$ or $k \mid d^4 - 98d^2e^2 + 49e^4$. Since $k \mid d$ we see that $k \mid 7e^2$ or $k \mid 49e^4$. We know that $k \neq 7$ because $7 \nmid f$. Thus $k \mid e$. We have already shown that d and e are relatively prime and thus we have reached a contradiction. □

Lemma 2.3.11. *The integers d and e have opposite parity and f is odd.*

Proof. The numbers d and e are related to b and c by the equation $b + 7^2c^3\sqrt{-7} = (d + e\sqrt{-7})^{14}$. We know that b and c are relatively prime and have opposite parity. If d and e are both even, then $b + 7^2c^3\sqrt{-7}$ is even and b and c have the same parity. If d and e are both odd then $b + 7^2c^3\sqrt{-7}$ is even and we reach the same contradiction. Now we will examine the number f. If we assume that d is even and e is odd we see that $f = (odd)(odd)$ so f is odd. When we switch the parities of d and e we see that f is still odd. We know that $7 \nmid f$ because we defined $f = b$ in our above equation and we know that 7 does not divide b. □

2.3.6 New Relatively Prime Factors

By factoring out a -7 we can rewrite the expression obtained in Lemma 2.3.9 as

$$7^2c^3 = 2 \cdot 7de[f^2 - (2^6 7d^3e^3)^2].$$

We can decompose this a product of three factors, $2 \cdot 7de$ and $f \pm 2^6d^3e^3$. We have already shown that d, e, f are relatively prime and that d and e have opposite parity. Now we will prove that these three factors are also relatively prime.

Lemma 2.3.12. *The numbers $f + 2^6 7d^3e^3$ and $f - 2^6 7d^3e^3$ are relatively prime.*

Proof. We will prove by contradiction. Assume that $k \mid f + 2^6 7d^3e^3$ and $k \mid f - 2^6 7d^3e^3$ where k is prime. By definition $k \mid f + 2^6 7d^3e^3$ and $k \mid f - 2^6 7d^3e^3$. Since k divides the sum and difference we know that $k \mid 2f$ and $k \mid 2^7 7d^3e^3$. First note that $f + 2^6 7d^3e^3$ and $f - 2^6 7d^3e^3$ are both odd so $k \neq 2$. Thus $k \mid f$ and $k \mid 7d^3e^3$. We showed above that $f = b$ and that b is not divisible by 7. Therefore $k \neq 7$ and $k \mid e^3$ or $k \mid d^3$. This means that k divides f and also e or d. This is a contradiction because the three numbers are pairwise relatively prime. □

Lemma 2.3.13. *The numbers $2 \cdot 7d$ and $f \pm 2^6 7d^3e^3$ are pairwise relatively prime.*

Proof. We will prove this by contradiction. Assume $k \mid 2 \cdot 7de$ and $k \mid f \pm 2^6 7d^3e^3$). This implies $k \mid 2 \cdot 7de$ and $k \mid f \pm 2^6 7d^3e^3$. We know that $k \neq 2$ because $f \pm 2^6 7d^3e^3$ is odd. Since $k \mid 2 \cdot 7de$ we know that $k \mid 2^6 7d^3e^3$ and therefore $k \mid f$. As before we know that $7 \nmid f$ so $k \neq 7$. Thus $k \mid 7de$ implies that $k \mid d$ or $k \mid e$. This is a contradiction because f, d and e are pairwise relatively prime. □

By using these lemmas and a few steps of algebraic manipulation we will find new $14th$ powers.

Lemma 2.3.14. *There exist integers Z and X such that $Z^{14} = f + 2^6 \cdot 7d^3e^3$ and $X^{14} = f - 2^6 \cdot 7d^3e^3$. Notice that $Z^{14} - X^{14} = 2^7 \cdot 7d^3e^3$, where $2 \cdot 7^5de$ is a $14th$ power.*

Proof. We know that

$$7^2c^3 = (2 \cdot 7de)(f \pm 2^6 \cdot 7d^3e^3)$$

Multiply both sides by 7^4 to get $7^6c^3 = (2 \cdot 7^5de)(f \pm 2^6 \cdot 7d^3e^3)$. Recall that 7^2c is a $14th$ power and notice that we can rewrite the equation as $(7^2c)^3 = (2 \cdot 7^5de)(f \pm 2^6 \cdot 7d^3e^3)$. We know that $f \pm 2^6 \cdot 7d^3e^3$ are not divisible by 7 because they are relatively prime to $2 \cdot 7de$. Thus the factors $2 \cdot 7^5de$ and $f \pm 2^6 \cdot 7d^3e^3$ are relatively prime and must each be $14th$ powers.

Let $Z^{14} = f + 2^6 \cdot 7d^3e^3$ and $X^{14} = f - 2^6 \cdot 7d^3e^3$. Notice that $Z^{14} - X^{14} = 2^7 \cdot 7d^3e^3$. □

We know that $2 \cdot 7^5de$ is a $14th$ power. If we cube it, then it is still a $14th$ power. Thus we find that $2^3 \cdot 7d^3e^3 \cdot 7^{14}$ is a $14th$ power and thus $2^3 \cdot 7d^3e^3$

is a $14th$ power. Thus $2^7 \cdot 7d^3e^3$ is 2^4 times a $14th$ power. We will use these facts to start our infinite descent.

We have found a solution to the equation $Z^{14} - X^{14} = 2^4Y^{14}$ where $Z = f + 2^6 \cdot 7d^3e^3$ and $X = f - 2^6 \cdot 7d^3e^3$. Starting with this equation we will repeat the procedure to find a solution to $Z_1^{14} - X_1^{14} = 2^{12}Y_1^{14}$. We have to repeat the procedure three times to arrive at another equation of the form $x^{14} + y^{14} = z^{14}$.

If we had found an equation equivalent to the one we assumed to be true initially we would have been done. Because of the addition of the extra factors of 2 we must do a few more steps to conclude that we have really established an infinite descent.

2.3.7 Starting the proof again

Lemma 2.3.15. *The numbers X, Z and Y that satisfy $Z^{14} - X^{14} = 2^4Y^{14}$ are pairwise relatively prime.*

Proof. First we will establish that Z and X are odd to help us deal with the complication of adding 2^4 to the equation. We know that $Z = f + 2^6 \cdot 7d^3e^3$ and that f is odd. Therefore Z must be odd. By the same argument we see that X is also odd. Let us assume that Z and X have a common factor k. We know that k is not even. If $k \mid Z$ and $k \mid X$ then we know that $k \mid Z^{14} - X^{14}$ and therefore $k \mid Y^{14}$. We could then factor out k from all three numbers to leave pairwise relatively prime variables. If k divides Z and Y or k divides X and Y then we can show by the same argument that k divides the third variable and can be factored out. □

We know from above that $2^4Y^{14} = 2^7d^3e^3$. We are trying to show that $7 \mid Y$. This is obvious as long as 7 was not one of the numbers we factored out when reducing our equations to pairwise relatively prime variables. We know that $7 \nmid Z$ or X because $7 \nmid f$ and $Z, X = f \pm 2^6 \cdot 7d^3e^3$. Thus we know that $7 \mid Y$.

Lemma 2.3.16. *The equation $z^{14} - x^{14} = 2^k y^{14} (k \geq 0)$ leads to $Z^{14} - X^{14} = 2^{4+9k}Y^{14}$ where Y is divisible by 7.*

Proof. Just as before we can rewrite $Z^{14} - X^{14} = a(a^6 + 7b^2)$ where a and b are relatively prime and of opposite parity. There are no changes to the proof of this fact. Our next equation must be slightly modified. We arrive

at the equation $7^2c(b^2 + 7(7^2c^3)^2) = 2^4Y^{14}$. If we multiply both sides of the equation by 2^{10} we can conclude as before that $2^{10}7^2c$ and $b^2 + 7(7^2c^3)^2$ are relatively prime. We must only note that c is even and since it is relatively prime to $b^2 + 7(7^2c^3)^2$ we know that multiplying 2^{10} by 7^2c does not affect the conclusion that the numbers are relatively prime. We can now factor the number $b^2+7(7^2c^3)^2$ exactly as before and eventually arrive at the conclusion that $7^2c^3 = 2 \cdot 7 \cdot de(f \pm 2^6 \cdot 7d^3e^3)$ where the factors are pairwise relatively prime.

Our proof now has to be slightly modified. This time we use the fact that $2^{10}7^2c$ is a $14th$ power. This implies that $2^{30}7^6c^3$ is also a $14th$ power. Multiply both sides of the equation $7^2c^3 = 2 \cdot 7 \cdot de(f \pm 2^6 \cdot 7d^3e^3$ by $2^{30}7^4$ to get

$$2^{10}7^6c^3 = 2^{31} \cdot 7^5 \cdot de(f \pm 2^6 \cdot 7d^3e^3).$$

These numbers are relatively prime so we know that 2^37^5de is a $14th$ power. Thus $2^9 \cdot 7^{15}d^3e^3$ is a $14th$ power and $2^7 \cdot 7d^3e^3$ is on the one hand a difference of $14th$ powers as before and 2^{12} times a $14th$ power. Thus we have found a solution to $Z_1^{14} - X_1^{14} = 2^{12}Y_1^{14}$ where Y_1 is divisible by 7. By doing the same thing one more time we find a solution to the equation $X_2 + Y_2 = Z_2$ and establish the infinite descent. We can continue this process again to find that generally $z^{14} - x^{14} = 2^ky^{14}(k \geq 0)$ leads to $Z^{14} - X^{14} = 2^{4+9k}Y^{14}$ where Y is divisible by 7. The details of this will be left to the reader as they are similar to what has been done before and are a good test of understanding. Our new numbers X, Y and Z are much smaller because of how they are defined. Thus $z^{14} - x^{14} = 2^ky^{14}$ is impossible by infinite descent. □

2.4 Computational Details

Here are the details for Lemma 2.3.9.

We can now rewrite this as $z^{14} - x^{14}$ was rewritten earlier in our proof. We let $z = d + e\sqrt{-7}$ and $x = d - e\sqrt{-7}$. As before I defined $a = z^2 - x^2$ and $b = zx(z^4 - z^2x^2 + x^4)$. We already have shown using Maple that $z^{14} - x^{14} = a(a^6 + 7b^2)$.

First we calculated the value of a. By substituting our values for x and z we see that $a = (d + e\sqrt{-7})^2 - (d - e\sqrt{-7})^2$. By multiplying and canceling terms we find that

$$a = 4de\sqrt{-7}.$$

We are trying to verify that $2 \cdot 7^2 c^3 \sqrt{-7} = a(a^6 + 7b^2)$. If we substitute our value for a we get $2 \cdot 7^2 c^3 \sqrt{-7} = 4de\sqrt{-7}(a^6 + 7b^2)$. Now we can cancel the 2 and $\sqrt{-7}$ to find that $7^2 c^3 = 2de(a^6 + 7b^2) = 2 \cdot de[2^{12}(-7)^3 d^6 e^6 + 7f^2]$. It is easy to see that $a^6 = (4de\sqrt{-7})^6 = 2^{12}(-7)^3 d^6 e^6$. Now we must only show that $f = b$ or that $z^4 - z^2x^2 + x^4 = d^4 - 98d^2e^2 + 49e^4$.

First rewrite the left side as $z^2(z^2 - x^2) + x^4$ so we can take advantage of the calculation for a. Now we have to finally get our hands dirty and make substitutions but it is really not too bad. Substituting $x = (d - e\sqrt{-7})$ and $z = (d + e\sqrt{-7})$ we get the expression

$$(d + e\sqrt{-7})^2 4de\sqrt{-7} + (d - e\sqrt{-7})^4.$$

After multiplying the terms out we get

$$4d^3e\sqrt{-7} - 56d^2e^2 - 28e^3d\sqrt{-7} + d^4 - 4d^3e\sqrt{-7} - 42d^2e^2 + 28de^3\sqrt{-7} + 49e^4.$$

After canceling and combining we see that $b = f = d^4 - 98d^2e^2 + 49e^4$.

By putting the pieces together we see that we have verified the expression $7^2 c^3 = 2 \cdot de[2^{12}(-7)^3 d^6 e^6 + 7f^2]$.

2.5 Conclusion

Although the details of the case $n = 14$ are long and tedious, the proof shares a similar structure to the proofs of $n = 3$ and $n = 5$. It is more difficult than the case $n = 4$ because one must take complex rings into account. Intuitive ideas about unique factorization must be proven rigorously and these notes only reference the complete proof. By comparing the three proofs presented here, one can begin to imagine the difficulty of of generalizing and infinite descent arugment to prove Fermat's Last Theorem. Although each proof has similarities, the calculations of each are different and require considerable creativity. Nothing in this approach clearly leads to a general proof. Sophie Germain was able to make considerable progress by proving Fermat's Last Theorem for an entire class of numbers but was still far from a complete proof. In fact the general proof utilized much more advanced and modern techniques that were well beyond the scope of this work. Wiles proof does not employ infinite descent and uses modern theorems about elliptical curves and modular forms. There are a number of books that explain his proof in varying levels of mathematical complexity but understanding it in its entirety is a major mathematical feat.

Bibliography

[1] Edwards, Harold M. "Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory." Springer-Verlag. New York. 1977.

[2] Ireland, Kenneth and Michael Rosen. "Elements of Number Theory: Including an Introduction to Equations over Finite Fields." Bogden & Quigley. New York. 1972.

[3] Singh, Simon. "Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem." Walker. New York. 1997.