4-23-2014

Fermat's Last Theorem

William Forcier
Lake Forest College, forciwc@lakeforest.edu

Fermat's Last Theorem

Abstract
First conjectured by Fermat in the 1630s, Fermat's Last Theorem has cause a great deal of advancement in the field of number theory. It would take the introduction of an entire new branch of mathematics in order to devise a proof for the rather simplistic looking equation. This document highlights the first major steps taken in proving the theorem, focusing on Kummer's proof for regular primes and the concepts that resulted. In particular Kummer's ideal numbers will be discussed as well as how they served as the precursors to ideals in ring theory.

Document Type
Thesis

Distinguished Thesis
Yes

Degree Name
Bachelor of Arts (BA)

Department or Program
Mathematics

First Advisor
David Yuen

Second Advisor
Enrique Treviño

Third Advisor
Jason A. Cody

Keywords
Fermat's last theorem, number theory, regular primes, ideal numbers

Subject Categories
Number Theory

LAKE FOREST COLLEGE

Senior Thesis

Fermat's Last Theorem

by

William Forcier

23 April 2014

The report of the investigation undertaken as
a Senior Thesis, to carry one course of credit in
the
Department of Mathematics.

Michael T. Orr Krebs Provost and Dean of the Faculty	David Yuen, Chairperson
	Enrique Treviño
	Jason A. Cody

Abstract

First conjectured by Fermat in the 1630s, Fermat's Last Theorem has cause a great deal of advancement in the field of number theory. It would take the introduction of an entire new branch of mathematics in order to devise a proof for the rather simplistic looking equation. This document highlights the first major steps taken in proving the theorem, focusing on Kummer's proof for regular primes and the concepts that resulted. In particular Kummer's ideal numbers will be discussed as well as how they served as the precursors to ideals in ring theory.

1 A Brief Introduction to Fermat's Last Theorem

Pierre de Fermat in the 1630s studied the book *Arithmetic* by Diophantus. During this time, he made several notes in the margin. Of these, Fermat wrote a note that states translated to English, "It is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as a 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. I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain." [1], [2]. While this was hardly Fermat's final mathematical statement, it remained unsolved until 1995. The theorem, in a much more familiar way, is written as such:

Theorem 1. *Let $n > 2$ be an integer. Then, the equation $X^n + Y^n = Z^n$ has no solutions where X, Y, Z are positive integers.*

While Fermat claimed to have a truly marvelous proof, one eluded mathematicians for hundreds of years, and the proof that does exist uses many concepts that did not exist in Fermat's time. We will focus on the development of a proof of Fermat's Last Theorem for a special class of numbers: the regular primes.

1.1 Limiting Conditions

In order to discuss Fermat's Last Theorem in full, it would help to only focus on the necessary components of the theorem. As such, we wish to limit the types of variables we need to consider for a general proof. These remarks are relatively simple, yet indispensable for any proof regarding the theorem.

Remark 1. *A proof of Fermat's Last Theorem for n=4 and all odd primes is sufficient to prove Fermat's Last Theorem for all n.*

Proof. Let $X^n + Y^n = z^m$ have solutions for positive integers X, Y, Z. Because $n > 2$, l is a divisor of n (we say $l|n$) such that l is 4 or an odd prime. Then, there exists an integer n, such that $n = lm$. We then have the equation

$$X^n + Y^n = Z^n$$
$$(X^m)^l + (Y^m)^l = (Z^m)^l$$

Therefore, X^m, Y^m, Z^m are integer solutions to the equation with exponent l, which equals 4 or an odd prime. □

Remark 2. *If the equation $X^n + Y^n = Z^n$ has solutions X, Y, Z, it has solutions such that X, Y, Z are pairwise coprime.*

Proof. Let $gcd(X, Y) = p$. The proof is similar if any other pair is chosen. Then,

$$X^n + Y^n = Z^n$$
$$(pX_o)^n + (pY_o)^n = Z^n$$
$$p^n(X_o^n + Y_o^n) = Z^n$$

Then $p|Z$, so

$$p^n(X_o^n + Y_o^n) = p^n(Z_o^n)$$
$$X_o^n + Y_o^n = Z_o^n$$

Therefore, X_o, Y_o are coprime now. □

2 The Biquadratic equation

The statement of Fermat's Last Theorem came about when Fermat attempted to solve the equation $X^4 - Y^4 = Z^2$. Fermat studied this equation as a means to determine if a Pythagorean triangle could have an area equal to the square of an integer [1]. A Pythagorean triangle is of the form $a^2 + b^2 = c^2$ with a, b, c being integers. If the area were equal to s^2 where s is an integer, then $2s^2 = ab$. Using these equations and some algebraic manipulation, we get $(a^2 - b^2)^2 = a^4 + b^4 - 2a^2b^2 = a^4 + b^4 + 2a^2b^2 - 4a^2b^2 = (a^2 + b^2)^2 - (2ab)^2 = c^4 - (2s)^4$. Therefore, if the equation $X^4 - Y^4 = Z^2$ had no integer solutions, there would be no such triangle with an area equal to an integer squared.

Besides this particular geometric interest, the biquadratic equation has a unique place in the solution of Fermat's Last Theorem. The first remark explains that a general solution of Fermat's Last Theorem only needs to consider the cases in which the exponent is prime or four. By determining that the Biquadratic has no solutions, we can turn our attention to exponent values that are prime. The idea behind these proofs came from [1].

2.1 The Pythagorean Theorem

While the Fermat equation, $X^n + Y^n = Z^n$ has no integer solutions for $n > 2$, it is actually quite simple to generate integer solutions when $n = 2$. These numbers, known as Pythagorean triples, were studied long before Fermat. In fact, generating Pythagorean triples such that $gcd(X, Y, Z) = 1$

will be pivotal to the solution of Fermat's Last Theorem for $n = 4$.

Remark 3. *If a, b are integers such that $a > b > 0$ and $gcd(a, b) = 1$, then the triple (x,y,z) given by*

$$\begin{cases} x = & 2ab \\ y = & a^2 - b^2 \\ z = & a^2 + b^2 \end{cases}$$

is a solution to the Pythagorean equation, and $gcd(x, y, z) = 1$.

Proof. First, $x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2$. Further, let $d = gcd(x, y, z)$. Then, d must divide $y + z = 2a^2$ and $z - y = 2b^2$. Since a and b are of different parity, both y and z must be odd. This implies that d divides both a and b, but $gcd(a, b) = 1$, so $d = 1$. □

2.2 Proof for n=4

Theorem 2. *The equation $X^4 - Y^4 = Z^2$ has no solution for positive integers X, Y, Z.*

Proof. Suppose $X^4 - Y^4 = Z^2$ has solutions for positive coprime integers X, Y, Z. Then, $X^4 - Y^4 = Z^2 \implies (X^2 + Y^2)(X^2 - Y^2) = Z^2$. We know that $gcd(X^2 - Y^2, X^2 + Y^2) = gcd(2X^2, X^2 + Y^2)$ as $gcd(x, y) = gcd(x + y, y)$. Since X and Y are relatively prime, either X and Y are both odd, and thus $X^2 + Y^2$ is even, which implies $gcd(2X^2, X^2 + Y^2) = 2$ or one of X and Y is even, which implies $gcd(2X^2, X^2 + Y^2) = 1$.

Case 1: $gcd((X^2 + Y^2), (X^2 - Y^2)) = 1$

Because $(X^2 + Y^2)$ and $(X^2 - Y^2)$ are coprime, they must both be squares for their product to equal a square, so let s and t be positive integers such that $s^2 = X^2 + Y^2$ and $t^2 = X^2 - Y^2$. Thus, the equation $s^2 + t^2 = 2X^2$ holds. Since s^2 and t^2 sum to an even number, s and t must both be even or both be odd, but since they are relatively prime s and t are both odd. Because they are odd, there exists a u and v in the integers such that $u = (s + t)/2$ and $v = (s - t)/2$. This leaves us with $uv = (s^2 - t^2)/4 = y^2/2$, so $y^2 = 2uv$. Since u and v are relatively prime and their produce equals two times a square, we say without loss of generality that $u = 2l^2$ and $v = m^2$. Consider

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

This leaves us with the Pythagorean Equation $u^2 + v^2 = X^2$. From the converse of Remark 3, a proof of which is in [1], since u, v, and X are relatively prime, we know that $u = 2ab = 2l^2$, $v = a^2 - b^2 = m^2$, and $X = a^2 + b^2$. Since $l^2 = ab$ there exists a c and d relatively prime such that $a = c^2$ and $b = d^2$, so $m^2 = a^2 - b^2 = c^4 - d^4$. Therefore, we have $X > u > a > c > 0$.

Case 2: $gcd((X^2+Y^2),(X^2-Y^2)) = 2$

So, we have the equation $Z^2 + Y^4 = X^4$. X and Y must both be odd for their squared sum to be even, which means Z is even, so by Remark 3, we know that $X^2 = a^2 + b^2$, $Y^2 = a^2 - b^2$, and $Z = 2ab$. So, $(XY)^2 = (a^2+b^2)(a^2-b^2) = a^4 - b^4$. Therefore, we have $X > a > 0$.

Both of these cases end the following way: given any solution (x, y, z) we can generate another solution (a, b, c) where $a < x$. However, the algorithm used above works on any solution, so by continuously applying it, we can generate an infinitely strictly decreasing sequence of solutions. However, there are not an infinite amount of positive integers strictly less than x, which is a contradiction. Therefore, there exists no solutions to the equation. □

Corollary 1. *The equation $X^4 + Y^4 = Z^4$ has no solutions for positive integers X, Y, Z.*

Proof.

$$X^4 + Y^4 = Z^4$$
$$X^4 = Z^4 - Y^4$$
$$(X^2)^2 = Z^4 - Y^4$$

By Theorem 2, the above equation has no solutions in the positive integers. □

3 Regular Primes

In the search for the solution to Fermat's Last Theorem, the first solution for a large class of numbers came from Ernst Kummer. Kummer's proof utilizes concepts of considering the equation over a ring other than the integers. By using a larger ring, it is possible to factor the Fermat equation into linear factors. The original proof was not originally submitted by Kummer and claimed to be a complete proof of the theorem. It was Kummer, however, who realized years before the proof came out, that these particular rings lacked unique factorization, a property the proof relied upon. The larger ring, the cyclotomic integers, and an introduction to them as well as Kummer's proof of Fermat's Last Theorem for regular primes, will be discussed. The proofs discussed in the proceeding sections take much from the discussion of Fermat's Last Theorem in [2].

3.1 The Cyclotomic Field

Consider the polynomial $x^n - 1$. By the Fundamental Theorem of Algebra, this polynomial has exactly n roots in $\mathbf{C}$. These particular roots are referred to as the nth roots of unity. It is possible

to generate these roots of unity utilizing the value $\zeta_n = e^{2\pi i/n}$.

$$\zeta_n^n = e^{2i\pi} = (-1)^2 = 1$$

Note that from this relation, for $0 \leq k < n$, $e^{k(2\pi i)/n}$ are all of the nth roots of unity. For any ζ we say that it is an nth primitive root of unity if $\zeta^d \neq 1$ for all $d < n$. Note that ζ_n is a primitive root of unity of order n. Consider the field generated by $\mathbf{Q}$ and ζ_n, notated as $\mathbf{Q}(\zeta_n)$. Every element in this field then, can be written as

$$\alpha = a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1}$$

In order to attempt to use members of this field for Fermat's Last Theorem, we will consider the nth roots of unity for prime n, and use this field to generate its ring of integers.

3.2 Cyclotomic Integers

Let n be a fixed prime and ζ be a primitive nth root of unity. The ring of Cyclotomic Integers can be represented as $\mathbf{Z}(\zeta)$, where each α can be expressed as $\alpha = a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1}$. This is not, however, a unique representation of $\alpha \in \mathbf{Z}(\zeta)$. Consider the polynomial $1 + x + x^2 + x^3 + \cdots + x^{n-1} = (x^n - 1)/(x - 1)$. Note that ζ is a zero, so $1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = 0$. Therefore, a unique representation can be gained by setting $a_0 = 0$ or $a_{n-1} = 0$. While a unique representation does exist, it is often simpler to use the nonunique version. We can write a particular cyclotomic integer as $f(\zeta)$, $g(\zeta)$, etc. This allows us to easily notate what are referred to as the conjugates of a cyclotomic integer $f(\zeta)$: $f(\zeta^2) \ldots f(\zeta^{n-1})$ where

$$f(\zeta^i) = a_0 + a_1\zeta^i + a_2(\zeta^i)^2 + \cdots + a_n(\zeta^i)^{n-1}$$

From here arises the concept of a norm of $f(\zeta)$

$$Nf(\zeta) = f(\zeta)f(\zeta^2) \ldots f(\zeta^{n-1})$$

It can be shown that that $Nf(\zeta) = 0 \iff f(\zeta) = 0$ and $f(\zeta)g(\zeta) = h(\zeta) \implies Nf(\zeta)Ng(\zeta) = Nh(\zeta)$. A less clear, but easily verifiable concept is that the norm is always a nonnegative integer. These concepts allow us to use the norm to factor cyclotomic integers into other cyclotomic integers with smaller norms. We can then discuss irreducible cyclotomic integers, where $Nh(\zeta) = p$, a prime. From the identity $f(\zeta)g(\zeta) = h(\zeta) \implies Nf(\zeta)Ng(\zeta) = Nh(\zeta)$, two factors of $h(\zeta)$ must have norm

1 and norm p. Consider an element with norm 1. Then,

$$1 = f(\zeta)f(\zeta^2)\dots f(\zeta^{n-1}) \implies f(\zeta)^{-1} = f(\zeta^2)\dots f(\zeta^{n-1})$$

Therefore, every element with norm 1 is a unit element. We define an element in any ring to be irreducible if it cannot be written as a product of non-units. Given that a particular $h(\zeta)$ with norm p when factored must have a factor of norm 1 implies that $h(\zeta)$ is irreducible. While we have a means now to factor a cyclotomic integer into irreducible numbers, there is no guarantee that these numbers are indeed prime. In particular, a cyclotomic integer, $f(\zeta)$ would be prime if

$$f(\zeta)|g(\zeta)h(\zeta) \implies f(\zeta)|g(\zeta) \text{ or } f(\zeta)|h(\zeta)$$

The fact that there exists cyclotomic integers that are irreducible but not prime is the reason that the later proof will not work for some exponents n, as unique factorization is not possible in some rings of cyclotomic integers.

3.3 Lamé's Proposed Proof

In 1847, Gabriel Lamé thought he had discovered a complete proof of Fermat's Last Theorem [2]. Having worked on previous cases, he had noticed a trend: as the values of n increase, the difficulty increased as well. While a general method existed, there were new difficulties with each increasing value. As such, Lamé wanted to find a way to simplify the factorization of the equation. In this endeavor, he turned to cyclotomic methods. In particular, given a fixed odd prime n, and a primitive nth root of unity ζ, we can factor the Fermat equation in the ring of cyclotomic integers $\mathbf{Z}(\zeta)$ as follows

$$x^n + y^n = (x + \zeta y)(x + \zeta^2 y)\dots(x + \zeta^{n-1} y)$$

This idea of factoring into complex numbers was not new. In fact, this exact type of factoring had previously been mentioned for use in Fermat's Last Theorem, but no one had claimed to have a proof using it until Lamé. It did not take long from the announcement for people to criticize the partially completed proof, the main hurdle being the need for unique factorization to hold for the cyclotomic integers. Despite Lamé's assurance that unique factorization held for the cyclotomic integers, it was Ernst Kummer, who had proven years earlier that unique factorization fails, that would take this idea to its culmination.

3.4 Prime Cyclotomic Numbers

While irreducible elements are useful, the concept of unique factorization requires that the elements be prime. Given our desire to factor the Fermat equation into linear factors, our initial focus is on prime factors of the form $(x+\zeta^i y)$, where x and y are relatively prime integers and $0 < i < n$. These prime elements are not only useful because of their relation to the Fermat equation, but they also compose the simplest prime elements in the cyclotomic integers. In order to analyze these prime elements we will suppose $h(\zeta)$ is a prime factor of $(x + \zeta^i y)$ and devise some useful properties that result.

Definition 1. *We say* $f(\zeta) \equiv g(\zeta)$ *mod* $h(\zeta)$ *if* $h(\zeta)|(f(\zeta) - g(\zeta))$

This relation maintains many of the same properties that normal modular congruence has as it is defined in a very similar way and follow directly from the definition. In a sense, the normal rules of modular arithmetic apply to this congruence relation. Consider a cyclotomic prime factor $h(\zeta)$ of $(x + \zeta^i y)$. Then, $h(\zeta)$ must be a factor of the norm of $(x + \zeta^i y)$ as the norm is a product that contains $(x + \zeta^i y)$. Since $N(x + \zeta^i y)$ is a normal integer, it is the product of normal prime integers. Then, since $h(\zeta)$ is prime, it must divide a particular p. In fact, it only divides integers which are multiples of p. Suppose $h(\zeta)$ divides k, which is not a multiple of p. Then, since p and k are relatively prime, then $1 = ap - bk$ for some integers a and b. From division rules, $h(\zeta)$ then must divide $ap - bk = 1$. However, that would imply $h(\zeta)$ is a unit element, which would mean it is not a prime. Thus, we are justified in saying the only integers that $h(\zeta)$ divides are multiples of p. From these statements, we have given u and v are integers,

$$u \equiv v \ mod \ h(\zeta) \iff u \equiv v \ mod \ p$$

This implies that both y and x are not zero mod p since $(x + \zeta^i y) \equiv 0 \bmod p$ would imply that both x and y have p as a factor, which contradicts x and y being relatively prime. Thus, y and p are relatively prime, so there exists an a such that $1 \equiv ay \bmod p$. Therefore, we have the following congruence mod $h(\zeta)$:

$$0 \equiv (x + \zeta^i y) \equiv a(x + \zeta^i y) \equiv ax + \zeta^i$$

So, ζ^i is congruent to an integer $-ax \bmod h(\zeta)$. Then, consider the integer j such that $\zeta = (\zeta^i)^j$. Which means that $\zeta \equiv (-ax)^j \bmod h(\zeta)$. This leads us to the following theorem.

Theorem 3. *Given* $h(\zeta)$ *is a prime cyclotomic integer that divides* $(x + \zeta^i y)$ *and* p*, there exists a* k *generated using the methods above such that given any cyclotomic integers* $f(\zeta)$ *and* $g(\zeta)$*:*

$$f(\zeta) \equiv g(\zeta) \ mod \ h(\zeta) \iff f(k) \equiv g(k) \ mod \ p$$

Where $f(k)$ is $h(\zeta)$ with ζ replaced by k in the expansion.

Proof. From the above, we know that $\zeta \equiv k \bmod h(\zeta)$. From the addition and multiplication properties, this implies any cyclotomic integer $\phi(\zeta) \equiv \phi(k) \bmod h(\zeta)$. Consider $f(k) \equiv g(k) \bmod p$. From the above, if two integers are equivalent mod p, they are equivalent mod $h(\zeta)$. So, $f(k) \equiv g(k) \bmod h(\zeta)$. From the congruence just stated, this implies $f(\zeta) \equiv g(\zeta) \bmod h(\zeta)$. □

This theorem provides us with a rather powerful statement about the values of p and k. Consider the cyclotomic integer

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1}$$

We have proven before that this integer is equal to zero, so the following equation must also hold by our above theorem.

$$1 + k + k^2 + \cdots + k^{n-1} \equiv 0 \; mod \; p$$

This means that $k^n \equiv 1 \bmod p$. Then, there exists a smallest integer d, such that $k^d \equiv 1 \bmod p$ and for all j such that $k^j \equiv 1 \bmod p$, $d|j$. Since $k^n \equiv 1 \bmod p$, and n is prime, then either d is 1 or n. If d is 1, by the above equation, $n = p$. If $d = n$, then by Fermat's Little Theorem, $k^{p-1} \equiv 1 \bmod p$. Therefore, $n|(p-1)$ or $p \equiv 1 \bmod n$.

If we consider the case of $p = n$, then $h(\zeta)$ must divide $\zeta - 1$. So, the norm of $h(\zeta)$ must divide the norm of $\zeta - 1$, and $N(\zeta - 1) = N(1 - \zeta) = (1 - \zeta)(1 - \zeta^2) \ldots (1 - \zeta^{n-1}) = n$. So $Nh(\zeta)$ divides n, but since n is a rational prime, $Nh(\zeta) = n$. Further, this implies that $h(\zeta)$ is a unit multiple of $\zeta - 1$. Considering the conjugates of $h(\zeta)$, each $h(\zeta^i)$ is prime (since conjugation maps preserve products) and each divides a binomial, which is the conjugate map of the polynomial $h(\zeta)$ divides, and p. Therefore, each have a $k \equiv 1 \bmod n$. Therefore, congruence mod $h(\zeta)$ is equivalent to congruence mod $h(\zeta^i)$. So, $h(\zeta)$ divides each conjugate and each conjugate divides $h(\zeta)$. Therefore, the conjugates of $h(\zeta)$ are all unit multiples of $\zeta - 1$.

Otherwise, $p \equiv 1 \bmod n$, which does not allow for a similar situation as above. In fact, if $h(\zeta^j)$ divided some $h(\zeta^i)$ where both are conjugates of $h(\zeta)$, then their modular congruences would be equal, so $\zeta^j \equiv k \equiv \zeta^i \bmod h(\zeta^i)$. From our previous reasoning, $h(\zeta^i)$ must divide $(\zeta^i - \zeta^j)$, so $Nh(\zeta)$ divides $N(\zeta^i - \zeta^j) = N(\zeta^{i-j} - 1) = n$. However, we have supposed that $p \neq n$, so no conjugate can divide any other. Further, since every $h(\zeta^i)$ divides p then.

$$\begin{aligned} p =& h(\zeta)q(\zeta) \\ p =& h(\zeta)h(\zeta^2)q_2(\zeta) \\ p =& h(\zeta)h(\zeta^2)\ldots h(\zeta^{n-1})q_{n-1}(\zeta) \end{aligned}$$

So, $p = Nh(\zeta)q$. Since p is a rational integer and the norm is a rational integer, then q must be a rational integer, namely 1, since p is prime. Therefore, we have that $p = Nh(\zeta)$. Combined with the previous case, we have:

Theorem 4. *Given $h(\zeta)$ a prime cyclotomic integer that divides a binomial $x+\zeta^i y$ (x and y relatively prime), $Nh(\zeta) = p$. Where p is some rational prime.*

From this theorem, which has been shown above, we move forward to the next step:

Theorem 5. *If $Nh(\zeta) = p$, a prime number, then $h(\zeta)$ is a prime element which divides a binomial $x + \zeta^i y$, where x and y relatively prime, $\zeta^i \neq 1$.*

Proof. Let $p \equiv 1 \bmod n$. Since it has been shown that if $h(\zeta)$ is prime there exists a k such that $\zeta \equiv k \bmod h(\zeta)$, we will prove that $h(\zeta)$ indeed divides a binomial of the form $\zeta - k$. Therefore, consider γ to be a primitive root mod p, that is γ^i represents all possible values mod p. Then $(\gamma^i)^n \equiv 1 \bmod p$ if and only if $p - 1$ divides in. Let $p - 1 = \mu n$. Then we have $(\gamma^i)^n \equiv 1 \bmod p$ if and only if μ divides i. Let $m = \gamma^\mu$. Then, $m, m^2, \ldots, m^n \equiv 1 \bmod p$ are n distinct solutions. Thus, finding our value k such that $h(\zeta)$ divides $\zeta - k$ is equivalent to finding the j such that $h(\zeta)$ divides $\zeta - m^j$ since $m^j \equiv k \bmod p$.

Now, treat $h(\zeta)$ as a polynomial, namely $h(X)$. Then, divide the polynomial $h(X)h(X^2)\ldots h(X^{n-1})$ by the polynomial $X^{n-1}+\cdots+X^1+1$. This will give us the form $q(X)\left(X^{n-1}+\cdots+X^1+1\right)+r(X)$. Now, with $X = m$, it is clear that $0 \equiv \left(m^{n-1}+\cdots+m+1\right)$, so $h(m)h(m^2)\ldots h(m^{n-1}) \equiv r(m) \bmod p$. Since $r(\zeta)$ is of degree less that $n-1$, $r(X)$ must equal p, so $h(m^j) \equiv 0$ for some j.

To determine if $h(\zeta)$ indeed divides $\zeta - m^j$ we will consider whether p, the norm of $h(\zeta)$ divides $(\zeta - m^j)h(\zeta^2)\ldots h(\zeta^{n-1})$. Divide the polynomial $X - m^j$ by $h(X)$ to get $h(X) = q(X)(X - m^j) + r$, where r is an integer. With $X = m^j$ it is clear that $r \equiv 0 \bmod p$, so for all values i, $h(\zeta^i) \equiv q(\zeta^i)(\zeta^i - m^j) \bmod p$. Since this is the case, we can substitute the values into our original equation to get:

$$(\zeta - m^j)h(\zeta)\ldots h(\zeta^{n-1}) \equiv N(\zeta - m^j)q(\zeta^2)\ldots q(\zeta^{n-1})$$

Consider, $N(\zeta - k) = (k^n - 1)/(k - 1) \equiv 0 \bmod p$, when $k = m^j$ So, $h(\zeta)$ must divide $\zeta - m^j$.

Then, consider $h(\zeta)$ divides $f(\zeta)g(\zeta)$. Then, $f(\zeta)g(\zeta) \equiv 0 \bmod h(\zeta)$, which means, because $\zeta \equiv k \bmod h(\zeta)$, $f(k)g(k) \equiv 0 \bmod p$. So, $f(k)$ or $g(k)$ is divisible by p since p is a rational prime, say without loss of generality p divides $f(k)$. This means that $f(k) \equiv 0 \bmod p$, which implies $f(\zeta) \equiv 0 \bmod h(\zeta)$. Finally, this culminates in $h(\zeta)$ divides $f(\zeta)$. Thus, $h(\zeta)$ is prime. □

3.5 Periods

In order to introduce the concepts of periods, and in turn develop our new concept of factorization, we first need a different form of notation. Let γ be a primitive root of unity mod n. Then let $\sigma f(\zeta) = f(\zeta^\gamma)$ and generally $\sigma^k f(\zeta) = f(\zeta^{k\gamma})$. Essentially, σ refers to the conjugate transformation that maps ζ to ζ^γ. Notably, the fact that γ is a primitive root ends up implying that $\sigma^n = \sigma$ and $\sigma^{n-1} f(\zeta) = f(\zeta)$.

Let e be some factor of $n-1$. Then, for a particular $f(\zeta)$ and e, define $F(\zeta) = f(\zeta)\sigma^e f(\zeta)\sigma^{2e} f(\zeta) \dots \sigma^{n-1-e} f(\zeta)$.

Theorem 6. $Nf(\zeta) = F(\zeta)\sigma F(\zeta) \dots \sigma^{e-1} F(\zeta)$

Proof. The norm of f is equal to $f(\zeta)f(\zeta^2)\dots f(\zeta^{n-1})$ and since γ is a primitive root mod n, then $Nf(\zeta) = f(\zeta)f(\zeta^\gamma)f(\zeta^{\gamma^2})\dots f(\zeta^{\gamma^{n-2}})$.

$$\begin{aligned}
F(\zeta) =& f(\zeta)f(\zeta^{\gamma^e})f(\zeta^{\gamma^{2e}})\dots f(\zeta^{\gamma^{n-1-e}}) \\
\sigma F(\zeta) =& f(\zeta^\gamma)f(\zeta^{\gamma^{e+1}})f(\zeta^{\gamma^{2e+1}})\dots f(\zeta^{\gamma^{n-e}}) \\
&\vdots \\
\sigma^{e-1} F(\zeta) =& f(\zeta^{\gamma^{e-1}})f(\zeta^{\gamma^{2e-1}})\dots f(\zeta^{\gamma^{n-2}})
\end{aligned}$$

This inevitably simplifies to $f(\zeta)f(\zeta^\gamma)f(\zeta^{\gamma^2})\dots f(\zeta^{\gamma^{n-2}})$. □

Because of the fact that $\sigma^e F(\zeta) = F(\zeta)$ as the conjugation simply permutes the factors of $F(\zeta)$, $F(\zeta)$ has a rather unique form with what are referred to as cyclotomic periods. We define $\eta_0 = \zeta + \sigma\zeta + \sigma^{2e}\zeta + \dots + \sigma^{n-1-e}\zeta$ and $\eta_{i+1} = \sigma\eta_i$. While the use of periods in the proceeding sections will be rather fleeting, they are useful in numerous applications in number theory and linear algebra and were studied extensively by Gauss prior to Kummer. The construction of the periods were dependent on values n and e, and utilized γ in their construction. Let $k = (n-1)/e$. We refer to the collection of periods as periods of length k, as they all have k terms. Note that these periods of length k are unique in the sense that a different γ only permutes terms and does not substantially change them.

The concept of periods will be used shortly to define the ideal numbers which will be used for ideal factorization.

3.6 Ideal Numbers and the Fundamental Theorem

Ideal numbers have the strange facet that they need not exist as real cyclotomic integers. As such, attempting to define them is a rather difficult task. However, even when ideal numbers do not exist

as cyclotomic integers, they exist in the sense that you can define actions utilizing them. We will begin with a introduction to a base type of ideal numbers known as the prime divisors.

Let n be an odd prime and ζ be a primitive nth root of unity. Then, let p be some prime number not equal to n. Let f be the smallest positive integer such that $p^f \equiv 1 \bmod n$. Then, f must divide $n-1$, so define $f = (n-1)/e$. Then, we consider the cyclotomic integers of the form $j - \eta_i$ where $1 \leq j \leq p$ and $1 \leq i \leq e$. Remove all of the values that are divisible by p. Define $\psi(\eta)_p$ to be the product of all remaining values. Utilizing this definition, we will discuss the concept of prime divisors.

A prime divisor P of a rational prime p can be viewed as both a literal divisor and an ideal divisor. If P is an element of the cyclotomic integers, then it will be a divisor in the sense defined below as well as the normal sense. However, if P is not an element of the cyclotomic integers, talking about normal divisibility does not make sense. There is, however, a number that would have the same properties as P if the ring of cyclotomic integers were extended in some way. In this sense, the ideal numbers fill in the gaps that make unique factorization impossible in the cyclotomic integers.

Our first concept will be congruence mod a prime divisor of p. Cyclotomic integers $g(\zeta)$ and $h(\zeta)$ are congruent mod a prime divisor of $p \neq n$ if and only if

$$g(\zeta)\sigma^i\psi(\eta)_p \equiv h(\zeta)\sigma^i\psi(\eta)_p \ mod\ p$$

In the event that $p = n$, $g(\zeta) \equiv h(\zeta) \bmod \zeta - 1$ is the definition. We define divisibility by a prime divisor from this definition. A number is said to be divisible by a prime divisor if and only if it is equivalent to zero mod that prime divisor.

An ideal number is a finite set of powers of prime divisors with multiplicity. The preceding sections should give notice to the fact that unique factorization for particular cyclotomic integers is hindered in some way for certain prime numbers n. However, we consider instead factorization into these ideal factors. We would then like this form of factorization to be unique.

An interesting aside involves the relations of these ideal numbers to the concept of ideals in ring theory. An additive subgroup I of a ring R is said to be ideal if for all x in I and y in R, xy and yx are in I. The definition has similar concepts to divisible. After all, if x is divisible by some p, so will xy. An ideal of the cyclotomic integers can then be viewed as the set of all elements divisible by P, a prime divisor.

In order to discuss factorization, it makes sense to first discuss the concept of divisibility. An ideal number A is divisible by B if and only if A contains the prime divisors of B with the same or greater multiplicity. We define I to be the special ideal number that contains no prime divisors. As such, it is clear that all ideal numbers are divisible by I. Thus, an ideal number A is said to be a

divisor of a cyclotomic integer $f(\zeta)$ if it is divisible by all of the prime divisors which divide $f(\zeta)$.

It is important to find out if prime divisors "act" like prime numbers in the sense that if $g(\zeta)h(\zeta)$ is divisible by a prime divisor P, then $g(\zeta)$ or $h(\zeta)$ is divisible by P. This follows quickly from the definitions above as this means that

$$g(\zeta)h(\zeta)\psi(\eta) \equiv 0 \ mod \ p$$

This means that $g(\zeta)h(\zeta)\psi(\eta)$ is divisible by p as a normal cyclotomic prime integer, which means that $g(\zeta)\psi(\eta)$ or $h(\zeta)\psi(\eta)$ are equivalent to 0 mod p, since p is a prime. Equivalence to zero mod p is the definition for divisibility by P.

Now that we have that prime divisors act as prime elements, we only need at this point a concept of unique factorization. That is if two cyclotomic integers are divisible by the same prime divisors, then they must be unit multiples of each other.

This question inevitably lead to Kummer's Fundamental Theorem.

Theorem 7. *A cyclotomic integer $g(\zeta)$ divides $h(\zeta)$ if and only if every prime divisor which divides $g(\zeta)$ also divides $h(\zeta)$ with greater than or equal to multiplicity.*

This theorem is fundamental in the sense that it provides us with the exact level of factorization that is needed. Consider our two cyclotomic integers that have the same prime divisors. Then they must divide each other. Then $g(\zeta)/h(\zeta)$ and $h(\zeta)/g(\zeta)$ are cyclotomic integers whose product equals one. Therefore, they are both units, so $g(\zeta)$ and $h(\zeta)$ are unit multiples.

Proof. Given a fixed cyclotomic ring of integers based on prime element n, let $f(\zeta)$ and $g(\zeta)$ be cyclotomic integers such that $f(\zeta) = q(\zeta)g(\zeta)$. Any prime divisor that would divide $g(\zeta)$ also divides $f(\zeta)$ with at least the same multiplicity. Similarly, any prime divisors which divide $Ng(\zeta)$ must divide $h(\zeta)g(\zeta^2)\dots g(\zeta)^{n-1}$. Since $Ng(\zeta)$ is a rational integer, it is sufficient to prove the theorem for just a rational integer.

Further, suppose all prime divisors that divide $f_1(\zeta)f_2(\zeta)$ also divide $g(\zeta)$. Then $f_1(\zeta)$ divides $g(\zeta)$, so there exists a $g_1(\zeta)$ such that $f_1(\zeta)g_1(\zeta) = g(\zeta)$. Similarly, every divisor of $g_2(\zeta)$ must divide $h_1(\zeta)$. Thus, there exists a $g_2(\zeta)$ such that $g_2(\zeta)f_2(\zeta) = g_1(\zeta)$. Thus, we have $g(\zeta) = f_1(\zeta)f_2(\zeta)g_2(\zeta)$, so $g(\zeta)$ is divisible by $f_1(\zeta)f_2(\zeta)$.

All that remains is to prove the theorem for prime rational integers. Suppose $f(\zeta) = n$. Then, $g(\zeta)$ is divisible by $(\zeta - 1)^{n-1}$, and thus divisible by $f(\zeta)$. Further, if $f(\zeta) = p$ and $p \neq n$, then since $g(\zeta)$ divides all the prime divisors of p, then $g(\zeta)$ is divisible by p. □

While this allows us the elusive ability of unique factorization, we actually lost something much more important: the ability to actually perform algebra on these ideal factors in a meaningful way.

In fact, the reason the proof of the Fermat Equation only works for the regular primes is that multiplying a set of prime divisors together need not generate an ideal number relating to an actual cyclotomic integer

3.7 Principle Divisors and the Class Number

Given a particular divisor, we would like to know if it can be said to actually relate to a particular cyclotomic number. We call these divisors principle. A divisor D is then principle if and only if there exists a unique cyclotomic integer $g(\zeta)$ such that $g(\zeta)$ divides a cyclotomic integer $h(\zeta)$ if and only if D divides $h(\zeta)$.

Two divisors A and B are said to be equivalent if AC is principle, then BC is principle (we say then that $A \sim B$). If we consider, for a moment, what happens when all of the ideals are in fact principle, a rather interesting thing happens. Since all ideals are principle, the definition above shows us that every ideal is in fact equivalent. That means that every divisor can be uniquely assigned a particular cyclotomic number. Since unique factorization holds for these prime ideals, then unique factorization must hold for cyclotomic integers. The reverse follows similarly, meaning that the cyclotomic integers for a particular n have unique factorization if and only if all of their ideals are principle.

From this concept, we define the class number. The class number is, in a sense, how far away from unique factorization the particular ring we are working with is. We define class number to be the amount of unique equivalence classes of the ideal numbers under the relation $\sim$.

3.8 Regular Primes

From the definition of the class number, we can determine what a regular prime is. A regular prime is defined by Kummer utilizing two criteria. However, the second follows from the first and is unnecessary to prove the first case of the theorem. As such, we will only consider the primary condition. A prime n is regular if and only if n does not divide the class number of the cyclotomic integers generated using the nth primitive root of unity.

The main result that this generates allows us to consider the first case of Fermat's Last Theorem utilizing these ideal numbers.

Lemma 1. *For any ideal C, if h is the class number, than C^h is principal.*

Proof. By the definition of class number, we know that all ideal numbers are equivalent to ideal numbers of a representative set $A_1, A_2, \ldots A_h$. Since there are h values, given $C, C^2, \ldots C^h$ contains $h+1$ values, there must be a C^j and a C^{j+k} such that they are both equivalent to the same A_l.

This means that C^j is equivalent to C^{j+k}. Let $B = N(C^j)/C^j$. Then $C^jB = N(C^j)$, since $N(C^j)$ is just a divisor for a rational integer, is principal.

So, C^jB and $C^{j+k}B$ are principle. Since C^jB is principal and C^jBC^k is principle, then C^k is also principle. Let d be the smallest number such that C^d is principle. Note that if $d = h$, we are done, so we consider the case where $d < h$ Then, $C, C^2, \dots C^{d-1}$ are all not principle and all not equivalent. In fact, this means that $I, C, C^2, \dots C^{d-1}$ represent d unique factors. Let E be some divisor not equivalent to this set of factors. Then, $E, EC, \dots EC^{d-1}$ are d more ideal numbers and they are all unique as EC^i equivalent to EC^{i+k} implies that C^k is principal. Further, the EC^i are all distinct from the C^j. If they were equivalent, then $j \geq i$ would give us that E were principle and $j < i$ would give us that C^j was principal.

Note that this particular method can be repeated until we exhaust all unique divisors. Note that because each of the EC are unique from all of the previous elements, as long as such an E exists, there will be d unique elements to generate. This means that if one divisor has not been listed, d divisors have not been listed. Therefore, d must divide h, so C^h must be principle. □

Theorem 8. *If n does not divide the class number and D^n is a principle ideal, then D is a principle ideal.*

Proof. Let h be the class number and D be any divisor such that D^n is principle. Since n is prime and n does not divide h, then there exists a, b rational integers such that $ah = bn + 1$. We know from our lemma above that D^h is principle, so $(D^h)^a$ is principle, but that is the same as $D^{ah} = D^{bn+1} = (D^n)^bD$. From our given, we know that D^n is principal, so $(D^n)^bD$ must be equivalent to D, so D is principal. □

3.9 The proof for Regular Primes

Traditionally, the proof of Fermat's Last Theorem has been split into two cases for prime n: the case in which n does not divide (x, y, z) and the case where n divides exactly one. We will prove the first case here for regular primes.

Theorem 9. *The equation $x^n + y^n = z^n$ has no solution in the positive integers when n is a regular prime.*

Proof. **Case 1:** n does not divide (X, Y, Z)

Assume x, y, z are relatively prime. We find a particular ζ, a primitive root of unity, such that $\zeta^n = 1$ and $\zeta^i \neq 1$ if $i < n$. Using this, we can factor $x^n + y^n$:

$$z^n = x^n + y^n = (x + y)(x + \zeta^n y) \cdots (x + \zeta^{n-1} y)$$

Since we are in case 1, all of the $(x+\zeta^j y)$ are relatively prime. Since their product in a nth power, then each divisor of the $(x+\zeta^j y)$ is a nth power. Let $j=1$. Then, there exists a divisor D such that $(x+\zeta y)=D^n$. D^n must be principal as it is associated with the cyclotomic integer $(x+\zeta y)$, so D must also be principal as n is a regular prime. This means that $(x+\zeta y)=ut^n$ where t is a cyclotomic integer and u is a unit. Consider the conjugacy homomorphism $\zeta \to \zeta^{-1}$. Then, if we let $\bar{\alpha}$ denote the complex conjugate of α, our equation becomes: $x+\zeta^{-1}y=\bar{u}\bar{t}^n$. Since u is a unit, $u\bar{u}=\zeta^j$ for some j. Further, $t^n \equiv \bar{t}^n \bmod n$ as nth powers are rational integers mod n, which the conjugation has no effect on.

$$\begin{aligned} x+\zeta^{-1}y &= \bar{u}\bar{t}^n \\ &= \zeta^{-r}e\bar{t}^n \\ &\equiv \zeta^{-r}et^n \ mod\ n \\ &\equiv \zeta^{-r}(x+\zeta y) \ mod\ n \\ \zeta^r(x+\zeta^{-1}y) &\equiv x+\zeta y \ mod\ n \end{aligned}$$

The value r cannot equal zero mod n as that would imply that $x+\zeta^{-1}y \equiv x+\zeta y \bmod n$, which implies y and n are not coprime. Therefore, we can assume that $0<r<n$. This means that

$$\zeta^r(x+\zeta^{-1}y) \equiv \zeta^{r-1}(x\zeta+y) \equiv [1+(\zeta-1)]^{r-1}\left[x+y+x(\zeta-1)\right] \ mod\ n$$

$$x+\zeta y \equiv x+(1+[\zeta-1])y \equiv x+y+y(\zeta-1) \ mod\ n$$

The combination of these two points gives us that $[1+(\zeta-1)]^{r-1}\left[x+y+x(\zeta-1)\right] \equiv x+y+y(\zeta-1) \bmod (\zeta-1)^{n-1}$. Note that coefficients of the powers of $(\zeta-1)$ must be congruent provided all powers are less than the $n-1$st. Note that if $2 \le r \le n-2$ this creates a contradiction, as this causes $x \equiv 0 \bmod n$, which is against our case 1 assumptions. If $r=n-1$, then consider the last two terms for the expansion of the above equation: $(n-2)[x(\zeta-1)^{n-3}+y(\zeta-1)^{n-3}+x(\zeta-1)^{n-2}]+[x(\zeta-1)^{n-2}+y(\zeta-1)^{n-2}+x(\zeta-1)^{n-1}]$. Collecting the $(\zeta-1)^{n-2}$, we get $(n-1)x(\zeta-1)^{n-2}$. So, this must be equal to zero mod n, which implies that $x \equiv 0 \bmod n$, also contradicting our case 1 assumptions.

The final case is then that $r=1$. This leaves us with the equivalence $[x+y+x(\zeta-1)] \equiv x+y+y(\zeta-1) \bmod n$. This, then, implies that $x \equiv y \bmod n$. Further, by the symmetry of the Fermat Equation, we know that $x \equiv y \equiv -z \bmod n$. Since $x^n \equiv x \bmod n$ by Fermat's Little Theorem, we know that $x^n+y^n-z^n \equiv x+y-z \equiv 3x \bmod n$. Because of our case 1 assumptions, we know that x is not equivalent to zero, so $n=3$, which is a contradiction for all regular primes

not equal to 3. □

4 Conclusion

The interesting part of this proof is less about the results and more about the methods utilized in reaching them. The concepts of prime divisors and ideal numbers present a rather useful notion to rings that do not have unique factorization. Kummer's fundamental theorem established what is essentially unique factorization for cyclotomic numbers into prime divisors. A logical extension would be to attempt to generalize this notion into something that can be tested on all integral domains. However, the definition of prime divisor is difficult to generalize to integral domains that aren't based on the rational integers.

The concept was formalized by Dedekind in the form of ideals, a relatively straight forward concept. An ideal is simply an additive subgroup of a ring such that any element of the ring multiplied by an element in the ideal produces and element in the ideal. Then, we can discuss a prime ideal to be an ideal such that ab in the ideal implies that a or b are in the ideal. From here, we can consider factorization into prime ideals. While the concept of factorization is not necessarily clear, allowing for factorization into prime ideals gives us increased structure that may not have existed in the original ring. Defining operations on these ideals allows us to perform algebraic proofs in a similar vein to the partial proof of Fermat's Last Theorem shown above.

This type of ring, referred to as a Dedekind domain, has significance based on the surprisingly simple condition it has. Compared to the requirements for a unique factorization domain, these are significantly easier to meet. Take for instance the cyclotomic integers of order p. The number of prime integers that create a unique factorization domain are not only finite, but few in number. While it is currently unknown the number of regular primes, it is expected that the number is infinite. The interesting part is that, the proof we have given for Fermat's Last Theorem, is relatively unchanged if we assume that the cyclotomic integers are a unique factorization domain. As such, these ideal numbers birthed by Kummer ended up becoming an incredibly powerful tool to solve algebraic problems.

References

[1] P. Ribenboim, *Fermat's last theorem for amateurs*, Springer. 1999.

[2] H. M. Edwards, *Fermat's last theorem: a genetic introduction to algebraic number theory.* Springer. 1977.