KUMMER, REGULAR PRIMES, AND FERMAT'S LAST THEOREM

ILA VARMA

CALIFORNIA INSTITUTE OF TECHNOLOGY

ABSTRACT. This paper rephrases Kummer's proof of many cases of Fermat's last theorem in contemporary notation that was in fact derived from his work. Additionally, it develops a reformulation of the proof using class field theory from a modern perspective in a manner similar to the tactics used for the complete proof, and describes how Kummer's proof strategy can generalize to solve the theorem for a broader set of primes.

1. INTRODUCTION

Ernst Kummer was a 19th century mathematician who came across Fermat's last theorem in attempts to generalize the law of quadratic reciprocity and study higher reciprocity laws. While he described those as "the principal subject and the pinnacle of contemporary number theory," he considered Fermat's last theorem a "curiosity of number theory rather than a major item" [1]. A priori, this was not an unreasonable opinion of a problem that could be understood by a 12-year-old. We state this mere curiosity below.

Theorem. *For any integer $n > 2$, the equation $x^n + y^n = z^n$ has no non-trivial solutions in the integers, i.e. if $x, y, z \in \mathbb{Z}$ satisfy this equation, then $xyz = 0$.*

Despite his disinterest, Kummer made the first substantial step in proving a part of Fermat's last theorem for many cases. This came only a few weeks after Gabriel Lamé incorrectly announced that he had found a complete proof [1]. Lamé did make the breakthrough in attempting to decompose $x^n + y^n$ into linear factors by introducing the complex numbers satisfying $\zeta^n = 1$, known today as roots of unity. This allowed for the algebraic identity

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

Thinking this was the only groundbreaking step needed to find the complete solution, Lamé presented a proof in March of 1847 using this fact while assuming incorrectly that this was a unique decomposition into prime ideals [1]. A few years before this, Kummer had already discovered that such unique factorization properties did not necessarily hold in the fields $\mathbb{Q}(\zeta_p)$ generated by these roots of unity. He introduced the origins of the notion of ideals in an attempt to salvage the disappearance of unique factorization, as well as the class number and an analytic formula describing it [3]. A few weeks after Lamé presented the incorrect proof, Kummer wrote a correct proof for a certain set of primes which had a property allowing for unique factorization to work in the step of Lamé's proof that went wrong. He called these regular primes, and in his later work, continued his examination of both regular and non-regular primes to find straightforwards characterizations and deeper properties. In his proof and this further examination, Kummer touched on ideas that would be developed into present-day ideal theory, Kummer theory, p-adic analysis & zeta functions, class field theory, etc. The core ideas on modern problems such as the Birth-Swinnerton-Dyer conjecture for the complex multiplication case and the theorems of Clausen and von Staudt are influenced by Kummer's work, not to mention the root for the eventual complete solution of Fermat's last theorem [4].

This article is intended to focus on Kummer's ideas for and influence on Fermat's last theorem, thus it stays in the realm of proving the theorem for regular primes. Many of the preceding lemmas are given in detail as a demonstration of the machinery needed, but additionally, a modern perspective is described, along with the generalization of Kummer's idea to a larger set of primes. Section 2 gives a background on cyclotomic fields and describes some properties needed for the proof based on Kummer's original work described in Sections 3 and 4. Section 5 reformulates the proof using an approach matching the strategies used for the complete solution. Finally, Section 6 is devoted to proving Fermat's last theorem for the most general characterization of primes on which Kummer's basic argument holds.

We must first describe general notation and some basic facts on cyclotomic fields and algebraic number theory. Then, we can go on to understand the core idea from the proof, and in particular where the regularity of primes fits in and therefore restricts the cases of Fermat's last theorem.

Roots of unity & cyclotomic fields. For any odd prime p, we denote a fixed *primitive pth root of unity* as ζ_p, i.e. $\zeta_p \in \mathbb{C}$ has the property that $\zeta_p^k \neq 1$ for any $k = 1, ...p - 1$ while $\zeta_p^p = 1$. It, along with all of its powers, is a root of the polynomial $x^p - 1$, hence it satisfies the equation $x^p = 1$, the motivation for its name. To find its minimal polynomial, we note that the only rational pth root of unity is $\zeta_p^p = 1$, hence we can factor $x^p - 1 = (x - 1)\Phi_p(x)$ where

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1.$$

This is called the *pth cyclotomic polynomial* as it is the minimal polynomial for ζ_p. Note that the other pth roots of unity are powers of ζ_p, and are all roots of $\Phi_p(x)$ (except for $\zeta_p^p = 1$). From an analytic perspective, we can think of $\zeta_p = e^{2\pi i/p}$, and subsequently, $\zeta_p^k = e^{2\pi ik/p}$. Here, we can see that all powers of ζ_p lie on unit circle ($f(z) = e^{2\pi iz}$) in the complex plane, and furthermore, the shape described with ζ_p^k as vertices is a regular p-gon. Furthermore in $\mathbb{C}$, we can factor $\Phi_p(x) = \prod_{k=1}^{p-1}(x - \zeta_p^k) = x^{p-1} + x^{p-2} + ... + x + 1$. From here, we know that the product of the non-trivial pth roots of unity (i.e. not including 1) has magnitude 1 (the constant coefficient) and the sum of the non-trivial pth roots of unity also has magnitude 1 (the x^{p-2} coefficient). More explicitly, we have the relation

$$\zeta_p + \zeta_p^2 + \zeta_p^3 + ... + \zeta_p^{p-1} = -1.$$

Hence, we have that the sum of all of the pth roots of unity is 0, i.e. any pth root of unity can be expressed as a linear sum of its other powers. It is in fact true that that any set of $p - 1$ roots of unity are linearly independent while the whole set is not.

We can also talk about the field generated by pth roots of unity over $\mathbb{Q}$ known as the *pth cyclotomic field*. Note that this field, denoted $K = \mathbb{Q}(\zeta_p)$, is automatically the splitting field for $\Phi_p(x)$ over $\mathbb{Q}$ as we have seen before that the rest of the roots are just subsequent powers of ζ_p. This extension has degree $p - 1$, coinciding with the degree of $\Phi_p(x)$, and furthermore, the group of automorphisms well-defined on K which fix $\mathbb{Q}$ is cyclic. More explicitly, the Galois group, $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ where the automorphism $\left[\sigma_k : \zeta_p \mapsto \zeta_p^k\right] \mapsto k$.

A bit of algebraic number theory. Stepping back from the specifics of cyclotomic fields, we can realize many useful properties of *number fields*, i.e. algebraic extensions over $\mathbb{Q}$ from algebraic number theory. First note that any <u>monic</u> polynomial with coefficients in $\mathbb{Z}$ that is known to have roots in $\mathbb{Q}$ in fact has roots in $\mathbb{Z}$ (known as the Rational Root theorem in high-school algebra). This interesting property can be used to describe the structure of $\mathbb{Z}$ within $\mathbb{Q}$, and we generalize this to any number field K. The elements of K which are roots of monic polynomials with coefficients in $\mathbb{Z}$ are known as the *algebraic integers* of K and furthermore produce a *ring of integers*, generally denoted $\mathcal{O}_K$. As an example, the ring of integers of any pth cyclotomic field $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p]$.

Like any other ring, $\mathcal{O}_K$ has ideals, and one property is that the ring of integers for any field K is a *Dedekind domain*, a type of integral domain with the added property that any ideal decomposes uniquely into a product of prime ideals. It is not necessarily true, however, that the elements of a Dedekind domain decompose uniquely into a prime or irreducible elements. It is not hard to find an example displaying this unfortunate fact: if $K = \mathbb{Q}(\sqrt{-5})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, and we can consider $6 = 2*3 = (1+\sqrt{-5})*(1-\sqrt{-5})$. Nevertheless, we can see that if all the ideals of a given $\mathcal{O}_K$ are principal, then the unique decomposition of prime ideals would give way to unique prime factorization of elements, as the factorization of any element $\alpha \in \mathcal{O}_K$ would be characterized by the decomposition of the ideal (α) into prime ideals generated by single irreducible elements. This motivates the construction of the *ideal class group* of K which is, loosely speaking, the quotient group of all the ideals in $\mathcal{O}_K$ modulo the principal ideals of $\mathcal{O}_K$. We are very lucky to find that

this group is always finite, and in fact, when the order is 1, we are in the previously described case of all ideals of $\mathcal{O}_K$ are principal. The *class number* of K, denoted h_K is the order of this ideal class group, hence if $h_K = 1$, $\mathcal{O}_K$ has unique prime factorization of elements. If $h_K > 1$, then $\mathcal{O}_K$ does not have unique prime factorization, but we can be more specific than that. The class number does describe the extent to which unique factorization holds; for example, there are properties about length of decompositions in fields of class number 2 that do not hold for fields with higher class number.

Regular primes. The property of whether a prime p is *regular* can be characterized based on the *class number* of $K = \mathbb{Q}(\zeta_p)$. As described above, we think of the class number as a scalar quantity describing how "close" elements of $\mathcal{O}_K$ are to having unique factorization, but explicitly the class number h_K is the order of the ideal class group.

Definition 2.1. An odd prime p is *regular* if the class group of $K = \mathbb{Q}(\zeta_p)$ has no p-torsion, i.e. if the class number h_K is prime to p.

It is astonishing to think that such a fact should be related to the ease of proving Fermat's last theorem, but it is in fact the case. Lamé's first step of decomposing a nontrivial counterexample $x^p + y^p = z^p$ in the field $\mathbb{Q}(\zeta_p)$ only goes so far when we don't have unique prime factorization of the elements. It is easy to work with z^p when considering it as an ideal of $\mathcal{O}_K$, but at some point, we must be able to look at specific elements of the ring of integers rather than the ideals they generate. A priori as ideals, we get

$$(z)^p = (x + y)(x + \zeta_p y)(x + \zeta_p^2 y)...(x + \zeta_p^{p-1} y).$$

On one side, we have a pth power of a principal ideal, and on the other, we have a decomposition into p ideals that are not only distinct, but can be shown to be relatively prime. The property of unique decomposition into prime ideals tells us that every ideal $(x + \zeta_p^k y)$ must independently be a pth power of an ideal A_k. Thinking about the structure of the ideal class group, we can consider what kinds of ideals of $\mathcal{O}_K$ have a pth power which is principal. As elements of this quotient group, the ideals of $\mathcal{O}_K$ modulo the principal ideals of $\mathcal{O}_K$, it is clear that $(x + \zeta_p^k y)$ is identified with the trivial element, but it is not necessarily true that A_k is. Nevertheless, if we have the added assumption that the prime p is regular, then we know that the class number is prime to p, hence no element in the ideal class group can have order p without being trivial. This directly implies that A_k is principal, and we can in fact think about the element α_k generating this ideal rather than the ideal $(\alpha_k) = A_k$ itself. From this point onward, Kummer's proof consists of algebraic manipulations of units and algebraic integers in K leading to a contradiction that cannot be done simply by working with ideals. It is easy to see that the regularity of p is the broadest way to guarantee that the pth "roots" of the ideals generated by $x + \zeta_p^k y$ are in fact principal, bringing the entire machinery down to elements of $\mathcal{O}_K$.

Prime decomposition. It is interesting to note that prime ideals of a base field may not stay prime in an extension. For example, we can show that in $K = \mathbb{Q}(\zeta_p)$, the ideal generated by p decomposes as

$$(p) = (1 - \zeta_p)^{p-1}.$$

where $(1 - \zeta_p)$ turns out to be a prime ideal of $\mathcal{O}_K$. In algebraic number theory, we are quite interested in <u>how</u> a prime ideal such as (p) in a base field $\mathbb{Q}$ occurs in a larger field such as K. It is "easiest" when a prime stays *inert*, i.e. stays prime in the larger field extension. However, in many cases, such as the above, a prime ideal of the base field will decompose further in the extension, and it is particular interesting to note when such a decomposition includes repeated factors, i.e. when the prime *ramifies*. The case where the prime of the base field can be written as a power of a single prime ideal in the extension is known as *total ramification*. Additionally, for total ramification, we require that the power of the single ideal coincides with the degree of the extension. As an example, we will prove that p totally ramifies in K as a power of $(1 - \zeta_p)$. To prove the above fact about (p), we first introduce the notion of *cyclotomic units*.

Definition 2.2. The *cyclotomic units* of $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ are elements of the form

$$\frac{\zeta_p^r - 1}{\zeta_p^s - 1} \quad \text{where } p \nmid rs.$$

It is easy to see that these are units as they have obvious inverses, $\frac{\zeta_p^s - 1}{\zeta_p^r - 1}$, hence the cyclotomic units are in fact a subgroup of $\mathcal{O}_K^\times$. Furthermore, we see that since $p \nmid rs$, we can find t such that $r = st \pmod{p}$ hence allowing us to express

$$\frac{\zeta_p^r - 1}{\zeta_p^s - 1} = \frac{\zeta_p^{st} - 1}{\zeta_p^s - 1} = 1 + \zeta_p^s + ... + \zeta_p^{s(t-1)} \in \mathcal{O}_K.$$

Lemma 2.3. *The principal ideal generated by p in $\mathcal{O}_K$ decomposes as $(1 - \zeta_p)^{p-1}$, and hence the principal ideal $(1 - \zeta_p)$ is prime in $\mathcal{O}_K$.*

Proof. Since the minimal polynomial of ζ_p is $\Phi_p(x) = \frac{x^p - 1}{x - 1}$, as a polynomial in $K[x]$, it can be decomposed as

$$\Phi_p(x) = \prod_{i=1}^{p-1}(x - \zeta_p^i).$$

Note that if we plug in $x = 1$ to $\Phi_p(x)$ we get from the polynomial in $\mathbb{Q}[x]$ and the polynomial in $K[x]$ that

$$p = \prod_{i=1}^{p-1}(1 - \zeta_p^i).$$

Note that $1 - \zeta_p$ is a unit away from $1 - \zeta_p^i$, i.e. $1 - \zeta_p^i = u(1 - \zeta_p)$ where u is the cyclotomic unit $\frac{\zeta_p^i - 1}{\zeta_p - 1}$. Thus we have an equality of ideals $(1 - \zeta_p) = (1 - \zeta_p^i)$. This, combined with the decomposition of p gives us $(p) = (1 - \zeta_p)^{p-1}$. Furthermore, since $[K : \mathbb{Q}] = p - 1$, from algebraic number theory we know that (p) can have at most $p - 1$ factors, hence the previous decomposition of (p) is in fact a prime decomposition, so we also get that $(1 - \zeta_p)$ is a prime ideal in $\mathcal{O}_K$. $\square$

3. Preliminaries

We now move to definitions and facts needed specifically for Kummer's proof. The following propositions and lemmas are crucial in Kummer's proof. The following lemmas allow us to relate the algebraic integers in $\mathcal{O}_K$ with the rational integers in $\mathbb{Z}$. Kummer's main breakthrough in his proof was to work in an extension of $\mathbb{Q}$ where $(x^p + y^p)$ decomposed, so within the proof, he must go back and forth when dealing with elements of $\mathcal{O}_K$ and elements of $\mathbb{Z}$ using properties outlined by these lemmas.

Lemma 3.1. *Suppose $\alpha = a_0 + a_1\zeta_p + ... + a_{p-1}\zeta_p^{p-1}$ with each $a_i \in \mathbb{Z}$. If $a_i = 0$ for at least one i, then if $n \in \mathbb{Z}$ such that $n \mid \alpha$, then $n \mid a_j$ for all j.*

Proof. We know that $1 + \zeta_p + ... + \zeta_p^{p-1} = 0$, hence any $p - 1$ elements of $\{1, \zeta_p, ..., \zeta_p^{p-1}\}$ is a basis for $\mathcal{O}_K$ over $\mathbb{Z}$. By assumption $a_i = 0$, so we choose the corresponding basis without ζ_p^i. The other coefficients make α an element of $\mathcal{O}_K$ with respect to this basis. Hence, if $n \mid \alpha$, then n must divide the coefficients of the basis representation of α, i.e. $n \mid a_j$ for each j. $\square$

Lemma 3.2. *Let $\alpha \in \mathcal{O}_K$. Then α^p is congruent $\pmod{p}$ to an element of $\mathbb{Z}$.*

Proof. Take $\{1, ..., \zeta_p^{p-2}\}$ as the basis of $\mathcal{O}_K$. We can then write $\alpha = a_0 + a_1\zeta_p + ... + a_{p-2}\zeta_p^{p-2}$, where $a_i \in \mathbb{Z}$. This gives

$$\alpha^p \equiv a_0^p + (a_1\zeta_p)^p + ... + (a_{p-2}\zeta_p^{p-2})^p \equiv a_0^p + a_1^p + ...a_{p-2}^p \pmod{p},$$

since all nontrivial binomial coefficients are congruent to $0 \pmod{p}$. $\square$

Lemma 3.3. *Assume x, y, z are a nontrivial solution to the equation $x^p + y^p = z^p$. The ideals $(x + \zeta_p^i y)$ with i ranging between $\{0, ..., p - 1\}$ are either relatively prime as ideals or have exactly 1 common factor $(1 - \zeta_p)$ such that the ideals generated by the quotients $\frac{x + \zeta_p^i y}{1 - \zeta_p}$ are relatively prime.*

Proof. We make the assumption that x and y are relatively prime. Suppose $\exists \, \mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ such that $\mathfrak{p} \mid (x + \zeta_p^i y)$ and $\mathfrak{p} \mid (x + \zeta_p^j y)$. From above, we know that $(1 - \zeta_p) = (1 - \zeta_p^k)$ as ideals when $p \nmid k$. Thus, $\mathfrak{p} \mid (x + \zeta_p^i y) - (x + \zeta_p^j y)$, however

$$(x + \zeta_p^i y) - (x + \zeta_p^j y) = (\zeta_p^i y - \zeta_p^j y) = (1 - \zeta_p)(y).$$

Hence, $\mathfrak{p} \mid (1 - \zeta_p)$ or $\mathfrak{p} \mid (y)$. Similarly, we know that $(x + \zeta_p^i y) = (\zeta_p^{j-i} x + \zeta_p^j y)$, hence $\mathfrak{p} \mid (\zeta_p^{j-i} x + \zeta_p^j y) - (x + \zeta_p^j y)$. Since $(\zeta_p^{j-i} x - x) = (1 - \zeta_p^{j-i})(x) = (1 - \zeta_p)(x)$, we get that $\mathfrak{p} \mid (1 - \zeta_p)$ or $\mathfrak{p} \mid (y)$. Since x and y are coprime, one of these two statements implies that $\mathfrak{p} \mid (1 - \zeta_p)$. However, since $(1 - \zeta_p)$ is a prime ideal, we in fact get equality. Furthermore, note that if $(1 - \zeta_p) \mid (x + \zeta_p^k y)$, then $(1 - \zeta_p) \mid (x + \zeta_p^{k+1} y)$ since

$$(x + \zeta_p^{k+1} y) = (x + \zeta_p^k y) + (\zeta_p^k)(\zeta_p - 1)(y).$$

Thus, if $(1 - \zeta_p)$ is a factor of $(x + \zeta_p^i y)$ for one i, then it is a factor for all i. In particular, we get that $x + y \equiv 0 \pmod{1 - \zeta_p}$. Since $x + y \in \mathbb{Z}$, then $x + y \equiv 0 \pmod{p}$, however $x^p + y^p \equiv x + y \pmod{p}$, hence $z \equiv z^p \equiv 0 \pmod{p}$, i.e. $p \mid z$. If $p \nmid z$, we've arrived at a contradiction here, and thus $(1 - \zeta_p)$ cannot be a common factor so in fact, the ideals $(x + \zeta_p^i y)$ have no common factors. If $p \mid z$, then we have that the only common factor between any two $(x + \zeta_p^i y)$ and $(x + \zeta_p^j y)$ is $1 - \zeta_p$.

It remains to be shown that $(1 - \zeta_p)^2$ is not a factor of any two $(x + \zeta_p^i y)$ and $(x + \zeta_p^j y)$. Recall that we are assuming that $p \mid z$, hence we can further assume that $p \nmid y$ as if this were the case, then $p \mid x$ as well, and we could reduce the counterexample $x^p + y^p = z^p$ by a factor of p^p (During the proof, we use this argument to claim that the counterexample x, y, z is relatively prime). Without loss of generality, assume that $i > j$ and note that

$$(x + \zeta_p^i y) - (x + \zeta_p^j y) = \zeta_p^i y - \zeta_p^j y = \zeta_p^j y(\zeta_p^{i-j} - 1).$$

From the fact that $(1 - \zeta_p) = (1 - \zeta_p^{i-j}) = (\zeta_p^{i-j} - 1)$ as ideals, we have that $1 - \zeta_p$ divides $\zeta_p^{i-j} - 1$ exactly once. Furthermore, since $1 - \zeta_p \mid y$ then $p \mid y$ (since $y \in \mathbb{Z}$) and $1 - \zeta_p$ is relatively prime to ζ_p^j, we have that $1 - \zeta_p \mid (x + \zeta_p^i y) - (x + \zeta_p^j y)$ but $(1 - \zeta_p)^2 \nmid (x + \zeta_p^i y) - (x + \zeta_p^j y)$. Hence, we know that the quotients $\frac{x + \zeta_p^i y}{1 - \zeta_p}$ are relatively prime. $\qquad\square$

For any prime p, $\mathbb{Q}(\zeta_p)$ is automatically a subfield of $\mathbb{C}$ but not of $\mathbb{R}$. We can see that the automorphisms of $\mathrm{Gal}(K/\mathbb{Q})$ never send $\mathbb{Q}(\zeta_p)$ into $\mathbb{R}$. Furthermore, one of these automorphisms is the map of conjugation, sending $a + bi \mapsto a - bi$, its conjugate. Since the automorphisms have a group structure, we can pair each automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ with its *conjugate*, the unique automorphism described by composing σ with the map of conjugation. Note that this is equivalent in pairing elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ with their additive inverse. However, there is a large subfield K^+ in $\mathbb{Q}(\zeta_p)$ which sits inside of $\mathbb{R}$, and properties of K and this subfield K^+ gives us information on the number of independent elements of each field and relates the corresponding rings of integers, $\mathcal{O}_K$ and $\mathcal{O}_{K^+}$ with the use of Dirichlet's Unit Theorem, stated below.

Theorem 3.4 (Dirichlet's Unit Theorem). *For any field K over $\mathbb{Q}$ with r real embeddings and s conjugate pairs of complex embeddings, the unit group $\mathcal{O}_K^\times$ is finitely generated with rank equal to*

$$\mathrm{rank}(\mathcal{O}_K^\times) = r + s - 1.$$

Proposition 3.5. *Fix some odd prime p, and let $K = \mathbb{Q}(\zeta_p)$. We have the following properties.*

(1) K is a totally complex field, i.e. $\exists$ 0 real embeddings and $\frac{p-1}{2}$ pairs of conjugate complex embeddings.
(2) The maximal totally real subfield of K is $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, i.e. $K \cap \mathbb{R} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Furthermore, $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ and $[K : K^+] = 2$.
(3) K and K^+ have the same unit rank, hence the embedding of the corresponding unit groups $\mathcal{O}_{K^+}^\times \hookrightarrow \mathcal{O}_K^\times$ has finite index.

Proof. (1) Since all nontrivial pth roots of unity are primitive, the automorphisms $\zeta_p \mapsto \zeta_p^k$ are embeddings into $\mathbb{C}$ that cannot be entirely contained in $\mathbb{R}$. Thus, there are no real embeddings and there are $p - 1$ complex embeddings, hence $r = 0$ and $s = \frac{p-1}{2}$.
(2) Geometrically, we can see that $\zeta_p + \zeta_p^{-1} \in \mathbb{R}$ as their imaginary coefficients are additive inverses, hence

$\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is a subfield of K entirely contained in $\mathbb{R}$. Note that ζ_p is the root of a polynomial in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})[x]$ defined as $f(x) = x^2 - (\zeta_p + \zeta_p^{-1})x + 1$. Since $f(x)$ is degree 2 and $x - \zeta_p$ is not a polynomial in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})[x]$, $f(x)$ is automatically the minimal polynomial for ζ_p over $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, hence $[K : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] = 2$. This additionally shows that $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is the maximal real subfield in K since we have already seen that K is not totally real.

(3) By Dirichlet's Unit Theorem, we know that the rank of $\mathcal{O}_K^{\times}$ is a $r + s - 1 = \frac{p-1}{2} - 1$. Furthermore, as K^+ is totally real, the rank of $\mathcal{O}_{K^+}^{\times}$ is $[K^+ : \mathbb{Q}] - 1 = \frac{p-1}{2} - 1$. $\qquad\square$

Units in $\mathcal{O}_K^{\times}$ can be be easily described in terms of units in $\mathcal{O}_{K^+}^{\times}$ since the maximal real subfield is rather large in such a manner that the index of the unit groups is finite. We show in the following proposition that any unit of K can be decomposed into a product of pth root of unity and a totally real unit in $\mathcal{O}_{K^+}^{\times}$.

Proposition 3.6. *For any $u \in \mathcal{O}_K^{\times}$, $\exists\ v \in \mathcal{O}_{K^+}^{\times}$ and an integer r such that $u = \zeta_p^r v$. It follows that the index of $\mathcal{O}_{K^+}^{\times}$ in $\mathcal{O}_K^{\times}$ is p.*

Sketch of proof. Consider some arbitrary unit $u \in \mathcal{O}_K^{\times}$ and let $\alpha = \frac{u}{\bar{u}}$ where $\bar{u}$ denotes the image of u under the map of conjugation. It follows that α is an algebraic integer and additionally, $|\alpha| = 1$. Furthermore, $|\sigma_k(\alpha)| = 1$ for each $\sigma_k \in \mathrm{Gal}(K/\mathbb{Q})$ since for all k, $\sigma_k(\bar{u}) = \overline{\sigma_k(u)}$. It is a fact used often in algebraic number theory that any algebraic integer whose Galois conjugates all have norm 1 must be a root of unity, so in particular, $\frac{u}{\bar{u}} = \pm\zeta_p^k$ for some k. It remains to show that $\alpha = +\zeta_p^k$. Assuming otherwise, we arrive at the contradiction that either 2 or $\bar{u}$ is contained in the prime ideal generated by $(1 - \zeta_p)$ from expressing both u and $\bar{u} \pmod{1 - \zeta_p}$. These two statements cannot be true based on a highly technical norm argument (not discussed here) and the fact that $\bar{u}$ is a unit. Hence, we have $\alpha = \zeta_p^k$ for some k. From here, we find r such that $2r \equiv k \pmod{p}$, we set $v = \zeta_p^{-r}u$, hence $u = \zeta_p^r v$ (Note that if $\alpha = -\zeta_p^k$, then finding such an r does not work). We see that $\bar{v} = \overline{\zeta_p^{-r}u} = \zeta_p^r \bar{u}$, hence $\frac{v}{\bar{v}} = \frac{\zeta_p^{-r}u}{\zeta_p^r \bar{u}} = \zeta_p^{-2r}\alpha = 1$, so v is in fact real, and therefore an element of K^+. $\qquad\square$

Kummer's Lemma. *If p is a regular prime and u is in $\mathcal{O}_K^{\times}$ such that u is congruent $\bmod\, p$ to an element of $\mathbb{Z}$, then u is a pth power of an element of $\mathcal{O}_K^{\times}$.*

The statement above, although seemingly simple, uses a lot of machinery, including the class number formula, p-adic L-functions, and the characterization of regular primes using Bernoulli numbers. In fact, when Kummer first defined regular primes, he included this property as another condition and proved it much later. Kummer's proof of this statement is given in [1].

4. CASE I: THE MAIN ARGUMENT

We are now ready to present the proof when $p \nmid xyz$, generally known as the first case of Fermat's last theorem for regular primes. With this added assumption, Lemma 3.3 proves that the ideals $(x + \zeta_p^i y)$ are pairwise coprime. The main steps in this proof are obtained from this fact and the regularity of p, and are also used in the main argument for the second case and its generalizations in the following sections. The proof from this section uses the main ideas from Kummer's proof but is reformulated in the language of modern mathematics and uses some new lemmas. It is based on the proof in [5]. We restate the assumptions for this case of the theorem that will be proved in this section.

Theorem 4.1. *Suppose $p > 3$ is a regular prime. Then*

$$x^p + y^p = z^p, \quad p \nmid xyz$$

has no nontrivial solutions in the rational integers, i.e. any integer solution (x, y, z) has the property that $xyz = 0$.

Proof. Fix some regular prime $p > 3$, and assume that we have a nontrivial $x, y, z \in \mathbb{Z}$ satisfying the hypothesis. First, we can assume x, y, z are relatively prime, otherwise we can divide by their greatest common denominator to get another counterexample. Additionally, we show that for any such counterexample (x, y, z) we can rearrange to ensure that $x \not\equiv y \pmod{p}$ (which will be needed later). Suppose that $x \equiv y \equiv -z \pmod{p}$. Then note that

$$z \equiv z^p \equiv x^p + y^p \equiv x + y \equiv -2z \pmod{p} \implies 3z \equiv 0 \pmod{p},$$

then $p \nmid z$ implies $p \mid 3$, a contradiction to the fact that $p > 3$. Since we know that $x \equiv y \not\equiv -z \pmod{p}$, we can exchange y and $-z$ to get another counterexample satisfying all the hypotheses and $x \not\equiv y \pmod{p}$.

Kummer's main argument. In $\mathcal{O}_K$, we have the decomposition of ideals

$$(z)^p = (z^p) = (x^p + y^p) = (x + y)(x + \zeta_p y)...(x + \zeta_p^{p-1} y),$$

and furthermore, all ideals on the right hand side are pairwise relatively prime. Since this decomposition is equal to the pth power of the ideal generated by z, we have that each $(x + \zeta_p^i y)$ must be a pth power of an ideal. (We can see this by considering the decomposition of (z) into prime ideals $\mathfrak{p}$. Since no $\mathfrak{p}$ is shared between various $(x + \zeta_p^i y)$, then in the corresponding decomposition of $(z)^p$, each $\mathfrak{p}^p$ is a factor of exactly one $(x + \zeta_p^i y)$.) Explicitly, we can write $(x + \zeta_p^i y) = \mathfrak{I}_i^p$ where $\mathfrak{I}_1 \mathfrak{I}_2 ... \mathfrak{I}_{p-1} = (z)$, and each $\mathfrak{I}_i^p$ is principal. This is where we use the regularity of p, and hence this is why the proof is limited to primes which do no divide the class number. Since each $\mathfrak{I}_i^p$ is principal, then in the class group defined as the group of ideals of $\mathcal{O}_K$ modulo the group of principal ideals of $\mathcal{O}_K$, we find that $\mathfrak{I}_i^p$ is trivial in the quotient group. However, the class group has order h_K which is not divisible by p, so there cannot exist a nontrivial element that has p-torsion, i.e. that is annihilated by the exponent p. Thus, $\mathfrak{I}_i$ must also be trivial in the class group, hence $\mathfrak{I}_i$ is also principal. Here, we see that if there was no assumption on the divisibility of h_K by p, then in fact $\mathfrak{I}_i$ need not be principal.

Since $\mathfrak{I}_i$ is principal, let $\alpha_i \in \mathcal{O}_K$ be its generator. Thus, $(x + \zeta_p^i y) = (\alpha_i)^p = (\alpha_i^p)$ hence $x + \zeta_p^i y = u\alpha_i^p$ for some unit $u \in \mathcal{O}_K^\times$. Note that we only need to treat the case for $i = 1$ (as we note that all nontrivial pth roots of unity are primitive so based on the choice of ζ_p we can cycle through all cases). From Proposition 3.6, we can write $u = \zeta_p^r v$ where r is an integer and $v = \overline{v}$ is an element of $\mathcal{O}_{K^+}^\times$. By Lemma 3.2, $\exists$ a rational integer $a \in \mathbb{Z}$ such that $\alpha_i^p \equiv a \pmod{p}$. Thus, $x + \zeta_p y = \zeta_p^r v \alpha_i^p \equiv \zeta_p^r v a \pmod{p}$. Furthermore, we get

$$x + \zeta_p^{p-1} y = x + \zeta_p^{-1} y = \zeta_p^{-r} v \overline{\alpha_i}^p \equiv \zeta_p^{-r} v \overline{a} \equiv \zeta_p^{-r} v a \pmod{p}.$$

We know that $x + \zeta_p y \equiv \zeta_p^r v a \equiv \zeta_p^{2r}(x + \zeta_p^{-1} y) \pmod{p}$ if and only if $x + \zeta_p y - \zeta_p^{2r} x - \zeta_p^{2r-1} y \equiv 0 \pmod{p}$. If $1, \zeta_p, \zeta_p^{2r}, \zeta_p^{2r-1}$ are distinct, then by Lemma 3.1, $p \mid x, y$ a contradiction, and we are done. We know that 1 and ζ_p must be distinct, and similarly, ζ_p^{2r} and ζ_p^{2r-1} must also be distinct, thus we are left with 3 cases, which all hinge on Lemma 3.1:

(1) $1 = \zeta_p^{2r}$: From this, we get $x + \zeta_p y - x - \zeta_p^{-1} y \equiv 0 \pmod{p}$, i.e. $\zeta_p y - \zeta_p^{p-1} y \equiv 0 \pmod{p}$, hence from Lemma 3.1, $p \mid y$, a contradiction.

(2) $\zeta_p = \zeta_p^{2r-1}$: This assumption reduces the congruence $x + \zeta_p y - \zeta_p^{2r} x - \zeta_p^{2r-1} y \equiv 0 \pmod{p}$ to $x - \zeta_p^2 x \equiv 0 \pmod{p}$, hence again from Lemma 3.1, $p \mid x$, a contradiction.

(3) $1 = \zeta_p^{2r-1}$: Note that this is equivalent to the relation $\zeta_p = \zeta_p^{2r}$, which reduces the congruence $x + \zeta_p y - \zeta_p^{2r} x - \zeta_p^{2r-1} y \equiv 0 \pmod{p}$ to $(x - y) - \zeta_p(x - y) \equiv 0 \pmod{p}$, so by Lemma 3.1, $p \mid x - y$, i.e. $x \equiv y \pmod{p}$, a contradiction to the choice of (x, y, z) made at the beginning of the proof. This proves that such a counterexample cannot exist, and the proof is complete.

$\square$

Note that Kummer's original proof did not end in the same manner. After showing that $x + \zeta_p y = \zeta_p^r v \alpha$, Kummer found a congruence similar to $x + \zeta_p y - \zeta_p^{2r} x - \zeta_p^{2r-1} y \equiv 0 \pmod{p}$, and looked at coefficients using the binomial expansion of $1 + (\zeta_p - 1)^{r-1}$ to show that such an r cannot exist. However, the main argument Kummer was able to make was in showing that $\mathfrak{I}_i$ were principal, and thus $(x + \zeta_p^y)$ where pth powers of

algebraic integers in $\mathcal{O}_K$. The final case $p \mid z$ still rests upon this main property, and is in fact, a reduction to the proof of the first case of Fermat's last theorem for regular primes.

5. CASE II: COMPLETING THE PROOF

In this section, we finish the proof by assuming $p \mid z$. We can make this stronger assumption instead of $p \mid xyz$ since for any counterexample (x, y, z) we can assume x, y, and z, are pairwise coprime, thus p only divides one of x, y, or z. We can rearrange and flip signs such that $p \mid z$. In this situation, Lemma 3.3 proves that the ideals $(x + \zeta_p^i y)$ have exactly one common factor, the prime ideal $(1 - \zeta_p)$. The proof from this section is the reformulation of Kummer's original proof for the second case in modern language. This proof uses the same main argument as the first case, but also involves the method of infinite descent in which a contradiction is reached by showing that if there is one "smallest" counterexample, then we can continue to construct "smaller" counterexamples ad infinitum. We restate the assumptions for this second case of the theorem that will be proved in this section.

Theorem 5.1. *Suppose $p > 3$ is a regular prime. Then*
$$x^p + y^p = z^p, \quad p \mid z$$
has no nontrivial solutions in the rational integers, i.e. any integer solution (x, y, z) has the property that $xyz = 0$.

Proof. We prove a stronger statement: There are no nontrivial solutions to $x^p + y^p = U(1 - \zeta_p)^{kp} z_0^p$ where $x, y, z_0 \in \mathcal{O}_K$ and $U \in \mathcal{O}_K^\times$ and relatively prime to each other as well as $1 - \zeta_p$. Note that the actual theorem is then just a special case where z is just written out as a product of its p-part and z_0, and x, y, z_0 are all integers.

Assume we have a counterexample satisfying the hypotheses. We have the decomposition of ideals $U(1 - \zeta_p)^{kp} z_0^p = (x+y)(x+\zeta_p y)...(x+\zeta_p^{p-1} y)$. By this equality, we know that for some i, $1 - \zeta_p \mid x + \zeta_p^i y$, however by the same argument in Lemma 3.3, this implies that for all i, $x + \zeta_p^i y$ is divisible by $1 - \zeta_p$, and furthermore, the quotients $\frac{x + \zeta_p^i y}{1 - \zeta_p}$ generate ideals which are pairwise relatively prime, again following from the same argument. We use the following lemma which allows us to assume that x and y are congruent to rational integers a and b modulo $(1 - \zeta_p)^2$.

Lemma 5.2. *For any algebraic integer $\alpha \in \mathcal{O}_K \backslash (1 - \zeta_p)$, $\exists l$ such that $\zeta_p^l \alpha \equiv a \pmod{(1-\zeta_p)^2}$ where $a \in \mathbb{Z}$.*

Proof of Lemma. Note that $\mathcal{O}_K = \mathbb{Z}[\zeta_p] = \mathbb{Z}[1 - \zeta_p]$, hence one integral basis for $\mathcal{O}_K$ involves the powers of $(1 - \zeta_p)$. Therefore, we can find integers $a_0, a_1 \in \mathbb{Z}$ such that $\alpha \equiv a_0 + a_1(1 - \zeta_p) \pmod{(1 - \zeta_p)^2}$. Furthermore, since a_0 is nonzero outside of $(1 - \zeta_p)$, we can find $l \in \mathbb{Z}$ such that $a_1 \equiv a_0 l \pmod{p}$. Since $\zeta_p = 1 - (1 - \zeta_p)$, we have $\zeta_p^l \equiv 1 - l(1 - \zeta_p) \pmod{(1 - \zeta_p)^2}$. Thus,
$$\zeta_p^l \alpha \equiv (1 - l(1 - \zeta_p))(a_0 + a_1(1 - \zeta_p)) \equiv a_0 + (a_1 - la_0)(1 - \zeta_p) \equiv a_0 \pmod{(1 - \zeta_p)^2}.$$
$\square$

Returning the the proof of the theorem, we know that $\zeta_p^l x$ and $\zeta_p^j y$ are congruent to rational integers modulo $(1 - \zeta_p)^2$. Since we merely need x and y to satisfy the equation $U(1 - \zeta_p)^{kp} z_0^p = x^p + y^p$, exchanging them for $\zeta_p^l x$ and $\zeta_p^j y$ does not change anything. We know that $x + y \equiv a + b \pmod{(1 - \zeta_p)^2}$, where $a, b \in \mathbb{Z}$ are the integers congruent to x, y respectively. Since $1 - \zeta_p \mid x + y$, then $1 - \zeta_p \mid a + b$, which implies $p \mid a + b$ since $a + b \in \mathbb{Z}$. This, in turn, proves that $(1 - \zeta_p)^2 \mid x + y$ which tells us that k must be strictly greater than 1. To use the method of infinite descent, we choose our nontrivial counterexample (x, y, z_0) such that k is minimal. Our contradiction will arise from the construction of a new counterexample (x', y', z_0') such that $x'^p + y'^p = U'(1 - \zeta_p)^{(k-1)p} z_0'^p$.

From above, we know that $(1 - \zeta_p)^2 \mid x + y$, and by Lemma 3.3, we know that the quotients $\frac{x + \zeta_p^i y}{1 - \zeta_p}$ are relatively prime, hence all of the extra powers of $(1 - \zeta_p)$ divide $x + y$ only. Since $(1 - \zeta_p)^{p-1} \mid (x +$

8

$\zeta_p y)(x + \zeta_p^2 y)...(x + \zeta_p^{p-1} y)$ exactly, (i.e. $(1 - \zeta_p)^p \nmid (x + \zeta_p y)(x + \zeta_p^2 y)...(x + \zeta_p^{p-1} y))$. We know further that $(1 - \zeta_p)^{kp} \mid x^p + y^p$ exactly, hence $(1 - \zeta_p)^{kp-p-1} \mid x + y$. Thus, $(1 - \zeta_p)^{(k-1)p} \mid \frac{x+y}{1-\zeta_p}$ exactly. This will be crucial when we consider the ideal generated by the quotients.

Changing Fermat's equation to ideals we have

$$\left((1 - \zeta_p)^{k-1} z_0\right)^p = \prod_{i=0}^{p-1} \left(\frac{x + \zeta_p^i y}{1 - \zeta_p} \right),$$

where the ideals on the right are relatively prime. As in the first case, by Kummer's main argument, we have that each ideal generated by $\frac{x+\zeta_p^i y}{1-\zeta_p}$ is a pth power of a principal ideal, hence $\exists\, \alpha_i \in \mathcal{O}_K$ such that we have the equalities $\frac{x+\zeta_p^i y}{1-\zeta_p} = u_i \alpha_i^p$ where u_i are units in $\mathcal{O}_K^\times$. Furthermore, we know that $\{\alpha_0, ..., \alpha_{p-1}\}$ are pairwise relatively prime since their pth powers are relatively prime. From the previous argument, we know that $(1 - \zeta_p)^{k-1} \mid \alpha_0$, and we can furthermore write $\alpha_0 = (1 - \zeta_p)^{k-1}\beta$ where β is relatively prime to $1 - \zeta_p$. From the equalities of $x + \zeta_p^i y$, we use $x + \zeta_p y$ and $x + \zeta_p^{p-1} y = x + \zeta_p^{-1} y$ as well as the new substitution for $x + y$ to get

$$(1 - \zeta_p)^{(k-1)p} u_0 \beta^p - u_1 \alpha_1^p = \frac{(x + y) - (x + \zeta_p y)}{1 - \zeta_p} \quad = \quad y$$

$$\zeta_p (1 - \zeta_p)^{(k-1)p} u_0 \beta^p - \zeta_p u_{-1} \alpha_{-1}^p = \frac{(x + \zeta_p^{-1} y) - (x + y)}{\zeta_p^{-1}(1 - \zeta_p)} \quad = \quad y$$

$$\left[\zeta_p (1 - \zeta_p)^{(k-1)p} u_0 \beta^p - \zeta_p u_{-1} \alpha_{-1}^p\right] - \left[(1 - \zeta_p)^{(k-1)p} u_0 \beta^p - u_1 \alpha_1^p\right] \quad = \quad 0$$

If we let $U' := \frac{(1+\zeta_p)u_0}{-u_1}$ and $V' := \frac{\zeta_p u_{-1}}{-u_1}$, then they are units and the last equation simplifies to $U'(1 - \zeta_p)^{(k-1)p}\beta^p = \alpha_1^p + V'\alpha_{-1}^p$. If we consider the equation modulo p, then since $p \mid (1 - \zeta_p)^{p-1}$, we have $0 \equiv \alpha_1^p + V'\alpha_{-1}^p \pmod{p}$. Recall from Lemma 3.2, we know that $\alpha_{\{1,-1\}}^p \equiv a_{\{1,-1\}} \pmod{p}$ where $a_1, a_{-1} \in \mathbb{Z}$, thus $0 \equiv a_1 + V'a_{-1} \pmod{p}$ (Note that a_1 and a_{-1} are nonzero as they are relatively prime to α_0 which is divisible by p). However, this implies that V' must in fact be congruent to a rational integer $\pmod{p}$. Kummer's Lemma then allows us to rewrite V' as a pth power of some unit $v \in \mathcal{O}_K^\times$. If we let $x' := \alpha_1$, $y' := v\alpha_{-1}$, and $z_0' = \beta$, then we have $U'(1 - \zeta_p)^{(k-1)p} z_0'^p = x'^p + y'^p$, another counterexample which contradicts the minimality of k. This completes the proof for the second case, and thus Fermat's last theorem holds for regular primes. $\qquad \square$

6. A MODERN VIEW

Kummer's proof of Fermat's last theorem can be reformulated to involve a modern approach that was attempted for the proof of the entire theorem. For any counterexample at prime p, the goal is to attach a representation ρ over $K = \mathbb{Q}(\zeta_p)$ from the algebraic closure $\overline{\mathbb{Q}(\zeta_p)}$ into a certain extension L viewed as vector spaces over K. In particular, the extension L/K would be equipped with Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$. Note that this gives rise to a map $\mathrm{Gal}(\overline{\mathbb{Q}(\zeta_p)}/\mathbb{Q}(\zeta_p)) \to \mathrm{Gal}(L/K) \hookrightarrow \mathbb{F}_p$. We do this by considering a different interpretation of regularity involving class field theory. Global class field theory tells us that there exists an extension of $K = \mathbb{Q}(\zeta_p)$ known as the *Hilbert class field* H_K with the defining property that $\mathrm{Gal}(H_K/K)$ is isomorphic to the ideal class group of K. Furthermore, we know that H_K is *totally unramified*, i.e. none of the prime ideals in K have a decomposition in H_K with repeated factors. Galois theory explains the extensions that lie between K and H_K in relation to $\mathrm{Gal}(H_K/K)$, i.e. in relation to the structure of the ideal class group of K. For example, if p does not divide h_K, there is no p-torsion in the ideal class group, i.e. there is definitely no extension of K of degree p that is in H_K. In particular, there does not exist a cyclic extension of degree p which is totally unramified. Hence, to every counterexample at a prime p, we construct a totally unramified extension L over $\mathbb{Q}(\zeta_p)$ with degree p in order to come to a contradiction. In terms of representations, we note that $\mathrm{Gal}(L/\mathbb{Q}(\zeta_p)) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, so by adding the zero automorphism we get $\mathbb{F}_p$. Facts from infinite Galois theory and Kummer theory allow us to form the representation ρ from the full Galois group of $\mathbb{Q}(\zeta_p)$ to $\mathbb{F}_p$. As expected, such ρ do not exist at regular primes

p. The following proof is based on [2]. For this proof, we need some more facts, the most important from class field theory. As usual, let $K = \mathbb{Q}(\zeta_p)$, and we take p to be a prime greater than 3.

Proposition 6.1. *(1) If u is a unit of $\mathcal{O}_K$ such that it is congruent to a rational integer modulo p and not a pth power in $\mathcal{O}_K$, then the field extension $K(u^{1/p})/K$ is a cyclic extensions of order p that has the property of being totally unramified. (This holds for any pth root of u.)*
(2) If $\mathfrak{I}$ is an ideal of $\mathcal{O}_K$ such that $\mathfrak{I}^p$ is principal, but $\mathfrak{I}$ is not, then there is a cyclic extension over K of order p that has the property of being totally unramified.

It is easy to see that the hypotheses in the above proposition, never hold for primes which are regular (this follows from the definition and Kummer's Lemma), hence one can understand that at such regular primes, a cyclic extension would never exist.

Theorem 6.2. *If there exists $x, y, z \in \mathbb{Z}$ such that $x^p + y^p = z^p$, then we can produce a cyclic extension L of $K = \mathbb{Q}(\zeta_p)$ of order p which has the property of being totally unramified.*

Proof. As expected, we have two cases, $p \nmid xyz$ and $p \mid z$. Furthermore, we assume as usual that x, y, and z are relatively prime. In this proof, we will reference the original proof from the previous sections, using the exact same notation.

Case I: $p \nmid xyz$. As in the original proof, we rearrange and flip signs such that $x \not\equiv y \pmod{p}$. We use the usual decomposition into relatively prime ideals $(z)^p = (x+y)(x+\zeta_p y)...(x+\zeta_p^{p-1}y)$ so that we can write $(x + \zeta_p^i) = \mathfrak{I}_i^p$ for all $i \in \{0, ..., p-1\}$. Here, we don't have the assumption that p is regular. However, from the argument of the original proof, we know that if $\mathfrak{I}$ is principal, then following the same argument, we obtain the congruence $x + \zeta_p y - \zeta_p^{2r} x - \zeta_p^{2r-1} y \equiv 0 \pmod{p}$ and eventually get contradictions to $p \nmid xyz$ or $x \not\equiv y \pmod{p}$ using Lemma 3.3. Thus, if x, y, and z exist, it must be that $\mathfrak{I}$ must be principal, hence by Proposition 6.1, there exists an extension of K with the needed properties.

Case II: $p \mid z$. Here, we generalize and consider the equation $x^p + y^p = U(1 - \zeta_p)^{kp} z_0^p$ where x, y, z_0 are elements of $\mathcal{O}_K$ such that they are relatively prime to each other as well as $1 - \zeta_p$, and we consider a solution such that k is minimal. We note that in the decomposition $U(1-\zeta_p)^{kp} z_0^p = (x+y)(x+\zeta_p y)...(x+\zeta_p^{p-1}y)$, each of factors $x + \zeta_p^{p-1} y$ is divisible by $1 - \zeta_p$ and we can change x and y accordingly such that $(1 - \zeta_p)^{k(p-1)+1} \mid x + y$. It follows that $\left((1 - \zeta_p)^{k-1} z_0\right)^p = \prod_{i=0}^{p-1}\left(\frac{x+\zeta_p^i y}{1-\zeta_p}\right)$, and the ideals generated by $\frac{x+\zeta_p^i y}{1-\zeta_p}$ are pth power of ideals $\mathfrak{I}_i \in \mathcal{O}_K$. Here since we do not have the assumption that p is regular, we do not know whether or not these ideals are principal. Nevertheless, if these ideals are principal, in particular, if $\mathfrak{I}_0$, $\mathfrak{I}_1$, and $\mathfrak{I}_{-1} = \mathfrak{I}_{p-1}$ are principal, then we have the following three equations

$$\begin{aligned} x + y &= (1 - \zeta_p)^{kp+1} u_0 \beta^p \\ x + \zeta_p y &= (1 - \zeta_p) u_1 \alpha_1^p \\ x + \zeta_p^{-1} y &= (1 - \zeta_p) u_{-1} \alpha_{-1}^p \end{aligned}$$

where $\beta, \alpha_1, \alpha_{-1}$ are elements of $\mathcal{O}_K$ and u_0, u_1, u_{-1} are units in $\mathcal{O}_K^{\times}$. Following the same argument, we arrive at an equation $U'(1 - \zeta_p)^{(k-1)p} \beta^p = \alpha_1^p + V\alpha_{-1}^p$ where U' and V' are units of K. Looking at this equation modulo p, we arrive at the conclusion that V' is congruent to an integer modulo p, so we either have the case that V' is not a pth power producing a cyclic extension $L = K(V'^{1/p})$ from Proposition 6.1 satisfying all needed properties or there exists $v \in \mathcal{O}_K^{\times}$ such that $V' = v^p$. If we let $x' := \alpha_1$, $y' := v\alpha_{-1}$, and $z_0' := \beta$, then we have $U'(1 - \zeta_p)^{(k-1)p} z_0'^p = x'^p + y'^p$, a contradiction to the minimality of k. Hence, we see that one of $\mathfrak{I}_1$, $\mathfrak{I}_0$, or $\mathfrak{I}_{-1}$ must not be principal, and by Proposition 6.1, we can produce the extension L over K with the needed properties. $\qquad\square$

From the existence of such an L, we can go further to produce a representation $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(L/K) \cong \mathbb{F}_p$. From Galois theory, we know that $\mathrm{Gal}(\overline{K}/K)$ can be expressed as an inverse limit of the Galois groups of its finite Galois subextensions, including L. In particular, we have a canonical homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/L) \cong \mathrm{Gal}(L/K)$, giving rise to the exact representation ρ that we need.

For the complete the proof for Fermat's last theorem, Andrew Wiles attempted to associate to every counterexample (x, y, z, p), a representation $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_n(\mathbb{F}_p)$ such that the representation was unramified away from p and had "nice" ramification at p. He immediately followed by proving no such representations exist, hence contradicting the existence of such counterexamples [2]. This is comparable to the strategy used here to prove Fermat's last theorem for regular primes.

7. Generalizing the second case

The method used in the second case of Kummer's proof can be generalized to prove Fermat's last theorem for more than just regular primes. The basic argument stays the same, but we instead consider the generalized equation

$$x^p + y^p = u\lambda^m z^p,$$

where p is an odd prime, $\lambda = (1 - \zeta_p)^2$, $x, y, z, \in \mathbb{Z}[\lambda]$ such that they are relatively prime with each other and λ, $u \in \mathbb{Z}[\lambda] \cap \mathbb{R}$, and $m \geq \frac{p(p-1)}{2}$. We want to show that this equation has no solutions. We must make two assumptions on our choice of p that loosely generalize the property of regularity. The first is that $p \nmid h_{K^+}$, i.e. p must not divide the class number of $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. The second assumption is that certain units η arising within the argument can be expressed as a pth power of a unit in K^+. We will state this assumption more accurately when these units show up. For this argument, we will need a couple of facts. The proof for the following lemma can be found in [5].

Lemma 7.1. *(1) For any $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv 1 \pmod{(1 - \zeta_p)^p}$, the extension $K(\alpha^{1/p})/K$ is unramified at $(1 - \zeta_p)$.*
(2) Assume $p \nmid h_{K^+}$. Let $\alpha \in \mathcal{O}_K$ be such that $\overline{\alpha} = \alpha^{-1}$ and $K(\alpha^{1/p})/K$ is unramified. Then there exists $\beta \in K$ such that $\alpha = \beta^p$.

Main Argument. We are ready for the main argument. We will only present a sketch of the proof. The full detailed proof can be found in [5].

Assume there exists a solution to the equation $u\lambda^m z^p = x^p + y^p$ satisfying the properties described above. We can decompose the right hand side in K to get $u\lambda^m z^p = (x+y)(x+\zeta_p y)...(x+\zeta_p^{p-1}y)$. The only common factor of any two $(x + \zeta_p^i y)$ and $(x + \zeta_p^j y)$ for $i \neq j$ is the prime ideal $(1 - \zeta_p)$. Furthermore, we know that $(1 - \zeta_p)^2 = (\lambda) \mid (x + y)$, so we have the equality

$$(x + y)\left(\frac{x + \zeta_y}{1 - \zeta_p}\right)\left(\frac{x + \zeta_y^2}{1 - \zeta_p}\right)...\left(\frac{x + \zeta_y^{p-1}}{1 - \zeta_p}\right) = v\lambda^{m-(p-1)/2}z^p,$$

where v is a unit and the algebraic integers on the right generate ideals which are pairwise relative prime, so in particular, since $1 - \zeta_p \mid x + y$, $1 - \zeta_p \nmid \frac{x+\zeta_p^i y}{1-\zeta_p}$ for any $i \in \{1, ..., p-1\}$. It follows that there exists ideals $\mathfrak{I}_i$ such that $\mathfrak{I}_0^p(\lambda)^{m-(p-1)/2} = (x + y)$ and $\mathfrak{I}_i^p = \frac{x+\zeta_p^i y}{1-\zeta_p}$ for all other i. Note that $\mathfrak{I}_{p-i} = \mathfrak{I}_{-i}$ is the complex conjugate of $\mathfrak{I}_i$.

If we assume that $p \nmid h_{K^+}$, then $\mathfrak{I}_0$ is principal in $\mathbb{Z}[\lambda]$ (Note that it is okay to think of $\mathfrak{I}_0$ in $\mathbb{Z}[\lambda]$ since $(1 - \zeta_p) \nmid \mathfrak{I}_0$). Furthermore, since $x + y$ and λ are elements of $\mathbb{R}$, the generator α_0 of $\mathfrak{I}_0$ is also real, so we get $x + y = u_0\lambda^{m-(p-1)/2}\alpha_0^p$ where u_0 is a unit which is also real. For any $i \neq 0$, define

$$a_i = -\zeta_p^{-i}\frac{x + \zeta_p^i y}{x + \zeta_p^{-i}y} \equiv 1 \pmod{(1 - \zeta_p)^{2m-p}},$$

so in particular $a_i \equiv 1 \pmod{(1 - \zeta_p)^p}$. Note that the principal ideal generated by a_i can be decomposed as a pth power of $(\mathfrak{I}_i/\mathfrak{I}_{-i})$. Thus, from Lemma 7.1, we not only know that the extension $K(a_i^{1/p})/K$ is unramified at $(1 - \zeta_p)$, we furthermore know that it is totally unramified. Additionally, from the second part of Lemma 7.1, $a_i = \beta_i^p$ where $\beta_i \in K$. This allows for us to find $\alpha_i \in \mathbb{Z}[\lambda]$ such that $\frac{x+\zeta_p^i y}{1-\zeta_p} = u_i\alpha_i^p$ where u_i is a real unit. Note that $(\overline{\alpha_i})^p = \alpha_{-i}^p$, so up to a root of unity, $\overline{\alpha_i} = \alpha_{-i}$.

11

From the equalities $x + \zeta_p^i y = (1 - \zeta_p)u_i\alpha_i^p$ and $x + \zeta_p^{-i}y = (1 - \zeta_p^{-i})u_{-i}\overline{\alpha_i}^p$ as well as the formula for $x + y$, we get

$$-xy = u_i^2(\alpha_i\overline{\alpha_i}) - u_0^2\lambda^{2m-p+1}\alpha_0^{2p}\lambda_a^{-1}.$$

For j such that $j \neq 0$ and $i \not\equiv \pm j \pmod{p}$, a similar equality holds. Combining the two gives us

$$\eta^2(\alpha_i\overline{\alpha_i})^p + (-\alpha_b\overline{\alpha_b})^p = \delta\lambda^{2m-p}(\alpha_0^2)^p,$$

where $\eta = u_i/u_j$ and δ is a real unit. Note that η defined here is the one needed as a pth power of a unit from K^+ in the second assumption. This allows us to define $x_1 = \eta^{2/p}\alpha_a\overline{\alpha_a}$, $y_1 = -\alpha_b\overline{\alpha_b}$, and $z_1 = \alpha_0^2$ so that the above equations turns into $x_1^p + y_1^p = \delta\lambda^{2m-p}z_1^p$. It is easy to show that x_1, y_1, z_1 are pairwise relatively prime and with λ. Again, we can use the method of infinite descent to produce a contradiction. If we assume that (z) has the smallest number of distinct prime ideal factors in its decomposition, we in fact know that $(z) = \mathfrak{I}_0\mathfrak{I}_1...\mathfrak{I}_{p-1}$ where $\mathfrak{I}_i$ and $\mathfrak{I}_j$ are relatively prime for $i \neq j$. However, $z_1 = \alpha_0^2$ and α_0 is the generator of $\mathfrak{I}_0$, hence $(z_1) = \mathfrak{I}_0^2$ so $\mathfrak{I}_1, ..., \mathfrak{I}_{p-1}$ must be trivial. However, this implies that each $\frac{x+\zeta_p^i y}{1-\zeta_p}$ is a unit for $i \neq 0$. With some manipulation, we arrive at the fact that either $x + y = 0$ or $\zeta_p^2 = 1$, both contradictions. Altogether, we see that such a solution cannot exist. $\qquad\square$

The above argument proves the second case of Fermat's last theorem for regular primes as well as other cases, although it remains to show why the two assumptions are satisfied by the property of regularity. Proofs demonstrating how to go about satisfying the two assumptions for regular primes as well as other cases can be found in [5].

References

[1] H.M. Edwards. *"Fermat's Last Theorem"*. Springer-Verlag, New York, first edition, 1977.
[2] K. Paranjape. "On (Kummer's approach to) Fermat's last theorem'. *Bona Mathematica*, 1994.
[3] P. Ribenboim. *"13 Lectures on Fermat's Last Theorem"*. Springer-Verlag, New York, first edition, 1979.
[4] A. van der Poorten. *"Notes on Fermat's Last Theorem"*. Wiley-Interscience, New York, first edition, 1996.
[5] L. Washington. *"Introduction to Cyclotomic Fields"*. Springer-Verlag, New York, second edition, 1997.