Kummer's Special Case of Fermat's Last Theorem*

Emily Riehl

May 18, 2005

Abstract

One particularly elegant example of an application of modern algebraic number theory to a classical problem about the integers is found in Kummer's special case of Fermat's Last Theorem. In this paper, we reduce Fermat's Last Theorem to the question of whether or not there exist integer solutions to $x^p + y^p = z^p$ for p an odd prime. We then give a thorough exposition of Kummer's proof that no such solutions exist in the case that p does not divide the class number of $\mathbb{Q}(e^{2\pi i/p})$, that is where p is a regular prime.

1 Introduction

Although a complete proof of Fermat's Last Theorem was finally given in 1994 by Andrew Wiles with help from Richard Taylor, the famous problem, which remained unsolved for three and a half centuries, is still of great interest to mathematicians and enthusiasts today. Part of the reason for this sustained interest is the vast quantity of mathematics developed over the past three centuries in an attempt to prove this elusive claim. Many of the major developments associated with famous historical attempts to prove Fermat's Last Theorem are surveyed in Hellegouarch [3] and Stewart and Tall [7] for the student familiar with the basics of modern algebra, or in Singh [5] for a more general audience.

One partial proof of Fermat's Last Theorem that is of particular interest to students acquainted with basic algebraic number theory is that given by Ernst Eduard Kummer in the case that p is a regular prime. His proof uses the concept of "ideal numbers," designed to restore unique factorization to all number fields. While Kummer's "ideal numbers" were developed in conjunction with his work on higher reciprocity laws (see [7] pp 3-5), his proof of this special case of Fermat's Last Theorem gave an early and important application of the concept that Dedekind would reformulate as "ideals." This paper gives a complete, modern version of Kummer's proof including all necessary pre-requisites at a level that would be easily understood by an undergraduate or graduate student who has taken a first course in algebraic number theory.

In Section 2, we define and discuss regular primes. In Section 3, we prove a number of necessary results and end with Kummer's proof of Fermat's Last Theorem for regular primes p. In Section 4, we give our acknowledgments.

*Math 129: Topics in Number Theory, William Stein, Spring 2005

2 Regular Primes

A prime p is said to be *regular* if it does not divide the class number C_K of $K = \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/p}$. While this definition is easy to state, it is not easy to compute the class number C_K in general or even in the case that $K = \mathbb{Q}(\zeta)$. So we would like to find another criterion for determining when p is regular.

Surprisingly, a link exists between regular primes and the *Bernoulli numbers* B_k defined by the following series:

$$\frac{x}{e^x - 1} = 1 + \sum_{k=1}^{\infty} \frac{B_k}{k!} x^k$$

When k is odd, the Bernoulli numbers are easy to describe, but for even k, they behave unpredictably. For $k = 1$, $B_1 = \frac{1}{2}$, and when k is odd and greater than 1, $B_k = 0$. When k is even, the first few values are

$$B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{8}, \quad B_{10} = \frac{5}{66},$$

$$B_{12} = -\frac{691}{2730}, \quad B_{14} = \frac{6}{6}, \quad B_{16} = -\frac{3617}{510}, \ldots$$

The desired criterion for determining when p is a regular prime is given in the following proposition, discovered by Kummer. The proof requires analytic techniques that are outside the scope of this paper, so it is not given here. We refer the interested reader to Borevich and Shafarevich [1] for details.

Proposition 2.1. *A prime p is regular if and only if p does not divide the numerators of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$.*

It is not hard to see with a computer that the only regular primes less than 100 are $37, 59$, and 67.

Kummer conjectured that there exist an infinite number of regular primes, but this fact has never been proven. Ironically, despite their apparent scarcity, it is quite easy to prove that there exist an infinite number of irregular primes (see [3]), although this is not directly of interest to this paper.

3 Fermat's Last Theorem

The task of showing that there exist no integer solutions to the equation $x^n + y^n = z^n$ for $n \geq 3$ can be simplified by making some elementary observations about the properties of this equation. First, we note that we may assume that x, y, and z are pairwise coprime. For if there existed a solution and an integer $a \neq 1$ such that a divides x and y, then a would divide z as well, and division by a^n would yield another integer solution without this common factor.

Furthermore, we note that if we can prove that there exists no solutions for some n, then the same must be true for multiples of n as well. For if $x^{mn} + y^{mn} = z^{mn}$ then $(x^m)^n + (y^m)^n = (z^m)^n$. Because every integer greater than 2 is divisible by either 4 or an odd prime, it suffices to prove Fermat's Last Theorem for these cases.

3.1 n=4

The proof of Fermat's Last Theorem for $n = 4$ can be given with elementary methods. This proof is often attributed to Fermat himself, although no records of it exist, because he posed this case as a challenge to others [7]. The proof attributed to Fermat relies on a well known characterization of Pythagorean triples given in the following lemma.

Lemma 3.1. *Any integer solution to $x^2 + y^2 = z^2$ where x, y, and z are pairwise coprime can be given in the following form (or with x and y interchanged)*

$$\begin{aligned} \pm x &= r^2 - s^2 \\ \pm y &= 2rs \\ \pm z &= r^2 + s^2 \end{aligned}$$

where r and s are coprime and exactly one is odd.

Proof. We may assume that x, y, and z are all positive. We first consider their parity. Clearly not all three may be odd, and because we assume that x, y, and z are pairwise coprime, it follows that precisely one is even. Furthermore, if $z = 2j$ is even and $x = 2k + 1$, $y = 2l + 1$ are odd, then $(2k + 1)^2 + (2l + 1)^2 = (2j)^2$, which is impossible because the left hand side is equivalent to 2 mod 4, while the right hand side is congruent to 0. Thus, we must have either x or y even, so we assume without loss of generality that y is even. Then $y^2 = (z-x)(z+x)$, and we can write $y = 2a$, $z - x = 2b$, and $z + x = 2c$, because all three are even and positive. Hence $(2a)^2 = (2b)(2c)$ so $a^2 = bc$.

We see that b and c must be coprime, for otherwise a common factor would divide both $z - x$ and $z + x$ and thus also z and x. So each prime factor of a must occur as a square factor of either b or c, and hence we may write $b = s^2$ and $c = r^2$ with r and s coprime. This implies that $z = r^2 + s^2$ and $x = r^2 - s^2$, and because both x and z are odd, precisely one of r and s is. Finally, subtracting $(r^2 - s^2)^2$ from $(r^2 + s^2)^2$ and taking the square root shows that $\pm y = 2rs$ as desired. □

We can now prove that there exist no integer solutions to the equation $x^4 + y^4 = z^4$ as a corollary to the following theorem.

Theorem 3.2. *There are no nonzero integer solutions to the equation $x^4 + y^4 = z^2$.*

Proof. Again, we may assume that x, y, and z are positive. Among the set of positive integer solutions for the above equation, we may choose a triple (x, y, z) for which z is minimal. Hence, x, y, and z are pairwise coprime, for otherwise we could cancel the common factor (which must divide all three) and obtain a smaller z. So we may apply Lemma 3.1 and write, relabeling x and y if necessary, $x^2 = r^2 - s^2$, $y^2 = 2rs$, and $z = r^2 + s^2$. The first equation gives us another Pythagorean triple $x^2 + s^2 = r^2$, and it is not hard to see that x, s, and r must also be relatively prime. From our first choice for x, we know that x is odd, so we may again imply Lemma 3.1 to see that $x = a^2 - b^2$, $s = 2ab$, and $r = a^2 + b^2$. We then see that

$$y^2 = 2rs = 4ab(a^2 + b^2) \tag{1}$$

From the lemma, a and b are relatively prime, so they must be pairwise coprime to $a^2 + b^2$ as well. Hence, a prime factorization of (1) shows that $a = c^2$, $b = d^2$, and $a^2 + b^2 = e^2$ must all

themselves be squares. A final substitution shows that $c^4+d^4 = e^2$, and as $e \leq a^2+b^2 = r < z$, this contradicts the minimality of z. Thus, no non-zero integer solution can exist. $\square$

Clearly a nonzero integer solution to Fermat's equation $x^4 + y^4 = z^4$ would provide a contradiction to this theorem, hence no such solution can exist.

3.2 Next Steps

We now turn our attention the case where n is an odd prime p. For this we are interested in the field $K = \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/p}$ because in this field the equation $x^p + y^p$ factors into linears. To see this, note that solutions to the equation $x^p - y^p = 0$ have the form $x = \zeta^k y$ for $k = 0, 1, \ldots, p-1$. Thus $(x^p - y^p) = (x-y)(x-\zeta y)\cdots(x-\zeta^{p-1}y)$. We substitute $-y$ for y and note that p is odd to conclude that $x^p + y^p = (x+y)(x+\zeta y)\cdots(x+\zeta^{p-1}y)$ over $\mathbb{Q}(\zeta)$.

The field $\mathbb{Q}(\zeta)$ has degree $p-1$ over $\mathbb{Q}$ because the minimal polynomial of ζ is $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, which can be shown to be irreducible by substituting $y+1$ for x and applying Eisenstein's criterion. Thus the set $\{1, \zeta, \cdots, \zeta^{p-2}\}$ forms a basis for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ as a vector space (a linear dependence would contradict the minimality of f).

The Galois conjugates of ζ are ζ^i for $i = 1, 2, \ldots, p-1$, which are precisely the roots of f. Thus, it is clear that $\mathrm{Tr}(\zeta^i) = -1$ for $1 \leq i \leq p-1$ by examining the x^{p-2} coefficient of the minimal polynomial. Similarly, $\mathrm{Norm}(\zeta^i) = \zeta\zeta^2\cdots\zeta^{p-1} = 1$, as this is the constant term of f. It will be useful to work with the ring of integers of K, which we determine with the following proposition.

Proposition 3.3. *The ring of integers $\mathcal{O}_K$ of $K = \mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$.*

Proof. Clearly $\mathbb{Z}[\zeta] \subset \mathcal{O}_K$ so we wish to prove the reverse inclusion. Let $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$ be in $\mathcal{O}_K$. We wish to show that each a_i is in $\mathbb{Z}$. Because the $\mathcal{O}_K$ is a ring and $\zeta \in \mathcal{O}_K$, for each $0 \leq k \leq p-2$, the element $\alpha\zeta^{-k} - \alpha\zeta$ is an algebraic integer, so its trace is integral. Recalling that the trace is additive, we compute $\mathrm{Tr}(\alpha\zeta^{-k} - \alpha\zeta) = \mathrm{Tr}(a_0\zeta^{-k} + \cdots + a_k + \cdots + a_{p-2}\zeta^{p-k-2} - a_0\zeta - \cdots - a_{p-2}\zeta^{p-1}) = pa_k - (a_0 + \cdots + a_{p-2}) + (a_0 + \cdots + a_{p-2}) = pa_k$ so $pa_k \in \mathbb{Z}$ for each k.

We let $\lambda = 1 - \zeta$ and write

$$p\alpha = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2} = c_0 + c_1\lambda + \cdots + c_{p-2}\lambda^{p-2} \tag{2}$$

where

$$c_i = \sum_{j=i}^{p-2} (-1)^i \binom{j}{i} b_j$$

is an integer. When we resubstitute $\zeta = 1 - \lambda$ and expand, we see by symmetry that

$$b_i = \sum_{j=i}^{p-2} (-1)^i \binom{j}{i} c_j. \tag{3}$$

We claim that each c_i is divisible by p and prove this with induction on i. As we have $\mathrm{Tr}(\alpha) = pa_0 - (a_1 + \cdots + a_{p-2})$, clearly $c_0 = b_0 + \cdots + b_{p-2} = p(b_0 - \mathrm{Tr}(\alpha))$, proving

the base case. Now we assume that $p \mid c_i$ for $i = 0, \ldots, k-1$. We see that $p = f(1) = \prod_{i=1}^{p-1}(1-\zeta^i) = (1-\zeta)^{p-1}\prod_{i=1}^{p-1}(1+\zeta+\cdots+\zeta^{i-1}) = \lambda^{p-1}\beta$ where $\beta \in \mathbb{Z}[\zeta] \subset \mathcal{O}_K$. Thus $p \equiv 0$ modulo the ideal $\langle\lambda^{k+1}\rangle$, and so the left hand side of (2) vanishes modulo this ideal. Of the terms on the right hand side, clearly $c_{k+1}\lambda^{k+1}, \ldots, c_{p-2}\lambda^{p-2} \in \langle\lambda^{k+1}\rangle$, and $c_0, \ldots, c_{k-1}\lambda^{k-1}$ vanish as well, because p divides them by the inductive hypothesis. Hence, $c_k\lambda^k \equiv 0$ so $c_k\lambda^k = \delta\lambda^{k+1} \Rightarrow c_k = \delta\lambda$ for some $\delta \in \mathcal{O}_K$. However, $\mathrm{Norm}(\lambda) = \prod_{i=1}^{p-1}(1-\zeta^i) = f(1) = p$, and this divides $\mathrm{Norm}(c_k) = c_k^{p-1}$ because the norm is multiplicative and $c_k \in \mathbb{Z}$. So $p \mid c_k$ for all k, and by (3) the same is true of each b_k. Thus $b_k = pa_k$ implies that $a_k \in \mathbb{Z}$ for each k, and hence $\alpha \in \mathbb{Z}[\zeta] = \mathcal{O}_K$ as desired.

□

We let $\lambda = 1-\zeta$ as above and consider the ideal $I = \langle\lambda\rangle \subset \mathbb{Z}[\zeta]$. A basic characterization of I is given in the following lemma.

Lemma 3.4. *The ideal $I = \langle\lambda\rangle$ of $\mathbb{Z}[\zeta]$ satisfies the following: $I^{p-1} = \langle p\rangle$ and $\mathrm{Norm}(I) = p$.*

Proof. The first claim is a consequence of the observation that the Galois conjugates of λ are in fact associates in K. We show that each Galois conjugate $1-\zeta^i$ for $i = 1, 2, \ldots, p-1$ is associate to $1-\zeta$. Clearly $1-\zeta \mid 1-\zeta^i$. For the converse, we use the fact that p is prime to see that there exists some j such that $ij \equiv 1 \mod p$. Thus, $1-\zeta = 1-\zeta^{ij}$ so $1-\zeta^i \mid 1-\zeta^{ij} = 1-\zeta$. Clearly $\langle p\rangle = \prod_{i=1}^{p-1}\langle 1-\zeta^i\rangle$, but we have just shown that each of the ideals on the right hand side equals I. Hence, $I^{p-1} = \langle p\rangle$ as desired.

For the second statement, we take the norms of the ideals in the previous equation. In particular, $\mathrm{Norm}(I^{p-1}) = \mathrm{Norm}(\langle p\rangle) = p^{p-1}$. Because $\mathrm{Norm}(I)$ is a positive integer, it follows from unique factorization of ideals that $\mathrm{Norm}(I) = p$. □

We recall that the norm of an ideal equals its index in the ring of integers, so we have shown that $|\mathbb{Z}[\zeta]/I| = p$. Thus, the canonical quotient map $\mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]/I$ shows that every element of $\mathbb{Z}[\zeta]$ is congruent to one of $0, 1, \ldots, p-1$ modulo I.

It will be of interest to characterize the units of $\mathbb{Z}[\zeta]$, which we shall denote U_K. By Dirichlet's Unit Theorem, $U_K \simeq \mathbb{Z}^n \times T$ for some positive integer n and torsion subgroup T (for proof, see [6]). It will be easiest to characterize T, so we begin with this. Clearly, $1 \in U_K$ is the identity element, so a unit is in the torsion subgroup if and only if it is a root of unity. Clearly, every root of unity in K is both an integer and a unit, so it suffices to classify exactly which roots of unity exist in $\mathbb{Q}(\zeta)$, which we do with the following proposition.

Proposition 3.5. *The only roots of unity in $\mathbb{Q}(\zeta)$ have the form $\pm\zeta^m$ for some integer m.*

Proof. It is clear that $\pm\zeta^m \in \mathbb{Q}(\zeta)$ for each integer m, and that each such element is a $2p$-th root of unity. So it only remains to show that there does not exist some primitive k-th root $\zeta_k \in \mathbb{Q}(\zeta)$ such that $k \nmid 2p$, i.e., such that ζ_k does not have this form. We will prove that such extraneous roots of unity cannot occur by using the following lemmas.

Lemma 3.6. *Let ζ_k be a primitive k-th root of unity. Then $[\mathbb{Q}(\zeta_k) : \mathbb{Q}] = \phi(k)$ where ϕ is the Euler ϕ function.*

Proof. We already know this result when k is prime because we have shown that the minimal polynomial for ζ_k has degree $\phi(k) = k-1$. We now give a general proof with a slightly

different flavor. Let f be the minimal polynomial for ζ_k. Then f divides $x^k - 1$. We know that all other primitive elements have the form ζ_k^q for q prime to k. Say $x^k - 1 = fh$, where f, as the minimal polynomial for an algebraic integer, and thus also h, are both monic and integral. If ζ_k^q is not a root of f then it must be a root of h, in which case ζ_k is a root of $h(x^q)$, which then must be divisible by f. This polynomial is again monic and integral so we may consider its residue modulo q. As f divides $h(x^q)$, it follows that $h(x^q) = h(x)^q = f(x)g(x)$ mod q. So the residues of f and h are not relatively prime which means that $x^k - 1 \equiv \overline{f}\overline{h}$ has multiple roots modulo q. But then $x^k - 1$ and its derivative would have a common factor, which is clearly false, so ζ_k^q must be a root of f.

Finally, if f has roots other than the primitive ones, there would exist an automorphism of $\mathbb{Q}(\zeta_k)$ that mapped a primitive root ζ_k to a non-primitive root. But the image of such an automorphism is clearly not an isomorphic embedding of K into $\mathbb{C}$. Thus, a primitive k-th root of unity cannot have the same minimal polynomial as a non-primitive root. Hence, the degree of f is $\phi(k)$, and the result follows. □

We make use of this fact in our final lemma.

Lemma 3.7. *Given integers k, p relatively prime, there is no primitive k-th root of unity ζ_k in $\mathbb{Q}(\zeta)$.*

Proof. We first note that $\mathbb{Q}(\zeta_k, \zeta) = \mathbb{Q}(\zeta_{kp})$ where $\mathbb{Q}(\zeta_{kp})$ is a primitive kp-th root of unity. This is clear because ζ_k and ζ are powers of ζ_{kp}^p and $\zeta_{kp}^k \in \mathbb{Q}(\zeta_{kp})$, respectively, and $\zeta_k\zeta$ is a primitive kp-th root of unity. By the previous lemma, $[\mathbb{Q}(\zeta_k) : \mathbb{Q}] = \phi(k)$, and it is well known that $\phi(kp) = \phi(k)\phi(p)$ when k and p are relatively prime. So $[\mathbb{Q}(\zeta_{kp}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_k, \zeta_p) : \mathbb{Q}] = [\mathbb{Q}(\zeta_k, \zeta) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}]$ implies that $[\mathbb{Q}(\zeta_k, \zeta) : \mathbb{Q}(\zeta)] = \phi(k) \neq 1$, so in particular, ζ_k is not in $\mathbb{Q}(\zeta)$. □

Now we relax the condition that k is relatively prime to p, and assume only that $k \nmid 2p$. Clearly we may write $k = ap^n$ where a and p are relatively prime and $a \geq 3$. Then if $\zeta_k \in \mathbb{Q}(\zeta)$, we would have $\zeta_k^{p^n} \in \mathbb{Q}(\zeta)$, and this is a primitive a-th root of unity that is not an integer. But this contradicts the previous Lemma, so $\zeta_k \notin \mathbb{Q}(\zeta)$ for any $\zeta_k \neq \pm\zeta^m$. □

Our case of Fermat's Last Theorem requires three more lemmas, which we will prove now.

Lemma 3.8. *For each $\alpha \in \mathbb{Z}[\zeta]$ there exists an integer a such that $\alpha^p \equiv a \pmod{I^p}$.*

Proof. By Lemma 3.4, $|\mathbb{Z}[\zeta]/I| = p$, for this is the definition of the norm of an ideal. Thus, when we consider the canonical homomorphism $\mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]/I$, it is clear that every $\alpha \in \mathbb{Z}[\zeta]$ is congruent to one of $0, 1, \ldots, p-1$ modulo I. Let b be that integer. Clearly, $\alpha^p - b^p = \prod_{i=0}^{p-1}(\alpha - \zeta^i b)$, and because $\zeta \equiv 1 \pmod{I}$, each factor on the right is congruent to $\alpha - b \equiv 0 \pmod{I}$. Thus, $\alpha^p \equiv b^p \pmod{I}$, as desired. □

Lemma 3.9. *If $g \in \mathbb{Z}[x]$ is a monic polynomial such that all of its roots in $\mathbb{C}$ lie on the unit circle, then every zero is a root of unity.*

Proof. We let $\alpha_1, \ldots, \alpha_r$ denote the roots of g. It follows that, for any integer k, $g_k(x) = (x - \alpha_1^k) \cdots (x - \alpha_r^k)$ is in $\mathbb{Z}[x]$ because the roots of this polynomial are permuted by the Galois group of $K/\mathbb{Q}$. If $g_k(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_0$, then it is not hard to see that

$a_j \leq \binom{r}{j}$ for $j = 0, 1, \ldots, r-1$ because each $|\alpha_j| = 1$. Hence, because we have bounded the coefficients, there can only be finitely many such polynomials. So $g_k = g_n$ for some $k \neq n$. Thus, there exists some permutation $\sigma \in S_r$ such that $\alpha_j^k = \alpha_{\sigma(j)}^n$ for each j. We apply this construction iteratively and note that the order of σ divides $r!$ to see that $\alpha_j^{k^{r!}} = \alpha_j^{n^{r!}}$ for each j. Hence, $\alpha_j^{k^{r!}-n^{r!}} = 1$, and because $k^{r!} \neq n^{r!}$ it follows that α_j is a root of unity. □

The final result is called Kummer's Lemma and will be central to his proof of the case of Fermat's Last Theorem.

Lemma 3.10. *Every element in the group of units U_K for $K = \mathbb{Q}(\zeta)$ has the form $r\zeta^k$ where $r \in \mathbb{R}$ and $k \in \mathbb{Z}$.*

Proof. Let $u \in \mathbb{Z}[\zeta]$ be a unit and $g(x) \in \mathbb{Z}[x]$ be the polynomial such that $u = g(\zeta)$. We let $u_j = g(\zeta^j)$ for $j = 1, \ldots, p-1$ and note that $1 = \pm\text{Norm}(u) = \pm u_1 \cdots u_{p-1}$ because the u_j are the Galois conjugates of u. So each u_j is also a unit. Furthermore, we see that $u_{p-j} = g(\zeta^{p-j}) = g(\overline{\zeta^j}) = \overline{g(\zeta^j)} = \overline{u_j}$, which means that u_j and u_{p-j} are complex conjugates. In particular, $u_j u_{p-j} = |u_j|^2 > 0$, so $\text{Norm}(u) = (u_1 u_{p-1})(u_2 u_{p-2}) \cdots > 0$, which means that $\text{Norm}(u)$ must be 1.

We see further that u_j/u_{p-j} must be a unit of absolute value 1 and that the polynomial $\prod_{j=1}^{p-1}(x - u_j/u_{p-j}) \in \mathbb{Z}[x]$ because it is fixed by the Galois group of $K/\mathbb{Q}$ as before. Hence, by Lemma 3.9, its zeros are roots of unity, and because the only roots of unity in K have the form $\pm\zeta^a$, there exists some $a \in \mathbb{Z}$ such that

$$u/u_{p-1} = \pm\zeta^a. \tag{4}$$

Because p is odd, either a or $a+p$ is even, so we may write $u/u_{p-1} = \pm\zeta^{2k}$ for $0 < k \in \mathbb{Z}$.

We wish to determine whether the sign of (4) is positive or negative. To begin, we note that for some $b \in \mathbb{Z}$, $\zeta^{-k}u \equiv b \pmod{I}$, so $\zeta^k u_{p-1} \equiv b \pmod{\langle\overline{\lambda}\rangle}$ by taking complex conjugates. We recall that $\overline{\lambda} = 1 - \zeta^{p-1}$, which is an associate of λ, so $\langle\overline{\lambda}\rangle = I$. So we can combine these congruences to see that $u/u_{p-1} \equiv \zeta^{2k} \pmod{I}$. If the sign in (4) is negative then $I \mid \langle 2\zeta^{2k}\rangle$ and $\text{Norm}(I) \mid 2^{p-1}$, contradicting Lemma 3.4. So the sign in (4) is positive, and $\zeta^{-k}u = \zeta^k u_{p-1}$. Because the two sides are complex conjugates, we have $\zeta^{-k}u = r \in \mathbb{R}$, and our proof is complete. □

3.3 Proof of Fermat's Last Theorem for Regular Primes

We have now arrived at the main theorem, which we will proof in two cases. Theorem 3.11 will deal with the case when x, y, and z are prime to p, and Theorem 3.13 will complete the proof by covering the remaining case: when p divides one of x, y, and z.

Theorem 3.11. *If p is an odd, regular prime, then the equation $x^p + y^p = z^p$ has no integer solutions such that x, y, and z are prime to p.*

Proof. As p is odd, we may consider instead the equation $x^p + y^p + z^p = 0$, for a solution to one can be transformed into a solution for the other by substituting $-z$ for z. We assume, for sake of contradiction, that there exists an integer solution to this equation given by x, y,

and z not divisible by p. As discussed previously, we may factor this equation over $\mathbb{Q}(\zeta)$ to obtain $\prod_{i=0}^{p-1}(x+\zeta^i y) = -z^p$, which gives us a similar equality of ideals:

$$\prod_{i=0}^{p-1}\langle x+\zeta^i y\rangle = \langle z\rangle^p. \tag{5}$$

We claim that the ideals on the left hand side are pairwise coprime. Otherwise, there would be a prime ideal $\mathfrak{p}$ containing $\langle x+\zeta^j y\rangle$ and $\langle x+\zeta^k y\rangle$ for some $0 \le j < k \le p-1$, in which case $\mathfrak{p}$ contains $(x+\zeta^j y)-(x+\zeta^k y) = y\zeta^j(1-\zeta^{k-j})$. We recall that $(1-\zeta^{k-j})$ is an associate of $1-\zeta = \lambda$, and naturally ζ^j is a unit, so $\mathfrak{p}$ contains $y\lambda$. As $\mathfrak{p}$ is prime, this means that either $\mathfrak{p} \supset \langle y\rangle$ or $\mathfrak{p} \supset \langle\lambda\rangle$. In the first case, $y \in \mathfrak{p}$ and $x+\zeta^j y \in \mathfrak{p}$ so $x \in \mathfrak{p}$. Because x and y are relatively prime, there exist integers a and b such that $ax+by=1$. But this would imply that $1 \in \mathfrak{p}$, which cannot be true. Hence, we must have $\lambda \in \mathfrak{p}$. We recall that $\mathrm{Norm}(\lambda) = f(1) = p$ where f is the minimal polynomial for ζ. But this implies that $I = \langle\lambda\rangle$ is a prime ideal, for norms of any prime factors of I would be integers greater than 1 and divide p. As p is a prime, I must be prime as well. Finally, the fact that $I \subset \mathfrak{p}$ and $\mathcal{O}_K$ is a Dedekind domain (see [6] chapter 3) implies that $\mathfrak{p} = I$. As I divides the left hand side of (5), it divides $\langle z\rangle$ as well, which means that $\mathrm{Norm}(I) = p$ divides $\mathrm{Norm}(z) = z^{p-1}$, so that $p \mid z$, contradicting our hypothesis. Thus, the ideals $\langle x+\zeta^i y\rangle$ are pairwise coprime as desired.

We know that the factorization of ideals into primes is unique (see [6] chapter 3), so the fact the prime ideals on the right hand side occur to the p-th power and the fact that the $\langle x+\zeta^i y\rangle$ are coprime implies that each $\langle x+\zeta^i y\rangle$ is itself a p-th power. We let $\mathfrak{m}$ be the ideal such that $\langle x+\zeta y\rangle = \mathfrak{m}^p$. In particular, $\mathfrak{m}^p$ is principal, and because p does not divide the class number of K, this implies that $\mathfrak{m}$ must be principal as well. Thus, there exists some α such that $\mathfrak{m} = \langle\alpha\rangle$, and it follows that $x+\zeta y = u\alpha^p$ where u is a unit. From our characterization of U_K in Lemma 3.10, we have $x+\zeta y = r\zeta^k\alpha^p$ where $r \in \mathbb{R}$ and k is an integer. Then by Lemma 3.8, there exists an integer a such that $\alpha^p \equiv a \mod I^p$, so $x+\zeta y \equiv ra\zeta^k$. We know from Lemma 3.4 that $\langle p\rangle \mid I^p$, so $x+\zeta y \equiv ra\zeta^k \pmod{\langle p\rangle}$ as well. As ζ^k is a unit, we can divide to obtain the congruence $\zeta^{-k}(x+\zeta y) \equiv ra \pmod{\langle p\rangle}$, and complex conjugation yields $\zeta^k(x+\zeta^{-1}y) \equiv ra \pmod{\langle p\rangle}$. Combining these facts, we see that

$$x\zeta^{-k} + y\zeta^{1-k} - x\zeta^k - y\zeta^{k-1} \equiv 0 \pmod{\langle p\rangle} \tag{6}$$

We claim that $\zeta+1$ is a unit. To see this, we first note that $f(-1) = 1$ as $p-1$ is even. But we know that $(x-\zeta)g(x) = f(x)$ for some polynomial g as $f(\zeta) = 0$, so $(-1-\zeta)g(-1) = 1$, from which it follows easily that $\zeta+1$ is a unit. If $k \equiv 0 \mod p$, then $\zeta^k = 1$ and (6) becomes $y(\zeta-\zeta^{-1}) \equiv y(-\zeta^{-1})(1-\zeta^2) \equiv y(1+\zeta)(1-\zeta) \equiv 0 \pmod{\langle p\rangle}$. As $1+\zeta$ is a unit, this shows that $y\lambda \equiv 0 \pmod{\langle p\rangle}$. But we showed that $\langle p\rangle = I^{p-1}$ in Lemma 3.4, and $p-1 \ge 2$, so this implies that $\lambda \mid y$. Hence, $\mathrm{Norm}(\lambda) \mid \mathrm{Norm}(y)$, so $p \mid y$, a contradiction. Thus, $k \neq 0 \mod p$. Similarly, if $k \equiv 1 \mod p$, then (6) becomes $x(\zeta^{-1}-\zeta) \equiv x\zeta^{-1}(1-\zeta^2) \equiv x(1-\zeta)(1+\zeta) \equiv 0 \pmod{\langle p\rangle}$. So the same argument shows that $p \mid x$, again a contradiction. Hence, $k \neq 0, 1 \mod p$.

From (6) we know that $x\zeta^{-k} + y\zeta^{1-k} - x\zeta^k - y\zeta^{k-1} = \alpha p$ for some $\alpha \in \mathbb{Z}[\zeta]$. Hence, $\alpha = \frac{x}{p}\zeta^{-k} + \frac{y}{p}\zeta^{1-k} - \frac{x}{p}\zeta^k - \frac{y}{p}\zeta^{k-1}$, and no exponent is divisible by p. We know that the set $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is a basis for $\mathbb{Z}[\zeta]$ over $\mathbb{Z}$, so if all of the exponents are not congruent

modulo p, linear independence of this set over $\mathbb{Q}$ would imply that $\frac{x}{p} \in \mathbb{Z}$, contradicting our hypothesis. So some pair of exponents must be congruent modulo p. As $p \neq 0, 1 \bmod p$, the only way this could happen is if $2k \equiv 1 \bmod p$, which would mean that $k \equiv 1 - k \bmod p$. Hence, $\alpha p\zeta^k = x + y\zeta - x\zeta^{2k} - y\zeta^{2k-1} = x + y\zeta - x\zeta - y = (x - y)\lambda$. Taking norms, we see that $p \mid (x - y)$. By the symmetry of the equation $x^p + y^p + z^p = 0$, we must also have $y \equiv z \bmod p$ so $x^p + y^p + z^p \equiv 3x^p \bmod p$. Because $p \nmid x$, we must have $p = 3$.

We note that modulo 9 the cubes of the numbers prime to p are congruent either to 1 or -1. Hence, a solution to $x^3 + y^3 + z^3 \equiv 0$ in integers prime to 3 takes the form $\pm 1 \pm 1 \pm 1 \equiv 0 \bmod 9$, which is clearly impossible. So there are no solutions for $p = 3$, and our proof is complete. □

We have thus reduced our proof of Fermat's Last Theorem for regular primes to the case where p divides exactly one of x, y, and z. For this case we need one result, also proven by Kummer, that is beyond the scope of this paper. We instead refer the reader to Borevich and Shafarevich [1].

Proposition 3.12. *If $\alpha \in \mathbb{Q}(\zeta)$ is a unit that is congruent to an element of $\mathbb{Z}$ modulo $\langle p \rangle$, then α is a p-th power of a unit.*

We are now ready to give the proof of the remaining case of Fermat's Last Theorem for regular primes, which is a bit messier.

Theorem 3.13. *If p is an odd, regular prime, then the equation $x^p + y^p = z^p$ has no integer solutions.*

Proof. We wish to show that there exist no integer solutions to the equation

$$x^p + y^p = z^p. \tag{7}$$

By Theorem 3.11, it remains to show that no such solutions exist in the case that p divides exactly one of these integers. Because p is odd, any solution to (7) gives a solution to $x^p + y^p + z^p = 0$, so without loss of generality, we may assume that $p \mid z$. Let $z = p^k z_0$ where z_0 is prime to p and $k \geq 1$. By Lemma 3.4, $p = u\lambda^{p-1}$ in $\mathbb{Q}(\zeta)$ for some unit u. Thus, a solution to equation (7) would give an equality of the form

$$x^p + y^p = u\lambda^{pm} z_0^p \tag{8}$$

where $m = k(p - 1) > 0$. We will prove the theorem by showing that an equation of the form (8) is impossible. We will actually show that (8) is impossible when x, y, and z_0 are elements of $\mathbb{Z}[\zeta]$ relatively prime to λ, which clearly implies the same is true when x, y, and z_0 are rational integers relatively prime to p.

Assuming such a solution to (8) exists, let $x, y, z_0 \in \mathbb{Z}[\zeta]$ be prime to λ, satisfying (8) for some unit u, and such that m is minimal. We factor the left hand side of (8) and pass to ideals to obtain:

$$\prod_{j=0}^{p-1} \langle x + \zeta^j y \rangle = I^{pm} \langle z_0 \rangle^p \tag{9}$$

Because $pm \geq p > 0$, it follows by unique factorization that at least one of the terms on the left hand side of (9) is divisible by I. But since the $x + \zeta^j y$ are all associates, this

means that each ideal is divisible by I. We see that if for some $0 \leq i < j \leq p-1$, $x + \zeta^i y \equiv x + \zeta^j y \pmod{I^2}$, then $\zeta^i y(1 - \zeta^{j-i}) \equiv 0 \pmod{I^2}$, which is impossible as $\zeta^i y$ is prime to λ and $1 - \zeta^{j-i}$ is associate to $1 - \zeta = \lambda$. Thus, the $x + \zeta^j y$ are distinct modulo I^2, so the

$$\frac{x + \zeta^j y}{\lambda} \quad (k = 0, 1, \ldots, p-1)$$

are pairwise-noncongruent modulo I. Because the norm of I is p, the order of $\mathbb{Z}[\zeta]/I$ is p, which means that these expressions form a complete set of residues modulo I. In particular, one must be an element of I. Because we may replace y by any $\zeta^j y$, we can assume that $x + y \in I^2$. So each $x + \zeta^j y$ for $j \neq 0$ is an element of $I \backslash I^2$. Hence, the left hand side of (9) is divisible by I^{p+1}, and $m > 1$.

We let $\mathfrak{m}$ denote the greatest common divisor of $\langle x \rangle$ and $\langle y \rangle$. We know that $\langle x \rangle$ and $\langle y \rangle$ are not divisble by I, so $\mathfrak{m}$ is not either. So $\langle x + \zeta^j y \rangle$ is divisible by $I\mathfrak{m}$ when $j \neq 0$ and $\langle x + y \rangle$ is divisible by $I^{p(m-1)+1}\mathfrak{m}$, and we let $\langle x + \zeta^j y \rangle = I\mathfrak{m}\mathfrak{p}_j$ for each $j \neq 0$ and $\langle x + y \rangle = I^{p(m-1)+1}\mathfrak{m}\mathfrak{p}_0$. We claim that the ideals $\mathfrak{p}_0, \ldots, \mathfrak{p}_{p-1}$ are pairwise coprime. If $\mathfrak{p}$ divides $\mathfrak{p}_i$ and $\mathfrak{p}_j$ for some $i < j$, then $\langle x + \zeta^i y \rangle$ and $\langle x + \zeta^j y \rangle$ would be divisible by $I\mathfrak{m}\mathfrak{p}$. But then $\zeta^j y(1 - \zeta^{j-i})$ and $x(1 - \zeta^{j-i})$ would be in $I\mathfrak{m}\mathfrak{p}$, which means that $x, y \in \mathfrak{m}\mathfrak{p}$, contradicting the choice of $\mathfrak{m}$. So the ideals $\mathfrak{p}_0, \ldots, \mathfrak{p}_{p-1}$ are pairwise coprime.

We substitute these new equations into (9) to get $\mathfrak{m}^p I^{pm} \mathfrak{p}_0 \cdots \mathfrak{p}_{p-1} = I^{pm}\langle z_0 \rangle^p$. Because the $\mathfrak{p}_j$ are pairwise coprime, we see that each $\mathfrak{p}_j$ must be the p-th power of some ideal dividing $\langle z_0 \rangle$. Let $\mathfrak{p}_j = \mathfrak{a}_j^p$ for $j = 0, 1, \ldots, p-1$. Then $\langle x + y \rangle = I^{p(m-1)+1}\mathfrak{m}\mathfrak{a}_0^p$ and $\langle x + \zeta^j y \rangle = I\mathfrak{m}\mathfrak{a}_k^p$. We solve the first equation for $\mathfrak{m}$ and substitute this into the second to obtain

$$\langle x + \zeta^j y \rangle I^{p(m-1)} = \langle x + y \rangle (\mathfrak{a}_j \mathfrak{a}_0^{-1})^p. \tag{10}$$

It follows that the ideals $(\mathfrak{a}_j \mathfrak{a}_0^{-1})^p$ are principal, because the left hand side is. We know that if J^p is any principal ideal of $\mathbb{Z}[\zeta]$, then J is principal as well, because p does not divide C_K (as the order of any non-principal ideal would). Thus, $\mathfrak{a}_j \mathfrak{a}_0^{-1}$ is principal as well. Hence, there exist $\alpha_j, \beta_j \in \mathbb{Z}[\zeta]$ such that $\mathfrak{a}_j \mathfrak{a}_0^{-1} = \langle \frac{\alpha_j}{\beta_j} \rangle$ for $j = 1, \ldots, p-1$. Because $\mathfrak{a}_j$ and $\mathfrak{a}_0$ are coprime to I, we may assume that neither α_j or β_j is in I. From (10), we see that

$$(x + \zeta^j y)\lambda^{p(m-1)} = (x + y)\left(\frac{\alpha_j}{\beta_j}\right)^p u_j \quad (j = 1, 2, \ldots, p-1) \tag{11}$$

where each $u_j \in \mathbb{Z}[\zeta]$ is a unit. It is clear that $(x + \zeta y)(1 + \zeta) - (x + \zeta^2 y) = \zeta(x + y)$. If we multiply this equation by $\lambda^{p(m-1)}$ and evaluate (11) at $j = 1$ and $j = 2$, we see that $(x + y)\left(\frac{\alpha_1}{\beta_1}\right)^p u_1(1 + \zeta) - (x + y)\left(\frac{\alpha_2}{\beta_2}\right)^p u_2 = (x + y)\zeta\lambda^{p(m-1)}$. Thus,

$$(\alpha_1\beta_2)^p - \frac{u_2}{u_1(1 + \zeta)}(\alpha_2\beta_1)^p = \frac{\zeta}{u_1(1 + \zeta)}\lambda^{p(m-1)}(\beta_1\beta_2)^p.$$

Again, we note that $1 + \zeta$ is a unit, this time because $(1 - \zeta)(1 + \zeta) = 1 - \zeta^2$, which is associate to $1 - \zeta = \lambda$. Thus, if we set $\alpha = \alpha_1\beta_2$, $\beta = \alpha_2\beta_1$, and $\gamma = \beta_1\beta_2$, we have the equality:

$$\alpha^p + e\beta^p = e'\lambda^{p(m-1)}\gamma^p \tag{12}$$

where $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta] \backslash I$ and $e, e' \in U_K$ are units. We hope to modify (12) to get an equation of the form (8).

Because $m > 1$, $p(m-1) \geq p$, and $\alpha^p + e\beta^p \equiv 0 \pmod{I^p}$. Because β is prime to I, there exists some β' such that $\beta\beta' \equiv 1 \pmod{I^p}$. We multiply the first congruence by β'^p and see that $e \equiv (-\alpha\beta')^p \pmod{I}$. Because the norm of I is p, and $-\alpha\beta' \in \mathbb{Z}[\zeta]$, as discussed previously, $-\alpha\beta'$ is congruent to some $a \in \mathbb{Z}$ modulo I. Then $(-\alpha\beta')^p \equiv a^p \pmod{I^p}$, so the same is true of the unit e. Because $\langle p \rangle \mid I^p$, we can apply Proposition 3.12 to see that e is a p-th power in K. We let $e = \eta^p$, where $\eta \in \mathbb{Z}[\zeta]$ is another unit. Then

$$\alpha^p + (\eta\beta)^p = e'\lambda^{p(m-1)}\zeta^p,$$

which is of the same type as the equation (8). But here we have replaced the exponent m by $m-1$, contradicting the minimality of m. Hence, (7) has no solution in $\mathbb{Z}$ where p divides one of x, y, and z, and we have completed the proof of Fermat's Last Theorem for regular primes. □

4 Acknowledgments

Most of the specifics of the proof of Kummer's special case of Fermat's Last Theorem were adapted from Stewart and Tall [7], although the case where p divides one of x, y,and z is omitted there and taken instead from Borevich and Shafarevich [1] as well as Hellegouarch [3]. The majority of the background material on algebraic number theory came from my memory of William Stein's course in the subject given at Harvard in the Spring of 2005, and this was supplemented with his online text [6] and my notes from class. Finally, the proof that a cyclotomic number field contains no other roots of unity was shamelessly plagiarized from my solution to problem 1 on problem set 6 for Math 129, although I did take care to adapt that solution to the case needed here.

References

[1] Z. I. Borevich and I. R. Shafarevich, Number Theory, Academic Press, New York, 1966.

[2] A. Fröhlich and M. J. Taylor, Algebraic number theory, Cambridge University Press, Cambridge, England, 1994 pp 251-254.

[3] Y. Hellegouarch, Invitation to the Mathematics of Fermat-Wiles, Academic Press, San Diego, CA, 2002 pp 18-35.

[4] I. Niven, H. Zuckerman, and H. Montgomery, An Introduction to the Theory of Numbers, John Wiley & Sons, New York, 1991 pp 291-292.

[5] S. Singh, Fermat's Enigma, Doubleday, New York, 1997.

[6] W. Stein, Introduction to Algebraic Number Theory, Unpublished manuscript, 2005.

[7] I. Stewart and D. Tall, Algebraic Number Theory and Fermat's Last Theorem, 3rd Ed, A K Peters, Natick, MA, 2002 pp 183-198.