KUMMER'S THEORY ON IDEAL NUMBERS AND FERMAT'S LAST THEOREM

FIZAY-NOAH LEE

Abstract. This paper is an exposition on Ernst Kummer's theory of ideal numbers, which "saves" unique factorization in the ring of integers of the cyclotomic field. A significant application of this theory is in proving a large subcase of Fermat's Last Theorem, namely, the case of regular prime exponents.

Contents

1. Cyclotomic Integers

The idea of unique factorization is a familiar concept because it is a property that holds true for the integers and because many properties of the integers depend on it. The failure of unique factorization in the ring of integers of certain cyclotomic fields is what motivated Ernst Kummer to develop his theory of ideal numbers, which restores unique factorization for the rings in question. To begin a study of this theory, we start by investigating the elements of the rings of integers of cyclotomic fields, which Kummer called cyclotomic integers.

Definition 1.1. Given a prime integer λ, a primitive λth root of unity is a complex number α that satisfies $\alpha^\lambda = 1$ and $\alpha^i \neq 1$ for $i = 1, 2, ..., \lambda - 1$.

Remark 1.2. Concretely, from Euler's formula, one choice of α is $\cos\frac{2\pi}{\lambda} + i\sin\frac{2\pi}{\lambda}$. Observe that $\overline{\alpha} = \alpha^{-1}$.

From this point on, we will fix λ to be an arbitrary odd prime integer and α will be understood to be a corresponding primitive λth root of unity. Later when we define regular prime integers, λ will refer specifically to a regular prime integer.

Definition 1.3. Cyclotomic integers are the elements of $\mathcal{O}_K = \mathbb{Z}[\alpha]$, the ring of integers of the cyclotomic field $\mathbb{Q}(\alpha)$.

Remark 1.4. Because of the identity $\alpha^\lambda = 1$, we can express every element of $\mathcal{O}_K$ in the form $a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{\lambda-1}\alpha^{\lambda-1}$, where $a_0, ..., a_{\lambda-1}$ are integers. And because of this form which resembles a polynomial in α, Kummer used the notation $f(\alpha), g(\alpha), ...$ to denote cyclotomic integers.

Definition 1.5. We define a norm N on cyclotomic integers by

$$Nf(\alpha) := f(\alpha)f(\alpha^2)...f(\alpha^{\lambda-1})$$

We state without proof that $Nf(\alpha) \in \mathbb{Z}^+ \cup \{0\}$, $Nf(\alpha) = 0 \Leftrightarrow f(\alpha) = 0$, $Nf(\alpha) = 1 \Leftrightarrow f(\alpha)$ is a unit in $\mathcal{O}_K$, and N is multiplicative, i.e. $N(f(\alpha)g(\alpha)) = Nf(\alpha)Ng(\alpha)$.

Definition 1.6. A cyclotomic integer $f(\alpha) \in \mathcal{O}_K$ divides $g(\alpha) \in \mathcal{O}_K$ if there exists $h(\alpha) \in \mathcal{O}_K$ such that $f(\alpha)h(\alpha) = g(\alpha)$.

Definition 1.7. A cyclotomic integer $f(\alpha)$ is prime if it satisfies the following condition: $f(\alpha)|g(\alpha)h(\alpha)$ implies $f(\alpha)|g(\alpha)$ or $f(\alpha)|h(\alpha)$.

Now we state a few basic lemmas (some without proof) that will be useful later.

Lemma 1.8. *Let p be a prime integer, and let k be an integer coprime with p. Then $k, 2k, 3k, ..., (p-1)k$ are distinct modulo p.*

Lemma 1.9. *For any $k \in \mathbb{Z}$ coprime with λ and $f(\alpha) \in \mathcal{O}_K$, we have $Nf(\alpha) = Nf(\alpha^k)$. That is, the norm is invariant under the conjugation $\alpha \mapsto \alpha^k$.*

Lemma 1.10. *Every cyclotomic integer is congruent modulo $\alpha - 1$ to an integer.*

Proof. Let $g(\alpha)$ be an arbitrary cyclotomic integer. Say $g(\alpha) = a_0 + a_1\alpha + ... + a_{\lambda-1}\alpha^{\lambda-1}$. Clearly $\alpha \equiv 1 \bmod (\alpha - 1)$. Therefore $g(\alpha) \equiv g(1) \equiv a_0 + a_1 + ... + a_{\lambda-1} \bmod (\alpha - 1)$. □

Lemma 1.11. *For a given cyclotomic integer $g(\alpha)$ and any positive integer k, there exist $a_0, ..., a_{k-1} \in \mathbb{Z}$ such that $g(\alpha) \equiv a_0 + a_1(\alpha - 1) + ... + a_{k-1}(\alpha - 1)^{k-1} \bmod (\alpha - 1)^k$*

Proof. By Lemma 1.10, there exists $a_0 \in \mathbb{Z}$ such that $a_0 \equiv g(\alpha) \bmod (\alpha - 1)$. So $h(\alpha) = \frac{g(\alpha)-a_0}{\alpha-1} \in \mathcal{O}_K$. Then, again, there exists $a_1 \in \mathbb{Z}$ such that $a_1 \equiv h(\alpha) \bmod (\alpha - 1)$. Then it follows that $(\alpha-1)|(h(\alpha)-a_1) \Rightarrow (\alpha-1)^2|(\alpha-1)(h(\alpha)-a_1) \Rightarrow g(\alpha) \equiv a_0+a_1(\alpha-1) \bmod (\alpha-1)^2$. If we continue this process, the theorem follows. □

2. Cyclotomic Periods

In this section, we develop the machinery necessary to define a notion of divisibility by "ideal numbers," which will be defined later.

Definition 2.1. A number γ is a primitive root modulo λ if each of $1, 2, ..., \lambda - 1$ is congruent to a power of γ modulo λ.

Remark 2.2. One can easily verify that if γ is a primitive root modulo λ, then $\gamma, \gamma^2, ..., \gamma^{\lambda-1}$ are all distinct and are, therefore, a permutation of $1, 2, ..., \lambda - 1$.

Remark 2.3. We state without proof that for every prime integer p, there exists a primitive root modulo p.

Definition 2.4. If γ is a primitive root modulo λ, let σ denote the conjugation $\alpha \mapsto \alpha^{\gamma}$.

Example 2.5. We have $\sigma f(\alpha) = f(\alpha^{\gamma})$, $\sigma^2 f(\alpha) = f(\alpha^{\gamma\gamma}) = f(\alpha^{\gamma^2})$, etc.
Also $Nf(\alpha) = \sigma f(\alpha)\sigma^2 f(\alpha)...\sigma^{\lambda-1} f(\alpha)$. But observe that $\sigma^{\lambda-1} f(\alpha) = f(\alpha^{\gamma^{\lambda-1}})$ and from Fermat's Little Theorem, we see that $\gamma^{\lambda-1} \equiv 1 \bmod \lambda$ (γ being a primitive root modulo λ must imply γ and λ are coprime). So $\sigma^{\lambda-1}$ is the identity conjugation. Therefore, $Nf(\alpha) = f(\alpha)\sigma f(\alpha)\sigma^2 f(\alpha)...\sigma^{\lambda-2} f(\alpha)$

Lemma 2.6. *Let e be a factor of $\lambda - 1$. Then given $g(\alpha) \in \mathcal{O}_K$, we can find $G(\alpha) \in \mathcal{O}_K$ such that $Ng(\alpha) = G(\alpha)\sigma G(\alpha)...\sigma^{e-1} G(\alpha)$*

Proof. I claim that

$$G(\alpha) = g(\alpha)g(\alpha^{\gamma^e})g(\alpha^{\gamma^{2e}})...g(\alpha^{\gamma^{\frac{\lambda-1}{e}}}) = g(\alpha)g(\alpha^{\gamma^e})g(\alpha^{\gamma^{2e}})...g(\alpha^{\gamma^{\lambda-1-e}}) \tag{2.7}$$

satisfies the theorem.
Note:

$$\sigma G(\alpha) = g(\alpha^{\gamma})g(\alpha^{\gamma^{e+1}})g(\alpha^{\gamma^{2e+1}})...g(\alpha^{\gamma^{\lambda-e}})$$

$$...$$

$$\sigma^{e-1} G(\alpha) = g(\alpha^{\gamma^{e-1}})g(\alpha^{\gamma^{2e-1}})g(\alpha^{\gamma^{3e-1}})...g(\alpha^{\gamma^{\lambda-2}})$$

So each of $G(\alpha), \sigma G(\alpha), ..., \sigma^{e-1} G(\alpha)$ is a product made up of $\frac{\lambda-1}{e}$ terms. Therefore, $G(\alpha)\sigma G(\alpha)...\sigma^{e-1} G(\alpha)$ is a product of $\lambda - 1$ terms, and it is clear that the terms have a one-to-one correspondence with $g(\alpha), g(\alpha^{\gamma})..., g(\alpha^{\gamma^{\lambda-2}})$ and hence also with $g(\alpha), g(\alpha^2), ..., g(\alpha^{\lambda-1})$.
Therefore $G(\alpha)\sigma G(\alpha)...\sigma^{e-1} G(\alpha) = g(\alpha)g(\alpha^2)...g(\alpha^{\lambda-1}) = Ng(\alpha)$ □

Theorem 2.8. *There exist $\eta_0, \eta_1, ..., \eta_{e-1} \in \mathcal{O}_K$ such that:*
1) $\eta_0 = \alpha + \sigma^e\alpha + \sigma^{2e}\alpha + ... + \sigma^{\lambda-1-e}\alpha$
2) $\eta_{i+1} = \sigma\eta_i$ for $i = 0, 1, ..., e-2$
3) $G(\alpha) = a_0 + a_1\eta_0 + a_2\eta_1 + ... + a_e\eta_{e-1}$ where $a_0, ..., a_e \in \mathbb{Z}$ and $G(\alpha)$ is defined as in Lemma 2.6.

Proof. It follows from Lemma 2.6 that $\sigma^e G(\alpha) = G(\alpha)$ because

$$\sigma^e G(\alpha) = g(\alpha^{\gamma^e})g(\alpha^{\gamma^{2e}})...g(\alpha^{\gamma^{\lambda-1}}) \text{ and } g(\alpha^{\gamma^{\lambda-1}}) = g(\alpha).$$

So, if we write $G(\alpha)$ as $a_0 + a_1\alpha + ... + a_{\lambda-1}\alpha^{\lambda-1}$, then comparing $\sigma^e G(\alpha)$ with $G(\alpha)$, we conclude that the coefficient of α^j in $G(\alpha)$ must be equal to the cofficient of $\sigma^e\alpha^j$ in $\sigma^e G(\alpha)$. Extending this reasoning (comparing $\sigma^{2e} G(\alpha)$ with $G(\alpha)$ and so on), we conclude that $G(\alpha)$ must be of the form

$$a_0 + a_1(\alpha + \sigma^e\alpha + \sigma^{2e}\alpha + ... + \sigma^{\lambda-1-e}\alpha) + a_2(\sigma\alpha + \sigma^{2e+1}\alpha + ... + \sigma^{\lambda-e}\alpha) + ...+$$
$$+a_e(\sigma^{e-1}\alpha + \sigma^{2e-1}\alpha + ... + \sigma^{\lambda-2}\alpha)$$

From above, it is clear that if we let

$$\eta_0 = \alpha + \sigma^e\alpha + \sigma^{2e}\alpha + ... + \sigma^{\lambda-1-e}\alpha$$

$$\eta_1 = \sigma\alpha + \sigma^{2e+1}\alpha + ... + \sigma^{\lambda-e}\alpha$$

$$...$$

$$\eta_{e-1} = \sigma^{e-1}\alpha + \sigma^{2e-1}\alpha + ... + \sigma^{\lambda-2}$$

then we have the cyclotomic integers $\eta_0, ...\eta_{e-1}$ satisfying conditions 1, 2 and 3. □

Remark 2.9. It is important to observe that although $\eta_0, ..., \eta_{e-1}$ were found by first fixing a $g(\alpha)$, ultimately, these cyclotomic integers are indepedent of the choice of $g(\alpha)$ and only depend on the choices of λ (and hence of α), γ, and e. (In fact, a different choice of γ only permutes the order of the cyclotomic periods, so in a sense, the periods are independent of the choice of primitive root modulo λ as well.) Hence we can make the following definition.

Definition 2.10. Given λ, γ (a primitive root modulo λ), and e (a rational factor of $\lambda - 1$), the cyclotomic integers $\eta_0, ..., \eta_{e-1}$, as found in Theorem 2.8, are called cyclotomic periods.

Remark 2.11. Observe that each η_i is a sum of $f = \frac{\lambda-1}{e}$ terms. Hence, we say each period has length f.

Remark 2.12. By convention, we set $\eta_e = \eta_0$ and $\eta_{-1} = \eta_{e-1}$. Thus η_i is defined for all $i \in \mathbb{Z}$.

Remark 2.13. It is easily verifiable through induction, and using the convention set in the remark above, that $\sigma^e \eta_i = \eta_i$. This property is the motivation for the name, periods.

Definition 2.14. Let $f = \frac{\lambda-1}{e}$. A cyclotomic integer is "made up of periods of length f" if it can be written in the form:

$$a_0 + a_1\eta_1 + a_2\eta_2 + ... + a_e\eta_e \tag{2.15}$$

where $a_0, ..., a_e \in \mathbb{Z}$ and $\eta_1, ..., \eta_e \in \mathcal{O}_K$ are cyclotomic periods of length f.

Theorem 2.16. *A cyclotomic integer $g(\alpha)$ is made up of periods of length $f = \frac{\lambda-1}{e}$ if and only if $\sigma^e g(\alpha) = g(\alpha)$.*

Proof. We will first prove the forward direction. Assume $g(\alpha)$ is made up of periods of length f. Then, by definition, there exist $a_0, ..., a_e \in \mathbb{Z}$ and $\eta_1, ..., \eta_e$ such that $g(\alpha) = a_0 + a_1\eta_1 + a_2\eta_2 + ... + a_e\eta_e$. But by Remark 2.13, we get $\sigma^e g(\alpha) = a_0 + a_1\sigma^e\eta_1 + a_2\sigma^e\eta_2 + ... + a_e\sigma^e\eta_e = a_0 + a_1\eta_1 + a_2\eta_2 + ... + a_e\eta_e$. So $\sigma^e g(\alpha) = g(\alpha)$. To prove the converse, assume that $\sigma^e g(\alpha) = g(\alpha)$. Then by the same reasoning used in the proof for Theorem 2.8, we can conclude that $g(\alpha)$ is made up of e periods. Then as we noted in Remark 2.11, each period has length f. □

3. Divisibility by Prime Divisors

With the machinery developed in the previous section, we can now define what it means for a cyclotomic integer to be divisible by a"prime divisor". As we will see later, these prime divisors are the building blocks for ideal numbers.

Definition 3.1. Given a prime $p \in \mathbb{Z}$ such that $p \neq \lambda$, if f is the smallest positive integer such that $p^f \equiv 1 \bmod \lambda$, then we say f is the exponent of p modulo λ.

From this point on p is always a prime integer distinct from λ unless otherwise stated and f is always the exponent of p modulo λ.

Lemma 3.2. *Let $k \in \mathbb{Z}$. Say $k^j \equiv 1 \bmod p$ for some $j \in \mathbb{Z}$. Then there exists a smallest positive integer d such that $k^d \equiv 1 \bmod p$ and $d|i$ whenever $k^i \equiv 1 \bmod p$.*

Proof. By the well-ordering principle, there exists a smallest positive integer d such that $k^d \equiv 1 \bmod \lambda$. Now assume $k^i \equiv 1 \bmod \lambda$. Then there exist $q, r \in \mathbb{Z}$ such that $i = qd + r$ and $0 \leq r < d$. Then $k^i \equiv k^{dq+r} \equiv (k^d)^q k^r \equiv k^r \equiv 1 \bmod \lambda$. If $0 < r < d$, then we have found a positive integer smaller than d that is congruent to 1 modulo λ, which leads to a contradiction. Therefore $r = 0$, and $i = dq \Rightarrow d|i$. □

Proposition 3.3. $f|(\lambda - 1)$

Proof. By definition, p^f is the lowest power of p such that $p^f \equiv 1 \bmod \lambda$. We also know that, by Fermat's Little Theorem, $p^{\lambda-1} \equiv 1 \bmod \lambda$. So it follows from Lemma 3.2 that $f|(\lambda - 1)$. □

Due to this proposition, we can now set $e = \frac{\lambda-1}{f} \in \mathbb{Z}$.

Lemma 3.4. *Let $h(\alpha)$ be a cyclotomic prime. Then there exists a prime integer p such that $h(\alpha)|p$.*

Proof. This lemma follows from the fact that $h(\alpha)$ is a factor of $Nh(\alpha)$, and $Nh(\alpha)$ is an integer which can be expressed as a product of prime integers. □

Lemma 3.5. *Let $g(\alpha) \in \mathcal{O}_K$ be made up of periods of length f (Definition 2.14). Then $g(\alpha) = g(\alpha^p)$*

Proof. Let τ be the conjugation $\alpha \mapsto \alpha^p$. We define the conjugation σ, $\alpha \mapsto \alpha^\gamma$, as in Defintion 2.4, where γ is a primitive root modulo λ. From the definition of a primitive root, we know there exists $k \in \mathbb{Z}$ such that $\tau = \sigma^k$. Then, $\tau^f = \sigma^{kf}$. Now note that τ^f maps α to α^{p^f}, and since $p^f \equiv 1 \bmod \lambda$, we have $\alpha^{p^f} = \alpha$. In other words, τ^f is the identity mapping, which implies σ^{kf} is the identity mapping. Now considering the group G (with the operation of composition, $\circ$) consisting of the elements $\sigma, \sigma^2, \sigma^3, ...$, we know from Remark 2.2 that the order of G is $\lambda - 1$ and the $\lambda - 1$ distinct elements are $\sigma, \sigma^2, ..., \sigma^{\lambda-1}$. From these observations, it is not hard to see that $G \cong \mathbb{Z}_\lambda$. Thus, applying Fermat's Little Theorem to G, $\sigma^{\lambda-1}$ is the lowest positive power of σ that is identical to the identity mapping. Similarly, applying Lemma 3.2 to G, we conclude that $\lambda - 1$ divides kf. And since $ef = \lambda - 1$, we conclude $ef|kf$, and hence $e|k$. Therefore, $\exists k' \in \mathbb{Z}$ such that $k = ek'$. Hence $\tau = \sigma^k = (\sigma^e)^{k'}$. So we have, from Theorem 2.16:

$$g(\alpha^p) = \tau g(\alpha) = [\overbrace{(\sigma^e) \circ ... \circ (\sigma^e)}^{k' \text{ times}}]g(\alpha) = g(\alpha)$$

□

Lemma 3.6. $(x + y)^p \equiv x^p + y^p \bmod p$.

Proof. This lemma follows from the Binomial Theorem once we observe that the coefficients of all the terms of $(x + y)^p$ other than x^p and y^p are divisible by p. □

Corollary 3.7. *For $g(\alpha) \in \mathcal{O}_K$, $g(\alpha)^p \equiv g(\alpha^p) \bmod p$.*

Proof. Observe that $g(\alpha)^p = (a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{\lambda-1}\alpha^{\lambda-1})^p$. Then the statement follows from Lemma 3.6 and applying Fermat's Little Theorem to the coefficients. □

We state the following technical lemma without proof.

Lemma 3.8. *For a prime integer p, we have*

$$X^p - X \equiv (X-1)(X-2)...(X-p) \bmod p.$$

Theorem 3.9. *Let $g(\alpha) \in \mathcal{O}_K$ be made up of periods of length f and let $h(\alpha)$ be a cyclotomic prime and let p be the prime integer that $h(\alpha)$ divides (Lemma 3.4). Then there exists an integer $u \in \{0, 1, ..., p-1\}$ such that $g(\alpha) \equiv u \bmod h(\alpha)$.*

Proof. By Lemma 3.8, setting $X = g(\alpha)$, we find that $g(\alpha)^p - g(\alpha) \equiv (g(\alpha) - 1)(g(\alpha)-2)...(g(\alpha)-p) \bmod h(\alpha)$ (since $h(\alpha)|p$). Then, by Corollary 3.7 and Lemma 3.5, we see that $0 \equiv g(\alpha) - g(\alpha) \equiv (g(\alpha)-1)(g(\alpha)-2)...(g(\alpha)-p) \bmod h(\alpha)$. Since $h(\alpha)$ is prime, one of the factors $g(\alpha)-1, ..., g(\alpha)-p$ must be divisible by $h(\alpha)$, so the theorem follows. □

The significance of Theorem 3.9 is that now we have integers $u_1, ..., u_i$ such that $\eta_i \equiv u_i \bmod h(\alpha)$, and as we will see, these integers will allow us to come up with a notion of divisibility by a prime divisor of p, without knowing anything else about the prime divisor.

Remark 3.10. Consider the polynomial

$$p(x) = \prod_{i=1}^{f} (x - \sigma^{ei}\alpha). \tag{3.11}$$

If we multiply this product out, we get the following form:

$$p(x) = x^f + \phi_1(\eta)x^{f-1} + ... + \phi_{f-1}(\eta)x + \phi_f(\eta). \tag{3.12}$$

where $\phi_i(\eta)$ are cyclotomic integers.
Note that $\sigma^e p(x) = p(x)$ since $\sigma^e p(x) = (x - \sigma^{2e}\alpha)(x - \sigma^{3e}\alpha)...(x - \sigma^{efe}\alpha)$ and $\sigma^{efe} = \sigma^e\sigma^{ef} = \sigma^e\sigma^{\lambda-1} = \sigma^e$. Extending the result from Theorem 2.16, we conclude that $p(x)$ consists of periods of length f so that $\phi_1(\eta), ..., \phi_f(\eta)$ have length f. Lastly, note that $p(\alpha) = 0$ because $\sigma^{ef} = \sigma^{\lambda-1}$ is the identity mapping (hence the last factor in (3.11) with $x = \alpha$ is $\alpha - \alpha = 0$). Therefore we have the relation

$$\alpha^f + \phi_1(\eta)\alpha^{f-1} + ... + \phi_{f-1}(\eta)\alpha + \phi_f(\eta) = 0 \tag{3.13}$$

Lemma 3.14. *Every cyclotomic integer $g(\alpha)$ can be expressed in terms of cycltomic integers made up of periods of length f such that*

$$g(\alpha) = g_1(\eta)\alpha^{f-1} + g_2(\eta)\alpha^{f-2} + ... + g_f(\eta)$$

where $g_1(\eta), ..., g_f(\eta)$ are cyclotomic integers made up of periods of length f.

Proof. From (3.13) we see that we have the relation $\alpha^f = -\phi_1(\eta)\alpha^{f-1} - ... - \phi_{f-1}(\eta)\alpha - \phi_f(\eta)$ where $\phi_1(\eta), ..., \phi_f(\eta)$ are cyclotomic integers made up of periods of length f. Therefore, for given $g(\alpha)$, we can keep reducing the powers of α using the identity given by (3.13) until the highest power in $g(\alpha)$ is less than f. □

Lemma 3.15. *The additive group of cyclotomic integers modulo p has $p^{\lambda-1}$ integers.*

Proof. This lemma follows when we observe that any cyclotomic integer can be expressed as $a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{\lambda-2}\alpha^{\lambda-2}$. This is the case because adding multiples of $0 = 1 + \alpha + \alpha^2 + ... + \alpha^{\lambda-1}$ eliminates the $\alpha^{\lambda-1}$ term. Then, modulo p, each coefficient is one of $0, 1, ..., p-1$, so the lemma follows. □

Theorem 3.16. *Let $h(\alpha)$ be a prime factor of p. Let*

$$S = \{a_1\alpha^{f-1} + a_2\alpha^{f-2} + ... + a_f \mid 0 \leq a_i < p\}.$$

Then for any cyclotomic integer $g(\alpha)$, one can find $\overline{g}(\alpha) \in S$ such that $g(\alpha) \equiv \overline{g}(\alpha) \bmod h(\alpha)$. Furthermore, two elements of S are congruent modulo $h(\alpha)$ if and only if they are identical.

Proof. (Outline) The first part of the theorem follows immediately from Lemma 3.14 and from noting that $g_i(\eta)$ is congruent to an integer modulo $h(\alpha)$. To prove the second part of the theorem, we simply need to show that there are exactly p^f incongruent elements modulo $h(\alpha)$ (it should be clear there are at most p^f). First note that since the additive group of cyclotomic integers modulo $h(\alpha)$ is a subgroup of the additive group of cyclotomic integers modulo p, the order of the additive group of cyclotomic integers modulo $h(\alpha)$ is a multiple of p, say p^n (Lemma 3.15; Langrange's Theorem). Next proceed to show that there are at least $\lambda + 1$ incongruent cyclotomic integers modulo $h(\alpha)$ (namely, $0, \alpha, \alpha^2, ..., \alpha^\lambda$) and conclude $n > 0$. Then finally show that the number of nonzero incongreunt cyclotomic integers modulo $h(\alpha)$ is a multiple of λ. So then for $m \in \mathbb{Z}^+$, we have $m\lambda = p^n - 1 \Rightarrow p^n \equiv 1 \bmod \lambda$, and by definition of f being an exponent of p modulo λ, we conclude $n \geq f$. □

This theorem gives us a test for divisibility by $h(\alpha)$ because it guarantees that $\overline{g}(\alpha) \in S$ can be found such that $g(\alpha) \equiv \overline{g}(\alpha) \bmod h(\alpha)$ and that $g(\alpha) \equiv 0 \bmod h(\alpha)$ if and only if $\overline{g}(\alpha) = 0$. So, we have the result that to test $g(\alpha)$ for divisibility by $h(\alpha)$ it is not necessary to know $h(\alpha)$ but only the integers $u_1, ..., u_e$ for which $\eta_i \equiv u_i \bmod h(\alpha)$ holds.

4. Ideal Numbers and Divisors

As per the previous section, if $u_1, ..., u_e$ are derived from an actual prime factor $h(\alpha)$ of p, then Theorem 3.16 allows us determine whether given cyclotomic integers are congruent modulo $h(\alpha)$. However, the fact that we do not need to know anything about $h(\alpha)$ to determine a cyclotomic integer's divisibility by it suggests that $h(\alpha)$ may not need to correspond to an actual cyclotomic integer. It is this consideration that lead's to Kummer's ideal numbers. As we will see, ideal numbers include both cyclotomic integers and the imaginary, constructed prime divisors of prime integers. This extension of the cyclotomic integers is what "saves" unique factorization.

We first investigate the number $\alpha - 1$, which, as we will see, is the sole prime divisor of λ.

Lemma 4.1. $(x - \alpha)(x - \alpha^2)...(x - \alpha^{\lambda-1}) = x^{\lambda-1} + x^{\lambda-2} + ... + x + 1$

Proof. This lemma follows from the following two equations, which are easy to verify:

$$x^\lambda - 1 = (x - 1)(x - \alpha)(x - \alpha^2)...(x - \alpha^{\lambda-1}) \tag{4.2}$$

$$x^\lambda - 1 = (x - 1)(x^{\lambda-1} + x^{\lambda-2} + ...x + 1) \tag{4.3}$$

□

Lemma 4.4. $N(\alpha - 1) = \lambda$

Proof. Since λ is odd, we have $N(\alpha - 1) = N(1 - \alpha)$. Then, applying the above lemma with $x = 1$, we have $N(1-\alpha) = 1 + ... + 1 = \lambda$. Therefore $N(\alpha - 1) = \lambda$. □

The following result is an immediate consequence of this lemma because λ is a prime integer.

Corollary 4.5. *$\alpha - 1$ is prime in $\mathcal{O}_K$.*

Lemma 4.6. *$\alpha^j - 1$ and $\alpha - 1$ are associate for $j \in \mathbb{Z}$.*

Proof. This lemma follows from the equation

$$\alpha^j - 1 = (\alpha - 1)(\alpha^{j-1} + \alpha^{j-2} + ... + \alpha + 1) \tag{4.7}$$

and the observation that $\alpha^j - 1$ and $\alpha - 1$ have the same norm because they are conjugates. □

The following corollaries follow immediately from Lemma 4.4 and Lemma 4.6.

Corollary 4.8. *$\alpha - 1$ and its conjugates are the only cyclotomic primes that divide λ.*

Corollary 4.9. *$(\alpha - 1)^{\lambda - 1}$ is associate with λ.*

Now we investigate the prime divisors of prime integers distinct from λ.

Definition 4.10. Consider the set

$$\Psi' = \{j - \eta_i \in \mathcal{O}_K \mid j = 1, 2, ..., p \text{ and } i = 1, 2, ..., e\}$$

where $\eta_1, ..., \eta_e$ are the cyclotomic periods as determined by e and λ. We know that the e elements $u_1 - \eta_1, ..., u_e - \eta_e$ (as determined through Theorem 3.9) are divisible by p, and we state without proof that these e elements are the only elements in Ψ' divisible by p. Let $\Psi = \Psi' \setminus \{u_1 - \eta_1, ..., u_e - \eta_e\}$.

We define $\psi(\eta)$ to be the product of the $ep - e$ elements in Ψ.

Remark 4.11. We claim without proof that the congruence relation defined by

$$g(\alpha)\psi(\eta) \equiv h(\alpha)\psi(\eta) \bmod p \Leftrightarrow g(\alpha) \sim h(\alpha) \tag{4.12}$$

satisfies the following properties:

(1) Reflexivity
(2) Symmetry
(3) Transitivity
(4) Consistency with addition and multiplication
(5) $\eta_i \sim u_i$
(6) $p \sim 0$
(7) $1 \not\sim 0$
(8) $ab \sim 0$ only if $a \sim 0$ or $b \sim 0$ (i.e $\sim$ is prime)
(9) The number of incongruent elements is exactly p^f

See [1] pg. 129 for proof.

Definition 4.13. We will call the congruence relation from Remark 4.11 congruence modulo the prime divisor of p corresponding to $u_1, ..., u_e$. If $g(\alpha)$ is congruent to 0 modulo this relation, then $g(\alpha)$ is said to be divisible by the prime divisor of p corresponding to $u_1, ..., u_e$.

One can verify that if there are integers $\overline{u}_1, \overline{u}_2, ..., \overline{u}_e$ satisfying all the conditions of Theorem 4.3, then $\overline{u}_1, \overline{u}_2, ..., \overline{u}_e$ is a cyclic permutation of $u_1, u_2, ..., u_e$. From this we reach the conclusion that there are e distinct prime divisors that can be constructed for each prime integer $p \neq \lambda$.

Furthermore, one can verify that a cyclotomic integer $g(\alpha)$ is divisible by a prime integer $p \neq \lambda$ if and only if $g(\alpha)$ is divisible by each of the e prime divisors of p.

Then, since $(\alpha-1)^{\lambda-1}$ is associate with λ, we have fully characterized all prime divisors: a prime divisor is either $\alpha-1$ or it is one of e prime divisors of a prime integer $p \neq \lambda$ (we are not considering unit multiples).

Remark 4.14. From the remarks above, it becomes clear that to check congruence modulo other prime divisors of p, one can simply substitute $\sigma\psi(\eta), ..., \sigma^{e-1}\psi(\eta)$ for $\psi(\eta)$ in (4.12).

Definition 4.15. As per Theorem 4.11, we say $f(\alpha), g(\alpha)$ are congruent modulo a prime divisor of prime integer $p \neq \lambda$ if $f(\alpha)\psi(\eta) \equiv g(\alpha)\psi(\eta) \bmod p$, (or $f(\alpha)\sigma\psi(\eta) \equiv g(\alpha)\sigma\psi(\eta) \bmod p, ..., f(\alpha)\sigma^{e-1}\psi(\eta) \equiv g(\alpha)\sigma^{e-1}\psi(\eta) \bmod p$) (See Remark 4.14) where $\psi(\eta)$ is defined as in Definition 4.10.

Definition 4.16. A cyclotomic integer $g(\alpha)$ is divisible by a prime divisor of p if $g(\alpha)\psi(\eta) \equiv 0 \bmod p$ (or $g(\alpha)\sigma\psi(\eta) \equiv 0 \bmod p, ..., g(\alpha)\sigma^{e-1}\psi(\eta) \equiv 0 \bmod p$).

Definition 4.17. As a natural extension, $g(\alpha)$ is divisible by a prime divisor of p with multiplicity n if $g(\alpha)[\psi(\eta)]^n \equiv 0 \bmod p^n$ (or $g(\alpha)[\sigma\psi(\eta)]^n \equiv 0 \bmod p^n$,...,$g(\alpha)[\sigma^{e-1}\psi(\eta)]^n \equiv 0 \bmod p^n$).

Definition 4.18. The "divisor of a nonzero cyclotomic integer $g(\alpha)$" is a list, with multiplicities, of all the prime divisors which divide $g(\alpha)$. A "divisor" is any finite list of prime divisors. The divisor I is the empty list; it divides all cyclotomic integers. These two definitions may cause some confusion. Note that asking for the divisor of a cyclotomic integer is like asking for the prime factorization of an integer in $\mathbb{Z}$; hence it is *the* divisor of said cyclotomic integer.

Definition 4.19. A divisor D is *principal* if there is some cyclotomic integer for which it is the divisor.

Definition 4.20. An ideal number has the same definition as a divisor, but is used more broadly (like with the integers, the number 2 is a divisor in the sense that it divides $4, 6, 8, ...$, but, more broadly, it is an integer).

Remark 4.21. The multiplication of two ideal numbers is simply a matter of combining two lists so that multiplicities add up.

Remark 4.22. By Theorem 4.11, the congruence relation, as defined by Definition 4.15, is prime. Therefore, Euclid's Lemma holds for prime divisors (i.e. if $f(\alpha)g(\alpha)$ is divisible by a prime divisor P, then $P|f(\alpha)$ or $P|g(\alpha)$).

Theorem 4.23. *(The Fundamental Theorem) Let $g(\alpha), h(\alpha) \in \mathcal{O}_K$. Then $g(\alpha)$ divides $h(\alpha)$ if and only if every prime divisor which divides $g(\alpha)$ also divides $h(\alpha)$ with multiplicity at least as great.*

Proof. Clearly if $g(\alpha)$ divides $h(\alpha)$, then for some $q(\alpha) \in \mathcal{O}_K$, we have $h(\alpha) = q(\alpha)g(\alpha)$. Therefore, every prime divisor which divides $g(\alpha)$ also divides $h(\alpha)$ with multiplicity at least as great.

To prove the converse, observe that $g(\alpha)$ divides $h(\alpha)$ if and only if $Ng(\alpha) = g(\alpha)g(\alpha^2)...g(\alpha^{\lambda-1})$ divides $h(\alpha)g(\alpha^2)...g(\alpha^{\lambda-1})$. Therefore, if every prime divisors which divides $g(\alpha)$ also $h(\alpha)$ with multiplicity as great, then every prime divisor which divides $Ng(\alpha)$ divides $h(\alpha)g(\alpha^2)...g(\alpha^{\lambda-1})$ with multiplicity as great. Hence,

since $Ng(\alpha) \in \mathbb{Z}$, we can assume $g(\alpha) \in \mathbb{Z}$ and set $h(\alpha) = h(\alpha)g(\alpha^2)...g(\alpha^{\lambda-1})$. Now we have three cases.

Case I ($g(\alpha)$ is a prime integer $p \neq \lambda$): from the comment following Definition 4.13, we know that if $h(\alpha)$ is divisible by each of the e prime divisors of p, then $h(\alpha)$ is divisible by p.

Case II ($g(\alpha) = p = \lambda$): since $(\alpha - 1)^{\lambda-1}$ is associate with λ, if $h(\alpha)$ is divisible by the prime divisors of $p = \lambda$, i.e. by $(\alpha - 1)^{\lambda-1}$, then clearly $h(\alpha)$ is divisible by $g(\alpha) = \lambda \sim (\alpha - 1)^{\lambda-1}$.

Case III ($g(\alpha)$ is a nonprime integer): Assume $g(\alpha) = g_1(\alpha)g_2(\alpha)$ and that the theorem is true for $g_1(\alpha)$ and $g_2(\alpha)$. Now assume $h(\alpha)$ is divisible by all the prime divisors of $g_1(\alpha)g_2(\alpha)$. Then since the theorem is true for $g_1(\alpha)$, there exists $h_1(\alpha)$ such that $h(\alpha) = g_1(\alpha)h_1(\alpha)$. Then, thinking about how ideal number multiplication works, it must be the case that every prime divisor which divides $g_2(\alpha)$ also divides $h_1(\alpha)$. Therefore there exists $h_2(\alpha)$ such that $h_1 = g_2(\alpha)h_2(\alpha)$. Hence, $h(\alpha) = g_1(\alpha)g_2(\alpha)h_2(\alpha)$ $g_1(\alpha)g_2(\alpha)|h(\alpha)$. Combining this result with the fact that prime factorization works for integers, the theorem follows. □

From this theorem, we have an immediate consequence:

Corollary 4.24. *If two cyclotomic integers $g(\alpha), h(\alpha)$ are divisible by exactly the same divisors with exactly the same multiplicities, then $g(\alpha)$ and $h(\alpha)$ are associates.*

By this Corollary, unique factorization is saved for cyclotomic integers. Now, after stating a few definitions, we verify that a familiar property (familiar because it is true for integers) holds true for the ideal numbers. This property is crucial to proving the special case of Fermat's Last Theorem, which we will later prove.

Definition 4.25. We define the function $(-,-)$ (or $\gcd(-,-)$) on ideal numbers in an intuitive way. Since ideal numbers are simply lists, the function $(-,-)$ takes two ideal numbers (lists) and returns the ideal number (list) containing the common prime divisors of the two ideal numbers with multiplicities. This definition merely expands on the greatest common divisor function that we were familiar with in the integers.

Proposition 4.26. *Given a prime divisor of $p \neq \lambda$, there is a cyclotomic integer made up of periods of length f (the exponent of p modulo λ) which is divisible exactly once by that prime divisor of p and which is not divisible by the remaining $e - 1$ prime divisors of p.*

Proof. We let $\psi(\eta)$ be constructed as in Definition 4.10 for the given prime divisor of p. By construction, $\psi(\eta)$ is divisible by all e of the prime divisors of p except the give one. Then one can see that

$$\phi(\eta) = \sigma\psi(\eta) + \sigma^2\psi(\eta) + ... + \sigma^{e-1}\psi(\eta)$$

is divisible by the given prime divisor but not by the other $e-1$. If $\phi(\eta)$ is divisible by the given prime divisor with multiplicity exactly one, $\phi(\eta)$ has the required properties. Otherwise, consider $\phi(\eta)+p$. It is clear that $\phi(\eta)+p$ is divisible by the given prime divisor since $\phi(\eta)$ and p both are. Also, it is clear that $\phi(\eta)+p$ is not divisible by the other $e-1$ prime divisors (because, otherwise, $(\phi(\eta)+p)-p$ would also be divisible by the others). Finally, it is clear that $\phi(\eta)+p$ is not divisible by the given prime divisor with multiplicity greater than one (because, otherwise,

$(\phi(\eta)+p)-\phi(\eta)=p)$ would also be divisible with multiplicity greater than one). Thus, in this second case, $\phi(\eta)+p$ has the required properties. □

Remark 4.27. Using the above proposition, we can denote a prime divisor of prime integer p with $(p,\phi(\eta))$, where $\phi(\eta)$ is constructed so that it is divisible only by the given prime divisor and not the other $e-1$. Hence we can make the following definitions.

Definition 4.28. We can define the σ conjugation on prime divisors by the following:

$$\sigma(p,\psi(\eta)) := (p,\sigma\psi(\eta)).$$

Definition 4.29. We define a norm N on a prime divisor P by the following:

$$N(P) := (P)(\sigma P)(\sigma^2 P)...(\sigma^{e-1}P). \tag{4.30}$$

We state without proof that this norm is always a positive integer and is multiplicative. Therefore:

Definition 4.31. We define the same norm N on an arbitrary ideal number A by the following:

$$N(A) := N(P_1)^{a_1}N(P_2)^{a_2}...N(P_n)^{a_n} \tag{4.32}$$

where $P_1,...P_n$ are the prime divisors that make up A and $a_1,...,a_n$ are the respective multiplicities. We state without proof that the norm on ideal numbers is always a positive integer and is multiplicative.

We state the following lemma without proof.

Lemma 4.33. *$N(P)=p$ where P is a prime divisor of prime integer $p\neq\lambda$.*

The following theorem is a familiar property for integers, but now we prove that it holds for ideal numbers, too. This property will enable us to prove Fermat's Last Theorem for regular primes.

Theorem 4.34. *Assume $(U,V)=I$ and $u(\alpha)v(\alpha)=w(\alpha)^n$ for some $n\in\mathbb{Z}$ and where U,V are the divisors of u,v respectively. Then there exist ideal numbers C,D such that $U=C^n$ and $V=D^n$.*

Proof. Let W be the divisor of $w(\alpha)$. Now, WLOG, assume there is no ideal number C such that $U=C^n$. We know $U\neq I$ since $I^n=I$. Therefore there exists a prime divisor P, which divides U. So, $U=PK$ for some ideal number K. Next, P divides W since $W^n=UV=PKV$ and we can apply Euclid's Lemma. Therefore, there exists an ideal number M such that $W=PM$. So now we have $W^n=P^nM^n$ and $W^n=PKV$, which give us

$$KV=P^{n-1}M^n. \tag{4.35}$$

Again from Euclid's Lemma, either $P|V$ or $P|K$, but we know P does not divide V since $(U,V)=I$. Therefore $P|K$. Repeating this argument for each P of P^{n-1}, we conclude there exists an ideal number Z such that $K=P^{n-1}Z$. Combining this last result with (4.35), we see that

$$ZV=M^n.$$

Since Z divides U, we know $(Z,V)=I$, and, if we note that $U=P^nZ$, it is clear that Z is not an nth power of an ideal number. Finally, $N(Z)<N(U)$

since $N(P^n) = p^n > 1$ (Lemma 4.33). Therefore, by infinite descent, we reach a contradiction, and we conclude there exists an ideal number C such that $U = C^n$. □

We now define a notion of equivalence between certain divisors (ideal numbers). This notion will come in handy in developing the following sections, eventually leading up to the proof of Fermat's Last Theorem for regular primes.

Definition 4.36. Two divisors A and B are equivalent, denoted $A \sim B$, if it is true that a divisor of the form AC is principal when and only when BC is principal.

Remark 4.37. The following properties of divisors are easily verifiable.
1) If A and B are principal, then AB is principal.
2) If A and B are divisors such that A and AB are principal, then B is principal.
3) A divisor A is principal if and only if $A \sim I$ where I is the empty divisor (see Definition something)
4) $A \sim B$ if and only if there exists divisor C such that AC and BC are both principal.
5) The equivalence relation $\sim$ is reflexive, symmetric, and transitive.
6) $A \sim B$ implies $AC \sim BC$ for all divisors C.
7) For any divisor A, there exists a divisor B such that $AB \sim I$.
8) If $A \sim B$, then there exist principal divisors M, N such that $AM = BN$.

5. Class Number and Regular Primes

From this point on, all definitions, propositions, theorems, etc. are building up to the proof of Fermat's Last Theorem for regular primes.

We begin this section by stating the familiar result that the class number of the ring of integers of a number field (such as $\mathbb{Q}(\alpha)$) is finite. The theorem is stated in accordance with Kummer's terminology.

Theorem 5.1. *For all cases of cyclotomic integers (letting λ be any prime integer greater than 2), there exists a finite set of divisors $A_1, ..., A_k$ such that every divisor is equivalent to one of the A_i.*

Definition 5.2. For a given set of cyclotomic integers based on an odd prime λ, the class number is the number of elements in the finite set of divisors that is described in the theorem above.

Proposition 5.3. *For any ideal number C, if h is the class number for the cyclotomic integers corresponding to λ, then $C^h \sim I$ (i.e. C^h is principal).*

Proof. By Theorem 5.1, we know that all ideal numbers are equivalent to one of the ideal numbers of a representative set: $\{A_1, ..., A_h\}$. Therefore, $C, C^2, C^3, ...$ are each equivalent to one of these ideal numbers from the representative set. Since this set is finite, there exist $j, k \in \mathbb{Z}$ such that $C^j \sim A_i$ and $C^{j+k} \sim A_i$ for some $i \in \{1, 2, ...h\}$. Also, by Property 7 from Remark 4.37, we know there exists an ideal number B such that $C^j B$ is principal. Therefore $C^{j+k}B$ is also principal. Then by Property 2 of Remark 4.37, C^k is also principal. Now let d be the smallest positive integer such that C^d is principal. Then we have $C^d \sim I$, and it is easy to show $C, C^2, ..., C^{d-1}$ are all distinct (not equivalent to each other) and not principal. So now we know that $I, C, C^2, ..., C^{d-1}$ correspond to d different elements of $\{A_1, ..., A_h\}$. If $d = h$, the proof is complete. The only other case we need to consider is $d < h$.

If $d < h$ then there exists $i \in \{1, 2, ...h\}$ such that A_i is not equivalent to any of $I, C, C^2, ..., C^{d-1}$. Let $E = A_i$. Now consider the ideal numbers $E, EC, ..., EC^{d-1}$. It is easy to verify that these ideal numbers are not eqvuialent to each other and not equivalent to any of $I, C, C^2, ..., C^{d-1}$. If we continue this process, we have disjoint (with respect to our equivalent relation) sets of d elements each. Therefore $d|h$, and $C^d \sim I \Rightarrow C^h \sim I$. □

Corollary 5.4. *If $C^\lambda \sim I$ and λ does not divide the class number h, then $C \sim I$.*

Proof. Since λ is prime and λ does not divide h, we know there exist integers m, n such that $mh = n\lambda + 1$ (Bezout's identity). Therefore $I \sim C^h$ (Proposition 5.3) $\Rightarrow I \sim (C^h)^m = (C^\lambda)^n C$. Since $C^\lambda \sim I$, we conclude $C \sim I$. □

Now we can define regular primes. The first part of the definition is motivated by the fact that we need the properties of the above proposition and corollary. The second part, as we will see, is crucial to the proof of Fermat's Last Theorem for regular primes.

Definition 5.5. A regular prime λ is a prime integer that satisfies the following two conditions:
(A) λ does not divide the corresponding class number h.
(B) λ has the property that the corresponding cyclotomic integers satisfy the following: let e be a unit; then e is congruent modulo λ to a nonzero integer if and only if $e = (e')^\lambda$, where e' is also a unit.

Remark 5.6. One can prove that condition (A) implies condition (B), so condition (A) suffices to define a regular prime. See [1] pg. 243 for the proof.

6. Fermat's Last Theorem for Regular Primes

Finally with the machinery that we have developed, we can prove Fermat's Last Theorem for regular primes, which seem to make up a large portion of prime numbers (we say "seem" because it has only been conjectured but not proved that there are infinitely many regular primes). We first state some technical lemmas. For the proof of Lemma 6.3, refer to [1] pg. 173.

Lemma 6.1. *If $g(\alpha) \in \mathcal{O}_K$, then $g(\alpha)^\lambda$ is congruent to an integer modulo λ.*

Proof. From Corollary 3.7, we know $g(\alpha)^\lambda \equiv g(\alpha^\lambda) \bmod \lambda$. Now observe that the exponent of every α in $g(\alpha^\lambda)$ is a power of λ, and since we have the identity that $\alpha^\lambda = 1$, the proposition follows. □

Lemma 6.2. *Given integers x, y, z, n and $x^n + y^n = z^n$, either x, y, z are coprime or it is possible to cancel out common factors out of x, y, z so that we derive a new equation $(x')^n + (y')^n = (z')^n$ where x', y', z' are coprime.*

Lemma 6.3. *Let e be a unit in $\mathcal{O}_K$. Then there exists $r \in \mathbb{Z}$ such that $e/\overline{e} = \alpha^r$.*

The following is the statement of Fermat's Last Theorem, specific for regular primes.

Theorem 6.4. *If x, y, z, n are integers and n is a regular prime, then $x^n + y^n = z^n \Rightarrow xyz = 0$.*

Proof. To follow Kummer's convention, we set $\lambda = n$. Also, by Lemma 6.2 we can assume x, y, z are coprime.

Let α be a primitive root of unity so that $\alpha^\lambda = 1$ and $\alpha^i \neq 1$ for $i = 1, 2, ..., \lambda - 1$. Now we can factor $x^\lambda + y^\lambda$ in the following way:

$$z^\lambda = x^\lambda + y^\lambda = \prod_{i=0}^{\lambda-1} (x + \alpha^i y) \tag{6.5}$$

Now I claim that all terms $(x + \alpha^i y)$ in the above product are either coprime or have only $\alpha - 1$ as a common factor. To prove this claim, assume that there is some non-unit $h(\alpha) \in \mathcal{O}_K$ such that $h(\alpha)|(x+\alpha^i y)$ and $h(\alpha)|(x+\alpha^{i+j} y)$. However, note:

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

So $h(\alpha)|(x+\alpha^i y)$ and $h(\alpha)|(x+\alpha^{i+j} y) \Rightarrow h(\alpha)|\alpha^i(\alpha^j - 1)y$ and $h(\alpha)|(-1)(\alpha^j - 1)x$. Since x, y are coprime and α^i is a unit in $\mathcal{O}_K$ ($\because (\alpha^i)(\alpha^{\lambda-i}) = 1$) and only units divide units, we conclude $h(\alpha)|(\alpha^j - 1)$. Then using Lemma 4.6, we conclude $h(\alpha)$ is associate with $\alpha - 1$. Finally, note that from the equation $(x+\alpha^{i+j} y) - (x+\alpha^i y) = \alpha^i(\alpha^j - 1)y$, we see that

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

from which it follows that if $\alpha - 1$ divides one of the factors $(x + \alpha^i y)$, then it divides all of them.

Thus far, we have shown that either all of the factors $(x + \alpha^i y)$ are relatively prime, or they share exactly one common factor, $1 - \alpha$. If they all share the factor $1 - \alpha$, this implies $(1 - \alpha)^{\lambda-1}$ divides the product in (6.5) and hence divides z^λ. However, from Corollary 4.9, we know $(1 - \alpha)^{\lambda-1}$ is associate with λ, so $\lambda|z^\lambda$. And since λ is prime, $\lambda|z$.

Now we can divide Fermat's Last Theorem into two cases:

Case I: $x^\lambda + y^\lambda = z^\lambda$ where x, y, z are pairwise relatively prime and all prime to λ (and all the factors $(x + \alpha^i y)$ are coprime).

Case II: $x^\lambda + y^\lambda = z^\lambda$ where x, y, z are pairwise relatively prime and $\lambda|z$.

One thing to note for Case II is we may have $\lambda|x$ or $\lambda|y$ instead of $\lambda|z$. But in either case, we may simply assume $\lambda|z$ because if, without loss of generality, $\lambda|x$, then because λ is odd, $y^\lambda = -(-y)^\lambda$. Hence $x^\lambda + y^\lambda = z^\lambda \Rightarrow x^\lambda = (-y)^\lambda + z^\lambda$, and we can relabel the variables so that $(z')^\lambda = (x')^\lambda + (y')^\lambda$. Basically, we can assume that z is the variable divisible by λ.

If the statement of the theorem holds for these two cases, the theorem is proven. □

Lemma 6.6. *(Proof for Case I) The statement of Fermat's Last Theorem holds for regular prime exponents in Case I.*

Proof. As seen previously, we can factor the equation in question as in (6.5). By assumption, the factors $(x + \alpha^j y)$ are relatively prime, so by Theorem 4.33, the divisor of each factor is a λth power. For now, just consider the factor $x + \alpha y$. This divisor, A, of this factor is a λth power, so there is an ideal number T such

that $A = T^\lambda$. Then since λ is a regular prime, by Corollary 5.4, T is principal. Therefore there exists $t \in \mathcal{O}_K$ for which T is the divisor and such that

$$x + \alpha y = et^\lambda \tag{6.7}$$

where e is a cyclotomic unit. Applying the conjugation $\alpha \mapsto \alpha^{-1}$ (or complex conjugation; see Remark 1.2) to (6.7), we get $x + \alpha^{-1}y = \overline{e}\overline{t}^\lambda$. Now by Lemma 6.3, we know there exists $r \in \mathbb{Z}$ such that $\overline{e} = \alpha^{-r}e$. Also, by Lemma 6.1, because t^λ is a λth power, $t^\lambda \equiv c \bmod \lambda$ for some $c \in \mathbb{Z}$. Now observe that congruence modulo λ is preserved under complex conjugation; therefore, we also have $\overline{t}^\lambda \equiv \overline{c} \bmod \lambda$, but because integers are invariant under complex conjugation, we get $t^\lambda \equiv \overline{t}^\lambda \bmod \lambda$. Therefore, we have the following:

$$x + \alpha^{-1}y = \alpha^{-r}e\overline{t}^\lambda \equiv \alpha^{-r}et^\lambda = \alpha^{-r}(x + \alpha y) \bmod \lambda. \tag{6.8}$$

At this point, we make two claims about r. First, $r \not\equiv 0 \bmod \lambda$. Second, assuming the first observation, we can assume $0 < r < \lambda$ becuase $\alpha^\lambda = 1$. Now we will show that the first claim is true.

Assume $r \equiv 0 \bmod \lambda$. Then from (6.8), we get

$$x + \alpha^{-1}y \equiv x + \alpha y \bmod \lambda \Rightarrow \alpha y - \alpha^{-1}y \equiv 0 \bmod \lambda$$

$$\Rightarrow (\alpha^2 - 1)y \equiv 0 \bmod \lambda \Rightarrow (\alpha^2 - 1)y \text{ is divisible by } (\alpha - 1)^{\lambda-1}.$$

The last implication follows from Corollary 4.9. Also, from Lemma 4.6, we note that $\alpha^2 - 1$ is associate with $\alpha - 1$. Therefore, it must be the case that $\alpha - 1$ divides y. However, this is a contradiction to y and λ being coprime.

Continuing with the main proof, we now rearrange (6.8) as

$$\alpha^{r-1}(\alpha x + y) \equiv x + \alpha y \bmod \lambda \tag{6.9}$$

$$[1 + (\alpha - 1)]^{r-1}[x + y + x(\alpha - 1)] \equiv x + y + y(\alpha - 1) \bmod (\alpha - 1)^{\lambda-1}. \tag{6.10}$$

Now we make a brief claim that a congruence of the form

$$a_0 + a_1(\alpha - 1) + a_2(\alpha - 1)^2 + ... + a_{\lambda-2}(\alpha - 1)^{\lambda-2} \equiv 0 \bmod (\alpha - 1)^{\lambda-1} \tag{6.11}$$

implies $0 \equiv a_1 \equiv a_2 \equiv ... \equiv a_{\lambda-2} \bmod \lambda$. This is true because the fact that the LHS of (6.11) is divisible by $\alpha - 1$ first implies that $a_0 \equiv 0 \bmod \alpha - 1$. Therefore, there exists $g(\alpha) \in \mathcal{O}_K$ such that

$$g(\alpha)(\alpha - 1) = a_0 \Rightarrow g(\alpha)^{\lambda-1}(\alpha - 1)^{\lambda-1} = {a_0}^{\lambda-1}$$

$$\Rightarrow {a_0}^{\lambda-1} \equiv 0 \bmod (\alpha - 1)^{\lambda-1} \Rightarrow {a_0}^{\lambda-1} \equiv 0 \bmod \lambda.$$

And, since λ is prime, we conclude $a_0 \equiv 0 \bmod \lambda$. By considering divisibility by $(\alpha-1)^2, ..., (\alpha-1)^{\lambda-1}$, we reach similar conclusions that $a_1 \equiv 0, ..., a_{\lambda-1} \equiv 0 \bmod \lambda$.

Having proved this claim, we look back at (6.10) and observe that if $1 < r < \lambda-1$, then the highest order term on the LHS is $x(\alpha - 1)^r$ where $1 < r < \lambda - 1$. Then by the above claim, we would claim $x \equiv 0 \bmod \lambda$, which contradicts x, λ being coprime.

Now we consider the case where $r = \lambda - 1$. In this case, the second to last term of the LHS of (6.10) is, by the Binomial Theorem,

$$(x + y)(\alpha - 1)^{r-1} + (r - 1)(\alpha - 1)^{r-2}x(\alpha - 1) = [x + y + (\lambda - 2)x](\alpha - 1)^{\lambda-2}.$$

Therefore, we conclude $x + y + (\lambda - 2)x \equiv 0 \bmod \lambda \Rightarrow x \equiv y \bmod \lambda$. In the case that $r = 1$, the same result, $x \equiv y \bmod \lambda$, immediately follows from the claim.

Finally, we note that Case I is symmetric; therefore it is helpful to write the equation of the claim as

$$x^\lambda + y^\lambda + z^\lambda = 0. \tag{6.12}$$

Then, what has just been shown is that if $x \not\equiv 0, y \not\equiv 0, z \not\equiv 0 \bmod \lambda$, then $x \equiv y \equiv z \bmod \lambda$. And, from Fermat's Little Theorem, we know $x^\lambda \equiv x, y^\lambda \equiv y, z^\lambda \equiv z \bmod \lambda$. Therefore, (6.12) becomes $x^\lambda + y^\lambda + z^\lambda \equiv 3x \equiv 0 \bmod \lambda$, from which we conclude $3 \equiv 0 \bmod \lambda$, and therefore $\lambda = 3$. This proves Case I for regular prime $\lambda \neq 3$. And, the proof for Fermat's Last Theorem for $n = 3$ is common and has many known proofs, perhaps the most well-known of which is Euler's proof. Together with Euler's proof [4], this proves Case I for all regular primes. □

Notice that the proof for Case I explicitly required only Condition (A) for regular primes.

Lemma 6.13. *(Proof for Case II) The statement of Fermat's Last Theorem holds for regular prime exponents in Case II.*

Proof. In this second case, we are assuming that all the factors of the product from (6.5) are divisible by $\alpha - 1$ and the quotients are relatively prime. The product of the quotients is $z^\lambda(\alpha-1)^{-\lambda}$, which is clearly a λth power. Therefore, by Theorem 4.33, the divisor of each factor divided by $\alpha - 1$ is a λth power, and by Corollary 5.4 and the Fundamental Theorem for cyclotomic integers, we conclude that $(\alpha - 1)^{-1}(x + \alpha^j y) = e_j {t_j}^\lambda$, where e_j is a unit and $t_j \in \mathcal{O}_K$. Since the factors divided by $\alpha - 1$ are relatively prime, we also see that t_j are also relatively prime. Now we note that $\alpha - 1$ divides t_0 from the following line of reasoning: $(\alpha-1)|(x+y) \Rightarrow (\alpha-1)^{\lambda-1}|(x+y)^{\lambda-1} \Leftrightarrow \lambda|(x+y)^{\lambda-1} \Rightarrow \lambda|(x+y) \Rightarrow (\alpha-1)^{\lambda-1}|(x+y)$. Furthermore, since t_j are coprime, only t_0 is divisible by $\alpha - 1$. Let $t_0 = (\alpha-1)^k w$ where $k > 1$ and w is not divisible by $\alpha - 1$. We can now derive three equations to work with:

$$x + \alpha^{-1} y = (\alpha - 1) e_{-1} {t_{-1}}^\lambda \tag{6.14}$$

$$x + y = (\alpha - 1) e_0 (\alpha - 1)^{k\lambda} w^\lambda \tag{6.15}$$

$$x + \alpha y = (\alpha - 1) e_1 {t_1}^\lambda. \tag{6.16}$$

Using the above three equations to eliminate x and y we get

$$(\alpha - 1)y = (\alpha - 1)[e_1 {t_1}^\lambda - e_0(\alpha - 1)^{k\lambda} w^\lambda] \tag{6.17}$$

$$\alpha^{-1}(\alpha - 1)y = (\alpha - 1)[e_0(\alpha - 1)^{k\lambda} w^\lambda - e_{-1} {t_1}^\lambda]. \tag{6.18}$$

And finally from the above two equations, we get

$$0 = e_1 {t_1}^\lambda - e_0(\alpha - 1)^{k\lambda} w^\lambda - \alpha e_0 (\alpha - 1)^{k\lambda} w^\lambda + \alpha e_{-1} {t_{-1}}^\lambda \tag{6.19}$$

Now observe that since $\alpha^2 - 1$ and $\alpha - 1$ are associate (Lemma 4.6), $\alpha + 1 = \frac{\alpha^2-1}{\alpha-1}$ is a unit. Therefore, we can write (6.19) in the following way:

$$E_0(\alpha - 1)^{k\lambda} w^\lambda = {t_1}^\lambda + E_{-1} {t_{-1}}^\lambda \tag{6.20}$$

where E_0 and E_{-1} are units.

Now, using the fact that λ is associate with $(\alpha - 1)^{\lambda-1}$ (and hence divides $(\alpha - 1)^{k\lambda}$) and Lemma 6.1, (6.20) is reduced, modulo λ, to

$$0 \equiv C_1 + E_{-1} C_{-1} \bmod \lambda \tag{6.21}$$

where C_1 and C_{-1} are integers and are nonzero modulo λ (because otherwise $\alpha-1$ would divide t_1 and t_{-1}, which is a contradiction to them being relatively prime to t_0). Therefore $E_{-1} \equiv integer \bmod \lambda$, and by Conditon B, $E_{-1} \equiv e^\lambda$ for some unit e. So, from (6.20), we now have

$$E_0(\alpha-1)^{k\lambda}w^\lambda = {t_1}^\lambda + (et_{-1})^\lambda \tag{6.22}$$

Observe the similarities between (6.22) and $z^\lambda = x^\lambda + y^\lambda$ (in particular, the forms of the equations). These similarities motivate us to consider the following equation as our starting point:

$$x^\lambda + y^\lambda = e(\alpha-1)^{k\lambda}w^\lambda \tag{6.23}$$

where e is a unit, k is a positive integer, and $x, y, w, \alpha-1$ are pairwise relatively prime cyclotomic integers. One can check that the equation of Case II of Fermat's Last Theorem is merely a special case of (6.23).

Since the RHS of (6.23) is divisible by $\alpha-1$, at least one of the factors of the LHS is divisible by $\alpha-1$, and, in fact, by the same argument as before (see proof of Theorem 6.4), all the factors are divisible by $\alpha-1$ and the quotients are relatively prime.

Now we claim that exactly one of the factors is divisible by $(\alpha-1)^2$. We prove this claim by noting that for some integers a_0, a_1, b_0, b_1, we have, from Lemma 1.11

$$x \equiv a_0 + a_1(\alpha-1) \bmod (\alpha-1)^2 \tag{6.24}$$

$$y \equiv b_0 + b_1(\alpha-1) \bmod (\alpha-1)^2 \tag{6.25}$$

from which we get

$$x + \alpha^j y \equiv [a_0 + a_1(\alpha-1)] + [1+(\alpha-1)]^j[b_0b_1(\alpha-1)] \bmod (\alpha-1)^2 \Rightarrow \tag{6.26}$$

$$x + \alpha^j y \equiv a_0 + b_0 + [a_1 + b_1 + jb_0](\alpha-1) \bmod (\alpha-1)^2 \tag{6.27}$$

From (6.27), we see, first, that since $\alpha-1$ divides $x+\alpha^j y$, $(\alpha-1)$ must divide a_0+b_0, and from the same argument as before, we conclude, because a_0, b_0 are integers, that $a_0+b_0 \equiv 0 \bmod \lambda$. Secondly, we see, also from (6.27), that $(\alpha-1)^2$ divides $x+\alpha^j y \Leftrightarrow a_1+b_1+jb_0$ is divisible by $\alpha-1 \Leftrightarrow a_1+b_1+jb_0 \equiv 0 \bmod \lambda$. Now notice that provided $b_0 \not\equiv 0 \bmod \lambda$, the condition that $a_1+b_1+jb_0 \equiv 0 \bmod \lambda$ holds for one and only one value of j modulo λ. This then shows that one and only factor $x+\alpha^j y$ is divisible by $(\alpha-1)^2$, as was to be shown. To show that, indeed, $b_0 \not\equiv 0 \bmod \lambda$, simply note that if $b_0 \equiv 0 \bmod \lambda$, then from (6.25), we'd have to conclude that $(\alpha-1)|y$, which would contradict y and $\alpha-1$ being coprime.

In sum, by showing that one of the factors is divisible by $(\alpha-1)^2$, we have shown that k from (6.23) must be greater than 1; say $k = K+1$ where K is a positive integer. Now note that substituting $\alpha^j y$ in for y on the LHS of (6.23) does not change the form; therefore, we can assume that it is the factor $x+y$ that is divisible by $(\alpha-1)^2$. Then, the $k\lambda$ factors of $\alpha-1$ in $x^\lambda+y^\lambda$ are distributed such that one factor is in each term $x+\alpha^j y$ for $j = 1, 2, ..., \lambda-1$ and $k\lambda-(\lambda-1) = 1+K\lambda$ factors are in $x+y$. Therefore, we again have three equations (refer to steps leading up to equations 6.14, 6.15, 6.16):

$$x + \alpha^{-1}y = (\alpha-1)e_{-1}{t_{-1}}^\lambda \tag{6.28}$$

$$x + y = (\alpha-1)e_0(\alpha-1)^{K\lambda}w^\lambda \tag{6.29}$$

$$x + \alpha y = (\alpha-1)e_1{t_1}^\lambda \tag{6.30}$$

where e_{-1}, e_0, e_1 are units and t_1, t_{-1}, w are cyclotomic integers not divisible by $\alpha - 1$ and relatively prime. By the same reasoning as before, the above three equations lead to an equation of the form (see steps leading up to equation 6.22)

$$X^\lambda + Y^\lambda = E(\alpha - 1)^{K\lambda} W^\lambda \tag{6.31}$$

where $X, Y, W, \alpha - 1$ are relatively prime cyclotomic integers, E is a unit, and $K = k - 1$, and we are essentially back to (6.23). However repetition of this process leads to the equation where $k = 1$, which we have shown to be impossible. Therefore, by infinite descent, we reach a contradiction. □

7. Acknowledgments

I would like to thank my mentor Kevin Casto for his guidance, for providing valuable feedback, and for suggesting this research topic to me. I would also like to thank Peter May for organizing the REU, for providing me and many others with an opportunity to learn math and to expand our horizons, and finally for reading and providing feedback on my paper.

References

[1] Harold M. Edwards. Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory. Springer-Verlag. 1977.
[2] Larry Freeman. Fermat's Last Theorem. http://fermatslasttheorem.blogspot.com/
[3] Ila Varma. Kummer, Regular Primes, and Fermat's Last Theorem. https://web.math.princeton.edu/∼ivarma/Kummer.pdf
[4] Cameron Byerly. Applications of Number Theory to Fermat's Last Theorem. https://www.whitman.edu/mathematics/SeniorProjectArchive/2006/byerleco.pdf