FERMAT'S LAST THEOREM FOR REGULAR PRIMES: KUMMER'S APPROACH

by
HANDE KUL

Submitted to the Institute of Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master in Sciences
in
Mathematics

Bilgi University
2017

FERMAT'S LAST THEOREM FOR REGULAR PRIMES: KUMMER'S APPROACH

DÜZENLİ ASAL SAYILAR İÇİN FARMAT'IN SON TEOREMİ: KUMMER'İN YAKLAŞIMI

HANDE KUL

112805001

APPROVED BY:

THESIS SUPERVISOR: Asst. Prof. Dr. Pınar Uğurlu KOWALSKI .....

JURY MEMBER: Asst. Prof. Dr. Kemal Ilgar EROĞLU.....

JURY MEMBER: Asst. Prof. Dr. Sonat SÜER .....

JURY MEMBER (İstanbul University): Assoc. Prof. Dr. Şükrü YALÇINKAYA .....

DATE OF APPROVAL: 12/06/2017

TOTAL PAGES: 53

KEY WORDS (English)

1) Fermat's Last Theorem
2) Cyclotomic Integers
3) Dedekind Domains
4) Number Rings
5) Regular Prime

KEY WORDS (Turkish)

1) Fermat'ın Son Teoremi
2) Döngüsel Sayılar
3) Dedekind Bölgeleri
4) Sayı Halkaları
5) Düzenli Asallar

ACKNOWLEDGEMENTS

First and foremost, I am very pleased to present all my thanks to my supervisor Asst. Prof. Dr. Pınar Uğurlu Kowalski. She encouraged me more than everyone and throughout this study she was my great booster. Even in day time or night time she helped me so much and attended to every point of this thesis. I cannot pay for her tremendous efforts. And then I want to thank to Dear Prof. Dr. Piotr Kowalski. He was a very helpful pathfinder for me. Especially in case II, he aided me so much to understand the proof.

Lastly, I want to thank to whole of my family. Among all of them, my mother never gave up by caring all my agonies during this journey. Also, my father always felt all my troubles in spite of the distance.

ABSTRACT

FERMAT'S LAST THEOREM FOR REGULAR PRIMES: KUMMER'S APPROACH

In this thesis we present a partial proof of Fermat's Last Theorem. We work on the Fermat equation $x^p + y^p = z^p$ and prove that it has no integer solutions (except trivial ones) if p is a regular odd prime. We follow Ernst Eduard Kummer's (1810-1893) proof and his ideas.

Cylotomic integers is the main interest of this thesis. We study number rings, Dedekind domains and some factorization and divisibility properties of these special rings. Some important properties of the trace and norm maps of algebraic integers are proved. We also study ideal class groups. Fractional ideals are also introduced to see the ideal class groups from another point of view.

By following Kummer's approach, we divide the problem into two cases. In the first case we assume that p does not divide any one of the integers x, y, z, and in the second one we work under the assumption that p divides exactly one of the integers x, y, z.

ÖZET

DÜZENLİ ASAL SAYILAR İÇİN FERMAT'NIN SON TEOREMİ: KUMMER'İN YAKLAŞIMI

Bu tezde Fermat'nın Son Teoremi'nin kısmi bir kanıtı sunulmuştur. Düzenli tek asal p sayıları için Fermat denklemi olarak adlandırılan $x^p + y^p = z^p$ denkleminin bariz çözümler dışında tam sayı bir çözümü olmadığı kanıtlanmıştır. Bunu yaparken kullanılan kanıt ve fikirler Ernst Eduard Kummer'e (1810-1893) aittir.

Döngüsel tam sayılar üzerinde önemli ölçüde durulmuştur. Sayı halkaları, Dedekind bölgeleri ve bu özel halkaların bazı çarpanlara ayırma ve bölünebilme özellikleri çalışılmıştır. Cebirsel sayıların iz ve norm fonksiyonlarının özellikleri aktarılmıştır. İdeal sınıflarının grubu ve tek elemanla gerilen ideallerin sınıfları üzerinde önemli ölçüde durulmuştur. Ayrıca ideal sınıflarının grubu kesirli idealler yolu ile de açıklanmıştır.

Kummer'in yaklaşımı izlenerek problem iki durumda incelenmiştir; birinci durumda p'nin x, y, z tamsayılarından hiçbirini bölmediği varsayılmıştır. İkinci durumda ise p'nin x, y, z tamsayılarından tam olarak birini böldüğü kabul edilmiştir.

TABLE OF CONTENTS

LIST OF SYMBOLS/ABBREVIATIONS

ξ	p^{th} root of unity
$\mathbb{Q}(\xi)$	The number field generated by ξ
$\mathbb{Z}[\xi]$	The number ring generated by ξ
$\mathbb{A}$	The set of algebraic integers in $\mathbb{C}$
R	Commutative ring with 1
$\mathbf{R}$	Dedekind domain
K	Any number field
$\mathcal{O}_K$	Number ring corresponding to the number field K
N^K, N	Norm map
T^K, T	Trace map
$Q(\mathbf{R})$	Field of fractions of the given ring $\mathbf{R}$
I, J	Ideals of the given ring
$\langle a \rangle$	The principal ideal generated by the element a in the given ring
$\mathbb{Z}^+$	The set of positive integers
I^{-1}	The inverse ideal of the given ideal I
$\gcd(I, J)$	The greatest possible ideal dividing both of the ideals I and J
$\text{lcm}(I, J)$	The least possible ideal which is divisible by the ideals I and J
$\sim$	Equivalence relation of the ideal classes
$\overline{u}$	Complex conjugate of u
$\text{cl}(R)$	The ideal class group of R
$\mathbb{I}_{\text{cl}(\mathcal{O}_K)}$	The set of all principal ideals of $\mathcal{O}_K$, identity element of the ideal class group of $\mathcal{O}_K$
$\lvert G \rvert$	The cardinality of any set G

$\mathbb{Z}_p$	The field of p-adic integers (integers modulo p)
$f'(x)$	Derivative of $f(x)$
$I \triangleleft R$	I is an ideal of the ring R
$(a, b) = 1$	a and b are relatively prime, the greatest common divisor of a and b is 1
$G_f(\mathcal{O}_K)$	The group of fractional ideals of $\mathcal{O}_K$
$K/\mathbb{Q}$	K is a field extension over $\mathbb{Q}$
FLT	Fermat's Last Theorem
KLU	Kummer's Lemma on Units
LHS	Left hand side
RHS	Right hand side

1. INTRODUCTION

Fermat's Last Theorem was one of the challenging problems in mathematics until the last century. In 17^{th} century, Fermat made this famous conjecture in a margin of a book, which is *Diophantus' Aritmetica*, and wrote his famous phrase;

> *"Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet." (Pierre de Fermat, 1637)*
>
> *"It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain." (Pierre de Fermat, 1637)*

Fermat never gave a proof of his conjecture. Many mathematicians worked on Fermat's Last Theorem and early attempts to prove it had developed Algebraic Number Theory. But Algebraic Number Theory solely is not enough to prove the theorem. In 20^{th} century it was proved by Andrew Wiles (1995), and his proof is far more beyond Algebraic Number Theory. Wiles used methods from Algebraic Geometry in his proof. He found a connection between elliptic curves, FLT (Fermat's Last Theorem) and modular forms.

The most well-known mathematicians who worked on Fermat's Conjecture are; Gauss, Euler, Lame, Germain, Drichlet, Legendre, Liouville, Cauchy, Kummer and Wiles. Kummer introduced the notion of regular primes and proved Fermat's Theorem for regular primes. A prime p is *regular* if it does not divide the order of the ideal class group of its corresponding ring of cylotomic integers.

Theorem 1.1. *[Fermat's Last Theorem, 1637] For any integer $n > 2$, the equation*

$$x^n + y^n = z^n$$

has no non-trivial integer solutions, that is, if $x, y, z \in \mathbb{Z}$ satisfy this equation, then $xyz = 0$.

We will present a partial proof of Fermat's Last Theorem by following the steps below: In step II, we prove Fermat's Last Theorem for regular odd primes.

Step I: $n = 4k$.

Step II: $n = pk$ where p is an odd regular prime which is greater than or equal to 3 and $k \in \mathbb{Z}$.

Case 1: $p \not| xyz$, i.e., p divides none of x, y, z.

Sub-case 1: $p = 3$.

Sub-case 2: $p > 3$.

Case 2: p divides exactly one of x, y, z.

In Section 2, we will present a proof of Fermat's Last Theorem for $n = 4$. It is proved by Fermat himself, and it is the only case known to be proved by Fermat. The case $n = 3$ is proved by Euler following Fermat and both of these basic cases uses the method of infinite descent. In the preliminaries part, we are going to introduce the basic definitions and tools that are needed. These cover the definitions of a *number field*, a *number ring* and a *Dedekind domain*; some important properties of cyclotomic integers, the trace and norm map defined on the number fields, *ideal class groups*, divisibility properties of ideals and elements in Dedekind domains, *fractional ideals*, *norm of an ideal* and *regular primes*. Then in Section 4 we are going to prove *Kummer's Lemma on Units*. In Section 5, we are going to prove the *first case of Fermat's Last Theorem* namely, when p does not divide xyz. In Section 6, we are going to prove the *second case of Fermat's Last Theorem* namely, namely p divides xyz.

2. FERMAT'S LAST THEOREM FOR n=4k

Fermat himself, after stating the famous conjecture, gave a proof only for the case $n = 4$. The proof uses the method of *infinite descent* which was introduced by Fermat. After Fermat, Euler gave a proof for $n = 3$ using infinite descent which is a bit more difficult than the case $n = 4$.

In this section, we will prove Fermat's Last Theorem for $n = 4$ and then conclude that Fermat's Last Theorem is true for $n = 4k$ where $k \in \mathbb{N}$.

Definition 2.1. Let a and b be two elements of $\mathbf{R} - 0$. If 1 is the only common divisor of a and b, then a and b are called *relatively prime*. It is denoted by $(a, b) = 1$.

Remark 2.2. If $(a, b) = 1$, then there exist $x, y \in \mathbf{R}$ such that

$$ax + by = 1.$$

Lemma 2.3. *[pp.186, Lemma 11.1 in [1]] Any pairwise coprime integer solutions to $x^2 + y^2 = z^2$ are in the following form*

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

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

Proof. Without loss of generality, assume that x, y, z are all positive. Moreover, we can observe that not all of x, y, z can be odd. If we find a triple (x, y, z) satisfying the Fermat equation $x^2 + y^2 = z^2$ with x and y are odd then z must be even since we assumed that x, y, z are pairwise coprime. Say z is even and x, y are odd. In other words,

$$x = 2k + 1, \quad y = 2l + 1, \quad z = 2j \text{ for some } j, k, l \in \mathbb{Z}.$$

Then we have,

$$(2k + 1)^2 + (2l + 1)^2 = (2j)^2 \text{ and hence } 4k^2 + 4k + 1 + 4l^2 + 4l + 1 = 4j^2.$$

The last equation is impossible since the LHS is equivalent to 2 modulo 4 while the RHS is equivalent to 0 modulo 4. This means that z cannot be even, that is to say x or y is even.

Assume, without loss of generality that y is even. Then we have:

$$y^2 = z^2 - x^2 = (z - x)(z + x).$$

Since x, z are odd, $z - x$ and $z + x$ are even. Also $z - x$ and $z + x$ must be all positive since we assumed x, y, z are all positive. Therefore we can say that $y = 2a$, $z - x = 2b$ and $z + x = 2c$ for some positive integers a, b, c. Then we have

$$(2a)^2 = (2b)(2c) \implies a^2 = bc$$

If $(b, c) \neq 1$ then this means that there is a prime h other than 2 dividing both $z + x$ and $z - x$. Then h divides their sum $2z$ and difference $2x$. Since h is an odd prime it divides both z and x. But since x, y, z are relatively prime we must have $(b, c) = 1$. So we conclude that each prime factor of a must occur as a square factor of either b or c. Say $b = s^2$ and $c = r^2$ where $(r, s) = 1$. Thus,

$$2z = (z - x) + (z + x) = 2b + 2c \implies z = b + c = s^2 + r^2$$
$$2x = (z + x) - (z - x) = 2c - 2b \implies x = c - b = r^2 - s^2$$

We already know that x and z are odd, so exactly one of r or s must be odd. Also we had shown that r and s are relatively prime. Moreover combining the above results we can write y as follows:

$$y^2 = z^2 - x^2 = (s^2 + r^2)^2 - (r^2 - s^2)^2 = s^4 + 2s^2r^2 + r^4 - r^4 + 2r^2s^2 - s^4 = 4r^2s^2,$$

which gives $y = \pm 2rs$.
Hence we have the desired result for x, y, z. □

Theorem 2.4. *[pp. 187, Theorem 11.2 in[1]] There exist no non-zero integer solutions to the equation $x^4 + y^4 = z^2$.*

Proof. Without loss of generality we may assume that x, y, z are positive. Consider the set of positive integer solutions of the equation $x^4 + y^4 = z^2$. Choose a triple (x, y, z) among them in which z is minimal. Consequently x, y and z are relatively prime because if not we might simplify the common factor. Applying Lemma 2.3 to the equation $(x^2)^2 + (y^2)^2 = z^2$, we obtain that

$$x^2 = r^2 - s^2, \quad y^2 = 2rs \text{ and } z = r^2 + s^2,$$

for some r, s as in Lemma 2.3. By the first equation above we obtained another Pythagorean triple $x^2 + s^2 = r^2$. Since r and s are relatively prime so are x, r, s.

From our first choice of x as in Lemma 2.3, we know that x is odd. Then applying Lemma 2.3 again to the equation $x^2 + s^2 = r^2$, we obtain a and b relatively prime such that

$$x = a^2 - b^2, \quad s = 2ab \quad r = a^2 + b^2.$$

Then we see that

$$y^2 = 2rs = 4ab(a^2 + b^2) \tag{2.1}$$

Since a and b are relatively prime they must be pairwise coprime to $a^2 + b^2$ as well. So, a prime factorization of equation (2.1) shows that there are integers c, d, e such that

$$a = c^2, \ b = d^2 \text{ and } a^2 + b^2 = e^2.$$

After arranging the above equation we obtain that

$$c^4 + d^4 = e^2.$$

As a result we get $e \leq a^2 + b^2 = r < z$ which contradicts to the minimality of z. This shows us that there is no non-zero solution to the equation $x^4 + y^4 = z^2$. □

Corollary 2.5. *The equation*

$$x^4 + y^4 = z^4$$

has no non-trivial integer solutions.

Proof. Let (x, y, z) be a non-trivial solution to the equation. But then we obtain a nontrivial solution (x, y, z^2) to the equation $x^4 + y^4 = z^2$. A contradiction to the Theorem 2.4. □

Ultimately, if x_0, y_0, z_0 is a solution of $x^{4k} + y^{4k} = z^{4k}$ for some $k \in \mathbb{N}$, then x_0^k, y_0^k, z_0^k is a solution of $x^4 + y^4 = z^4$. But this contradicts to Corollary 2.5. As a result, Fermat equation has no nontrivial solution for all multiples of 4.

3. PRELIMINARIES

In this section, we will introduce the fundamental definitions and tools that will be useful for the rest of the thesis. These methods are mostly introduced by Kummer on the way of proving Fermat's Last Theorem which constitutes the basics of Algebraic Number Theory.

3.1 NUMBER FIELD, NUMBER RING AND DEDEKIND DOMAIN

Throughout this thesis, we let $\xi = e^{\frac{2\pi i}{p}}$ unless stated otherwise. Let R denote a commutative ring with 1, and K denote a number field that is finite extension of $\mathbb{Q}$. In this subsection, we will introduce required definitions. Also we will explain the algebraic structure of the set of cyclotomic integers, namely $\mathbb{Z}[\xi]$. The definitions in this section are taken from Marcus's book which is titled as *"Number Fields"*, [2].

Definition 3.1. Let K be a finite extension of $\mathbb{Q}$ and let $\alpha \in K$. Then the monic irreducible polynomial of α having coefficients from $\mathbb{Q}$ is called the *minimal polynomial* of α over $\mathbb{Q}$.

Definition 3.2. A complex number α is an *algebraic integer* if and only if it is a root of some monic polynomial with coefficients from $\mathbb{Z}$. We will denote the set of all algebraic integers in $\mathbb{C}$ by $\mathbb{A}$.

Definition 3.3. Let K be an extension of $\mathbb{Q}$. Then $K/\mathbb{Q}$ is called an *algebraic extension* if every element of K is algebraic over $\mathbb{Q}$. In other words, if every element of K is a root of some monic polynomial with coefficients from $\mathbb{Q}$.

Fact 3.4. *A field extension is algebraic if and only if it is a finite extension.*

Definition 3.5. A subfield K of $\mathbb{C}$ is called a *number field* if K is a finite extension of $\mathbb{Q}$.

By Primitive Element Theorem [pp. 595, Theorem 25 in[4]] the field K in Definition 3.5 has the form $\mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{C}$ which is algebraic over $\mathbb{Q}$. If α is a root of an irreducible polynomial over $\mathbb{Q}$ of degree n for some $n \in \mathbb{N}$, then

$$\mathbb{Q}(\alpha) = \left\{ a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \ : a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q} \right\}.$$

It can be easily seen that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $\mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$, and hence the above representation of $\mathbb{Q}(\alpha)$ is unique.

Example 3.6. The field $\mathbb{Q}(\xi)$ is a number field, since ξ is algebraic over $\mathbb{Q}$ with the minimal polynomial $x^{p-1} + x^{p-2} + \ldots + x + 1$. Then so, $\{1, \xi, \ldots, \xi^{p-2}\}$ is a basis for $\mathbb{Q}(\xi)$ over $\mathbb{Q}$.
More generally, $\mathbb{Q}(\omega)$ is a number field where $\omega = e^{\frac{2\pi i}{m}}$ such that $m \in \mathbb{Z}^+$. It is called the m^{th} cyclotomic field.

Fact 3.7. *[pp. 16, [2]] The set of algebraic integers in $\mathbb{C}$ form a ring. Furthermore the set of algebraic integers in a number field K form a ring.*

Definition 3.8. For any number field K, $K \cap \mathbb{A}$ is called the number ring corresponding to the *number field* K and denoted by $\mathcal{O}_K$. It is also called the ring of integers of K.

Fact 3.9. *[pp. 67, Theorem 3.5 in [1]] The ring of integers of $\mathbb{Q}(\xi)$ is $\mathbb{Z}[\xi]$.*

It is not always true that the ring of integers of an arbitrary number field $\mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$. For example, the ring of integers of $\mathbb{Q}(\sqrt{-3})$ is not $\mathbb{Z}[\sqrt{-3}]$. By Example 3.6, we know that the cyclotomic field $\mathbb{Q}(\xi)$ has dimension $p-1$. So, we may classify the elements of $\mathbb{Z}[\xi]$ as follows.

Remark 3.10. The corresponding ring of integers of $\mathbb{Q}$ has the form

$$\mathbb{Z}[\xi] = \left\{a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{p-2}\xi^{p-2}\right\}.$$

Definition 3.11. An integral domain $\mathbf{R}$ is called a *Dedekind domain* if the following conditions are satisfied:

1. Every ideal is finitely generated. (i.e. $\mathbf{R}$ is a Noetherian ring)
2. Every non-zero prime ideal is a maximal ideal.
3. $\mathbf{R}$ is integrally closed in its field of fractions

$$Q(\mathbf{R}) = \left\{\frac{\alpha}{\beta} \ : \ \alpha, \beta \in \mathbf{R} \ s.t. \ \beta \neq 0\right\},$$

i.e., if $\frac{\alpha}{\beta} \in Q(\mathbf{R})$ is a root of some monic polynomial over $\mathbf{R}$, then in fact $\frac{\alpha}{\beta} \in \mathbf{R}$.

Fact 3.12. *[pp. 56, Theorem 14 in [2]] Every number ring is a Dedekind domain.*

Lemma 3.13. *Let K be any number field. Then the field of fractions $Q(\mathcal{O}_K)$ of $\mathcal{O}_K$ is K.*

Proof. If $x \in Q(\mathcal{O}_K)$, then $x = \frac{\alpha}{\beta}$ for some $\alpha, \beta \in \mathcal{O}_K$ such that $\beta \neq 0$. Then $\alpha, \beta \in \mathcal{O}_K \subseteq K$. So, $\frac{\alpha}{\beta} \in K$. Thus $Q(\mathcal{O}_K) \subseteq K$.

Now take any element $x \in K$. Since K is a number field, $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. Then,

$$x = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$$

for some $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$. Let d be the product of denominators of $a_0, a_1, \ldots, a_{n-1}$. Then $dx \in \mathcal{O}_K = \mathbb{Z}[\alpha]$. So, $x \in Q(\mathcal{O}_K)$. As a result $K = Q(\mathcal{O}_K)$. □

3.2 CYCLOTOMIC INTEGERS

In this section we will introduce some basic and important properties of $\mathbb{Z}[\xi]$ where ξ denotes the primitive *pth* root of unity $e^{\frac{2\pi i}{p}}$. The elements of the ring $\mathbb{Z}[\xi]$ are called the *cyclotomic integers*. The term cyclotomic is inherited from the corresponding number field $\mathbb{Q}(\xi)$, namely the cyclotomic field.

Definition 3.14. Let R be any commutative ring with 1. An element y is called an associate of x in R if $x = uy$ for a unit $u \in R$. Equivalently two elements x and y are associates if $x|y$ and $y|x$.

Lemma 3.15. *The elements $1 - \xi^k$ and $1 - \xi^l$ are associates in $\mathbb{Z}[\xi]$ for any $k, l \in \mathbb{Z}$ which are not divisible by p.*

Proof. Without loss of generality we may assume that $1 \leq l < k \leq p - 1$. Since p is a prime, then l, k are units in the finite field $\mathbb{Z}_p$. So there are s, t in $\mathbb{Z}$ such that

$$k \equiv ls \text{ (mod p)} \qquad l \equiv kt \text{ (mod p)}.$$

Then we have that,

$$1 - \xi^k = \frac{1-\xi^k}{1-\xi^l}(1-\xi^l) = \frac{1-\xi^{ls}}{1-\xi^l}(1-\xi^l) = \underbrace{(1 + \xi^l + \xi^{2l} + \ldots + \xi^{l(s-1)})}_{\in \mathbb{Z}[\xi]}(1-\xi^l) \tag{3.1}$$

$$1 - \xi^l = \frac{1-\xi^l}{1-\xi^k}(1-\xi^k) = \frac{1-\xi^{kt}}{1-\xi^k}(1-\xi^k) = \underbrace{(1 + \xi^k + \xi^{2k} + \ldots + \xi^{k(t-1)})}_{\in \mathbb{Z}[\xi]}(1-\xi^k). \tag{3.2}$$

Equations (3.1) and (3.2) imply that $1 - \xi^k$ and $1 - \xi^l$ divide each other in $\mathbb{Z}[\xi]$, and hence they are associates in $\mathbb{Z}[\xi]$. □

Corollary 3.16. *For any $k = 1, \ldots, p-2$, the element $1 + \xi + \xi^2 + \ldots + \xi^k$ is a unit in $\mathbb{Z}[\xi]$.*

Proof. We know that $1+\xi+\xi^2+\ldots+\xi^k = \dfrac{1-\xi^{k+1}}{1-\xi}$. Since we know $1-\xi^{k+1}$ and $1-\xi$ are associates by Lemma 3.15, $1+\xi+\xi^2+\ldots+\xi^k$ is a unit. □

As a result of this corollary we obtain the following lemma.

Corollary 3.17. *For any $k, l \in \mathbb{Z}$ which are not divisible by p, we have*

$$\left\langle 1-\xi^k \right\rangle = \left\langle 1-\xi^l \right\rangle = \langle 1-\xi \rangle .$$

Proof. Since $1-\xi^k$, $1-\xi^l$ and $1-\xi$ are all associates, they differ only by a unit. This means that they generate the same ideals. □

Lemma 3.18. *We have $p = (1-\xi)(1-\xi^2)\ldots(1-\xi^{p-1})$ in $\mathbb{Z}[\xi]$.*

Proof. Since $1, \xi, \ldots, \xi^{p-1}$ are the all roots of the polynomial x^p-1, we can decompose this polynomial in $\mathbb{Z}[\xi]$ as follows,

$$x^p - 1 = (x-1)(x-\xi)(x-\xi^2)\ldots(x-\xi^{p-1}). \tag{3.3}$$

On the other hand we have $(x^p-1)/(x-1) = x^{p-1}+x^{p-2}+\ldots+x+1$. Then combining this with Equation (3.3) we obtain,

$$x^{p-1}+x^{p-2}+\ldots+x+1 = (x^p-1)/(x-1) = (x-\xi)(x-\xi^2)\ldots(x-\xi^{p-1}).$$

Then substituting $x=1$ in the above equation we get that,

$$p = (1-\xi)(1-\xi^2)\ldots(1-\xi^{p-1}).$$

□

3.3 THE TRACE AND NORM

Let K be a number field having degree n over $\mathbb{Q}$. We will define the trace and the norm maps on K, denoted by T^K and N^K respectively.

Since K is a number field of degree n, $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{C}$ satisfying an irreducible polynomial of degree n over $\mathbb{Q}$. Since α satisfies an irreducible polynomial of degree n over $\mathbb{Q}$, say $f(x)$, then K is a separable extension of $\mathbb{Q}$ by Appendix 1 of [2] [pp. 254-258, Appendix 1 and Appendix 2 in [2]]. So any embedding of K into $\mathbb{C}$ will naturally fix $\mathbb{Q}$ and send a root of $f(x)$ to another root of $f(x)$. Since there are exactly

n distinct roots, this gives us exactly n such distinct embeddings. Let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of K in $\mathbb{C}$ fixing $\mathbb{Q}$. For each $\alpha \in K$, define

$$T^K(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha).$$
$$N^K(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_n(\alpha).$$

Since $\sigma_1, \ldots, \sigma_n$ are field embeddings of K fixing $\mathbb{Q}$, then the definition above gives us that,

$$T^K(\alpha + \beta) = T^K(\alpha) + T^K(\beta)$$
$$N^K(\alpha\beta) = N^K(\alpha)N^K(\beta).$$

for all $\alpha, \beta \in K$. Moreover, for $r \in \mathbb{Q}$ and $\alpha \in K$ we have

$$T^K(r) = \sigma_1(r) + \ldots + \sigma_n(r) = nr.$$
$$N^K(r) = \sigma_1(r)\ldots\sigma_n(r) = r^n.$$
$$T^K(r\alpha) = \sigma_1(r\alpha) + \ldots + \sigma_n(r\alpha) = r\sigma_1(\alpha) + \ldots + r\sigma_n(\alpha) = rT^K(\alpha).$$
$$N^K(r\alpha) = \sigma_1(r\alpha)\ldots\sigma_n(r\alpha) = r\sigma_1(\alpha)\ldots r\sigma_n(\alpha) = r^nN^K(\alpha).$$

In the rest of the thesis we will need the fact that $T^K(\alpha)$ and $N^K(\alpha)$ are rational for each $\alpha \in K$. But to prove this we establish another formulation for the *trace* and *norm*. For this let $\alpha \in K$ have degree d over $\mathbb{Q}$ (i.e. the minimal polynomial of α over $\mathbb{Q}$ has degree d over $\mathbb{Q}$, or equivalently α has d conjugates over $\mathbb{Q}$, or equivalently $\mathbb{Q}(\alpha)$ has degree d over $\mathbb{Q}$.) Let $T^{\mathbb{Q}(\alpha)}(\alpha)$ and $N^{\mathbb{Q}(\alpha)}(\alpha)$ denote the sum and product of d conjugates of α, respectively. Then we have the following result.

Fact 3.19. *[pp. 21, Theorem 4 in [2]] Let K be a number field of degree n and let $\alpha \in K$ have degree d over $\mathbb{Q}$. Then we have,*

$$T^K(\alpha) = \frac{n}{d}T^{\mathbb{Q}(\alpha)}(\alpha).$$
$$N^K(\alpha) = (N^{\mathbb{Q}(\alpha)}(\alpha))^{\frac{n}{d}}.$$

(Note that $\frac{n}{d}$ is an integer, in fact $\frac{n}{d} = [K : \mathbb{Q}(\alpha)]$.)

Corollary 3.20. *For any $\alpha \in K$, $T^K(\alpha)$ and $N^K(\alpha)$ are rational.*

Proof. Let $f(x)$ be the minimal polynomial of α over $\mathbb{Q}$. Then so, the coefficients of $f(x)$ are from $\mathbb{Q}$. In other words, if

$$f(x) = \underbrace{a_0}_{N^{\mathbb{Q}(\alpha)}(\alpha)} + a_1x + \ldots + \underbrace{a_{d-1}}_{-T^{\mathbb{Q}(\alpha)}(\alpha)}x^{d-1} + x^d,$$

then $a_0, a_1, \ldots, a_{d-1} \in \mathbb{Q}$. Then a_0 is the product of all conjugates of α (roots of the minimal polynomial of α over $\mathbb{Q}$), which is equal to $N^{\mathbb{Q}(\alpha)}(\alpha)$. Also $-a_{d-1}$ is the sum

of all conjugates of α, which is equal to $T^{\mathbb{Q}(\alpha)}(\alpha)$. Thus, $N^{\mathbb{Q}(\alpha)}(\alpha)$ and $T^{\mathbb{Q}(\alpha)}(\alpha)$ are rational. It follows that,

$$T^K(\alpha) = \frac{n}{d}T^{\mathbb{Q}(\alpha)}(\alpha) \quad \text{and} \quad N^K(\alpha) = (N^{\mathbb{Q}(\alpha)}(\alpha))^{\frac{n}{d}}$$

are also rational since $\frac{n}{d}$ is integer. □

The following corollary shows that if $\alpha \in \mathbb{Z}[\xi]$ then the *trace* and *norm* maps send α to a rational integer (In other words, $T^K(\alpha), N^K(\alpha) \in \mathbb{Z}$).

Corollary 3.21. *If $\alpha \in K$ is an algebraic integer, then $T^K(\alpha)$ and $N^K(\alpha)$ are in $\mathbb{Z}$.*

Proof. If α is an algebraic integer, then its minimal polynomial over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$. Then $N^{\mathbb{Q}(\alpha)}(\alpha)$ and $T^{\mathbb{Q}(\alpha)}(\alpha)$ are in $\mathbb{Z}$ and so, $N^K(\alpha)$ and $T^K(\alpha)$ are in $\mathbb{Z}$. □

To simplify the notation we use N for the norm map on the field $\mathbb{Q}(\xi)$. The following well-known results are very important for Kummer's proof of FLT.

Lemma 3.22. *For any $1 \leq i \leq p-1$ we have*

$$N(1-\xi^i) = N(1-\xi) = (1-\xi)\dots(1-\xi^{p-1}) = p.$$

Proof. We know that all Galois conjugates of ξ are given by $\xi, \dots, \xi^{p-1}$ because they all satisfy the minimal polynomial

$$f(x) = 1 + x + \dots + x^{p-1}$$

of ξ over $\mathbb{Q}$. Then if σ_i is an embedding of $\mathbb{Q}(\xi)$ into $\mathbb{C}$ such that $\sigma_i(\xi) = \xi^i$ where $i \in 1, \dots, p-1$, then

$$\sigma_i(1-\xi) = 1 - \xi^i.$$

Thus $(1-\xi), \dots, (1-\xi^{p-1})$ are all Galois conjugates of $1-\xi$, i.e., they satisfy the minimal polynomial of $1-\xi$. So, they are in the splitting field of $1-\xi$. Hence we obtain that,

$$N(1-\xi) = (1-\xi)\dots(1-\xi^{p-1}) = p.$$

The last equality in the above follows from Lemma 3.18. Similarly for any $i \in \{1, \dots, p-1\}$ the Galois conjugates of $1-\xi^i$ are given by $1-\xi, \dots, 1-\xi^{p-1}$, and this gives us that

$$N(1-\xi^i) = (1-\xi)\dots(1-\xi^{p-1}) = N(1-\xi) = p.$$

So we are done. □

Lemma 3.23. *Let $u \in \mathcal{O}_K$. Then u is a unit in $\mathcal{O}_K$ if and only if $N(u) = \pm 1$.*

Proof. If u is a unit in $\mathcal{O}_K$, then there exists a $v \in \mathcal{O}_K$ such that $uv = 1$. Then taking norms on both sides, we get $N(uv) = N(u)N(v) = N(1) = 1$ in $\mathbb{Z}$. Since $N(u)$ and $N(v)$ are both integers by Corollary 3.21, this give us $N(u) = \pm 1$.
Now assume that $N(u) = \pm 1$. By definition, $N(u) = uc(u)$ where $c(u)$ denotes the product of all conjugates of u. Clearly, $c(u)$ is an algebraic number because every conjugate of u is a root of the minimal polynomial of u, and this means that every conjugate of u is an algebraic number. But it may not be the case that every conjugate of u is in K. However K is the field of fractions of its corresponding number ring $\mathcal{O}_K$, which gives us that

$$c(u) = \pm\frac{1}{u} \in K.$$

Hence

$$c(u) \in K \cap \mathbb{A} = \mathcal{O}_K.$$

Thus u is a unit in $\mathcal{O}_K$. □

As a corollary of the above lemmas we have an important result.

Corollary 3.24. *For any $1 \leq i \leq p-1$, the element $1 - \xi^i$ is irreducible in $\mathbb{Z}[\xi]$.*

Proof. Assume that $1 - \xi^i = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[\xi]$. Then taking norms of both sides and using Lemma 3.22 we obtain,

$$p = N(1 - \xi^i) = N(\alpha)N(\beta) \quad \text{in } \mathbb{Z}.$$

But then either $N(\alpha) = 1$ or $N(\beta) = 1$. Thus by Lemma 3.23, either α or β is unit. Then $1 - \xi$ is irreducible in $\mathbb{Z}[\xi]$. □

Corollary 3.25. *For any $1 \leq i \leq p-1$ we have $N(\xi) = N(\xi^i) = 1$.*

Proof. We know that ξ and ξ^i are conjugates for any $1 \leq i \leq p-1$. So they have the same norm (since they are roots of the same minimal polynomial). Also,

$$N(\xi) = N(\xi^i) = \xi\xi^2 \dots \xi^{p-1}.$$

So, it is easy to see that $N(\xi)$ is the constant coefficient of the minimal polynomial of ξ which is $1 + x + \ldots + x^{p-1}$. We have $N(\xi) = 1$. □

3.4 IDEAL CLASS GROUP

Kummer's idea to prove FLT was based on Unique Factorization Property of ideals in a ring. He discovered that not all rings are unique factorization domain. But, it is proved that every ideal in a Dedekind domain, and so in a number ring, can be written as a product of *prime ideals* in a unique way. Also, Kummer's discovery of *ideal classes* gave rise to many important tools, such as ideal class groups and *class numbers* which is defined as the cardinality of the ideal class group. For some special primes that we will see later, the ideal class group has important features and these features give us FLT for these special primes. In this subsection, we will define the notion of the class of an ideal and then show that these classes form an abelian group.

Let R be a number ring. Define a relation $\sim$ on the set of ideals of R as follows.
For ideals I and J of R

$$I \sim J \quad \text{if and only if} \quad \alpha I = \beta J \quad \text{for some} \quad \alpha, \beta \in R - \{0\}.$$

We can easily check that this is an equivalence relation:

- $I \sim I$ (we choose $\alpha = 1 = \beta$).
- $I \sim J$.
  $\Leftrightarrow$ there exists $\alpha, \beta \in R$ such that $\alpha I = \beta J$.
  $\Leftrightarrow \beta J = \alpha I$.
  $\Leftrightarrow J \sim I$.
- $I \sim J$ *and* $J \sim S$.
  $\Leftrightarrow$ there exists $\alpha, \beta, \sigma, \gamma \in R - \{0\}$ such that $\alpha I = \beta J$ *and* $\sigma J = \gamma S$.
  $\Rightarrow \sigma\alpha I = \sigma\beta J$ *and* $\underbrace{\beta\sigma}_{\sigma\beta} J = \beta\gamma S$.
  $\Rightarrow \sigma\alpha I = \beta\gamma S$.
  $\Leftrightarrow I \sim S$.

We denote by $[I]$ the class of I under $\sim$ (Ideal class corresponding to the ideal I).
Now, we can define the multiplication $\cdot$ on the set of ideal classes of R as follows,

$$[I] \cdot [J] := [IJ]$$

where $[I], [J]$ are two ideal classes. Note also that this operation is well-defined. The following lemma shows that the set of non-zero principal ideals of R form an ideal class under the above equivalence relation.

Lemma 3.26. *If I and J are two non-zero principal ideals in R, then they are equivalent with respect to the above equivalence relation $\sim$.*

Proof. Assume $I = \langle\alpha\rangle$ and $J = \langle\beta\rangle$ for some non-zero $\alpha, \beta \in R$. Then clearly, $\beta I = \alpha J$. Then, $I \sim J$. □

As a result of the lemma above, all principal ideals belongs to the same ideal class. Therefore we can define $\mathbb{I}_{\mathrm{cl}(\mathcal{O}_K)}$ as the set of all principal ideals of R. Then $\mathbb{I}_{\mathrm{cl}(\mathcal{O}_K)}$ will be the identity element of the ideal class group of R that we will define later. Because if $A = \langle a\rangle$ is any principal ideal in R, then for any ideal I we have,

$$[I] \cdot [A] = [I] \cdot [aR] = [IaR] = [I]$$

where $a \in R$.

Fact 3.27. *[pp. 57, Theorem 15 in [2]] Let I be an ideal in a Dedekind domain $\mathbf{R}$. Then there is an ideal J of $\mathbf{R}$ such that IJ is principal.*

Fact 3.27 is essential to show that ideal classes of a Dedekind domain form a group.

Fact 3.28. *[pp. 58, Corollary 1 in [2]] The ideal classes in a Dedekind domain form a group where the identity of the group is $\mathbb{I}_{\mathrm{cl}(\mathcal{O}_K)}$. Then so the ideal classes of a number ring form a group.*

For any number ring R, we denote the ideal class group by $\mathrm{cl}(R)$.

Fact 3.29. *[pp. 132, Corollary 2 in [2]] Ideal class group of a number ring is finite.*

So the ideal class group of any number ring has finite order. This will be an essential part of the proof of Fermat's Last Theorem. We will see later in Sections 5 and 6 how the following Remark 3.31 is useful in the proof of Fermat's Last Theorem. Actually it is a consequence of the following group theoretical fact.

Fact 3.30. *If a finite group has order m, then the m^{th} power of every element is equal to the identity.*

In ideal class groups, the above group theoretical fact takes the following form.

Remark 3.31. If the ideal class group of any number ring has order h, then the h^{th} power of any ideal is principal.

By the definition of the multiplication defined on the set of ideal classes of $\mathcal{O}_K$ we have,

$$\left[I^h\right] = [I]^h = \mathbb{I}_{\mathrm{cl}(\mathcal{O}_K)}.$$

This means that I^h is principal.

Remark 3.33 below follows from the follow ing very well-known group theoretical fact.

Fact 3.32. *[Lagrange Therorem; pp.89, Theorem 8 in [4]] Every element of a finite group has order dividing the order of the group, i.e., if an element g of any finite group G has order relatively prime to $|G|$, then g must be identity.*

Remark 3.33. Let $|\mathrm{cl}(\mathcal{O}_K)| = h$ and p be a number relatively prime to h. Also, let $I \triangleleft \mathcal{O}_K$ such that I^p is a principal ideal. Then I is a principal ideal.

3.5 IDEALS AND DIVISIBILITY IN DEDEKIND DOMAINS

Here we will see some divisibility properties of ideals in Dedekind domains. Unless stated otherwise $\mathbf{R}$ denotes a Dedekind domain in this subsection.

Definition 3.34. Let I and J be two ideals of $\mathbf{R}$ and b be an element of $\mathbf{R}$.

- $I|J$ if and only if $J = IS$ for some non-zero ideal S of $\mathbf{R}$.
- If $I|\langle b\rangle$, then we write $I|b$ and say I divides b.

Lemma 3.35. *Let I and J be ideals in a Dedekind domain $\mathbf{R}$. Then $I|J$ if and only if $J \subseteq I$.*

Proof. Assume that $I|J$. Then, there exists a non-zero ideal S of $\mathbf{R}$ such that $J = IS$. So, we have $J = IS \subseteq I$ naturally.
Conversely, if $J \subseteq I$ then fix an ideal S of $\mathbf{R}$ such that IS is principal by Fact 3.27. Say $IS = \langle\alpha\rangle$ for some $\alpha \in \mathbf{R}$.
Since $SJ \subseteq SI = \langle\alpha\rangle$, $C = \frac{1}{\alpha}SJ$ is an ideal in $\mathbf{R}$. Then

$$IC = I\frac{1}{\alpha}SJ = IS\frac{1}{\alpha}J = \langle\alpha\rangle\frac{1}{\alpha}J \subseteq \mathbf{R}J \subseteq J.$$

Also $J \subseteq IC$, because

$$J \subseteq \langle\alpha\rangle\frac{1}{\alpha}J = IS\frac{1}{\alpha}J = IC.$$

We get $IC = J$. □

Theorem 3.36. *[pp. 59, Corollary 2 in [2]] For any non-zero ideals I, J and S in $\mathbf{R}$, we have $IJ = IS$ if and only if $J = S$.*

Lemma 3.37. *Let I be a non-zero, nontrivial ideal in $\mathbf{R}$, then for any non-zero ideal J in $\mathbf{R}$, $IJ \subset J$ with strict inclusion.*

Proof. Clearly, $IJ \subseteq J$. We will show that $IJ \neq J$. If equality holds then by canceling J we obtain $I = \langle 1 \rangle = \mathbf{R}$. This gives us a contradiction as we have chosen I to be nontrivial. □

Lemma 3.38. *If I is a non-zero ideal in $\mathbf{R}$, then I divides some principal ideal. In other words, it contains a principal ideal as a subset.*

Proof. Pick some $a \in I$. Then $\langle a \rangle \subseteq I$. So, $I \mid \langle a \rangle$. Hence, $\langle a \rangle$ is a principal ideal multiple of I. □

Definition 3.39. Let I and J be two non-zero ideals in a Dedekind domain **R**. Then I and J are called *relatively prime ideals* if there exists no proper ideal of **R** dividing both I and J.

Fact 3.40. *[pp. 59, Theorem 16 in [2]] Every non-zero ideal in a Dedekind domain R is uniquely representable as a product of prime ideals.*

Since every number ring is a Dedekind domain, the following corollary follows subsequently.

Corollary 3.41. *[pp. 60, Corollary of Theorem 16 in [2]] The ideals in a number ring factor uniquely into prime ideals.*

Theorem 3.40 is called as the *Fundamental Theorem of Ideal Theory* [pp. 13, Section 5 in [3]].

Remark 3.42. [pp. 115, Lemma 5.8 in [1]] Take any two non-zero ideals I and J in **R**. Since we know that ideals in a Dedekind domain factors uniquely into prime ideals (by Theorem 3.40) we may write

$$I = \prod_i P_i^{m_i} \text{ and } J = \prod_i P_i^{n_i}$$

where P_i's are distinct non-zero prime ideals in **R** and $m_i, n_i \in \mathbb{Z}$. Then the *greatest common divisor* and *least common multiple* of I and J are respectively as following,

$$\gcd(I, J) = I + J = \prod_i P_i^{min(m_i, n_i)} \quad \text{and} \quad \operatorname{lcm}(I, J) = I \cap J = \prod_i P_i^{max(m_i, n_i)}.$$

Moreover, $(I + J)(I \cap J) = IJ$.

Remark 3.43. [pp. 768, Proposition 17 in [4]] If I and J are relatively prime ideals in **R**, then $I + J = \langle 1 \rangle = \mathbf{R}$.

Lemma 3.44. *Let I be a prime ideal of $\mathbf{R}$ and $\beta \in \mathbf{R}$. If $I \nmid \beta$, then I^k and β are relatively prime for any $k \geq 1$.*

Proof. Consider the ideal generated by β. Since $\mathbf{R}$ is a Dedekind domain it has a unique factorization into prime ideals, say

$$\langle\beta\rangle = P_1^{k_1} \dots P_m^{k_m}$$

where $P_1, \dots, P_m$ are prime ideals of $\mathbf{R}$ and $k_1, \dots, k_m \in \mathbb{Z}^+$. If I and $\langle\beta\rangle$ are not relatively prime ideals, then there are prime ideals appearing in the decompositions of both I and $\langle\beta\rangle$. But since I is a prime ideal itself, this means that I appears in the decomposition of $\langle\beta\rangle$. But this means that $I \,|\, \langle\beta\rangle$, then so by Definition 3.34 I divides β. Contradicting to our assumption.
Also, β and I^k are relatively prime for $k > 1$. Because if not there would be at least one prime ideal appearing in the factorizations of both $\langle\beta\rangle$ and I^k. But since I is a prime ideal and $\mathbf{R}$ has the property of unique factorization of ideals, the prime decomposition of I^k is obvious. Thus we conclude that I must appear in the factorization of $\langle\beta\rangle$. So, $I \,|\, \langle\beta\rangle$, i.e., $I|\beta$. Again contradicting to our assumption. □

Lemma 3.45. *Let $a, p \in \mathbf{R}$ such that $\langle p\rangle$ is a prime ideal of $\mathbf{R}$. Then $p \nmid a$ if and only if $\langle a\rangle$ and $\langle p\rangle$ are relatively prime.*

Proof. Assume $\langle a\rangle$ and $\langle p\rangle$ are not relatively prime. Since $\mathbf{R}$ is a Dedekind Domain there is a unique factorization of ideals into prime ideals and $\langle p\rangle$ is a prime ideal. So there must be an ideal I_0 of $\mathbf{R}$ such that,

$$\langle a\rangle = \langle p\rangle \, I_0.$$

Then we have,

$$\langle p\rangle \,|\, \langle a\rangle \implies \langle p\rangle \supset \langle a\rangle \quad \text{by Lemma 3.35.}$$

And this means that, p divides a.
Conversely, assume $p|a$. Then $a = pb$ for some $b \in \mathbf{R}$. We get,

$$\langle a\rangle = \langle bp\rangle = \langle p\rangle \, \langle b\rangle \implies \langle p\rangle \,|\, \langle a\rangle \,.$$

□

Lemma 3.46. *Let α and β be some elements in a commutative ring R. Then we have, $\alpha|\beta$ as elements if and only if $\langle\alpha\rangle \,|\, \langle\beta\rangle$ as ideals.*

Proof. Assume α divides β. Then $\beta = \alpha\gamma$ for some $\gamma \in R$. As R is a commutative ring with 1, by considering the ideals generated by β and $\alpha\gamma$, we have

$$\langle\beta\rangle = \langle\alpha\gamma\rangle = \langle\alpha\rangle \, \langle\gamma\rangle \,.$$

Hence, $\langle\alpha\rangle \mid \langle\beta\rangle$ as ideals.
For the converse, assume that $\langle\alpha\rangle \mid \langle\beta\rangle$ as ideals. Then $\langle\beta\rangle = \langle\alpha\rangle C$ for some ideal C of R. Since

$$\beta \in \langle\alpha\rangle C = \{\alpha c : c \in C\},$$

we have $\beta = \alpha c_1$ for some $c_1 \in C$. Hence, $\alpha|\beta$ as elements of R. □

As we see, Lemma 3.46 says that divisibility relations does not differ between elements and the principal ideals they generate. Kummer's proof of FLT typically takes elements of $\mathbf{Z}[\xi]$ and passes the corresponding ideals generated by these elements. So, Theorem 3.46 will be one of the cornerstone ideas when proving FLT for regular primes.

The following lemma summarizes the relation between the relatively prime elements of $\mathbf{R}$ and the relatively prime principal ideals of $\mathbf{R}$.

Lemma 3.47. *Let α and β be two elements of $\mathbf{R}$. Then α and β are relatively prime if and only if $\langle\alpha\rangle$ and $\langle\beta\rangle$ are relatively prime as ideals.*

Proof. Assume α and β are relatively prime. Let I be any ideal in $\mathbf{R}$ dividing both $\langle\alpha\rangle$ and $\langle\beta\rangle$. Then by Lemma 3.35,

$$\langle\alpha\rangle \subseteq I \quad \text{and} \quad \langle\beta\rangle \subseteq I.$$

Then $\alpha \in I$ and $\beta \in I$, but since they are relatively prime this means that there are $x, y \in \mathbf{R}$ such that

$$\alpha x + \beta y = 1.$$

This means that $1 \in I$ and so $I = \mathbf{R}$. So the only ideal dividing both $\langle\alpha\rangle$ and $\langle\beta\rangle$ is $\mathbf{R}$. Thus $\langle\alpha\rangle$ and $\langle\beta\rangle$ are relatively prime ideals.
Assume on the contrary that $\langle\alpha\rangle$ and $\langle\beta\rangle$ are relatively prime as ideals. Say there is an $a \in \mathbf{R}$ and $r_1, r_2 \in \mathbf{R}$ such that

$$\alpha = ar_1 \qquad \beta = ar_2.$$

Then by Theorem 3.46 $\langle a\rangle \mid \langle\alpha\rangle$ and $\langle a\rangle \mid \langle\beta\rangle$, contradicting to the assumption that $\langle\alpha\rangle$ and $\langle\beta\rangle$ are relatively prime as ideals. □

Since every number ring is a Dedekind domain all the results shown in this subsection are also true in $\mathcal{O}_K$.

3.6 FRACTIONAL IDEALS

In this section, we will describe the ideal class group from another point of view. Throughout this subsection, R denotes an integral domain and K denotes its field of fractions.

Definition 3.48. An R-submodule F of K is called a *fractional ideal* of R if

$$\alpha F \subseteq R$$

for some non-zero $\alpha \in R$.

Definition 3.49. Let I be a non-zero ideal of R. Define *the inverse ideal of* I as follows

$$I^{-1} := \{x \in K : xI \subseteq R\}.$$

Note that I^{-1} is an R-submodule of K.

Remark 3.50. For any ideal I of R, I^{-1} is a fractional ideal.

The reason for this is that if I is any non-zero ideal of R then for any $c \in I$, $c \neq 0$ we get,

$$cI^{-1} = \{cx : x \in K \text{ and } xI \subseteq R\} \subseteq Ix \subseteq R.$$

Remark 3.51.

- $II^{-1} \subset R$ for any ideal I of an integral domain R.
- $R \subset I^{-1}$ for any ideal I of an integral domain R.

Definition 3.52. If $F = xR$ for some $x \in K$, then F is called a *principal fractional ideal* of R.

Lemma 3.53. *If I is a non-zero principal ideal of R, then I^{-1} is also a principal ideal.*

Proof. Assume that $I = \alpha R$ for some non-zero $\alpha \in R$. Then,

$$\begin{aligned} I^{-1} = \{x \in K : xI \subseteq R\} &= \{x \in K : x\alpha R \subseteq R\} \\ &= \{x \in K : x\alpha \in R\} \\ &= \left\{x \in K : x \in \alpha^{-1}R\right\} \\ &= \left\{x \in K : x = \alpha^{-1}r \text{ for some } r \in R\right\} \\ &= \alpha^{-1}R \end{aligned}$$

As a result, since $\alpha^{-1} \in K$ where K is the field of fractions of R, then I^{-1} is a principal fractional ideal. □

Definition 3.54. An R-submodule F of K is called an *invertible fractional ideal* of R if there exists another fractional ideal $F' \subseteq K$ such that $FF' = R$. In this case F' is called as the fractional inverse of F.

Theorem 3.55. *[pp. 110, (vii) in the proof of Theorem 5.6 in [1]] Every non-zero fractional ideal of a Dedekind domain is invertible.*

Corollary 3.56. *[pp. 107, Theorem 5.5 in [1]] In a Dedekind domain* $\mathbf{R}$*, the set of non-zero fractional ideals forms an abelian group under multiplication of ideals. Also,* $\mathbf{R}$ *is the identity element of the group.*

Remember that $\mathcal{O}_K$ is the ring of integers of the number field K. By Lemma 3.13, we know that K is the field of fractions of $\mathcal{O}_K$. Since every number ring is a Dedekind domain this gives us the set of fractional ideals in $\mathcal{O}_K$ forms an group under multiplication [pp. 56, Theorem 14 in [2]]. This group is called as the *fractional ideal group of* $\mathcal{O}_K$, and denoted as $G_f(\mathcal{O}_K)$. Also this group is abelian, because $\mathcal{O}_K$ is a commutative ring with 1 and so, the multiplication of ideals is commutative in $\mathcal{O}_K$.

Let us denote the set of principal fractional ideals of $\mathcal{O}_K$ by $N_f(\mathcal{O}_K)$. For any two principal ideals $x\mathcal{O}_K$ and $y\mathcal{O}_K$, we have $(x\mathcal{O}_K)(y\mathcal{O}_K) = xy\mathcal{O}_K$ by commutativity of the ring. So, $N_f(\mathcal{O}_K)$ is closed under multiplication. Also, $(x\mathcal{O}_K)(x^{-1}\mathcal{O}_K) = \mathcal{O}_K$. so, we have $(x\mathcal{O}_K)^{-1} = x^{-1}\mathcal{O}_K$. Hence, $N_f(\mathcal{O}_K)$ is closed under taking inverse. Then we have the following proposition.

Remark 3.57. The set $N_f(\mathcal{O}_K)$ of principal fractional ideals is a normal subgroup of the fractional ideal group $G_f(\mathcal{O}_K)$.

Since $G_f(\mathcal{O}_K)$ is an abelian group, then $N_f(\mathcal{O}_K)$ is a normal subgroup of it. The quotient group $G_f(\mathcal{O}_K)/N_f(\mathcal{O}_K)$ is considered as the *fractional ideal class group* of $\mathcal{O}_K$. And it can be observed that this definition of the ideal class group is the same as the ideal class group $\mathrm{cl}(\mathcal{O}_K)$ that we defined in the previous section (Section 3.4).

3.7 NORM OF AN IDEAL

In this section we define the notion of the norm of an ideal. It is different from the norm of an element, but they have some connections for principal ideals.

Definition 3.58. Let I be a non-zero ideal of the ring of integers $\mathcal{O}_K$ of a number field K. We define *the norm of* I to be

$$N(I) = |\mathcal{O}_K/I| .$$

By definition it is seen that the norm of any ideal is positive. In fact, the norm of an ideal is the index of this ideal in its number ring (considered as additive subgroup).

Fact 3.59. *[pp. 115, [1]]If I is a non-zero ideal of $\mathcal{O}_K$, then $|\mathcal{O}_K/I|$ is finite.*

Fact 3.60. *[pp. 116, Corollary 5.10 in [1]] If $I = \langle a \rangle$ is a principal ideal then*

$$N(I) = |N(a)|.$$

Corollary 3.61. *If ξ is a primitive p^{th} root of unity, then we have $N(\langle 1 - \xi \rangle) = p$.*

Proof. By Lemma 3.22, Lemma 3.60 and Lemma 3.22 we have,

$$N(\langle 1 - \xi \rangle) = |N(1 - \xi)| = p.$$

□

Fact 3.62. *[pp. 116, Theorem 5.2 in [1]] If I and J are non-zero ideals of $\mathcal{O}_K$ then*

$$N(IJ) = N(I)N(J).$$

Theorem 3.63. *[pp. 118, Theorem 5.14 in [1]] Let I be a non-zero ideal of $\mathcal{O}_K$. Then,*

(a) If $N(I)$ is prime number, then I is a prime ideal.

(b) $N(I)$ is an element of I, or equivalently $I|N(I)$.

(c) If I is a prime ideal then it divides exactly one rational prime p, and we have

$$N(I) = p^m$$

where $m \leq n$, the degree of the number field K.

Proof. For this theorem we will only prove the first item which is essential for the rest of the thesis. The proof of the other items can be found in [1].

(a) Since I is an ideal of $\mathcal{O}_K$, then it has a factorization into prime ideals. Let's say,

$$I = P_1^{n_1} \dots P_k^{n_k}$$

for some prime ideals $P_1, \dots, P_k$ and $n_1, \dots, n_k \in \mathbb{N}$. Then by the Fact 3.62 we have

$$N(I) = N(P_1)^{n_1} \dots N(P_k)^{n_k}.$$

Since $N(I)$ is prime, then so it is also irreducible and $N(I) = N(P_i)$ for some i. Also, $N(P_j) = \pm 1$ for all $i \neq j$. By definition $N(P_j)$ cannot be negative, so $N(P_j) = 1$ for all $i \neq j$.. This means by the definition that

$$|\mathcal{O}_K/P_j| = 1 \implies P_j = \mathcal{O}_K \quad \text{for all } i \neq j.$$

Then $I = P_i$ is a prime ideal.

□

Lemma 3.64. *Let $I = \langle 1 - \xi \rangle$ be the ideal generated by $1 - \xi$ in $\mathbb{Z}[\xi]$ where $\xi = e^{2\pi i/p}$. Then the following statements hold.*

(a) $I^{p-1} = \langle p \rangle$.

(b) $N(I) = p$.

Proof. (a) By Lemma 3.18, $p = \prod_{i=1}^{p-1}(1 - \xi^i)$. Since we are working in a commutative ring with 1, the ideal generated by p in $\mathbb{Z}[\xi]$ is

$$\langle p \rangle = \prod_{i=1}^{p-1} \langle 1 - \xi^i \rangle .$$

By Lemma 3.17 we know $\langle 1 - \xi^k \rangle = \langle 1 - \xi \rangle$ so,

$$\langle p \rangle = \prod_{i=1}^{p-1} \langle 1 - \xi \rangle = \langle 1 - \xi \rangle^{p-1} = I^{p-1}.$$

(b) Follows by Corollary 3.61.

□

3.8 REGULAR PRIMES

The notion of regular prime was introduced by Kummer. In this subsection we will introduce the definition of *regular prime*

Definition 3.65 (Regular Prime, Kummer, 1850)**.** A prime p is *regular* if and only if

$$p \nmid |\mathrm{cl}(\mathbb{Z}[\xi])|$$

where $\xi = e^{2\pi i/p}$.

Remark 3.66. By a well-known result in group theory (Lagrange Theorem) it follows that, if p is a regular prime then $\mathrm{cl}(\mathbb{Z}[\xi])$ does not contain an element of order p in other words, for a *regular prime* p if the p^{th} power of an ideal I is a principal ideal, then I must be principal ideal by Remark 3.66.

Kummer made a conjecture that *"there are infinitely many regular primes"* however, this conjecture is still open. Ironically, *Jensen* (1915) proved that "there are infinitely many irregular primes" [pp. 82, [8]]. It is well-known that irregular primes less than 100 are only $37, 59$ and 67. All primes less than 100 except $37, 59$ and 67 are regular. For example, $2, 3, 5, 7, 11, 13, 17, 19, 23$ are regular primes.

4. KUMMER'S LEMMA ON UNITS

In this section we assume that p is an odd prime number and ξ is a primitive p^{th} root of unity as usual.

Notation 4.1. Let u be an element of $\mathbb{Z}[\xi]$. Then we can write it as $u = g(\xi)$ for some $g(t) \in \mathbb{Z}[t]$. Then $g(\xi^s) \in \mathbb{Z}[\xi]$ for all conjugates ξ^s of ξ where $s = 1, ..., p-1$. In this case we define $u_s := g(\xi^s)$ and it is a Galois conjugate of u.

In fact if σ_i is an embedding from $\mathbb{Q}(\xi)$ to $\mathbb{C}$ such that $\sigma_i(\xi) = \xi^i$ then,

$$\sigma_i(u) = \sigma_i(g(\xi)) = g(\sigma_i(\xi)) = g(\xi^i) = u_i.$$

Hence, $u_1, u_2, \ldots, u_{p-1}$ are all Galois conjugates of u.

Fact 4.2. *[pp. 189, Lemma 11.4 in [1]] The only roots of unity in $K = \mathbb{Q}(\xi)$ are $\pm\xi^m$ for integers m.*

Fact 4.3. *[pp. 191, Lemma 11.6 in [1]] If $p(t) \in \mathbb{Z}[t]$ is a monic polynomial, all of whose zeros in $\mathbb{C}$ have absolute value 1, then every zero of it is a root of unity.*

Lemma 4.4. *[Kummer's Lemma on Units; pp. 191, Lemma 11.7 in [1], pp.191] Every unit of $\mathbb{Z}[\xi]$ is of the form $r\xi^k$ where $r \in \mathbb{R}$ and $k \in \mathbb{Z}$.*

Proof. Let u be a unit in $\mathbb{Z}[\xi]$. Then $u = g(\xi)$ for some polynomial $g(t) \in \mathbb{Z}[t]$. For $s = 1, \ldots, p-1$ define,

$$u_s = g(\xi^s).$$

By the notion of conjugates, u_s is a Galois conjugate of u. Since u is a unit in $\mathbb{Z}[\xi]$, by Lemma 3.23 we have that

$$\pm N(u) = \pm u_1.u_2 \ldots .u_{p-1} = 1.$$

Hence each u_s is also a unit for $s = 1, \ldots, p-1$. Furthermore for any $s \in \{1, \ldots, p-1\}$ we have

$$u_{p-s} = g(\xi^{p-s}) = g(\xi^{-s}) = g(\overline{\xi^s}) = \overline{g(\xi^s)} = \overline{u_s}$$

where the bar represents complex conjugation, i.e., $\overline{\xi^s} = \xi^{-s}$.
Then we have $u_s u_{p-s} = |u_s|^2 > 0$.
It follows that $\pm 1 = N(u) = (u_1 u_{p-1})(u_2 u_{p-2}) \ldots (u_k u_{p-k}) > 0$ as all the pairs $u_i u_{p-i} > 0$.

Thus $N(u) > 0$, this means that $N(u) = 1$. We claim that each $\dfrac{u_s}{u_{p-s}}$ is a unit of absolute value 1. To see this observe that

$$\frac{u_s}{u_{p-s}}(u_{p-s})^2 \prod_{k \neq s} u_k u_{p-k} = N(u) = 1,$$

so $\dfrac{u_s}{u_{p-s}}$ is a unit for all $s = 1, \ldots, p-1$. Also since $|u_s| = |\overline{u_s}| = |u_{p-s}|$, we get $\left|\dfrac{u_s}{u_{p-s}}\right| = 1$.

Now consider the product

$$\prod_{s=1}^{p-1}(t - \frac{u_s}{u_{p-s}}) = f(t).$$

Claim 1. $f(t) \in \mathbb{Z}[t]$.

Proof of the Claim. First we will show that $\dfrac{u_1}{u_{p-1}}, \dfrac{u_2}{u_{p-2}}, \ldots, \dfrac{u_{p-1}}{u_1}$ are all conjugates of $\dfrac{u_1}{u_{p-1}}$ not necessarily distinct. Let σ_i be any embedding form $\mathbb{Q}(\xi)$ to $\mathbb{C}$ such that $\sigma_i(\xi) = \xi^i$. Then σ_i is a field isomorphism from $\mathbb{Q}(\xi)$ to $\mathbb{Q}(\xi^i)$ for any $i \in \{1, \ldots, p-1\}$. Then for any $i \in \{1, \ldots, p-1\}$ we have

$$\begin{aligned}\sigma_i\left(\frac{u_1}{u_{p-1}}\right) = \sigma_i\left(\frac{g(\xi)}{g(\xi^{p-1})}\right) = \frac{\sigma_i(g(\xi))}{\sigma_i(g(\xi^{p-1}))} = \frac{g(\sigma_i(\xi))}{g(\sigma_i(\xi^{p-1}))} = \frac{g(\xi^i)}{g(\xi^{i(p-1)})} \\ = \frac{g(\xi^i)}{g(\xi^{-i})} = \frac{g(\xi^i)}{g(\xi^{p-i})} = \frac{u_i}{u_{p-i}}. \qquad (4.1)\end{aligned}$$

But these conjugates do not have to be distinct, because we may have $g(\xi^i) = g(\xi^j)$ for some $i \neq j$. In fact, there are $(p-1)/m$ many conjugates of $\dfrac{u_1}{u_{p-1}}$ where m is the degree of the minimal polynomial of $\dfrac{u_1}{u_{p-1}}$. Now we will observe that, if $p(t)$ is the minimal polynomial of $\dfrac{u_1}{u_{p-1}}$ over $\mathbb{Z}$, then $p(t)$ divides $f(t)$, in fact $f(t) = (p(t))^k$ for some $k \in \mathbb{Z}$. Say $f(t) = (p(t))^k h(t)$ for some $h(t)$ relatively prime to $p(t)$. If $h(t)$ is not constant polynomial, then some $\dfrac{u_i}{u_{p-i}}$ is a root of $h(t)$. But then,

$$h\left(\frac{u_i}{u_{p-i}}\right) = h\left(\frac{g(\xi_i)}{g(\xi_{p-i})}\right) = h\left(g\left(\frac{\xi_i}{\xi_{p-i}}\right)\right) = 0.$$

Let $k(t) = h(g(t))$. Then $\dfrac{\xi^i}{\xi^{p-i}}$ is a root of $k(t)$. Let $p_0(t)$ be the minimal polynomial of $\dfrac{\xi}{\xi^{p-1}}$ over $\mathbb{Z}$ (Note that $\dfrac{\xi}{\xi^{p-1}}$ is algebraic over $\mathbb{Z}$, because it is a unit in $\mathbb{Z}[\xi]$). Then,

we have $p_0(t)|k(t)$. So, $\dfrac{\xi}{\xi^{p-1}}$ is also a root of $k(t)$. Thus

$$k\left(\frac{\xi}{\xi^{p-1}}\right) = h\left(g\left(\frac{\xi}{\xi^{p-1}}\right)\right) = h\left(\frac{u_1}{u_{p-1}}\right) = 0.$$

Since $p(t)$ is the minimal polynomial of $\dfrac{u_1}{u_{p-1}}$, then $p(t)|h(t)$. This contradicts to the fact that $p(t)$ and $h(t)$ are relatively prime. So, $h(t)$ must be a constant polynomial. Thus we know $p(t) \in \mathbb{Z}[t]$, this implies that $f(t) \in \mathbb{Z}[t]$. □

Hence by Lemma 4.3, zeros of $f(t)$ are roots of unity. Since any root of unity is of the form $\pm\xi^m$ by Lemma 4.2, we get

$$u/u_{p-1} = \pm\xi^m = \pm\xi^m.\xi^p = \pm\xi^{m+p}.$$

Since p is odd either m or $p+m$ is even. Then we may assume

$$u/u_{p-1} = \pm\xi^{2n} \tag{4.2}$$

for some $0 < n \in \mathbb{Z}$. In fact it can be shown that $u/u_{p-1} = +\xi^{2n}$. To see this remember that $I = \langle 1-\xi \rangle$. Then,

$$\xi^{-n}u = \xi^{-n}g(\xi) = \xi^{-n}(g_0 + g_1\xi + \ldots + g_r\xi^r) = g_0\xi^{-n} + g_1\xi^{1-n} + \ldots + g_r\xi^{r-n} \tag{4.3}$$

$$\equiv v \pmod{(1-\xi)} \tag{4.4}$$

for some $v \in \mathbb{Z}$. The last equality (4.4) follows by (b) of Lemma 3.64 (Since $|\mathbb{Z}[\xi]/I| = p$, every element of $\mathbb{Z}[\xi]$ is congruent to one of $0, 1, \ldots, p-1$ modulo I). Thus,

$$\xi^{-n}u - v \in I \quad \text{for some } v \in \mathbb{Z}. \tag{4.5}$$

This means that

$$\xi^{-n}u - v = (1-\xi)w$$

for some $w \in \mathbb{Z}[\xi]$. Then by taking complex conjugation

$$\overline{\xi^{-n}u - v} = \overline{(1-\xi)w}$$

we have that

$$\xi^n u_{p-1} \equiv v \pmod{(1-\xi^{p-1})}. \tag{4.6}$$

This comes from the fact that $1-\xi$ and $1-\xi^{p-1}$ are associates by Lemma 3.15. So,

we have $I = \langle 1 - \xi \rangle = \langle 1 - \xi^{p-1} \rangle$. So, by Equations (4.5) and (4.6) we have that

$$\xi^{-n}.u - \xi^n u_{p-1} \in I \tag{4.7}$$

$\implies u/u_{p-1} \equiv \xi^{2n} \pmod{(1-\xi)}$.
If we had negative sign in Equation (4.2), i.e., if it were $-u/u_{p-1} = \xi^{2n}$, then combining with the last equality we get

$$-\xi^{2n} = u/u_{p-1} \equiv \xi^{2n} \pmod{(1-\xi)} \quad \implies \quad 2\xi^{2n} \equiv 0 \pmod{(1-\xi)}.$$

So, we would have that

$$(1-\xi) | 2\xi^{2n}.$$

Then this would imply that $N(1-\xi) | N(2\xi^{2n})$. Then, $p | 2^{p-1}$ because we have $N(1-\xi) = p$ by Lemma 3.22 and $N(2\xi^{2n}) = N(2)N(\xi^{2n}) = 2^{p-1}$ by Corollary 3.25 (Note that $\pm u/u_{p-1} = \xi^{2n}$ is a unit in $\mathbb{Z}[\xi]$. So, its norm is 1). But $p | 2^{p-1}$ gives us a contradiction as p is an odd prime.

Therefore, we must have $u/u_{p-1} = \xi^{2n}$. So, we have that $\xi^{-n}u \equiv \xi^n u_{p-1} \pmod{(1-\xi)}$. It can easily be seen that they are complex conjugates, as $\overline{\xi^{-n}u} = \xi^n u_{p-1}$. So, $\xi^n u_{p-1} \in \mathbb{R}$. Now we are done with $u = \xi^n(\underbrace{\xi^n u_{p-1}}_{\in \mathbb{R}})$. □

Corollary 4.5. *If u is a unit of $\mathbb{Z}[\xi]$ and if $\overline{u}$ is its complex conjugate then $u/\overline{u} = \xi^k$ for some $k \in \mathbb{Z}$.*

5. FERMAT'S LAST THEOREM: CASE 1

It was Germain's idea to divide Fermat's Last Theorem into two cases such as p does not divide xyz and $p|xyz$. Although she gave a wrong proof, her idea and Lame's clever factorization helped Kummer to prove Fermat's Theorem for regular primes. In this section we are assuming that p is an odd prime which does not divide any of x, y, z in the equation

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

5.1 FLT FOR p=3

Now we will prove Fermat's Last Theorem for $p = 3$ under the assumption that none of x, y, z is divisible by 3. Actually the whole proof of case $p = 3$ was given by Euler by using the method of infinite descent but we will not present it here.

Theorem 5.1. *The equation*

$$x^3 + y^3 = z^3 \tag{5.1}$$

has no non-trivial solution in $\mathbb{Z}$ *where* x, y, z *are not divisible by* 3.

Proof. Let $x, y, z \in \mathbb{Z}$ be a solution of Equation (5.1) such that $3 \nmid x, y, z$. Then if we consider x, y, z in modulo 9, each of them are equivalent to $1, 2, 4, 5, 7, 8$ modulo 9. In other words,

$$x^3, y^3, z^3 \equiv \pm 1 \pmod 9.$$

Then we have only 3 possibilities for the sum of x^3 and y^3,

$$x^3 + y^3 \equiv 2, -2, 0 \pmod 9.$$

But z^3 is either 1 or -1 modulo 9. So we cannot have $x^3 + y^3 \equiv z^3 \pmod 9$. So there is no solution for Equation (5.1) in which x, y, z are not divisible by 3. □

5.2 FERMAT'S LAST THEOREM FOR $p > 3$

Let ξ denote a primitive p^{th} root of unity as before.

Lemma 5.2. *If* $\alpha \in \mathbb{Z}[\xi]$*, then there is an element* $m \in \mathbb{Z}$ *such that*

$$\alpha^p \equiv m \pmod p.$$

Proof. Take any $\alpha \in \mathbb{Z}[\xi]$, then by Corollary 3.10

$$\alpha = a_0 + a_1\xi + \ldots + a_{p-2}\xi^{p-2} \quad \text{where } a_i \in \mathbb{Z} \text{ for all } i = 0, 1, \ldots, p-2.$$

Then by the binomial theorem modulo p it can be shown that,

$$\left(a_0 + a_1\xi + \ldots + a_{p-2}\xi^{p-2}\right)^p \equiv a_0^p + a_1^p + \ldots + a_{p-2}^p \pmod{p}.$$

Then, since $a_i \in \mathbb{Z}$ for all $i = 0, 1, \ldots, p-2$ we have $a_0^p + a_1^p + \ldots + a_{p-2}^p \in \mathbb{Z}$. □

Lemma 5.3. *If p divides an element γ of $\mathbb{Z}[\xi]$, then p divides all the coefficients of γ in $\mathbb{Z}$.*

Proof. Say $\gamma = g_0 + g_1\xi + \ldots + g_{p-2}\xi^{p-2}$ where $g_i \in \mathbb{Z}$ for all $i = 0, 1, \ldots, p-2$. Since p divides γ in $\mathbb{Z}[\xi]$, then $\gamma = p\beta$ for some $\beta \in \mathbb{Z}[\xi]$. Then by Corollary 3.10,

$$\beta = b_0 + b_1\xi + \ldots + b_{p-2}\xi^{p-2}$$

for some $b_0, b_1, \ldots, b_{p-2} \in \mathbb{Z}$. Hence,

$$\begin{aligned} g_0 + g_1\xi + \ldots + g_{p-2}\xi^{p-2} = \gamma = p\beta &= p(b_0 + b_1\xi + \ldots + b_{p-2}\xi^{p-2}) \\ &= pb_0 + pb_1\xi + \ldots + pb_{p-2}\xi^{p-2} \end{aligned}$$

By the uniqueness of the representation of γ, we have $g_i = pb_i$ for all $i = 0, 1, \ldots, p-2$. Thus $p | g_i$ for all $i = 0, 1, \ldots, p-2$. □

So, we can prove the *first case of Fermat's Last Theorem* for regular primes in light of the above lemmas and *Kummer's Lemma on Units*.

Theorem 5.4. *If p is an odd regular prime then the equation*

$$x^p + y^p = z^p \tag{5.2}$$

has no integer solutions x, y, z where

$$p \nmid x, \ p \nmid y, \ p \nmid z.$$

Proof. Without loss of generality we may take x, y, z relatively prime.
Factorize Equation (5.2) in $\mathbb{Z}[\xi]$ as follows

$$(x + y)(x + y\xi)\ldots\left(x + y\xi^{p-1}\right) = z^p. \tag{5.3}$$

By passing to ideals, we get

$$\langle x+y\rangle \langle x+y\xi\rangle \dots \left\langle x+y\xi^{p-1}\right\rangle = \langle z\rangle^p . \tag{5.4}$$

Claim 1. The ideals on the left side of Equation (5.4) are pairwise coprime.

Proof of the Claim. Say $I = \langle x+y\xi^i\rangle$ and $J = \langle x+y\xi^j\rangle$ for $i \neq j$. Let P be a prime ideal of $\mathbf{Z}[\xi]$ such that $P|I$ and $P|J$. This means that $I \subset P$ and $J \subset P$. Then without loss of generality assuming $i < j$ we get,

$$(x+y\xi^i) - (x+y\xi^j) \in P.$$

So,

$$y\xi^i(1-\xi^{j-i}) \in P. \tag{5.5}$$

We will see that we must have $(1-\xi^{j-i}) \in P$.

Multiplying Equation (5.5) by ξ^{p-i}, we get $y(1-\xi^{j-i}) \in P$. Then since P is a prime ideal either $y \in P$ or $(1-\xi^{j-i}) \in P$.
Assume that $(1-\xi^{j-i}) \notin P$, this means that y must be an element of the ideal P. By our assumption $I = \langle x+y\xi^i\rangle \subset P$, i.e., $x+y\xi^i \in P$. Since P is an ideal of $\mathbb{Z}[\xi]$, by Equation (5.3) it follows that $z^p \in P$. Then since P is a prime ideal $z \in P$. But then we have,

$$1 = \gcd(y,z) \in P.$$

This gives us a contradiction as P is a prime ideal. Hence we have $(1-\xi^{j-i}) \in P$.

As we know $1-\xi$ and $1-\xi^{j-i}$ are associates in $\mathbb{Z}[\xi]$, so we have

$$\left\langle 1-\xi^{j-i}\right\rangle = \langle 1-\xi\rangle \qquad \text{in } \mathbb{Z}[\xi].$$

So

$$\begin{aligned}\langle 1-\xi\rangle \subset P &\Rightarrow P|\langle 1-\xi\rangle \\ &\Rightarrow \langle 1-\xi\rangle = P.Q \quad \text{for some ideal } Q \text{ of } \mathbb{Z}[\xi]\end{aligned}$$

We know that $N(\langle 1-\xi\rangle) = p$ and by properties of the Norm of ideals

$$p = N(\langle 1-\xi\rangle) = N(P)N(Q)$$

Then as p is prime, $N(P)$ is either p or 1. Since $P \neq \mathbb{Z}[\xi]$, $N(P) = |\mathbb{Z}[\xi]/P| \neq 1$. So

we get $N(P) = p$ and $N(Q) = 1$, that is $Q = \mathbb{Z}[\xi]$. Hence $\langle 1 - \xi \rangle = P$.
Since $P|I$, by Equation (5.4) we get

$$P| \langle z \rangle^p$$

and moreover $P| \langle z \rangle$ as P prime. Therefore, $\langle z \rangle = PQ$ for some ideal Q of $\mathbb{Z}[\xi]$. This means that

$$\underbrace{N(P)}_{p} | N(\langle z \rangle) = |N(z)| = \left| z^{p-1} \right| .$$

So, we obtain $p|z$ which gives us a contradiction as $p \not| z$.
By assuming $I = \langle x + y\xi^i \rangle$ and $J = \langle x + y\xi^j \rangle$ have a common divisor, we obtained a contradiction. This proves Claim 1. □

By Corollary 3.41, prime factorization of ideals is unique in $\mathbb{Z}[\xi]$. The RHS of Equation (5.4) is a p^{th} power and the ideals on the LHS are pairwise relatively prime. So, we obtain that there are ideals I_i of $\mathcal{O}_K = \mathbb{Z}[\xi]$ such that $I_i \neq I_j$ when $i \neq j$ and

$$\left\langle x + y\xi^i \right\rangle = I_i^p \quad i = 0, 1, 2, \ldots, p-1.$$

Thus, I_i^p is a principal ideal. This means that

$$[I_i^p] = [I_i]^p = \mathbb{I}_{\mathrm{cl}(\mathcal{O}_K)}$$

where $\mathbb{I}_{\mathrm{cl}(\mathcal{O}_K)}$ denotes the class of principal ideals, which is the identity of the ideal class group of $\mathbb{Z}[\xi]$. So, the order of $[I_i]$ divides p in the ideal class group of $\mathbb{Z}[\xi]$. Therefore the order of $[I_i]$ is either 1 or p. But $p \not| |\mathrm{cl}(\mathbb{Z}[\xi])|$ as p is a regular prime. This means that $\mathrm{cl}(\mathbb{Z}[\xi])$ cannot have an element of order p. Hence $[I_i]$ must have order 1, i.e., I_i is a principal ideal for each $1 \leq i \leq p-1$.

In particular I_1 is principal, i.e., for some $\alpha \in \mathbb{Z}[\xi]$,

$$\langle x + y\xi \rangle = \langle \alpha \rangle^p = \langle \alpha^p \rangle .$$

So we get,

$$x + y\xi = u\alpha^p$$

for some unit $u \in \mathbb{Z}[\xi]$. Then by Lemma 5.2,

$$x + y\xi \equiv u.m \pmod{p}$$

for some $m \in \mathbb{Z}$. By taking complex conjugation we get

$$x + y\xi^{-1} \equiv x + y\overline{\xi} \equiv \overline{x + y\xi} \equiv \overline{um} \equiv \overline{u}.m \pmod{p}.$$

By the corollary of *Kummer's Lemma on Units* (KLU in short), $\frac{u}{\overline{u}} = \xi^k$ for some $k \in \mathbb{Z}$.
So we have, $x + y\xi \equiv um \overset{KLU}{=} \overline{u}\xi^k m = \overline{u}m\xi^k \equiv (x + \xi^{-1}y)\xi^k \pmod{p}$.
This means, $x + y\xi \equiv x\xi^k + y\xi^{k-1} \pmod{p}$.
In other words,

$$x + y\xi - x\xi^k - y\xi^{k-1} \equiv 0 \pmod{p}. \tag{5.6}$$

Now we will show that this k must be equal to 1.

Claim 2. $k \equiv 1 \pmod{p}$.

Proof of the Claim. Without loss of generality we may assume $0 \leq k \leq p-1$. Now we will show that $k = 1$ by by eliminating the other cases by means of Equation (5.6) and Lemma 5.3.
Let $\gamma := x + y\xi - x\xi^k - y\xi^{k-1}$. Note that since $p|\gamma$ (by Equation (5.6)) p divides all the coefficients of γ in the unique representation of it in the basis $\{1, \xi, ..., \xi^{p-2}\}$.
Case 1: If $k = 0$.
In this case, we have

$$\begin{aligned} p|x + y\xi - x.\underbrace{\xi^0}_{1} - y\xi^{-1} &\Rightarrow p|y(\xi - \xi^{-1}) = y(\xi - \xi^{p-1}) \\ &\Rightarrow p|y(\xi + 1 + \xi + \xi^2 + \ldots + \xi^{p-2}) \\ &\Rightarrow p|\underbrace{y + 2y\xi + y\xi^2 + \ldots + y\xi^{p-2}}_{\in \mathbb{Z}[\xi]} \\ &\Rightarrow p|y. \end{aligned}$$

But this gives us a contradiction since we have chosen y relatively prime to p. Thus, $k = 0$ cannot be true.
Case 2: If $k = p - 1$.
Here we have,

$$\begin{aligned} \gamma &= x + y\xi - x\xi^{p-1} - y\xi^{p-2} \\ &= x + y\xi - x(-(1 + \xi + \ldots + \xi^{p-2})) - y\xi^{p-2} \\ &= 2x + (x + y)\xi + x\xi^2 + \ldots + (x - y)\xi^{p-2}. \end{aligned}$$

Now, if $p|\gamma$, then $p|2x$ by Lemma 5.3. This implies that $p|x$ as p is odd. Again we get

a contradiction since x was chosen to be relatively prime to p. Thus $k \neq p-1$.

Case 3: If $1 < k \leq p-2$.
In this case we have the following information,

$$\xi^k \neq 1 \text{ and } \xi^k \neq \xi \text{ and } \xi^k \neq \xi^{k-1}.$$

Then by Equation (5.6) the coefficient of ξ^k in the unique decomposition of γ is equal to $-x$. But then

$$p|\gamma = x + y\xi - \xi^k x - \xi^{k-1} y \Rightarrow p|x.$$

Then again we obtain a contradiction as x is not divisible by p. Thus $k \neq 2, \ldots, p-2$. As a result, we can conclude that $k = 1$ and Claim 2 follows. □

Claim 3. $x \equiv y \pmod{p}$.

Proof of the Claim. By Claim 2, $k = 1$. So, $\gamma = x + y\xi - x\xi - y = (x-y)(1-\xi)$. Since $p|\gamma$ (Equation (5.6)), we get p divides $(x-y)$ by Lemma 5.3 again. Hence,

$$x \equiv y \pmod{p}.$$

□

We had chosen pairwise relatively prime x, y, z as a solution of $x^p + y^p = z^p$ where p is a regular prime and concluded that $x \equiv y \pmod{p}$. But if x, y, z is a solution, then $x, -z, -y$ is also a solution to $x^p + y^p = z^p$ as p is prime. So, we may conclude that

$$x \equiv -z \pmod{p}. \tag{5.7}$$

Since $x \equiv y \pmod{p}$, then $x^p \equiv y^p \pmod{p}$. Also, $z^p \equiv (-x)^p \pmod{p}$ Then, (remembering that p is odd)

$$2x^p \equiv x^p + x^p \equiv x^p + y^p \equiv z^p \equiv (-x)^p \equiv -x^p \pmod{p}.$$

This implies that $p|3x^p$. This means that either $p = 3$ or $p|x^p$. However, if $p = 3$ then Equation (5.2) has no integer solutions by Theorem 5.1. If $p|x^p$ then we obtain that $p|x$. This leads to a contradiction by the assumption of the theorem. □

In the next section, we will prove Fermat's Last Theorem for the regular primes which divide one of the integers x, y, z. The next case is a little bit harder and messier than Case 1.

6. FERMAT'S LAST THEOREM: CASE 2

In this section we will prove that there is no solution for p^{th} Fermat equation when p divides the solutions. As in the other sections, throughout this section, ξ refers to a primitive p^{th} root of unity and $\mathcal{O}_K = \mathbb{Z}[\xi]$ is the ring of cyclotomic integers. We will assume all the properties of Dedekind domains and cyclotomic integers mentioned before.

6.1 FURTHER PROPERTIES OF CYCLOTOMIC INTEGERS

In this section we are going to present some important properties of cyclotomic integers which are essentially used in the proof of *Fermat's Last Theorem*. Especially Lemma 6.2 below constitutes an important part of the proof of Fermat's Last Theorem, by creating a connection between integer solutions of Fermat's equation which are relatively prime to p in $\mathbb{Z}$ and cyclotomic integer solutions which are relatively prime to $1-\xi$ in $\mathbb{Z}[\xi]$.

Lemma 6.1. *[pp. 157, Lemma 1 in [5]] In the ring $\mathbb{Z}[\xi]$, the ideal $\langle 1-\xi \rangle$ is prime and p has the factorization*

$$p = (1-\xi)^{p-1}\epsilon \tag{6.1}$$

where ϵ is a unit in $\mathbb{Z}[\xi]$.

Proof. We know that $N(1-\xi) = (1-\xi)\dots(1-\xi^{p-1}) = p$ by Lemma 3.22, and hence

$$p = (1-\xi)^{p-1}(1+\xi)(1+\xi+\xi^2)\cdots(1+\xi+\cdots+\xi^{p-2}).$$

By the Corollary 3.16, we know that $1+\xi+\ldots+\xi^k$ is a unit for any $k \in \{1,\dots,p-2\}$. Then so writing $\epsilon = (1+\xi)(1+\xi+\xi^2)\dots(1+\xi+\ldots+\xi^{p-2})$, we obtain

$$p = (1-\xi)^{p-1}\epsilon \quad \text{where } \epsilon \text{ is a unit in } \mathbb{Z}[\xi].$$

Clearly by the first assertion of Theorem 3.63, $\langle 1-\xi \rangle$ is a prime ideal of $\mathbb{Z}[\xi]$ as $N(\langle 1-\xi \rangle) = p$ is prime in $\mathbb{Z}$. □

Lemma 6.2. *[pp. 158, Lemma 2 in [5]] If $a \in \mathbb{Z}$ is divisible by $1-\xi$ (in the ring $\mathbb{Z}[\xi]$), then it is also divisible by p for some $p \in \mathbb{Z}$.*

Proof. Assume $a = (1-\xi)\alpha$ for some $\alpha \in \mathbb{Z}[\xi]$. Taking the norm of both sides, by Lemma 3.22 we obtain

$$a^{p-1} = N(1-\xi)N(\alpha) = pN(\alpha)$$

where $N(\alpha) \in \mathbb{Z}$ by Corollary 3.21. So, the above equation is in $\mathbb{Z}$. Since p is a prime dividing a^{p-1}, this gives us that p divides a in $\mathbb{Z}$. □

Actually the converse of the lemma above also holds, that is, a is divisible by $1-\xi$ in $\mathbb{Z}[\xi]$ if and only if a is divisible by p in $\mathbb{Z}$. However, we will only need the statement of Lemma 6.2.

Lemma 6.3. *Let $w \in \mathbb{Z}[\xi]$ be such that*

$$w \equiv a \pmod{I} \quad \textit{for some} \quad a \in \mathbb{Z}.$$

Then we have that $w^p \equiv a^p \pmod{I^p}$ (Note that $I = \langle 1-\xi \rangle$).

Proof. Since $w \equiv a \pmod{I}$, there exists $v \in \mathbb{Z}[\xi]$ such that,

$$w = a + (1-\xi)v.$$

In $\mathbb{Z}[\xi]$ we may write,

$$w^p - a^p = (w-a)(w-a\xi)\dots(w-a\xi^{p-1}).$$

Then for any $i = 0, 1, \dots, p-1$ we have,

$$w - a\xi^i = \underbrace{(a+(1-\xi)v)}_{w} - a\xi^i = a(1-\xi^i) + (1-\xi)v = \underbrace{(1-\xi)[\overbrace{a(1+\xi+\cdots+\xi^{i-1})+v}^{\in\mathbb{Z}[\xi]}]}_{\in I = \langle 1-\xi\rangle}.$$

Thus, $w - a\xi^i \in \mathrm{I}$ for all $i = 0, 1, \dots, p-1$, i.e., $w - a\xi^i \equiv 0 \pmod{I}$. In other words, since $w - a\xi^i \in I$ for all $i = 0, 1, \dots, p-1$, then

$$(w-a)(w-a\xi)\cdots(w-a\xi^{p-1}) \in I^p.$$

As a result we get,

$$w^p \equiv a^p \pmod{I^p}.$$

□

Lemma 6.4. *$1+\xi$ is a unit in $\mathbb{Z}[\xi]$.*

This follows by Corollary 3.16.

6.2 KUMMER'S LEMMA

The following theorem is originally proved by Kummer, which is essential to prove second case of Fermat's Last Theorem. It is different from *Kummer's Lemma on Units* (Lemma 4.4), although they all classify the units of cyclotomic integers. We will not give a proof of *Kummer's Lemma*, because the tools used to prove it are beyond the scope of this thesis. We refer the reader to the book [5] for the proof.

Theorem 6.5. *[Kummer's Lemma; pp. 377, Theorem 3 in[5]] Let p be a prime number. If a unit u of $\mathbb{Z}[\xi]$, is congruent modulo p to a rational integer a, then the unit is the p^{th} power of another unit $\eta \in \mathbb{Z}[\xi]$, i.e., $u = \eta^p$.*

6.3 FERMAT'S LAST THEOREM: CASE 2

In this section, we will present a proof of Fermat's Last Theorem when $p \geq 3$ is an odd regular prime dividing the product xyz.

Theorem 6.6. *If p is an odd regular prime then the equation,*

$$x^p + y^p = z^p \tag{6.2}$$

has no integer solutions x, y, z satisfying $p|xyz$.

Proof. We will prove this theorem by contradiction. Assume that there are integers x, y, z satisfying Equation (6.2) and $p|xyz$. Without loss of generality we may assume that x, y, z are relatively prime positive integers and p divides only z. Since $p|z$ we may write $z = p^k z_0$ for some integers $k \geq 1$ and z_0 such that $(z_0, p) = 1$. By Lemma 6.1 p has the factorization,

$$p = (1 - \xi)^{p-1}\epsilon$$

in $\mathbb{Z}[\xi]$ for some unit $\epsilon \in \mathbb{Z}[\xi]$. So we can rewrite Equation (6.2) as follows,

$$x^p + y^p = \epsilon^p (1 - \xi)^{pm} z_0^p \tag{6.3}$$

where $m = k(p-1) > 0$. Since $p - 1 \geq 2$ and $k \geq 1$, so we have

$$m = k(p-1) \geq 1 \cdot 2 > 1.$$

In order to show that an equation of the form (6.2) is impossible in $\mathbb{Z}$, we will show that an equation of the form (6.3) is impossible in $\mathbb{Z}[\xi]$ where x, y, z_0 are relatively

prime to $1-\xi$. Because if we can find a solution in $\mathbb{Z}$ which is divisible by $1-\xi$ in $\mathbb{Z}[\xi]$, then this gives rise to a solution in $\mathbb{Z}$ which is divisible by p by Lemma 6.2 and so we get a contradiction to our assumption.

Assume that there is a solution x, y, z_0 of Equation (6.3) not divisible by $1-\xi$ in $\mathbb{Z}$ such that $m > 1$ is smallest (To avoid introducing new notation, suppose this solution is given by Equation (6.3)). As usual let $\mathrm{I} = \langle 1-\xi \rangle$. Then I is a prime ideal of $\mathcal{O}_K$ by Lemma 3.64 and Theorem 3.63. Let $\mathrm{J} = \langle z_0 \rangle$ be the ideal generated by z_0. By factorizing Equation (6.3) as in Case 1 and passing to ideals we obtain,

$$\prod_{k=0}^{p-1} \left\langle x + y\xi^k \right\rangle = \mathrm{I}^{pm}\mathrm{J}^p. \tag{6.4}$$

Here I and J are relatively prime by Lemma 3.45 as $\langle 1-\xi \rangle$ is a prime ideal and $1-\xi$ is taken to be relatively prime with z_0.

Since $m > 1$, we have $pm > p > 0$. Now we will show that all the terms on the left side of Equation (6.4) are divisible by I and exactly one of them is divisible by I^2.

Claim 1. For all $i = 0, 1, \ldots, p-1$, we have $\mathrm{I} \mid \langle x + y\xi^i \rangle$.

Proof of the Claim. Since I is a prime ideal, at least one of the terms on the left of Equation (6.4) is divisible by I. Say $\langle x + y\xi^{i_0} \rangle$ is divisible by I for some $i_0 = 0, 1, \ldots, p-1$. This means that $x + y\xi^{i_0} \in \mathrm{I}$. Clearly, for any $i = 0, 1, \ldots, p-1$ we have the following equality in $\mathbb{Z}[\xi]$,

$$x + y\xi^{i_0} = x + y\xi^i - y\xi^i(1 - \xi^{i_0 - i}). \tag{6.5}$$

Passing to ideals in Equation (6.5) and using the fact that $\langle 1 - \xi^{i_0-i} \rangle = \langle 1-\xi \rangle = \mathrm{I}$ by Lemma 3.15 and Lemma 3.17, we get;

$$x + y\xi^{i_0} - x - y\xi^i \in \mathrm{I}.$$

Then it can be easily seen that I must divide $\langle x + y\xi^i \rangle$ for any $i = 0, 1, \ldots, p-1$, as it divides $\langle x + y\xi^{i_0} \rangle$. □

Claim 2. There is no $i, j \in \{0, 1, \ldots, p-1\}$ such that $i \neq j$ and the following is true,

$$\left\langle x + y\xi^i \right\rangle \equiv \left\langle x + y\xi^j \right\rangle \pmod{\mathrm{I}^2}.$$

Proof of the Claim. Assume that the equivalence holds for some $i < j$. This means that,

$$(x + y\xi^i) - (x + y\xi^j) = y\xi^i(1 - \xi^{j-i}) \in \mathrm{I}^2.$$

Then by Definition 3.34, $\mathrm{I}^2 \mid \langle y\xi^i(1 - \xi^{j-i})\rangle = \langle y\rangle\,\mathrm{I}$. Since we are working in a Dedekind domain, we get $\mathrm{I} \mid \langle y\rangle$. But by Theorem 3.46 this contradicts to the assumption that y is relatively prime to $1 - \xi$. □

Claim 3. There exists a unique $k \in \{0, 1, \ldots, p-1\}$ such that, $\mathrm{I}^2 \mid \langle x + y\xi^k\rangle$.

Proof of the Claim. By Claim 2, $\langle x + y\xi^i\rangle$'s are pairwise non-congruent modulo I^2 and by Claim 1 we have,

$$\frac{x + y\xi^i}{1 - \xi} \in \mathbb{Z}[\xi]$$

for all $i = 0, 1, \ldots, p-1$. So, Claim 1 and Claim 2 imply that,

$$\frac{x + y\xi^i}{1 - \xi}, \qquad i = 0, 1, \ldots, p-1$$

are pairwise non-congruent modulo $1 - \xi$. Since $N(\langle 1 - \xi\rangle) = N(\mathrm{I}) = p$, the quotient group $\mathbb{Z}[\xi]/\mathrm{I}$ has order p. Therefore, the ideals $\left\langle \frac{x + y\xi^i}{1 - \xi} \right\rangle$ form a complete set of residues modulo I and hence there exists only one $k \in 0, 1, \ldots, p-1$ such that,

$$\left\langle \frac{x + y\xi^k}{1 - \xi} \right\rangle \equiv 0 \pmod{\mathrm{I}}.$$

As a result, only one $\langle x + y\xi^k\rangle$ is divisible by I^2. □

Remark 6.7. In Equation (6.3), we could replace y by $y\xi^k$ for an arbitrary k and perform the factorization in (6.4) according to this. Therefore, without loss of generality, we may assume $\langle x + y\rangle$ is divisible by I^2 and $\langle x + y\xi^i\rangle$ is divisible by I, but not I^2 for all $i = 1, \ldots, p-1$. Since we have p many factors on the left hand side of Equation (6.4), it is divisible at least by $\mathrm{I}^{p-1}\mathrm{I}^2 = \mathrm{I}^{p+1}$. Moreover, the left hand side of Equation (6.4) is also divisible by I^{pm}, because I^{pm} divides the right hand side of Equation (6.4). Since $\mathrm{I}^2 \nmid \langle x + y\xi^i\rangle$ for all $i = 1, 2, \ldots, p-1$, we have $\mathrm{I}^{pm-(p-1)}$ divides $\langle x + y\rangle$ (Note that $m > 1$). As a result, $\langle x + y\rangle$ is divisible by $\mathrm{I}^{p(m-1)+1}$ by Equation (6.4).

Let M denote the greatest common divisor of the ideals $\langle x\rangle$ and $\langle y\rangle$. Since x and y are relatively prime to $1 - \xi$, M is not divisible by $\mathrm{I} = \langle 1 - \xi\rangle$.

Claim 4. M divides $\langle x + \xi^i\rangle$ for all $i = 0, 1, \ldots, p-1$.

Proof of the Claim. Since $\mathsf{M}|\langle x\rangle$ and $\mathsf{M}|\langle y\rangle$, by Lemma 3.35,

$$\langle x\rangle \subset \mathsf{M} \text{ and } \langle y\rangle \subset \mathsf{M} \Longrightarrow x \in \mathsf{M} \text{ and } y \in \mathsf{M}.$$

Thus in $\mathbb{Z}[\xi]$ for any $i = 0, 1, \ldots, p-1$,

$$x + y\xi^i \in \langle x, y\rangle \subseteq \mathsf{M}.$$

Hence, $\langle x + y\xi^i\rangle$ is divisible by M for all i. □

Since $\mathbb{Z}[\xi]$ is a Dedekind domain and I is relatively prime to M, $\mathsf{MI}|\langle x + y\xi^i\rangle$ for all $i = 0, 1, \ldots, p-1$ by Claims 4, 3 and 1. Therefore by Remark 6.7, $\langle x + y\rangle$ is divisible by $\mathsf{MI}^{p(m-1)+1}$ as $m > 1$. Moreover, we will observe in Claim 5 that MI is the largest common factor of $\langle x + y\xi^i\rangle$ for all $i = 0, 1, \ldots, p-1$. So there are ideals $\mathsf{N_0}, \mathsf{N_1}, \ldots, \mathsf{N_{p-1}}$ such that,

$$\begin{aligned}\langle x + y\rangle &= \mathsf{MI}^{p(m-1)+1}\mathsf{N_0}\\ \left\langle x + y\xi^i\right\rangle &= \mathsf{MIN_i} \quad (i = 1, \ldots, p-1).\end{aligned}$$

Claim 5. The ideals $\mathsf{N_0}, \mathsf{N_1}, \ldots, \mathsf{N_{p-1}}$ are pairwise relatively prime.

Proof of the Claim. Assume that $\mathsf{N_i}$ and $\mathsf{N_j}$ have a common divisor P for some $0 \le i < j \le p-1$. Note that this P must be relatively prime to MI. But this means that $\langle x + y\xi^i\rangle$ and $\langle x + y\xi^j\rangle$ has a common divisor MIP. This means that,

$$x + y\xi^i \in \mathsf{MIP} \text{ and } x + y\xi^j \in \mathsf{MIP}.$$

Considering the below equations in $\mathbb{Z}[\xi]$,

$$\begin{aligned}\underbrace{x + y\xi^i}_{\in \mathsf{MIP}} &= \underbrace{x + y\xi^j}_{\in \mathsf{MIP}} + y\xi^i(1 - \xi^{j-i}) \Rightarrow\ y\xi^i(1 - \xi^{j-i}) \in \mathsf{MIP}\\ \underbrace{x + y\xi^j}_{\in \mathsf{MIP}} &= \xi^{j-i}\underbrace{(x + y\xi^i)}_{\in \mathsf{MIP}} + x(1 - \xi^{j-i}) \Rightarrow\ x(1 - \xi^{j-i}) \in \mathsf{MIP}\end{aligned}$$

we get,

$$\mathsf{MIP}|\langle y\rangle\,\mathrm{I} \text{ and } \mathsf{MIP}|\langle x\rangle\,\mathrm{I}.$$

However, since $\mathbb{Z}[\xi]$ is a Dedekind domain, factorization of ideals into prime ideals is unique and cancellation law holds. Hence we get,

$$\mathsf{MP}|\langle y\rangle \text{ and } \mathsf{MP}|\langle x\rangle.$$

So, we get a contradiction to the fact that M is the greatest common divisor of $\langle x \rangle$ and $\langle y \rangle$. $\square$

Claim 6. For each $i = 0, 1, \ldots, p-1$, there is an ideal J_i of $\mathbb{Z}[\xi]$ such that $\mathsf{N}_i = \mathrm{J}_i^p$ and $\mathrm{J}_i \neq \mathrm{J}_k$ if $i \neq k$. Moreover, I is relatively prime to each J_i.

Proof of the Claim. We may rewrite Equation (6.4) in the following form,

$$\mathsf{M}^p \mathrm{I}^{pm} \mathsf{N}_0 \mathsf{N}_1, \ldots, \mathsf{N}_{\mathsf{p}-1} = \mathrm{I}^{pm} \mathrm{J}^p.$$

Since $\mathbb{Z}[\xi]$ is a Dedekind domain we may cancel I^{pm}'s to get,

$$\mathsf{M}^p \mathsf{N}_0 \mathsf{N}_1, \ldots, \mathsf{N}_{\mathsf{p}-1} = \mathrm{J}^p. \tag{6.6}$$

Then since M and J have factorizations into prime ideals and each prime appearing in the factorization of M must also appear in the factorization of J, we get

$$\mathsf{M} = \mathsf{p}_0^{s_0} \mathsf{p}_1^{s_1} \ldots \mathsf{p}_m^{s_m} \quad \text{and} \quad \mathrm{J} = \mathsf{p}_0^{t_0} \mathsf{p}_1^{t_1} \ldots \mathsf{p}_m^{t_m},$$

for some prime ideals $\mathsf{p}_0, \mathsf{p}_1, \ldots, \mathsf{p}_m$ and $0 \leq s_i \leq t_i$. As a result we have

$$\begin{aligned} \mathsf{N}_0 \mathsf{N}_1 \ldots \mathsf{N}_{p-1} &= \mathsf{p}_0^{(t_0 - s_0)p} \mathsf{p}_1^{(t_1 - s_1)p} \ldots \mathsf{p}_m^{(t_m - s_m)p} \\ &= \left(\mathsf{p}_0^{t_0 - s_0} \mathsf{p}_1^{t_1 - s_1} \ldots \mathsf{p}_m^{t_m - s_m} \right)^p. \end{aligned}$$

Also if one prime appears in the ideal factorization of N_i, then it must not appear in the factorization of N_j since N_i's are relatively prime.
In other words,

$$\text{if } \mathsf{p}_k | \mathsf{N}_i \text{ for some } k \in \{0, 1, \ldots, m\}, \quad \text{then } \mathsf{N}_i = \mathsf{p}_k^{(t_k - s_k)p}.$$

Therefore, there are relatively prime ideals $\mathrm{J}_0, \mathrm{J}_1, \ldots, \mathrm{J}_{p-1}$ such that each of them is a product of ideals $\mathsf{p}_0, \mathsf{p}_1, \ldots, \mathsf{p}_m$ and,

$$\mathsf{N}_i = \mathrm{J}_i^p \qquad i \in \{0, 1, \ldots, p-1\}.$$

Moreover, since I and J are relatively prime it is easy to observe that I is relatively prime to each J_i by Equation (6.6). $\square$

As a result we have,

$$\langle x+y\rangle = \mathsf{M}\mathrm{I}^{p(m-1)+1}\mathrm{J}_0^p \tag{6.7}$$

$$\left\langle x+y\xi^i\right\rangle = \mathsf{M}\mathrm{I}\mathrm{J}_i^p \qquad (i=1,\ldots,p-1). \tag{6.8}$$

Solving Equation (6.7) for M and substituting in (6.8), we obtain

$$\left\langle x+y\xi^i\right\rangle \mathrm{I}^{p(m-1)} = \langle x+y\rangle\,(\mathrm{J}_i\mathrm{J}_0^{-1})^p. \tag{6.9}$$

Note that the ideal on the left hand side is principal since it is a product of principal ideals. Then since $\langle x+y\rangle$ is principal, its inverse is a principal fractional ideal by Lemma 3.53. Then so, $(\mathrm{J}_i\mathrm{J}_0^{-1})^p$ is a principal fractional ideal. Now consider the (fractional) ideal class group of the number ring $\mathbb{Z}[\xi]$. Since p is a regular prime, p does not divide the order of $\mathrm{cl}(\mathbb{Z}[\xi])$. Therefore $\mathrm{J}_i\mathrm{J}_0^{-1}$ is a principal fractional ideal by Remark 3.33. This means that,

$$\mathrm{J}_i\mathrm{J}_0^{-1} = \left\langle \frac{\alpha_i}{\beta_i}\right\rangle \quad 1\le i\le p-1 \tag{6.10}$$

for some $\alpha_i,\beta_i\in\mathbb{Z}[\xi]$.

Claim 7. For any $1\le i\le p-1$, the elements α_i,β_i are not divisible by $(1-\xi)$ in $\mathbb{Z}[\xi]$.

Proof of the Claim. By Claim 6 we know that $\mathrm{J}_0,\ldots,\mathrm{J}_{p-1}$ are not divisible by I. Note that we may choose α_i,β_i such that not both of them are divisible by $1-\xi$. Now, $\mathrm{J}_i\mathrm{J}_0^{-1} = \left\langle \frac{\alpha_i}{\beta_i}\right\rangle$ implies

$$\langle\alpha_i\rangle\,\mathrm{J}_0 = \langle\beta_i\rangle\,\mathrm{J}_i. \tag{6.11}$$

If $1-\xi$ divides α_i, then $\langle 1-\xi\rangle$ divides LHS and hence also RHS of the Equation (6.11). Since $1-\xi$ does not divide β_i (as it can not divide both α_i,β_i) the ideal J_i is divisible by $\langle 1-\xi\rangle = \mathrm{I}$ which is not the case by Claim 6. As a result $1-\xi$ does not divide α_i. Symmetrically, it can not divide β_i. □

If two principal ideals are equal then their generators differ only by a unit factor in any ring. Hence combining Equations (6.9) and (6.10) and passing to elements from ideals we obtain,

$$(x+y\xi^i)(1-\xi)^{p(m-1)} = (x+y)\left(\frac{\alpha_i}{\beta_i}\right)^p\epsilon_i \quad (1\le i\le p-1), \tag{6.12}$$

where $\epsilon_i \in \mathbb{Z}[\xi]$ is a unit for all $1 \leq i \leq p-1$.

Consider now the equation below,

$$(x+y\xi)(1+\xi) - (x+y\xi^2) = x\xi + y\xi = (x+y)\xi.$$

Multiplying it by $(1-\xi)^{p(m-1)}$ we get

$$(x+y\xi)(1+\xi)(1-\xi)^{p(m-1)} - (x+y\xi^2)(1-\xi)^{p(m-1)} = (x+y)\xi(1-\xi)^{p(m-1)}. \quad (6.13)$$

Now consider Equation (6.12) for $i=1$ and $i=2$.

$$\text{for } i=1: \qquad (x+y\xi)(1-\xi)^{p(m-1)} = (x+y)\left(\frac{\alpha_1}{\beta_1}\right)^p \epsilon_1 \quad (6.14)$$

$$\text{for } i=2: \qquad (x+y\xi^2)(1-\xi)^{p(m-1)} = (x+y)\left(\frac{\alpha_2}{\beta_2}\right)^p \epsilon_2. \quad (6.15)$$

Substituting Equations (6.14) and (6.15) into Equation (6.13) we get,

$$(x+y)\left(\frac{\alpha_1}{\beta_1}\right)^p \epsilon_1(1+\xi) - (x+y)\left(\frac{\alpha_2}{\beta_2}\right)^p \epsilon_2 = (x+y)\xi(1-\xi)^{p(m-1)}. \quad (6.16)$$

Simplifying $(x+y)$'s and making some rearrangements in Equation (6.16) we get

$$(\alpha_1\beta_2)^p - (\alpha_2\beta_1)^p \frac{\epsilon_2}{\epsilon_1(1+\xi)} = (\beta_1\beta_2)^p \frac{\xi}{\epsilon_1(1+\xi)}(1-\xi)^{p(m-1)}. \quad (6.17)$$

By Claim 7 and the fact that $1-\xi$ is a prime in $\mathbb{Z}[\xi]$, $\alpha_1\beta_2$, $\alpha_2\beta_1$ and $\beta_1\beta_2$ are all in $\mathbb{Z}[\xi]$ and not divisible by $1-\xi$. Let $\alpha = \alpha_1\beta_2$, $\beta = \alpha_2\beta_1$, $\gamma = \beta_1\beta_2$ and $u_1 = -\dfrac{\epsilon_2}{\epsilon_1(1+\xi)}$, $u_2 = \dfrac{\xi}{\epsilon_1(1+\xi)}$. Since $1+\xi$ is a unit by Lemma 6.4, u_1 and u_2 are units in $\mathbb{Z}[\xi]$.

Rewriting Equation (6.17) again, we have

$$\alpha^p + \beta^p u_1 = \gamma^p u_2 (1-\xi)^{p(m-1)} \quad \text{in } \mathbb{Z}[\xi]. \quad (6.18)$$

By passing to ideals and going back again we will transform Equation (6.18) to the form of Equation (6.3).

If we consider Equation (6.18) in ideal form, the right hand side becomes $\langle\gamma\rangle^p \, \mathrm{I}^{p(m-1)}$ and by Lemma 3.37 it is strictly contained in I^p (because $m>1$, so that $p(m-1) \geq p$).

Thus,

$$\alpha^p + \beta^p u_1 \in \mathrm{I}^p,$$

in other words

$$\alpha^p + \beta^p u_1 \equiv 0 \pmod{\mathrm{I}^p}. \tag{6.19}$$

Since β is relatively prime to I, then by Lemma 3.44, β is also relatively prime to I^p, i.e.,

$$\langle \beta \rangle + \mathrm{I}^p = \langle 1 \rangle .$$

This means that for some $\beta' \in \mathbb{Z}[\xi]$, $\beta\beta' - 1 \in \mathrm{I}^p$, i.e., $\beta\beta' \equiv 1 \pmod{\mathrm{I}^p}$. Multiplying Equation (6.19) with $(\beta')^p$ we get,

$$(\beta')^p\alpha^p + (\beta')^p\beta^p u_1 \equiv (\beta'\alpha)^p + (\beta'\beta)^p u_1 \equiv (\beta'\alpha)^p + u_1 \equiv 0 \pmod{\mathrm{I}^p}.$$

Letting $w = -\beta'\alpha \in \mathbb{Z}[\xi]$, we have

$$u_1 \equiv w^p \pmod{\mathrm{I}^p}. \tag{6.20}$$

Claim 8. There exists a in $\mathbb{Z}$ such that $w \equiv a \pmod{\mathrm{I}}$.

Proof of the Claim. We know that $N(\mathrm{I}) = |\mathbb{Z}[\xi]/\mathrm{I}| = p$. This gives us an isomorphism

$$f : \mathbb{Z}[\xi]/\mathrm{I} \longrightarrow \mathbb{Z}_p$$

since any ring with p elements is isomorphic to $\mathbb{Z}_p$. Consider the following diagram

$$\begin{array}{ccccc} \mathbb{Z} & \xrightarrow{\ i\ } & \mathbb{Z}[\xi] & \xrightarrow{\ \pi\ } & \mathbb{Z}[\xi]/\mathrm{I} \\ & \searrow^{\sigma} & & & \downarrow f \\ & & & & \mathbb{Z}_p \end{array} \quad , \tag{6.21}$$

where i is the inclusion map and π and σ are the natural quotient maps. Clearly, both σ and $f \circ \pi \circ i$ are ring homomorphisms taking 1 to 1, hence they coincide on $\mathbb{Z}$ and so the diagram is commutative. Now, consider $f(\pi(w))$. Clearly, there is $a \in \mathbb{Z}$ such that $\sigma(a) = f(\pi(w))$. We will show that this a is a good choice, that is, $w + I = a + I$. We have $f(\pi(w)) = \sigma(a) = f(\pi(i(a)))$ where the last equality follows from the commutativity of the diagram. Since f is one-to-one, we get $\pi(w) = \pi(i(a))$, which gives the result. □

Hence $w \equiv a \pmod{\mathrm{I}}$ for some $a \in \mathbb{Z}$. Then by Lemma 6.3,

$$w^p \equiv a^p \pmod{\mathrm{I}^p}$$

where $a \in \mathbb{Z}$. By Equation (6.20), u_1 is congruent to a rational integer modulo I^p, namely

$$u_1 \equiv a^p \pmod{\mathrm{I}^p}.$$

But by Lemma 3.64 (a), we have $\mathrm{I}^{p-1} = \langle p \rangle$. Also by Lemma 3.37, we have

$$\mathrm{I}^p = \mathrm{I}^{p-1}\mathrm{I} \subset \mathrm{I}^{p-1} = \langle p \rangle .$$

Hence, $u_1 - a^p \in \mathrm{I}^p \subset \langle p \rangle$ which means that

$$u_1 \equiv a^p \pmod{p} \qquad a \in \mathbb{Z}.$$

So by *Kummer's Lemma* (Theorem 6.5), the unit u_1 is a p^{th} power of another unit $\eta \in \mathbb{Z}[\xi]$, i.e., $u_1 = \eta^p$.

Therefore, by replacing $u_1 = \eta^p$, Equation (6.18) turns to be

$$\alpha^p + (\beta\eta)^p = \gamma^p u_2 (1-\xi)^{p(m-1)}. \tag{6.22}$$

Remember that $\alpha, \beta\eta, \gamma$ are elements of $\mathbb{Z}[\xi]$ which are relatively prime to $1-\xi$. (η is a unit.) Then we may easily notice that the above equation has the similar form of Equation (6.3). But this time we have the exponent $m-1$ instead of m. So we get a contradiction to the assumption that m is the smallest such possible power. As a consequence of this and Lemma 6.2, Fermat's Equation (6.2) for p is a regular prime has no nontrivial solutions in $\mathbb{Z}$ for which one of x, y, z is divisible by p. □

As a result, Theorem 6.6 and Theorem 5.4 shows that Fermat's equation has no non-trivial integer solutions for regular prime exponents.

References

[1] Stewart, I. and Tall, D., *Algebraic Number Theory and Fermat's Last Theorem*, third edition, A K Peters Ltd., Canada, 2002.

[2] Marcus, D. A., *Number Fields*, Springer, New York, 1977.

[3] Hilbert D., *The Theory of Algebraic Number Fields*, Springer, Germany, 1991.

[4] Dummit, D. and Foote, R. *Abstract Algebra*, third edition, Willey, USA, 2004.

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

[6] Edwards, H., *Fermat's Last Theorem*, Springer, New York, 1977.

[7] Washington, L., "Fermat's Last Theorem" in L. Washington, *Introduction to Cyclotomic Fields*, second edition, pp. 1-8, Springer, New York, 1997.

[8] Vandiver, H.Â S. and Wahlin, G.Â E., *Algebraic Numbers*, Bull. Nat. Res. Council, No.Â 62, 1928.

[9] Riehl, E., *Kummer's Special Case of Fermat's Last Theorem*, May 18, 2005.

[10] Boyajian, B., *Dedekind Domains and the Ideal Class Group*, August 26, 2011.

[11] Conrad, K. *Ideal Factorization*, Conrad's expository papers, *http* : *//www.math.uconn.edu/ kconrad/blurbs/gradnumthy/idealfactor.pdf*.