Fermat's Last Theorem for regular primes

A foray into algebraic number theory

Sayan Das,
UG-2 Mathematics Department,
Jadavpur University

May 17, 2025

Contents

1 Introduction and algebraic preliminaries

The broad aim of number theory is to solve *Diophantine equations* i.e. polynomial equations with integer or rational coefficients for which we seek integer or rational solutions. Possibly the most famous example of a Diophantine equation is *Fermat's Last Theorem*, which was conjectured by Pierre de Fermat but not proven until 1995 by Andrew Wiles. It states that for $n \geq 3$ the equation $x^n + y^n = z^n$ has no solutions with $xyz \neq 0$.

Wiles' full proof is quite advanced, but for the case of n being a special kind of prime, called a *regular prime*, Ernst Kummer had already studied and proved it in the 19th century. Much of his work would become foundational to what we now call *algebraic number theory.*

For completeness, we define some algebraic structures that will be vital in our foray into algebraic number theory. However we assume familiarity with linear algebra.

Definition 1 (Group)**.** A *group* is a triple $(G, \cdot, e)$, where G is a set, $\cdot : G \times G \to G$ is a binary operation and $e \in G$ is an element such that

1. For all $a, b, c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (associativity)
2. For all $a \in G$, we have $a \cdot e = e \cdot a = a$. (identity)
3. For all $a \in G$, there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$. (inverse)

A group is said to be *abelian* if the commutative law holds: $a \cdot b = b \cdot a$.

Definition 2 (Ring)**.** A *ring* is a quintuple $(R, +, \cdot, 0_R, 1_R)$ where $0_R, 1_R \in R$, and $+, \cdot :$ $R \times R \to R$ are binary operations such that

1. $(R, +, 0_R)$ is an abelian group.
2. The operation $\cdot : R \times R \to R$ satisfies associativity, i.e. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, and identity: $1_R \cdot a = a \cdot 1_R = a$.
3. Multiplication distributes over addition, i.e.

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c). \end{aligned}$$

A ring is said to be *commutative* if the commutative law holds: $a \cdot b = b \cdot a$.

A commutative ring with $a \cdot b = 0 \implies a = 0$ or $b = 0$ is called an *integral domain.*

In number theory, two of our principal objects of study are the integers $\mathbb{Z}$ and the integers modulo some positive integer $\mathbb{Z}_m = \{0, \ldots, m-1\}$. These are *commutative* rings. As it gets tedious to assume a ring to be commutative everytime, in number theory we just assume all rings to be commutative by default - which we shall follow in this article as well. Another important example is the ring $R[X]$ of polynomials in X with coefficients in R.

The concept of ideal numbers as "missing factors" in a number ring was also developed by Kummer originally, and later extended by Dedekind, Hilbert and finally Noether to its current definition which is as follows:

Definition 3 (Ideal)**.** Let R be a ring. A subset $I \subseteq R$ is an *ideal* if

1. It is an additive subgroup of $(R, +, 0_R)$, i.e. it is closed under addition and additive inverses. (additive closure)
2. If $a \in I$ and $b \in R$, then $a \cdot b \in I$. (strong closure)

We say I is a proper ideal if $I \neq R$.

Definition 4 (Principal ideal)**.** An ideal I of a ring R generated by a single element $a \in R$ is called a *principal ideal*, denoted

$$(a) = \{ra : r \in R\}.$$

An ring in which every ideal is principal is called a *principal ideal domain (PID).*

Definition 5 (Group of units)**.** An element u of a ring R is a *unit* if there is another element $v \in R$ such that $u \cdot v = 1_R$. The set of all units in a ring R forms a group, called the *group of units* $R^\times$ of R.

It is important that this depends on R, not just on u. For example, $2 \in \mathbb{Z}$ is not a unit, but $2 \in \mathbb{Q}$ is a unit (since $\frac{1}{2}$ is an inverse).

Definition 6 (Field)**.** A *field* $\mathbb{F}$ is a non-zero ring where every $0_{\mathbb{F}} \neq u \in \mathbb{F}$ is a unit.

$\mathbb{Z}$ is not a field but $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.

Definition 7 (Noetherian rings)**.** A ring R is *Noetherian* if every ideal I in R is finitely generated i.e. there exist $a_1, \ldots, a_n \in I$ such that $I = Ra_1 + \cdots + Ra_n$.

Definition 8 (Prime and maximal ideals)**.** An ideal $\mathfrak{p}$ is *prime* if $\mathfrak{p} \neq (1)$ and
if $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

An ideal $\mathfrak{m}$ is *maximal* if $\mathfrak{m} \neq (1)$ and if there is no ideal $\mathfrak{a}$ such that $\mathfrak{m} \subset \mathfrak{a} \subset (1)$ (strict inclusions).

When solving Diophantine equations we often encounter the problem that a equation with integer coefficients may not have rational (or even real) solutions. For example, consider $x^2 + 1 = 0$ or $x^2 - 2 = 0$. In both cases we can adjoin the roots to $\mathbb{Q}$ to get the fields

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\} \text{ and } \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

respectively, both of which contain $\mathbb{Q}$. Similarly $\mathbb{Q}(i, \sqrt{2})$ contains the roots to both equations, and contains both $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$.

$$\begin{tikzcd}
 & \mathbb{Q}(i, \sqrt{2}) & \\
\mathbb{Q}(i) \arrow[ur] & & \mathbb{Q}(\sqrt{2}) \arrow[ul] \\
 & \mathbb{Q} \arrow[ul, "x^2+1=0"] \arrow[ur, "x^2-2=0"'] &
\end{tikzcd}$$

Such fields constructed by adjoining (finitely many) roots to $\mathbb{Q}$ are *number fields* which are examples of *finite field extensions.*

Definition 9 (Field extension)**.** Let $\mathbb{K}$ be a field. A field $\mathbb{L} \supseteq \mathbb{K}$ is called an *extension* of $\mathbb{K}$. Such a field extension is denoted $\mathbb{L}/\mathbb{K}$. In such a field extension, $\mathbb{L}$ is a $\mathbb{K}$-vector space with $\dim_{\mathbb{K}}(\mathbb{L}) = [\mathbb{L} : \mathbb{K}]$ called the *degree* of the extension. A *finite extension* is a field extension of finite degree.

In a finite extension for $\alpha \in \mathbb{L}$ we have the linear operator $m_\alpha : \mathbb{L} \to \mathbb{L}$ defined as $\ell \mapsto \alpha\ell$. We define the norm and trace of α as

$$N_{\mathbb{L}/\mathbb{K}}(\alpha) = \det(m_\alpha) \text{ and } \operatorname{tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = \operatorname{tr}(m_\alpha).$$

Definition 10 (Number field)**.** A *number field* $\mathbb{K}$ is a finite extension of $\mathbb{Q}$.

Definition 11 (Algebraic numbers)**.** An element $\alpha \in \mathbb{L}/\mathbb{K}$ is *algebraic over* $\mathbb{K}$ if $\exists 0 \neq f(X) \in \mathbb{K}[X]$ such that $f(\alpha) = 0$. Otherwise we say that α is *transcendental over* $\mathbb{K}$. It is easily shown that every element of a finite extension is algebraic - in particular, every element of a number field is algebraic and called an *algebraic number.*

Definition 12 (Algebraic integer)**.** Let $\mathbb{K}$ be a number field. Then $\alpha \in \mathbb{K}$ is an *algebraic integer* if there exists a monic polynomial $f(X) \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. The set of all algebraic integers of a number field $\mathbb{K}$, denoted $\mathcal{O}_{\mathbb{K}}$, forms a ring. We sometimes call $\mathcal{O}_{\mathbb{K}}$ a *number ring.*

$\sqrt{2}$ is an algebraic integer as it is a root of $f(X) = X^2 - 2$. $\frac{1}{2}$ is not an algebraic integer as $f(X) = 2X - 1$ is not monic (leading coefficient is $2 \neq 1$). So we think of algebraic integers as not having denominators, just the same as in rational integers.

In rings of algebraic integers, elements that were prime as rational integers may not be "prime" as algebraic integers. For example, in the Gaussian integers $\mathbb{Z}[i]$ we can write $5 = (2 + i)(2 - i)$ so it is not "prime" in $\mathbb{Z}[i]$.

Definition 13 (Irreducible, prime and assoicate elements)**.** Let R be an integral domain and let $r \in R$ be nonzero and not a unit. For any $a, b \in R$

1. if $r = ab \implies a$ or b is a unit in R then r is *irreducible* in R,
2. if $r \mid ab \implies r \mid a$ or $r \mid b$ then r is *prime* in R,
3. if there is a unit $u \in R^\times$ such that $a = ub$ then a and b are *associates* in R.

In an integral domain a prime element is always irreducible but not vice-versa. We think of irreducibility as a generalisation of primality. Rings in which irreducible elements are prime are called *unique factorisation domains* (UFDs).

Definition 14 (Galois group and extension)**.** Let $\mathbb{L}/\mathbb{K}$ be a field extension and $\operatorname{Aut}(\mathbb{L}/\mathbb{K})$ be the set of automorphisms of $\mathbb{L}/\mathbb{K}$, i.e., bijections $\sigma : \mathbb{L} \to \mathbb{L}$ such that

$$\sigma(xy) = \sigma(x)\sigma(y), \ \sigma(x + y) = \sigma(x) + \sigma(y), \ \sigma(1) = 1 \text{ and } \sigma(0) = 0$$

with $x \in \mathbb{K} \implies \sigma(x) = x$. Then the set $\operatorname{Aut}(\mathbb{L}/\mathbb{K})$ with function compositon forms a group. If $\mathbb{L}/\mathbb{K}$ is algebraic and $\operatorname{Aut}(\mathbb{L}/\mathbb{K}) = \mathbb{K}$ then the $\mathbb{L}/\mathbb{K}$ is said to be a *Galois extension* and its group of automorphisms is called the *Galois group* $\operatorname{Aut}(\mathbb{L}/\mathbb{K}) = \operatorname{Gal}(\mathbb{L}/\mathbb{K})$.

2 Ideal class group and Dedekind domains

To prove Fermat's Last Theorem (FLT) it is enough to prove it for all primes $p \geq 3$. This is because if FLT holds for some $m \geq 3$ then it holds for all multiples km of m. So proving FLT even for special kinds of primes was realised to be very important towards solving it. Also we can assume $\gcd(x, y, z) = 1$ since if they did have a common divisor d we could divide both sides of the equation by d and then $\gcd(x/d, y/d, z/d) = 1$.

We now consider some special number fields. A generalisation of the Gaussian numbers $\mathbb{Q}(i)$ could be the *cyclotomic fields*

$$\mathbb{Q}(\zeta_n) = \left\{ \sum_{k=0}^{n-1} a_k \zeta_n^k : a_k \in \mathbb{Q} \right\}$$

where $\zeta_n = e^{2i\pi/n}$ is an n-th root of unity (as $\zeta_n^n = 1$). ζ_n is a point on the unit circle in the complex plane, hence the name *cyclotomic* field as it essentially divides the unit circle into exactly n parts. The ring of integers of the cyclotomic number field is

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \left\{ \sum_{k=0}^{n-1} a_k \zeta_n^k : a_k \in \mathbb{Z} \right\} = \mathbb{Z}[\zeta_n].$$

The nth cyclotomic polynomial is denoted $\Phi_n = \prod_{\gcd(k,n)=1, 1 \leq k \leq n} \left(x - \zeta_n^k \right)$.

In the 19th century, there were attempts to solve FLT using cyclotomic number fields. Assuming $\gcd(x, y, z) = 1$ with $xyz \neq 0$, and $p \geq 3$ prime, we have

$$x^p + y^p = z^p \implies y^p = z^p - x^p = \prod_{k=0}^{p-1} (z - \zeta_p^k x).$$

$$\text{because } z^p - 1 = \prod_{k=0}^{p-1} (z - \zeta_p^k).$$

Moreover,

$$\frac{z^p - 1}{z - 1} = \sum_{k=0}^{p-1} z^k = (z - \zeta_p)(z - \zeta_p^2) \cdots (z - \zeta_p^p). \tag{1}$$

Conjecture 1 (Kummer)**.** If p is an odd prime and if "unique factorisation" holds in $\mathbb{Z}[\zeta_p]$ then

$$x^p + y^p = z^p \text{ has no solutions with } xyz \neq 0.$$

However, this line of attack fails as Kummer himself showed that unique factorisation doesn't hold in $\mathbb{Z}[\zeta_p]$. In the rational integers $\mathbb{Z}$, we have the fundamental theorem of arithmetic, also known as the unique factorisation theorem:

Theorem 1 (Unique factorisation theorem)**.** *Every positive rational integer n can be factorised uniquely as a product of primes*

$$n = p_1^{a_1} \cdots p_k^{a_k}$$

in exactly one way upto rearrangement of the primes p_i.

In the ring $\mathbb{Z}[\zeta_p]$, unique factorisation may not hold. The first prime for which it fails to hold is $p = 23$; 2 is an irreducible element in $\mathbb{Z}[\zeta]$ (setting $\zeta = \zeta_{23}$)

$$\begin{aligned} 2 &\nmid (1+\zeta^2+\zeta^4+\zeta^5+\zeta^6+\zeta^{10}+\zeta^{11}) = a \\ 2 &\nmid (1+\zeta+\zeta^5+\zeta^6+\zeta^7+\zeta^9+\zeta^{11}) = b \\ \text{but } 2 &\mid ab = 2\zeta^{17}+2\zeta^{16}+2\zeta^{15}+2\zeta^{13}+2\zeta^{12}+6\zeta^{11}+2\zeta^{10}+2\zeta^9+2\zeta^7+2\zeta^6+2\zeta^5. \end{aligned}$$

To calculate the product ab above observe that in equation (1) ζ is a root so we get the identity

$$1+\zeta+\cdots+\zeta^{p-1} = 0.$$

For $p = 23$, the identity is

$$1+\zeta+\cdots+\zeta^{22} = 0.$$

So, we first brute force distribute and multiply, then reduce using our identity:

$$\begin{aligned} ab = 1+\zeta+\zeta^2+\zeta^3+\zeta^4+3\zeta^5+3\zeta^6+3\zeta^7+\zeta^8+3\zeta^9+3\zeta^{10}+7\zeta^{11}+3\zeta^{12}+3\zeta^{13}+\zeta^{14} \\ +3\zeta^{15}+3\zeta^{16}+3\zeta^{17}+\zeta^{18}++\zeta^{19}+\zeta^{20}+\zeta^{21}+\zeta^{22} \\ = 2\zeta^{17}+2\zeta^{16}+2\zeta^{15}+2\zeta^{13}+2\zeta^{12}+6\zeta^{11}+2\zeta^{10}+2\zeta^9+2\zeta^7+2\zeta^6+2\zeta^5. \end{aligned}$$

As 2 divides this product but neither of the factors, it is not prime yet irreducible so $\mathbb{Z}[\zeta]$ can't be a UFD. This was in fact the example that Kummer gave in his original paper.

To remedy this failure of unique factorisation in a number ring, Kummer came up with the concept of "ideal number" - an algebraic integer which represents an ideal in the ring of algebraic integers. They were meant to be the "missing factors" that would help achieve unique factorisation in a number ring. Number rings are examples of Dedekind domains - integral domains where unique factorisation of ideals holds.

Definition 15 (Integral closure)**.** Let R_1, R_2 be rings such that $R_2 \supseteq R_1$. Then $\alpha \in R_2$ is said to be *integral over* R_1 if there exists a monic polynomial $f(X) \in R_1[X]$ such that $f(\alpha) = 0$. *Integral closure* of R_1 in R_2 is the set of all $\alpha \in R_2$ that are integral over R_1. R_1 is *integrally closed over* R_2 if it equals its integral closure in R_2.

Definition 16 (Dedekind domain)**.** A *Dedekind domain* is an integral domain $\mathcal{O}_{\mathbb{K}}$ with a field of fractions $\mathbb{K}$ such that

1. $\mathcal{O}_{\mathbb{K}}$ is Noetherian,
2. $\mathcal{O}_{\mathbb{K}}$ is integrally closed in $\mathbb{K}$, and
3. every nonzero prime ideal in $\mathcal{O}_{\mathbb{K}}$ is maximal.

Every number ring is a Dedekind domain.

Theorem 2 (Unique factorisation holds in Dedekind domains)**.** *In a Dedekind domain every nonzero proper ideal can be uniquely factorised as a product of nonzero prime ideals.*

So just as in the ring of rational integers we have unique factorisation of positive integers into a product of prime numbers, in a number ring we have unique factorisation of nonzero proper ideals into a product of nonzero prime ideals.

The problem with unique factorisation of ideals in a number ring is that we may not get principal ideal factors. Consider the simpler number ring $\mathbb{Z}[\sqrt{-5}]$. It is not UFD as

$$6 = 2 \cdot 3 = (1+\sqrt{5})(1-\sqrt{5}).$$

But if we consider the ideals we have

$$\begin{aligned}(2) &= (2, 1+\sqrt{-5})(2, 1-\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2\\ (3) &= (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = \mathfrak{p}_3\mathfrak{p}_4\\ (1+\sqrt{-5}) &= (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3\\ (1-\sqrt{-5}) &= (2, 1-\sqrt{-5})(3, 1-\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4\end{aligned}$$

where $\mathfrak{p}_i$ are prime ideals and thus the ideal factorisation

$$(6) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$$

is unique. However note that none of the factors $\mathfrak{p}_i$ are principal which means $\mathbb{Z}[\sqrt{-5}]$ is not PID. We want to measure the deviation of a number ring from being a PID. For that we introduce the notion of an ideal class group.

Definition 17 (Ideal class group)**.** On the nonzero ideals in a number ring $\mathcal{O}_\mathbb{K}$ we define an equivalence relation as follows: nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_\mathbb{K}$ are in the same equivalence class iff $\exists \alpha, \beta \in \mathcal{O}_\mathbb{K} \setminus \{0\} : \alpha\mathfrak{a} = \beta\mathfrak{b}$. If we denote the class of $\mathfrak{a}$ by $c(\mathfrak{a})$, then we have $c(\mathfrak{a})c(\mathfrak{b}) = c(\mathfrak{a}\mathfrak{b})$ which yields a well-defined multiplication operation on the set of these ideal classes. The set of these ideal classes together with the aforementioned multiplication operation form an abelian group called the *ideal class group* of $\mathbb{K}$, denoted $C_\mathbb{K}$.

The ideal class group of a number field is finite and the number of elements in it is called the *class number* $h(\mathbb{K}) = |C_\mathbb{K}|$.

3 Regular primes and Fermat's Last Theorem

Kummer used the class number to prove FLT for special primes which he defined as:

Definition 18 (Regular prime)**.** A prime p is *regular* if $p \nmid h_p = h(\mathbb{Q}(\zeta_p))$.

For all primes $p \leq 19$ $h_p = 1$ so they are regular. Also $h_{23} = 3$ so $p = 23$ is regular. [1] The significance of a prime p being regular is that if $\mathfrak{a}^p$ is principal for an ideal $\mathfrak{a} \subseteq \mathbb{Z}[\zeta_p]$ then $\mathfrak{a}$ is itself principal. This is because if $\mathfrak{a}^p$ is principal then it is trivial in $C_{\mathbb{Q}(\zeta_p)}$ and as $p \nmid h_p$ we have $\mathfrak{a}$ is trivial in the class group and so a principal ideal.

Lemma 3. *In $\mathbb{Z}[\zeta_p]$ the numbers $1-\zeta_p, 1-\zeta_p^2, \ldots, 1-\zeta_p^{p-1}$ are all associates and $1+\zeta_p$ is a unit. Further, $p = u(1-\zeta_p)^{p-1}$ for some unit u and $(1-\zeta_p)$ is the only prime ideal in $\mathbb{Z}[\zeta_p]$ dividing p.*

See [1, page 1, Lemma 1] for a proof.

Lemma 4 (Kronecker)**.** *If α is an algebraic integer such that for every automorphism σ in its Galois group the absolute value of $\sigma(\alpha)$ is 1, then α is a root of unity.*

See [2, page 4, Lemma 1.6] for a proof of the above lemma.

Lemma 5. *For $v \in \mathbb{Z}[\zeta_p]^\times$, $v/\overline{v}$ is a root of unity.*

Proof. For $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ we have $\sigma(\overline{v}) = \overline{\sigma v}$. Thus $v/\overline{v}$ and $\sigma(v/\overline{v})$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ have absolute value 1, as

$$|\sigma(v/\overline{v})| = |\sigma(v)||\sigma(1/\overline{v})| = |\sigma(v)||\overline{\sigma(1/v)}| = |\sigma(v)||\sigma(1/v)| = |\sigma(v/v)| = 1.$$

Therefore by the previous lemma we have that $v/\overline{v}$ is a root of unity. ■

The roots of unity of finite order in $\mathbb{Z}[\zeta_p]$ are $\pm\zeta_p^k$ for $0 \leq k \leq p-1$.

Theorem 6 (Kummer)**.** *For a* regular prime $p \geq 3$, *the equation $x^p + y^p = z^p$ has no solutions with $xyz \neq 0$ and* $\gcd(x, y, z) = 1$.

Proof. We divide the proof into two cases. In case 1 we assume that $p \nmid xyz$. In case 2 we assume that $p \mid xyz$. Also for convenience we write $\zeta = \zeta_p$. We will just do case 1 as case 2 is a bit more involved (the full proof is in [1]; our proof of case 1 also follows what is discussed there).

We factorise Fermat's equation in $\mathbb{Z}[\zeta]$ as

$$z^p = x^p + y^p = (x+y)(x+\zeta^2 y)\cdots(x+\zeta^{p-1}y) = \prod_{k=0}^{p-1}(x+\zeta^k y). \tag{1}$$

We now show that each of the factors $(x + \zeta^k y)$ generate coprime ideals.

For $0 \leq k < k' \leq p-1$, a common ideal factor $\mathfrak{d}$ of $(x + \zeta^k y)$ and $(x + \zeta^{k'} y)$ must be a factor of the difference

$$x + \zeta^k y - x - \zeta^{k'} y = \zeta^k y(1 - \zeta^{k'-k}) = vy(1-\zeta)$$

for some unit v using Lemma 3. As $y(1-\zeta) \mid yp$, we have $\mathfrak{d} \mid (yp)$. From equation (1) we have $\mathfrak{d} \mid (z)^p$. As $\gcd(yp, z^p) = 1$ we conclude that $\mathfrak{d} = (1)$. Thus the ideals $(x + \zeta^k y)$ are coprime. As the product of these ideals is $(z)^p$ and $\mathbb{Z}[\zeta]$ is a Dedekind domain, unique ideal factorisation holds so that each factor is a pth power. Then $(x + \zeta y) = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$. So $\mathfrak{a}^p$ is trivial in $C_{\mathbb{Q}(\zeta)}$ and as $p \nmid h = h(\mathbb{Q}(\zeta))$ we have $\mathfrak{a}$ trivial in $C_{\mathbb{Q}(\zeta)}$. Thus $\mathfrak{a}$ is principal, so $\mathfrak{a} = (t)$ for some $t \in \mathbb{Z}[\zeta]$. So there exists a unit $u \in \mathbb{Z}[\zeta]$ such that $x + \zeta y = ut^p$.

Writing $t = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}$ (not upto $p-1$ as it would become zero then) with $b_k \in \mathbb{Z}$ we get

$$t^p \equiv b_0^p + (b_1\zeta)^p + \cdots + (b_{p-2}\zeta^{p-2})^p \equiv b_0^p + b_1^p + \cdots + b_{p-2}^p \bmod p\mathbb{Z}[\zeta] \tag{2}$$

and hence $t^p \equiv \overline{t^p} \bmod p\mathbb{Z}[\zeta]$. By Lemma 5, we have $u/\overline{u} = \pm\zeta^k$ for some $o \leq k \leq p-1$. If $u/\overline{u} = \zeta^k$ then

$$\begin{aligned} x + \zeta y &= ut^p \\ &= \zeta^k \overline{u} t^p \\ &\equiv \zeta^k \overline{u}\overline{t^p} \bmod p\mathbb{Z}[\zeta] \\ &\equiv \zeta^k (x + \overline{\zeta} y) \bmod p\mathbb{Z}[\zeta]. \end{aligned}$$

Thus (using $\zeta^k\overline{\zeta} = \zeta^{k-1}$)

$$u/\overline{u} = \zeta^k \implies x + y\zeta - y\zeta^{k-1} - x\zeta^k \equiv 0 \bmod p\mathbb{Z}[\zeta]. \tag{3}$$

Similarly

$$u/\overline{u} = -\zeta^k \implies x + y\zeta + y\zeta^{k-1} + x\zeta^k \equiv 0 \bmod p\mathbb{Z}[\zeta]. \tag{4}$$

We'll now show that neither congruence holds for $0 \leq k \leq p-1$ and x, y coprime to p. As x, y are nonzero $\bmod p$ the above congruences appear to show linear dependence over $\mathbb{Z}/(p)$ among certain powers of ζ in $\mathbb{Z}[\zeta]/(p)$. But in $\mathbb{Z}[\zeta]/(p)$ the powers $1, \zeta, \ldots, \zeta^{p-2}$ are linearly independent over $\mathbb{Z}/(p)$ as

$$\mathbb{Z}[\zeta]/(p) \cong \mathbb{Z}[X]/(p, \Phi_p(X)) \cong (\mathbb{Z}/(p))[X]/\Phi_p(X) \cong (\mathbb{Z}/(p))[X]/(X-1)^{p-1},$$

and $\{1, X, \ldots, X^{p-2}\}$ is a basis of the last ring over $\mathbb{Z}/(p)$. For those $k \leq p-1$ such that $1, \zeta, \zeta^{k-1}, \zeta^k$ are distinct powers in the set $\{1, \zeta, \ldots, \zeta^{p-2}\}$ i.e. as long as $0, 1, k-1, k$ are distinct integers with $k \leq p-2$ the congruences in (3) and (4) both yield a contradiction. So for $3 \leq k \leq p-2$ there is a contradiction in case 1. Now it remains to check the remaining cases $k = 0, 1, 2, p-1$.

First, we may assume that $p \geq 5$ as the equation $x^3 + y^3 = z^3$ has no solutions in integers coprime to 3; even the congruence $x^3 + y^3 \equiv z^3 \bmod 9$ has no solutions in integers coprime to 3 as the cubes of units $\bmod 9$ are ± 1.

For $k = p-1$, in (3) the left side becomes

$$x(1 - \zeta^{p-1}) + y(\zeta - \zeta^{p-2}) = 2x + (x+y)\zeta + x(\zeta^2 + \cdots + \zeta^{p-3}) + (x-y)\zeta^{p-2}$$

which contradicts the linear independence of $1, \zeta, \ldots, \zeta^{p-2} \bmod p$ over $\mathbb{Z}/(p)$ by looking at the coefficient for ζ^2 (for example). A similar contradiction is reached for (4).

For $k = 0$, (3) becomes $y(\zeta - \zeta^{-1}) \equiv 0 \bmod p\mathbb{Z}[\zeta]$ and as $p \nmid y$ we can divide by it and get $\zeta^2 - 1 \equiv 0 \bmod p$ which contradicts the linear independence of 1 and $\zeta^2 \bmod p$ since $p \geq 5$. Similarly (4) becomes $2x\zeta + y\zeta^2 + y \equiv 0 \bmod p$ which is again a contradiction.

For $k = 2$ we get similar contradictions of linear independence. So we're left to check $k = 1$. For $k = 1$ (4) implies $(x+y)(1+\zeta) \equiv 0 \bmod p$ so $x + y \equiv 0 \bmod p\mathbb{Z}$ using Lemma 3. Thus $z^p = x^p + y^p \equiv (x+y)^p \bmod p$ so $p \mid z$. This contradicts our assumption $p \nmid xyz$. Finally, we need to show (3) leads to a contradiction.

Summarising our results so far, we have shown that if $x^p + y^p = z^p$ and $p \nmid xyz$ then $x + \zeta y = ut^p$ where $u/\overline{u} = \zeta$. Setting $k = 1$ in (3) yields

$$x(1 - \zeta) + y(\zeta - 1) \equiv 0 \bmod p. \tag{5}$$

Using Lemma 3, $p = u(1-\zeta)^{p-1}$ in (5) implies

$$x \equiv y \bmod (1-\zeta)^{p-2}.$$

Since $p - 2 \geq 1$ and $x, y \in \mathbb{Z}$ this forces $x \equiv y \bmod p\mathbb{Z}$. Observe that $x^p + y^p = z^p \iff x^p - z^p = -y^p$. So we can interchange y and $-z$ to get $x \equiv -z \bmod p\mathbb{Z}$, so

$$0 = x^p + y^p - z^p \equiv 3x^p \bmod p.$$

As $p \neq 3$ and $p \nmid x$ we have a contradiction. Thus, there are no integer solutions $xyz \neq 0$ to Fermat's equation for p being a regular prime not dividing xyz. ■

Approximately 61% of all primes are conjectured to be regular [2, pages 62-63] so the fact that FLT holds for regular primes is a very significant result.

References

[1] Keith Conrad. *Fermat's Last Theorem for Regular Primes*. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/fltreg.pdf (pages 6, 7).

[2] Lawrence Clinton Washington. *Introduction to Cyclotomic Fields*. Springer New York, NY, 1997 (pages 7, 8).

[3] Walter Fröhlich and Martin John Taylor. *Algebraic Number Theory*. Cambridge University Press, 1991.