Cyclotomic Integers, Regular Primes, & Fermat's Last Theorem

Rylie Platt and Lena Pang

MATH-371 — Number Theory (Dr. Anurag Agarwal)

Final Project

April 29, 2025

Introduction

In this paper, we introduce p-cyclotomic rings and ideals, and examine how they can be utilized to prove cases of Fermat's Last Theorem—a conundrum that took over 350 years to solve completely—when p is a regular prime.

History

In the late 1630's, Pierre de Fermat first conjectured that $x^n + y^n = z^n$ does not have nonzero integer solutions for x, y and z when $n > 2$, claiming he had a remarkable proof too large for his margin. This note was discovered after he passed; however, Fermat's own proof was never discovered for anything other than $n = 4$, leaving a mystery for mathematicians after his death.

For centuries, number theorists fought with Fermat's Last Theorem. Euler had an attempt for $n = 3$ that was flawed at first, but was eventually corrected. While proofs for specific exponents emerged over time, a general solution remained elusive.

In the 19th century, progress on the problem was made with Carl Friedrich Gauss's introduction of cyclotomic fields and Ernst Kummer's use of ideal numbers to handle factorization within them. Kummer eventually proved FLT for all regular primes by utilizing the ring $\mathbb{Z}[\zeta_p]$, where ζ_p is a primitive pth root of unity for an odd, regular prime p.

Despite the progress made by Gauss and Kummer, FLT was not solved in full until 1994 by Andrew Wiles, who proved FLT by linking elliptic curves and modular forms through the Modularity Theorem.

Even though the theorem has been fully proved, the mathematics developed in the pursuit of its solution, especially cyclotomic numbers and fields, continue to be fundamental in modern number theory research.

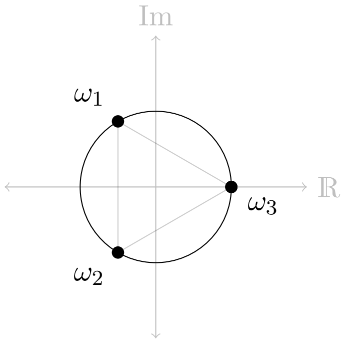
Background

Roots of 1

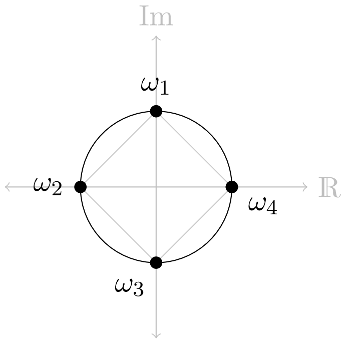
In the real numbers, the roots of 1 are $+1$ and -1. In the complex numbers, however, there are more options: the ***roots of unity***. The nth roots of unity are defined as:

$$U_n := \{\omega_k = e^{-2\pi i \times k/n} \mid 1 \leq k \leq n\}$$

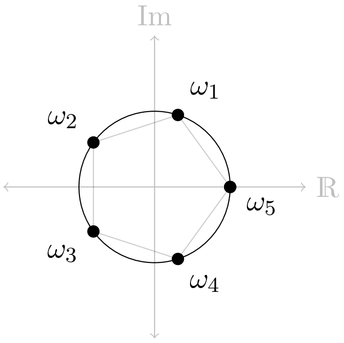
As depicted below, roots of unity can be visualized as equal subdivisions of the unit circle in the complex plane. Each set U_n is closed under multiplication, contains a unique multiplicative identity 1, and a unique multiplicative inverse ω_k^{-1} for each element ω_k.



3rd roots of unity (U_3)



4th roots of unity (U_4)



5th roots of unity (U_5)

A ***primitve root*** ζ (or for more specificity, ζ_p) can generate all the other roots; in other words, when multiplied by itself repeatedly, it produces all other ω_i in the set. In the diagram above, we can see $\omega_2 \in U_4$ is not a primitive root because $(\omega_2)^2 = (-1)^2 = 1$, so it cannot generate ω_1 or ω_3.

Another way to look at the nth roots of 1 are with ***cyclotomic polynomials***:

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - e^{i2\pi \times k/n}) = \prod (x - \zeta) \text{ where } \zeta \text{ is a primitive } n\text{th root of unity}$$

Every cyclotomic polynomial is monic, of degree $\varphi(n)$, and, most notably, irreducible in $\mathbb{Z}$. This gives us a way to factor the polynomial $x^n - 1$ for any n into irreducibles:

$$x^n - 1 = \prod_{d|n} \Phi_n(x)$$

As an example, $x^8 - 1 = (x^4+1)(x^2+1)(x+1)(x-1) = \Phi_8(x)\Phi_4(x)\Phi_2(x)\Phi_1(x)$.

Rings

A ***ring*** $(R, +, \times)$ is an algebraic structure consisting of a non-empty set of elements R with two binary operations—for consistency, referred to as addition $+$ and multiplication $\times$—that satisfy the following **Ring Axioms**:

I. $(R, +)$ is an abelian group: a nonempty set closed under addition, contains a unique additive identity, and a unique additive inverse for each element

II. Multiplication is associative: $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in R$

III. Multiplication is distributive (on both sides): $(a + b) \times c = (a \times c) + (b \times c)$ and $a \times (b + c) = (a \times b) + (a \times c)$ for all $a, b, c \in R$

Because it's a group under addition, there are additive inverses, but there need not be multiplicative inverses. If multiplication is commutative, we call R a ***commutative ring***. If there is unique factorization, we call R a ***unique factorization domain***, or UFD.

An ***ideal*** I is a subring (a subset of R that still fulfills all the axioms) where $ar \in I$ for all elements $r \in R, a \in I$. In other words, the subring is closed under multiplication with elements in the subring and elements not in the subring, though still in R. We can denote the ideal in terms of the generators: $I = \big(g_1, g_2, ...\big)$. An nonzero ideal $I \neq R$ is a ***prime ideal*** if and only if $I = JK \implies J = I$ or $K = I$ for any ideals $J, K \in R$, and any nonzero ideal can be written uniquely as a product of prime ideals (up to order).

We can use an ideal $I \subset R$ to make a ***quotient ring*** R/I, which, for simplicity, act like taking the ring elements "modded" by the ideal elements.

p-Cyclotomic Integers

In class, we've used ring extensions of the integers $\mathbb{Z}$ such as the quadratic integers $\mathbb{Z}[\sqrt{d}]$ and the Gaussian integers $\mathbb{Z}[i]$. In essence, this type of ***ring extension*** consists of introducing a new element α to an existing ring R to create a new, larger set:

$$R[\alpha] := \{c_n\alpha^n + ...c_1\alpha + c_0 \mid c_i \in R\}$$

This extension is called a ***polynomial ring*** in α over R, and may affect the primality and irreducibility of elements in the original ring R. For example, we saw that when we extend $\mathbb{Z}$ to $\mathbb{Z}[i]$, we get new primes: the Gaussian primes. Conversely, we saw that primes in $\mathbb{Z}$ of the form $4k+1$ are no longer prime in $\mathbb{Z}[i]$. We also introduced new units, $\pm i$.

Similarly, we can extend the integers to the ***p-cyclotomic integers*** $\mathbb{Z}[\zeta_p]$, where ζ_p is the primitive pth root of 1 for some odd prime p. Primes also change here. Notably, $p \in \mathbb{Z}[\zeta_p]$ is no longer prime, because $(1-\zeta_p), (1-\zeta_p)^2, ..., (1-\zeta_p)^{p-1} \mid p$, and all of these divisors are non-units. On the other hand, any element a where $a = bc \implies b$ or c is a unit is a ***cyclotomic prime***. Finally, $\mathbb{Z}[\zeta_p]$ is only a UFD when p is a ***regular prime***.

For the sake of brevity, we will not prove, but these are some important facts in $\mathbb{Z}[\zeta]$. First, $1+\zeta$ is a unit. $1-\zeta, 1-\zeta_p^2, ..., 1-\zeta^{p-1}$ are all associates. $p = u(1-\zeta)^{p-1}$ for some unit u. $\big(1-\zeta\big)$ is the only prime ideal in $\mathbb{Z}[\zeta]$ that divides p. And lastly, any unit u divided by its conjugate $\bar{u}$ is a root of unity.

Results

We consider cases of $x^n + y^n = z^n$ where the power is a regular prime, $p > 2$.

$$x^p + y^p = z^p \implies \left(\frac{x}{-y}\right)^p - 1 = \left(\frac{z}{-y}\right)^p \text{ because } p \text{ is odd}$$

This is similar to the first steps of the method of intersecting lines. But here, we notice the left hand side, $\left(\frac{x}{-y}\right)^p - 1$, is a cyclotomic polynomial in $\mathbb{Z}[\zeta]$, which we can expand to $\left(\frac{x}{-y}\right)^p - 1 = \left(\frac{x}{-y} - 1\right)\left(\frac{x}{-y} - \zeta\right) ... \left(\frac{x}{-y} - \zeta^{p-1}\right)$. Multiplying both sides by $-y^p$, we get:

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

Because p is a regular prime, unique factorization holds. Now we consider two cases where x, y, z are pairwise relatively prime integers: $p \nmid xyz$, and $p \mid xyz$.

Case 1: $p \nmid xyz$

Reconsidering the factors we got as ideals, we get $\big(z\big)^p = \prod \big(x+\zeta^i y\big)$. Now we examine any possible common ideal factors, denoted D, of $\big(x+\zeta^k y\big)$ and $\big(x+\zeta^l y\big)$ for some $0 \le k \le l < p$. By the rules of divisibility, D will also be a factor of the difference of the two:

$$x + \zeta^k y - (x + \zeta^l y) = \zeta^k y(1 - \zeta^{l-k}) = uy(1 - \zeta) \text{ for some unit } u$$

Because $D \mid uy(1-\zeta)$ and $\big(1-\zeta\big) \mid p \implies y\big(1-\zeta\big) \mid yp$, it must be that D divides the ideal $\big(yp\big)$. We know D also divides the product, $\big(z\big)^p$, but because $\gcd(yp, z^p) = 1$, this forces D to be the unit ideal. Thus the ideals $\big(x + \zeta^i y\big)$ are pairwise relatively prime.

Because the product of the ideals is $\big(z\big)^p$, it must be that each ideal $\big(x + \zeta^i y\big) = \mathfrak{a}_i^p$ for some ideal $\mathfrak{a}_i$. So $\big(a_i\big)$ is trivial in the class group of $\mathbb{Q}[\zeta]$. Because p is a regular prime, that means $\mathfrak{a}_i$ is principal, with generator $a_i \in \mathbb{Z}[\zeta]$. So we get $x + \zeta^i y = ua_i^p$.

Looking more closely at a_i, we can write an expansion in $\mathbb{Z}[\zeta]$:

$$a_i = b_{p-1}\zeta^{p-2} + ... + b_1\zeta + b_0$$

$$a_i^p \equiv b_{p-2} + ... + b_1 + b_0 \pmod{p\mathbb{Z}[\zeta]}$$

Because each unit divided by its conjugate is $\pm\zeta^k$ for some $0 \le k \le p-1$, then:

$$x + \zeta^i y = ua_i^p = \pm\zeta^k \bar{u} a_i^p$$

$$\implies x + \zeta^i y \equiv \pm\zeta^k \bar{u}\bar{a}_i{}^p \equiv \pm\zeta^k(x + \bar{\zeta}y) \pmod{p\mathbb{Z}[\zeta]}$$

$$\implies x + \zeta^i y \mp (y\zeta^{k-i} + x\zeta^k) \equiv 0 \pmod{p\mathbb{Z}[\zeta]} \qquad (1)$$

We consider the quotient ring (essentially equivalent to our mod above):

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

In the last isomorphic ring, $\{1, X, ..., X^{p-2}\}$ form a basis, but a linear combination of any basis elements cannot be equivalent to zero without zero coefficients, so we get a contradiction in eq. (1).

Case 2: $p \mid xyz$

Because x, y, z are relatively prime, that means p divides exactly one of them. Without loss of generality, let $p \mid z$, so $z^p = p^k \hat{z}^p$ for some $k \geq 1$ and $\hat{z}$ relatively prime to p. Because $p^k = u(1-\zeta)^{pk(p-1)}$ for some unit u, we combine with our original equality to get:

$$\prod \big(x + \zeta^i y\big) = u\big(1-\zeta\big)^{pk}\big(\hat{z}\big)^p \text{ where each } \big(x + \zeta^i y\big) \text{ may not be relatively prime}$$

We examine the quotient rings $\mathbb{Z}[\zeta]/\big(1-\zeta\big)$ and $\mathbb{Z}[\zeta]/\big(1-\zeta\big)^2$, noting that there are p multiples of $\big(1-\zeta\big)$ in $\mathbb{Z}[\zeta]/\big(1-\zeta\big)^2$.

We observe that $x + \zeta^i y \equiv x + y \mod \big(1-\zeta\big)$ for any $1 \leq i \leq p-1$. Because we've let the prime ideal $\big(1-\zeta\big)$ divide $\big(z\big)^p$, then $\big(1-\zeta\big)$ must divide some factor on the left as well. Because all factors on the left are equivalent $\mathrm{mod}\big(1-\zeta\big)$, that means $\big(1-\zeta\big)$ divides all of them. Now we move to $\mathbb{Z}[\zeta]/\big(1-\zeta\big)^2$.

Assume $x + \zeta^i y \not\equiv 0 \mod \big(1-\zeta\big)^2$. So $x + \zeta^i y$ reduces to some nonzero multiple of $1-\zeta \mod \big(1-\zeta\big)^2$. With the results above, we know that there are p multiples of $1-\zeta$ in $\mathbb{Z}[\zeta]/\big(1-\zeta\big)^2$, which means it must be that $x + \zeta^i y \equiv x + \zeta^j y$ for some $0 \leq i \leq j \leq p-1$. So $(1-\zeta^{j-i})y \equiv 0 \mod \big(1-\zeta\big)^2$. However, $1-\zeta^{k-i}$ is an associate of $1-\zeta$, which forces $1-\zeta$ to divide y, a contradiction. Thus $x + \zeta^i y \equiv 0 \mod \big(1-\zeta\big)^2$.

This sets a lower bound of $k \geq 2$.

Then there is some unique i_0 such that $x + \zeta^{i_0} y \equiv 0 \mod \big(1-\zeta\big)^2$. We replace $y := \zeta^{i_0} y$, so we can now say $x + y \equiv 0 \mod \big(1-\zeta\big)^2$, and $x + \zeta^i y \not\equiv 0 \mod \big(1-\zeta\big)^2$. Any common ideal divisor of x, y will be of the form $\big(x, y\big)\big(1-\zeta\big)$. D is the same for any i, so the complement $\big(c_i\big)$ must be a pth power and not divisible by $\big(1-\zeta\big)$:

$$\big(x + \zeta^i y\big) = \big(x, y\big)\big(1-\zeta\big)\big(c_i\big)_i^p \text{ and } \big(x + y\big) = \big(x, y\big)\big(1-\zeta\big)^{kp-(p-1)}\big(c_0\big)^p$$

We then observe that $\big(c_i\big)^p\big(c_0\big)^{-p}$ is a principal fractional ideal, and since p is regular, $\big(c_i\big)\big(c_0\big)^{-1}$ is also a fractional ideal. So $\big(c_i\big)\big(c_0\big)^{-1} = t_i\mathbb{Z}[\zeta]$ for some $t_i \in \mathbb{Q}(\zeta)^\times$ that is relatively prime to $1-\zeta$. So we can rewrite ideals with elements:

$$\big(x+\zeta^i y\big)\big(x+y\big)^{-1} = \big(t_i\big)^p(1-\zeta)^{-p(k-1)} \text{ becomes } \frac{x+\zeta^i y}{x+y} = \frac{b_i t_i^p}{(1-\zeta)^{p(k-1)}}$$

Then we consider the equation:

$$\zeta(x+\bar{\zeta}y) + (x+\zeta y) - (1+\zeta)(x+y) = 0$$

$$\implies \frac{\zeta b_{p-1}t_{p-1}^p}{(1-\zeta)^{p(k-1)}} + \frac{b_1 t_1^p}{(1-\zeta)^{p(k-1)}} - (1+\zeta) = 0$$

$$\implies \zeta b_{p-1}t_{p-1}^p + b_1 t_1^p - (1+\zeta)(1-\zeta)^{p(k-1)} = 0$$

If we reconsider $t_i = m_i/n_i$ for $m_i, n_i \in \mathbb{Z}[\zeta]$, we can factor out any powers of $1-\zeta$ in m_i, n_i to produce rational numbers $c_0, c_1, c_{p-1} \in \mathbb{Z}[\zeta]$ that are relatively prime to $\big(1-\zeta\big)$:

$$\zeta b_{p-1}c_{p-1}^p + b_1 c_1^p - (1+\zeta)(1-\zeta)^{p(k-1)}c_0^p = 0$$

$$\implies c_{p-1}^p + \frac{b_1}{\zeta b_{p-1}}c_1^p - \frac{1+\zeta}{\zeta b_{p-1}}(1-\zeta)^{p(k-1)}c_0^p = 0$$

$$\implies c_{p-1}^p + \frac{b_1}{\zeta b_{p-1}}c_1^p \equiv 0 \mod p\mathbb{Z}[\zeta]$$

$$\implies \frac{b_1}{\zeta b_{p-1}} \equiv \frac{c_{p-1}^p}{c_1^p} \mod p\mathbb{Z}[\zeta]$$

Because c_{p-1}^p and c_1^p are both rational numbers, their quotient is a rational number, and thus $\frac{b_1}{\zeta b_{p-1}}$ is a rational number. By Kummer's Lemma, which states that a unit u is the pth power of some $m \in \mathbb{Z}$ if $u \equiv m \pmod{p\mathbb{Z}[\zeta]}$ when p is a regular prime, we can replace $\frac{b_1}{\zeta b_{p-1}}$ with 1:

$$c_{p-1}^p + c_1^p - \frac{1+\zeta}{\zeta b_{p-1}}(1-\zeta)^{p(k-1)}c_0^p = 0$$

Here, $k-1 \geq 1$, whereas we previously had $k \geq 2$, a contradiction by descent.

Thus there are no nonzero integer solutions for $x^p + y^p = z^p$ when p is a regular prime.

Applications

0.1 Basic "Toy" Example: $p = 3$

Proof. The equation $x^3 + y^3 = z^3$ has no solutions where x, y, and z are non-zero integers.

Consider this problem generalized to the ring of Eisenstein Integers;
$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}, \omega = e^{2\pi i/3}\}$ (in other words, ω is a primitive third root of unity).

Assume that there exists a solution, (ξ, η, ψ) to $\xi^3 + \eta^3 + \psi^3 = 0$ where ξ, η, ψ are non-zero Eisenstein integers and pairwise co-prime.

Let $\lambda = 1 + 2\omega = -i\sqrt{3}$ be a prime element in $\mathbb{Z}[\omega]$ with norm $N(\lambda) = 3$. If $\alpha \in \mathbb{Z}[\omega]$ and $\lambda \nmid \alpha$, then $\alpha^3 \equiv \pm 1 \pmod{\lambda^4}$. Considering $\xi^3 + \eta^3 + \psi^3 = 0 \pmod{\lambda^4}$, there is exactly one of ξ, η, ψ that must be divisible by λ let ξ be that value.

Let $\xi = \lambda^n \gamma$, where $\lambda \nmid \gamma$ and $n \geq 1$. Substituting $\kappa = -\eta$, the equation becomes:

$$\epsilon \lambda^{3n} \gamma^3 = \kappa^3 - \psi^3$$

where ϵ is a unit, and $\lambda \nmid \gamma, \kappa, \psi$, with γ, κ, ψ pairwise co-prime.

Considering the equation mod λ^4, we know $\kappa^3 - \psi^3 \equiv 0 \pmod{\lambda^4}$, which implies $n \geq 2$. Next we must factor the right-hand side:

$$\epsilon \lambda^{3n} \gamma^3 = (\kappa - \psi)(\kappa - \psi\omega)(\kappa - \psi\omega^2)$$

We also know the GCD of any two factors on the right is λ. The factors are pairwise co-prime after dividing by λ which means we have

$$\kappa - \psi = \epsilon_1 \lambda \nu_1^3 \quad \kappa - \psi\omega = \epsilon_2 \lambda \nu_2^3 \quad \kappa - \psi\omega^2 = \epsilon_3 \lambda \nu_3^3$$

where $\epsilon_1, \epsilon_2, \epsilon_3$ are units and ν_1, ν_2, ν_3 are pairwise co-prime.

Comparing powers of λ we find $\nu_1 = \lambda^{n-1}\gamma_1$ with $\lambda \nmid \gamma_1$ and $n - 1 \geq 1$. Considering the linear combination: $(\kappa - \psi) + \omega(\kappa - \psi\omega) + \omega^2(\kappa - \psi\omega^2) = 0$, we can substitute ν_1 giving us

$$\epsilon_1 \lambda \nu_1^3 + \epsilon_4 \lambda \nu_2^3 + \epsilon_5 \lambda \nu_3^3 = 0, \qquad \text{where } \epsilon_4 = \epsilon_2 \omega \text{ and } \epsilon_5 = \epsilon_3 \omega^2$$

We can then substitute $\nu_1\lambda^{n-1}\gamma_1$ and divide the equation by $\epsilon_5\lambda$ which after some rearrangements leaves us with

$$\epsilon_6\lambda^{3(n-1)}\gamma_1^3 = \epsilon_7\nu_2^3 - \nu_3^3, \qquad \text{where } \epsilon_6, \epsilon_7 \text{ are units}$$

Consider our problem mod λ^3. Since $n \geq 2$ the left side is congruent to 0 mod λ^3. Any Eulerian integer is congruent to exactly one of $0, 1, -1 \pmod{\lambda}$ and they cannot be congruent to 0 therefore $\lambda \nmid \nu_2$ and $\lambda \nmid \nu_3$ so we have $\nu_2^3 \equiv \pm 1 \pmod{\lambda^3}$ and $\nu_3^3 \equiv \pm 1 \pmod{\lambda^3}$ Which leaves us with

$$0 \equiv \epsilon_7(\pm 1) - (\pm 1) \pmod{\lambda^3}$$

This means $\lambda_3 \mid \epsilon_7 \pm 1$. The norm $N(\lambda^3) = 27$ so the norm of $\epsilon_7 - 1$ or $\epsilon_7 + 1$ must be a multiple of 27. After checking the units $\epsilon_7 = \pm 1, \pm\omega, \pm\omega^2$ only $\epsilon_7 = 1$ or $\epsilon_7 = -1$ makes this possible. Therefore, we can write the equation as:

$$\epsilon_6\lambda^{3(n-1)}\gamma_1^3 = (\pm\nu_2)^3 - \nu_3^3$$

This shows that we have found another solution of the same form but with the power of λ reduced from n to $n-1$ which leads to an infinite descent which is impossible for a positive integer n. The contradiction implies that our initial assumption of a non-trivial solution is false. Therefore, the equation $x^3 + y^3 = z^3$ has no solutions in non-zero integers. ■

0.2 Complex Example (Larger Number): $k = 13$

Proof. **Theorem:** $x^{13} + y^{13} = x^{13}$ has no solutions in non-zero integers x,y,z.

We must consider two cases, $13 \nmid x, y, z$ and $13 \mid x, y, z$ given that x,y,z are pairwise relatively prime.

First we can divide the entire equation by $-y^{13}$ which leaves us with; $\frac{x^{13}}{-y^{13}} - 1 = \frac{z^{13}}{-y^{13}}$. The left-hand side of this equation is a Cyclotomic polynomial that can be factored out and then multiplied by $-y^{13}$ to get the factors in the ring $\mathbb{Z}[\zeta_{13}]$.

$$\frac{x^{13}}{-y^{13}} - 1 = x^{13} + y^{13} = (x+y)(x+\zeta_{13}y)(x+\zeta_{13}^2 y)...(x+\zeta_{13}^{12}y) = z^{13}$$

Case 1: Each of the factors $(x+\zeta_{13}^i y)$ is an ideal in $\mathbb{Z}[\zeta_{13}]$ and pairwise relatively prime. If a prime ideal $\mathfrak{p}$ divided two of them, it would divide their difference, leading to $\mathfrak{p} \mid (y(1-\zeta_{13}))$ and $\mathfrak{p} \mid (x(1-\zeta_{13}))$. Since $13 \nmid xy$, $\mathfrak{p}$ must divide $(1-\zeta_{13})$. However, this would imply $(1-\zeta_{13})$ divides all factors, leading to $13 \mid z$, a contradiction.

Since the ideals are pairwise relatively prime and their product is $\big(z\big)^{13}$ each ideal is the 13th power of some ideal $\mathfrak{a}_i$ such that $(x+\zeta_{13}^i y)=\mathfrak{a}_i^{13}$. 13 is a regular prime, so any ideal whose 13th power is principal is itself principal, therefore $\mathfrak{a}_i=(a_i)$ for some $a_i \in \mathbb{Z}[\zeta_{13}]$, and $x+\zeta_{13}^i y = u_i a_i^{13}$ for some unit $u_i \in \mathbb{Z}[\zeta_{13}]$

Consider $x+\zeta_{13}y = ua^{13}$. Mod 13 a^{13} behaves like an integer. Units mod 13 involve roots of unity. There is a congruence $x+\zeta_{13}y \equiv (\text{unit}) \times (\text{integer}) \pmod{13\mathbb{Z}[\zeta_{13}]}$. By relating this to its conjugate $x+\zeta_{13}^{-1}y$, we get a linear combination of powers of ζ_{13} with integer coefficients being congruent to zero $\pmod{13\mathbb{Z}[\zeta_{13}]}$:

$$x(1 \pm \zeta_{13}^k) + y(\zeta_{13} \pm \zeta_{13}^{k-1}) \equiv 0 \pmod{13\mathbb{Z}[\zeta_{13}]}.$$

Since $\{1, \zeta_{13}, \ldots, \zeta_{13}^{11}\}$ are linearly independent over $\mathbb{Z}/13\mathbb{Z}$, all these integer coefficients must be divisible by 13, which contradicts $13 \nmid x, y$.

Case 2: Since x, y, z are pairwise co-prime, 13 divides one of them. Assume $13 \mid z$. This implies $13 \nmid x$ and $13 \nmid y$. Let $z = 13^k \hat{z}$ with $k \geq 1$ and $13 \nmid \hat{z}$.

Let $\zeta = e^{2\pi i/13}$. In the ring $\mathbb{Z}[\zeta]$, the ideal $\mathfrak{p} = (1-\zeta)$ is prime and $13\mathbb{Z}[\zeta] = \mathfrak{p}^{12}$. When factored, $z^{13} = \prod_{i=0}^{12}(x+\zeta^i y)$. Since $13 \mid z$, $\mathfrak{p} \mid z$. Thus $\mathfrak{p}^{156k} \mid (z)^{13} = \prod(x+\zeta^i y)$. As $x+\zeta^i y \equiv x+y \pmod{\mathfrak{p}}$, if $\mathfrak{p}$ divides one factor, it divides all. So, $\mathfrak{p} \mid (x+\zeta^i y)$ for all i.

The gcd of distinct ideal factors is $\gcd((x+\zeta^i y),(x+\zeta^j y)) = \mathfrak{p}$ (since $\gcd(x,y)=1$ and $13 \nmid x, y$).

Let $\nu_{\mathfrak{p}}(\alpha)$ be the exponent of $\mathfrak{p}$ in the prime factorization of the ideal (α). Exactly one factor has $\nu_{\mathfrak{p}} > 1$. Assume that this factor is $x+y$. Then $\nu_{\mathfrak{p}}(x+y) = 156k-12$ and $\nu_{\mathfrak{p}}(x+\zeta^i y) = 1$ for $i = 1, \ldots, 12$ assuming $k \geq 2$.

This gives the ideal factorizations: $(x+y) = \mathfrak{p}^{156k-12}\mathfrak{c}_0^{13}$ $(x+\zeta^i y) = \mathfrak{p}\mathfrak{c}_i^{13}$ for $i = 1, \ldots, 12$. The ideals $\mathfrak{c}_i$ are pairwise co-prime and co-prime to $\mathfrak{p}$. Since $p = 13$ is regular, the ideals $\mathfrak{c}_i$ must be principal. Let $\mathfrak{c}_i = (\gamma_i)$ for $\gamma_i \in \mathbb{Z}[\zeta]$ co-prime to $1-\zeta$.

This gives us the element equations: $x+y = \epsilon_0(1-\zeta)^{156k-12}\gamma_0^{13}$ $x+\zeta^i y = \epsilon_i(1-\zeta)\gamma_i^{13}$ for $i = 1, \ldots, 12$, where ϵ_i are units. Using the identity $\zeta(x+\zeta^{-1}y)+(x+\zeta y)-(1+\zeta)(x+y) = 0$, substituting the element relations (for $i = 1, 12$), and dividing by $(1-\zeta)$ gives us:

$$\zeta\epsilon_{12}\gamma_{12}^{13} + \epsilon_1\gamma_1^{13} - (1+\zeta)\epsilon_0(1-\zeta)^{156k-13}\gamma_0^{13} = 0$$

Let $b_1 = \epsilon_1/\epsilon_{12}$, $c_1 = \gamma_1$, $c_{12} = \gamma_{12}$, $c_0 = \gamma_0$. Through some substitutions we get:

$$\zeta c_{12}^{13} + b_1 c_1^{13} - (\text{unit}) \times (1+\zeta)(1-\zeta)^{13(k-1)} c_0^{13} = 0$$

Consider this equation modulo $13\mathbb{Z}[\zeta] = \mathfrak{p}^{12}$. Since $k \geq 2$, $13(k-1) \geq 13$. The last term vanishes as $(1-\zeta)^{13(k-1)}$ is divisible by $\mathfrak{p}^{13}$, and therefore by 13.

$\zeta c_{12}^{13} + b_1 c_1^{13} \equiv 0 \pmod{13\mathbb{Z}[\zeta_{13}]}$. Let $U = b_1/\zeta$, so U is a unit. $c_{12}^{13} + U c_1^{13} \equiv 0 \pmod{13\mathbb{Z}[\zeta_{13}]}$. By Fermat's Little Theorem ($a^{13} \equiv a \pmod{13}$ in $\mathbb{Z}[\zeta]$): $c_{12} + U c_1 \equiv 0 \pmod{13\mathbb{Z}[\zeta_{13}]}$.

So $U \equiv -c_{12}c_1^{-1} \pmod{13\mathbb{Z}[\zeta_{13}]}$. U is congruent to a rational integer modulo 13. By Kummer's Lemma for the regular prime $p = 13$, this implies $U = \eta^{13}$ for some unit η. Assuming $U = 1$, the equation before reduction becomes:

$$c_{12}^{13} + c_1^{13} = (\text{unit})' \times (1+\zeta)(1-\zeta)^{13(k-1)} c_0^{13}$$

This final equation relates 13-th powers in a form similar to the original equation. The factor $(1-\zeta)^{13(k-1)}$ contains 13^{k-1} which suggests a descent mechanism with $k-1 \geq 1$, whereas we previously had $k \geq 2$, a contradiction by descent.

Therefore, the initial assumption of a non-trivial integer solution must be false. ■

Conclusion

The rings of p-cyclotomic integers and their ideals prove that the diophantine equation, $x^p + y^p = z^p$, has no integer solutions when p is a regular prime. Delving into more general cases of Fermat's Last Theorem would require intricate knowledge of modular semistable elliptic curves over $\mathbb{Q}$, which is just a bit out of our depth—but with approximately 61% of primes being regular, we've definitely made a solid start.

References

Conrad, K. (1999). *Fermat's Last Theorem for Regular Primes.* University of Connecticut. https://kconrad.math.uconn.edu/blurbs/gradnumthy/fltreg.pdf

Dummit, D., Foote, R. (2004). *Abstract Algebra* (3rd Ed.). John Wiley and Sons, Inc.

Freud, R., Gyarmati, E. (2010). *Number Theory.* American Mathematical Society.

Grosswald, E. (2009). *Topics from the Theory of Numbers.* Birkhauser Boston.

Ozaki, M. (1997). Kummer's lemma for Zp-extensions over totally real number fields. *Acta Arithmetica, 81, no. 1*, 37–44. http://matwbn.icm.edu.pl/ksiazki/aa/aa81/aa8114.pdf

Ribenboim, P. (1999). *Fermat's Last Theorem for Amateurs.* Springer-Verlag.

Ribenboim, P. (1996). *The New Book of Prime Number Records.* Springer Science+ Business Media.

Ribenboim, P. (1979). *13 Lectures on Fermat's Last Theorem.* Springer-Verlag.

Rubin, K., Silverberg, A. *Wiles' Proof of Fermat's Last Theorem.* https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4974d9c3dc8d1b56193e9d5f868d6b0ded0f62fe

Washington, L. (1992). Kummer's Lemma for Prime Power Cyclotomic Fields. *Journal of Number Theory, 40* 165-173. https://core.ac.uk/download/pdf/81217125.pdf

Wiles, A. (1995). Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics, 142*, 443-551. https://staff.fnwi.uva.nl/a.l.kret/Galoistheorie/wiles.pdf