Formalising Fermat's Last Theorem for Exponent 3 in Lean

Pietro Monticone

Department of Mathematics, University of Trento

May 14, 2024

Contents

Introduction

Chapter 1

Preliminaries

1.1 Notation

Symbol	Description
$\neg$	Logical negation
$\top$	Logical truth / Tautology
$\bot$	Logical falsehood / Contradiction
$\wedge$	Logical conjunction
$\vee$	Logical inclusive disjunction
$:=$	Definition
$\forall$	Universal quantification
$\exists$	Existential quantification
$\exists!$	Unique existential quantification
$\mathbb{N}$	Set of natural numbers
$\mathbb{Z}$	Set of integer numbers
$\mathbb{Z}_n$	Set of integers modulo n
$\mathbb{Q}$	Set of rational numbers
X/Y	Field extension
$[Y : X]$	Degree of field extension
$\times$	Cartesian product
$[n]$	Equivalence class of n
$\mid$	Divisibility relation
$\nmid$	Negation of divisibility relation
gcd	Greatest common divisor
ζ_n	Primitive n-th root of unity

1.2 Definitions

Definition 1.1 (Monoid)**.**
Let X be a non-empty set.
Let $\circ : X \times X \to X$ be an internal composition law on X.

A *monoid* is a pair $\mathcal{M} := (X, \circ)$ satisfying:

(A) $\forall x, y, z \in X,\ (x \circ y) \circ z = x \circ (y \circ z) = x \circ y \circ z$

(N) $\exists e \in X : \forall x \in X,\ x \circ e = e \circ x = x$

Definition 1.2 (Commutative Monoid)**.**
Let X be a non-empty set.
Let $\circ : X \times X \to X$ be an internal composition law on X.

A *commutative monoid* is a pair $\mathcal{M}_c := (X, \circ)$ satisfying:

(A) $\forall x, y, z \in X,\ (x \circ y) \circ z = x \circ (y \circ z) = x \circ y \circ z$

(N) $\exists e \in X : \forall x \in X,\ x \circ e = e \circ x = x$

(C) $\forall x, y \in X,\ x \circ y = y \circ x$

Definition 1.3 (GCD Monoid)**.**
Let X be a non-empty set.
Let $\circ : X \times X \to X$ be an internal composition law on X.

A *gcd monoid* is a pair $\mathcal{M}_{\text{gcd}} := (X, \circ)$ satisfying:

(A) $\forall x, y, z \in X,\ (x \circ y) \circ z = x \circ (y \circ z) = x \circ y \circ z$

(N) $\exists e \in X : \forall x \in X,\ x \circ e = e \circ x = x$

(C) $\forall x, y \in X,\ x \circ y = y \circ x$

(G) $\forall x, y \in X,\ \exists d \in X : (d \mid x) \wedge (d \mid y) \wedge (\forall c \in X,\ c \mid x \wedge c \mid y \Rightarrow c \mid d)$

Definition 1.4 (Group)**.**
Let X be a non-empty set.
Let $\circ : X \times X \to X$ be an internal composition law on X.

A *group* is a pair $\mathcal{G} := (X, \circ)$ satisfying:

(A) $\forall x, y, z \in X,\ (x \circ y) \circ z = x \circ (y \circ z) = x \circ y \circ z$

(N) $\exists e \in X : \forall x \in X,\ x \circ e = e \circ x = x$

(I) $\forall x \in X,\ \exists x' \in X : x \circ x' = x' \circ x = e$

Definition 1.5 (Commutative Group)**.**
Let X be a non-empty set.
Let $\circ : X \times X \to X$ be an internal composition law on X.

A *commutative group* is a pair $\mathcal{G}_c := (X, \circ)$ satisfying:

(A) $\forall x, y, z \in X,\ (x \circ y) \circ z = x \circ (y \circ z) = x \circ y \circ z$

(N) $\exists e \in X : \forall x \in X,\ x \circ e = e \circ x = x$

(I) $\forall x \in X,\ \exists x' \in X : x \circ x' = x' \circ x = e$

(C) $\forall x, y \in X,\ x \circ y = y \circ x$

Definition 1.6 (Semiring)**.**
Let X be a non-empty set.
Let $+ : X \times X \to X$ be an additive internal composition law on X.
Let $\cdot : X \times X \to X$ be a multiplicative internal composition law on X.

A *semiring* is a triple $\mathcal{S} := (X, +, \cdot)$ satisfying:

(A1) $\forall x, y, z \in X,\ (x + y) + z = x + (y + z) = x + y + z$

(C1) $\forall x, y \in X,\ x + y = y + x$

(N1) $\exists 0 \in X : \forall x \in X,\ x + 0 = 0 + x = x$

(A2) $\forall x, y, z \in X,\ (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y \cdot z$

(N2) $\exists 1 \in X : \forall x \in X,\ x \cdot 1 = 1 \cdot x = x$

(D1) $\forall x, y, z \in X,\ x \cdot (y + z) = x \cdot y + x \cdot z$

(D2) $\forall x, y, z \in X,\ (x + y) \cdot z = x \cdot z + y \cdot z$

Definition 1.7 (Commutative Semiring)**.**
Let X be a non-empty set.
Let $+ : X \times X \to X$ be an additive internal composition law on X.
Let $\cdot : X \times X \to X$ be a multiplicative internal composition law on X.

A *commutative semiring* is a triple $\mathcal{S}_c := (X, +, \cdot)$ satisfying:

(A1) $\forall x, y, z \in X,\ (x + y) + z = x + (y + z) = x + y + z$

(C1) $\forall x, y \in X,\ x + y = y + x$

(N1) $\exists 0 \in X : \forall x \in X,\ x + 0 = 0 + x = x$

(A2) $\forall x, y, z \in X,\ (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y \cdot z$

(C2) $\forall x, y \in X,\ x \cdot y = y \cdot x$

(N2) $\exists 1 \in X : \forall x \in X,\ x \cdot 1 = 1 \cdot x = x$

(D1) $\forall x, y, z \in X,\ x \cdot (y + z) = x \cdot y + x \cdot z$

(D2) $\forall x, y, z \in X,\ (x + y) \cdot z = x \cdot z + y \cdot z$

Definition 1.8 (Ring)**.**
Let X be a non-empty set.
Let $+ : X \times X \to X$ be an additive internal composition law on X.
Let $\cdot : X \times X \to X$ be a multiplicative internal composition law on X.

A *ring* is a triple $\mathcal{R} := (X, +, \cdot)$ satisfying:

(A1) $\forall x, y, z \in X,\ (x + y) + z = x + (y + z) = x + y + z$

(C1) $\forall x, y \in X,\ x + y = y + x$

(N1) $\exists 0 \in X : \forall x \in X,\ x + 0 = 0 + x = x$

(I1) $\forall x \in X,\ \exists (-x) \in X : x + (-x) = (-x) + x = 0$

(A2) $\forall x, y, z \in X,\ (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y \cdot z$

(N2) $\exists 1 \in X : \forall x \in X,\ x \cdot 1 = 1 \cdot x = x$

(D1) $\forall x, y, z \in X,\ x \cdot (y + z) = x \cdot y + x \cdot z$

(D2) $\forall x, y, z \in X,\ (x + y) \cdot z = x \cdot z + y \cdot z$

Definition 1.9 (Commutative Ring)**.**
Let X be a non-empty set.
Let $+ : X \times X \to X$ be an additive internal composition law on X.
Let $\cdot : X \times X \to X$ be a multiplicative internal composition law on X.

A *commutative ring* is a triple $\mathcal{R}_c := (X, +, \cdot)$ satisfying:

(A1) $\forall x, y, z \in X,\ (x + y) + z = x + (y + z) = x + y + z$

(C1) $\forall x, y \in X,\ x + y = y + x$

(N1) $\exists 0 \in X : \forall x \in X,\ x + 0 = 0 + x = x$

(I1) $\forall x \in X,\ \exists (-x) \in X : x + (-x) = (-x) + x = 0$

(A2) $\forall x, y, z \in X,\ (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y \cdot z$

(C2) $\forall x, y \in X,\ x \cdot y = y \cdot x$

(N2) $\exists 1 \in X : \forall x \in X,\ x \cdot 1 = 1 \cdot x = x$

(D1) $\forall x, y, z \in X,\ x \cdot (y + z) = x \cdot y + x \cdot z$

(D2) $\forall x, y, z \in X,\ (x + y) \cdot z = x \cdot z + y \cdot z$

Definition 1.10 (Domain)**.**
Let X be a non-empty set.
Let $+ : X \times X \to X$ be an additive internal composition law on X.
Let $\cdot : X \times X \to X$ be a multiplicative internal composition law on X.

A *domain* is a triple $\mathcal{D} := (X, +, \cdot)$ satisfying:

(A1) $\forall x, y, z \in X,\ (x + y) + z = x + (y + z) = x + y + z$

(C1) $\forall x, y \in X,\ x + y = y + x$

(N1) $\exists 0 \in X : \forall x \in X,\ x + 0 = 0 + x = x$

(I1) $\forall x \in X,\ \exists (-x) \in X : x + (-x) = (-x) + x = 0$

(A2) $\forall x, y, z \in X,\ (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y \cdot z$

(N2) $\exists 1 \in X : \forall x \in X,\ x \cdot 1 = 1 \cdot x = x$

(D1) $\forall x, y, z \in X,\ x \cdot (y + z) = x \cdot y + x \cdot z$

(D2) $\forall x, y, z \in X,\ (x + y) \cdot z = x \cdot z + y \cdot z$

(Z2) $\forall x, y \in X,\ x \cdot y = 0 \Rightarrow x = 0 \lor y = 0$

Definition 1.11 (Commutative Domain)**.**
Let X be a non-empty set.
Let $+ : X \times X \to X$ be an additive internal composition law on X.
Let $\cdot : X \times X \to X$ be a multiplicative internal composition law on X.

A *commutative* or *integral domain* is a triple $\mathcal{D}_c := (X, +, \cdot)$ satisfying:

(A1) $\forall x, y, z \in X,\ (x + y) + z = x + (y + z) = x + y + z$

(C1) $\forall x, y \in X,\ x + y = y + x$

(N1) $\exists 0 \in X : \forall x \in X,\ x + 0 = 0 + x = x$

(I1) $\forall x \in X,\ \exists (-x) \in X : x + (-x) = (-x) + x = 0$

(A2) $\forall x, y, z \in X,\ (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y \cdot z$

(C2) $\forall x, y \in X,\ x \cdot y = y \cdot x$

(N2) $\exists 1 \in X : \forall x \in X,\ x \cdot 1 = 1 \cdot x = x$

(D1) $\forall x, y, z \in X,\ x \cdot (y + z) = x \cdot y + x \cdot z$

(D2) $\forall x, y, z \in X,\ (x + y) \cdot z = x \cdot z + y \cdot z$

(Z2) $\forall x, y \in X,\ x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$

Definition 1.12 (Field)**.**
Let X be a non-empty set.
Let $+ : X \times X \to X$ be an additive internal composition law on X.
Let $\cdot : X \times X \to X$ be a multiplicative internal composition law on X.

A *field* is a triple $\mathbb{F} := (X, +, \cdot)$ satisfying:

(A1) $\forall x, y, z \in X,\ (x + y) + z = x + (y + z) = x + y + z$

(C1) $\forall x, y \in X,\ x + y = y + x$

(N1) $\exists 0 \in X : \forall x \in X,\ x + 0 = 0 + x = x$

(I1) $\forall x \in X,\ \exists (-x) \in X : x + (-x) = (-x) + x = 0$

(A2) $\forall x, y, z \in X,\ (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y \cdot z$

(N2) $\exists 1 \in X : \forall x \in X,\ x \cdot 1 = 1 \cdot x = x$

(I2) $\forall x \in X,\ \exists x^{-1} \in X : x \cdot x^{-1} = x^{-1} \cdot x = 1$

(D1) $\forall x, y, z \in X,\ x \cdot (y + z) = x \cdot y + x \cdot z$

(D2) $\forall x, y, z \in X,\ (x + y) \cdot z = x \cdot z + y \cdot z$

Definition 1.13 (Commutative Field)**.**
Let X be a non-empty set.
Let $+ : X \times X \to X$ be an additive internal composition law on X.
Let $\cdot : X \times X \to X$ be a multiplicative internal composition law on X.

A *commutative field* is a triple $\mathbb{F}_c := (X, +, \cdot)$ satisfying:

(A1) $\forall x, y, z \in X,\ (x + y) + z = x + (y + z) = x + y + z$

(C1) $\forall x, y \in X,\ x + y = y + x$

(N1) $\exists 0 \in X : \forall x \in X,\ x + 0 = 0 + x = x$

(I1) $\forall x \in X,\ \exists (-x) \in X : x + (-x) = (-x) + x = 0$

(A2) $\forall x, y, z \in X,\ (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y \cdot z$

(C2) $\forall x, y \in X,\ x \cdot y = y \cdot x$

(N2) $\exists 1 \in X : \forall x \in X,\ x \cdot 1 = 1 \cdot x = x$

(I2) $\forall x \in X,\ \exists x^{-1} \in X : x \cdot x^{-1} = x^{-1} \cdot x = 1$

(D1) $\forall x, y, z \in X,\ x \cdot (y + z) = x \cdot y + x \cdot z$

(D2) $\forall x, y, z \in X,\ (x + y) \cdot z = x \cdot z + y \cdot z$

Definition 1.14 (Vector Space)**.**
Let X be a non-empty set.
Let $(\mathbb{K}, +, \cdot)$ be a field.
Let $+ : X \times X \to X$ be an additive internal composition law on X.
Let $\cdot : \mathbb{K} \times X \to X$ be a multiplicative external composition law on X.

A $\mathbb{K}$-**vector space** or $\mathbb{K}$-**linear space** is a triple $\mathcal{V} := (X, +, \cdot)_{\mathbb{K}}$ satisfying:

(A) $\forall x, y, z \in X,\ (x + y) + z = x + (y + z) = x + y + z$

(C) $\forall x, y \in X,\ x + y = y + x$

(N) $\exists 0 \in X : \forall x \in X,\ x + 0 = 0 + x = x$

(I) $\forall x \in X,\ \exists (-x) \in X : x + (-x) = (-x) + x = 0$

(P) $\forall x \in X,\ \forall k, \ell \in \mathbb{K},\ k \cdot_X (\ell \cdot_X x) = (k \cdot_{\mathbb{K}} \ell) \cdot_X x$

(U) $\exists 1 \in \mathbb{K} : \forall x \in X,\ 1 \cdot x = x$

(D1) $\forall x, y \in X,\ \forall k \in \mathbb{K},\ k \cdot (x +_X y) = k \cdot x +_X k \cdot y$

(D2) $\forall k, \ell \in \mathbb{K},\ \forall x \in X,\ (k +_{\mathbb{K}} \ell) \cdot x = k \cdot x +_X \ell \cdot x$

From now on, we shall employ the notation X in place of the more explicit $(X, +, \cdot)$ to denote a field, commutative ring, domain, or similar algebraic structures when the context unambiguously implies the operations involved.

Definition 1.15 (Field Extension)**.**
Let $(X, +, \cdot)$ be a field.
Let $(Y, +, \cdot)$ be a field such that $Y \subseteq X$.

A *field extension* is the pair X/Y such that the operations of Y are those of X restricted to Y.

Definition 1.16 (Degree of Field Extension)**.**
Let $(X, +, \cdot)$ be a field.
Let $(Y, +, \cdot)$ be a field such that $Y \subseteq X$.
Let X/Y be a field extension.

The *degree* of X/Y, denoted as $[Y : X]$, is the dimension of X as a vector space over Y.

Definition 1.17 (Algebraic Field Extension)**.**
Let $(X, +, \cdot)$ be a field.
Let $(Y, +, \cdot)$ be a field such that $Y \subseteq X$.
An *algebraic field extension* is the field extension X/Y such that its degree $[Y : X]$ is finite.

Definition 1.18 (Extension Field)**.**
Let $(X, +, \cdot)$ be a field.
Let $(Y, +, \cdot)$ be a field such that $Y \subseteq X$.
Let X/Y be a field extension.

The field X is said to be an *extension field* of Y.

Definition 1.19 (Subfield)**.**
Let $(X, +, \cdot)$ be a field.
Let $(Y, +, \cdot)$ be a field such that $Y \subseteq X$.
Let X/Y be a field extension.

The field Y is said to be a *subfield* of X.

Definition 1.20 (Number Field)**.**
Let $(X, +, \cdot)$ be a field.
Let $(\mathbb{Q}, +, \cdot)$ be the field of rational numbers such that $\mathbb{Q} \subseteq X$.
Let $X/\mathbb{Q}$ be an algebraic field extension.

The extension field X is said to be a *number field* or an *algebraic number field*.

1.3 Results

Theorem 1.21.
Let $p \in \mathbb{N}$ be prime.

If ζ_p is a primitive p-th root of unity, then $\zeta_p - 1$ is prime.

Proof. This has already been formalised and included in Mathlib. □

Lemma 1.22.
Let R be a commutative semiring, domain and normalised gcd monoid.
Let $a, b, c \in R$.
Let $n \in \mathbb{N}$.

Then, to prove Fermat's Last Theorem for exponent n in R, one can assume, without loss of generality, that $\gcd(a, b, c) = 1$.

Proof. This has already been formalised and included in Mathlib. $\square$

Lemma 1.23.
Let $\mathbb{Z}_9$ be the ring of integers modulo 9.
Let $\mathbb{Z}_3$ be the ring of integers modulo 3.
Let $n \in \mathbb{Z}_9$.
Let $\phi : \mathbb{Z}_9 \to \mathbb{Z}_3$ be the canonical ring homomorphism.
Let $\phi(n) \neq 0$.

Then $n^3 = 1 \vee n^3 = 8$.

Proof. This has already been formalised and included in Mathlib. $\square$

Chapter 2

Third Cyclotomic Extensions

Theorem 2.1.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $u \in \mathcal{O}_K^\times$ be a unit.

Then $u \in \{1, -1, \eta, -\eta, \eta^2, -\eta^2\}$.

Proof. Let $\mathcal{F}$ be the fundamental system of K.
By properties of cyclotomic fields, we know that $\operatorname{rank}(K) = 0$ (see this lemma, this lemma and this lemma which have already been formalised and included in Mathlib). By the Dirichlet Unit Theorem (see Mathlib), we know that

$$\exists x \in K \text{ with finite order, such that } u = x \prod_{v \in \mathcal{F}} v,$$

but since $\operatorname{rank}(K) = 0$, then $\mathcal{F} = \emptyset$, which implies that $u = x$.
Since $u = x$ has finite order, by properties of primitive roots (see this lemma that has already been formalised and included in Mathlib), we can deduce that

$$\exists r < 3 \text{ such that } u = \eta^r \vee u = -\eta^r.$$

Therefore, we can conclude

$$u \in \{\pm\eta^r \mid r \in \{0, 1, 2\}\} = \left\{1, -1, \eta, -\eta, \eta^2, -\eta^2\right\}.$$

$\square$

Theorem 2.2.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $m \in \mathbb{Z}$.

Then $3 \nmid \eta - m$.

Proof. By properties of cyclotomic fields, we know that $\{1, \eta\}$ is an integral power basis of $\mathcal{O}_K$ (see this lemma, this lemma and this lemma which have already been formalised and included in Mathlib).
For every $\xi \in \mathcal{O}_K$, we define $\pi_1(\xi)$ and $\pi_2(\xi)$ to be the first and second coordinates of ξ with respect to the basis $\{1, \eta\} \in \mathcal{O}_K$, i.e.

$$\xi = \pi_1(\xi) + \pi_2(\xi)\eta.$$

By contradiction we assume that

$$\exists m \in \mathbb{Z} \text{ such that } 3 \mid \eta - m,$$

which implies that

$$\exists x \in \mathcal{O}_K \text{ such that } \eta - m = 3x.$$

By linearity of π_2,

$$\pi_2(\eta) = \pi_2(3x + m) = 3\pi_2(x) + \pi_2(m).$$

Since $\pi_2(\eta) = 1$ and $\pi_2(m) = 0$, then we have that $3 \mid 1$, which is a contradiction. $\square$

Lemma 2.3.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.

Then $\lambda^2 = -3\eta$.

Proof. By definition we have that $\lambda = \eta - 1$, which implies that

$$\lambda^2 = (\eta - 1)^2 = \eta^2 - 2\eta + 1.$$

Since η corresponds to a root of the equation $x^2 + x + 1 = 0$, then $\eta^2 = -1 - \eta$. Substituting back, we can conclude that

$$\lambda^2 = (-1 - \eta) - 2\eta + 1 = -3\eta.$$

□

Theorem 2.4.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $u \in \mathcal{O}_K^\times$ be a unit.

If $\exists m \in \mathbb{Z}$ such that $\lambda^2 \mid u - m$, then $u = 1 \vee u = -1$.
This is a special case of the Kummer's Lemma.

Proof. By Lemma 2.3, we have that $-3\eta = \lambda^2 \mid u - m$, which implies that $3 \mid u - m$.
By Theorem 2.1, we know that $u \in \{1, -1, \eta, -\eta, \eta^2, -\eta^2\}$.
We proceed by analysing each case:

- Case $u = 1 \vee u = -1$. This finishes the proof.
- Case $u = \eta$.
  Since $3 \mid u - m$, we have that $3 \mid \eta - m$, which contradicts Theorem 2.2 forcing us to conclude that $u \neq \eta$.
- Case $u = -\eta$.
  Since $3 \mid u - m$, we have that $3 \mid -\eta - m$, then by properties of divisibility $3 \mid \eta + m$, which contradicts Theorem 2.2 forcing us to conclude that $u \neq -\eta$.
- Case $u = \eta^2$.
  Since $3 \mid u - m$, we have that $3 \mid \eta^2 - m$, which contradicts Theorem 2.2 since η^2 is a third root of unity (see Mathlib), forcing us to conclude that $u \neq \eta^2$.
- Case $u = -\eta^2$.
  Since $3 \mid u - m$, we have that $3 \mid -\eta^2 - m$, then by properties of divisibility $3 \mid \eta^2 + m$, which contradicts Theorem 2.2 since η^2 is a third root of unity (see Mathlib), forcing us to conclude that $u \neq -\eta^2$.

Therefore, $u = 1 \vee u = -1$. □

Lemma 2.5.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.

Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.

Then the norm of λ is 3.

Proof. Since the third cyclotomic polynomial over $\mathbb{Q}$ is irreducible, then the norm of λ is 3 by properties of primitive roots (see this lemma that has already been formalised and included in Mathlib). □

Lemma 2.6.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.

Then the norm of λ is a prime number.

Proof. It directly follows from Lemma 2.5 since 3 is a prime number. □

Lemma 2.7.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.

Then $\lambda \mid 3$.

Proof. By properties of norms and divisibility, if the norm of an element in the ring of integers divides a number, then the element itself must divide that number. In this case, by Lemma 2.5 we know that the norm of λ is 3, that divides 3, which implies that $\lambda \mid 3$. □

Lemma 2.8.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.

Then λ is prime.

Proof. Since 3 is prime and ζ_3 is a primitive third root of unity, then λ is prime by Theorem 1.21. $\square$

Lemma 2.9.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.

Then $\lambda \neq 0$.

Proof. It directly follows from Lemma 2.8 since zero is not prime. $\square$

Lemma 2.10.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.

Then λ is not a unit.

Proof. It directly follows from Lemma 2.8 since prime numbers are not units. $\square$

Lemma 2.11.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let I be the ideal generated by λ.

Then $\mathcal{O}_K/I$ has cardinality 3.

Proof. It directly follows from Lemma 2.5 by the fundamental properties of ideals. $\square$

Lemma 2.12.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let I be the ideal generated by λ.
Let $2 \in \mathcal{O}_K/I$.

Then $2 \neq 0$.

Proof. By contradiction we assume that $2 \in I$, then, by definition, λ would divide $2 \in \mathcal{O}_K$. Recall from Lemma 2.5 that the norm of λ is 3. If λ divided 2, then by properties of divisibility in number fields, the norm of λ would also divide 2. However $3 \nmid 2$ showing a contradiction. Therefore, $\lambda \nmid 2$, then $2 \notin I$, which implies that $2 \in \mathcal{O}_K/I$ is non-zero. $\square$

Lemma 2.13.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.

Then $\lambda \nmid 2$.

Proof. By contradiction we assume that $\lambda \mid 2$, that implies that $2 \in I$ from which it follows that $2 = 0$ contradicting Lemma 2.12 forcing us to conclude that $\lambda \nmid 2$. $\square$

Lemma 2.14.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let I be the ideal generated by λ.

Then $\mathcal{O}_K/I = \{0, 1, -1\}$.

Proof. By Lemma 2.11, the cardinality of $\mathcal{O}_K/I$ is 3, so it suffices to prove that $1, -1$

and 0 are distinct.
We proceed by contradiction analysing each case:

- Case $1 = -1$. By basic algebraic properties, $1 = -1$ implies that $2 = 0$, which contradicts Lemma 2.12 forcing us to conclude that $1 \neq -1$.
- Case $1 = 0$. Trivial contradiction.
- Case $-1 = 0$. It implies that $1 = 0$, which is a contradiction.

□

Lemma 2.15.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $x \in \mathcal{O}_K$.

Then $(\lambda \mid x) \vee (\lambda \mid x - 1) \vee (\lambda \mid x + 1)$.

Proof. Let I be the ideal generated by λ. Let $\pi : \mathcal{O}_K \to \mathcal{O}_K/I$.
By Lemma 2.14, we have that $\pi(x) \in \mathcal{O}_K/I = \{0, 1, -1\}$.
We proceed by analysing each case:

- Case $\pi(x) = 0$. By properties of ideals, $\lambda \mid x$.
- Case $\pi(x) = 1$. Then $0 = \pi(x) - 1 = \pi(x - 1)$, which, by properties of ideals, implies that $\lambda \mid x - 1$.
- Case $\pi(x) = -1$. Then $0 = \pi(x) + 1 = \pi(x + 1)$, which, by properties of ideals, implies that $\lambda \mid x + 1$.

□

Lemma 2.16.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.

Then $\eta^3 = 1$.

Proof. Since $\zeta_3 \in K$ is a primitive third root of unity, then $\zeta_3^3 = 1$. Given that $\eta \in \mathcal{O}_K$ is the element corresponding to $\zeta_3 \in K$, then $\eta^3 = 1$ by the extension of the field properties into the ring of integers. □

Lemma 2.17.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.

Then η is a unit.

Proof. It directly follows from Lemma 2.16. □

Lemma 2.18.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.

Then $\eta^2 + \eta + 1 = 0$.

Proof. Since η corresponds to a root of the equation $x^2+x+1 = 0$, then $\eta^2+\eta+1 = 0$. □

Lemma 2.19.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $x \in \mathcal{O}_K$.

Then $x^3 - 1 = (x-1)(x-\eta)(x-\eta^2)$.

Proof. Applying Lemma 2.16 and Lemma 2.18, we have that

$$\begin{aligned}(x-1)(x-\eta)(x-\eta^2) &= x^3 - x^2(\eta^2+\eta+1) + x(\eta^2+\eta+\eta^3) - \eta^3 \\ &= x^3 - x^2(\eta^2+\eta+1) + x(\eta^2+\eta+1) - 1 \\ &= x^3 - 1.\end{aligned}$$

□

Lemma 2.20.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $x \in \mathcal{O}_K$.

Then $\lambda \mid x(x-1)(x-(\eta+1))$.

Proof. By Lemma 2.15, we have that

$$(\lambda \mid x) \vee (\lambda \mid x-1) \vee (\lambda \mid x+1).$$

We proceed by analysing each case:

- Case $\lambda \mid x$.
  By properties of divisibility, we have that $\lambda \mid x(x-1)(x-(\eta+1))$.
- Case $\lambda \mid x-1$.
  By properties of divisibility, we have that $\lambda \mid x(x-1)(x-(\eta+1))$.
- Case $\lambda \mid x+1$.
  By properties of divisibility, it suffices to prove that

  $$\lambda \mid x-(\eta+1) = x+1-(\eta-1+3).$$

  By definition of λ, we have that

  $$x+1-(\eta-1+3) = x+1-(\lambda+3).$$

  By properties of divisibility and Lemma 2.7, we can deduce that $\lambda \mid \lambda+3$.
  Therefore, by properties of divisibility, we can conclude that

  $$\lambda \mid x(x-1)(x-(\eta+1)).$$

□

Lemma 2.21.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.

Let $x \in \mathcal{O}_K$.

If $\lambda \mid x - 1$, then $\lambda^4 \mid x^3 - 1$.

Proof. Let $\lambda \mid x - 1$, which is equivalent to say that

$$\exists y \in \mathcal{O}_K \text{ such that } x - 1 = \lambda y.$$

By ring properties and Lemma 2.19, we have that

$$x^3 - 1 = \lambda^3(y(y-1)(y-(\eta+1))).$$

By properties of divisibility and Lemma 2.20, we can conclude that

$$\lambda^4 \mid x^3 - 1.$$

□

Lemma 2.22.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $x \in \mathcal{O}_K$.

If $\lambda \mid x + 1$, then $\lambda^4 \mid x^3 + 1$.

Proof. By properties of divisibility, if $\lambda \mid x + 1$ then

$$\lambda \mid -(x+1) = (-x) - 1.$$

By Lemma 2.20, we can deduce that

$$\lambda^4 \mid (-x)^3 - 1.$$

By divisibility and ring properties we can conclude that

$$\lambda^4 \mid x^3 + 1.$$

□

Lemma 2.23.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.

Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $x \in \mathcal{O}_K$.

If $\lambda \nmid x$, then $(\lambda^4 \mid x^3 - 1) \vee (\lambda^4 \mid x^3 + 1)$.

Proof. By Lemma 2.15, we have that

$$(\lambda \mid x) \vee (\lambda \mid x - 1) \vee (\lambda \mid x + 1).$$

We proceed by analysing each case:

- Case $\lambda \mid x$. From trivially contradictory hypotheses we can conclude that

$$(\lambda^4 \mid x^3 - 1) \vee (\lambda^4 \mid x^3 + 1).$$

- Case $\lambda \mid x - 1$. By Lemma 2.21, we have that $\lambda^4 \mid x^3 - 1$, which implies that

$$(\lambda^4 \mid x^3 - 1) \vee (\lambda^4 \mid x^3 + 1).$$

- Case $\lambda \mid x + 1$. By Lemma 2.22, we have that $\lambda^4 \mid x^3 + 1$, which implies that

$$(\lambda^4 \mid x^3 - 1) \vee (\lambda^4 \mid x^3 + 1).$$

$\square$

Chapter 3

Fermat's Last Theorem for Exponent 3

3.1 Case 1

Lemma 3.1.
Let $n \in \mathbb{N}$.
Let $[n] \in \mathbb{Z}_9$.
Let $3 \nmid n$.

Then $[n]^3 = 1 \vee [n]^3 = 8$.

Proof. By Lemma 1.23, we can conclude that $[n]^3 = 1 \vee [n]^3 = 8$. □

Theorem 3.2 (Fermat's Last Theorem for 3: Case 1)**.**
Let $a, b, c \in \mathbb{N}$.
Let $3 \nmid abc$.

Then $a^3 + b^3 \neq c^3$.

Proof. By hypothesis we know that $3 \nmid abc$, which implies that $3 \nmid a$, $3 \nmid b$ and $3 \nmid c$. By repeatedly applying Lemma 3.1 for each case, we can conclude that

$$a^3 + b^3 \neq c^3.$$

□

3.2 Case 2

Lemma 3.3.
Let $a, b, c \in \mathbb{N}$.
Let $3 \mid a$ and $3 \mid b$.
Let $a^3 + b^3 = c^3$.

Then $3 \mid \gcd(a, b, c)$.

Proof. By hypothesis we have that $3 \mid a^3 + b^3 = c^3$, which implies that $3 \mid c$, from which we can conclude that $3 \mid \gcd(a, b, c)$. □

Lemma 3.4.
Let $a, b, c \in \mathbb{N}$.
Let $3 \mid a$ and $3 \mid c$.
Let $a^3 + b^3 = c^3$.

Then $3 \mid \gcd(a, b, c)$.

Proof. By hypothesis we have that $3 \mid c^3 - a^3 = b^3$, which implies that $3 \mid b$, from which we can conclude that $3 \mid \gcd(a, b, c)$. □

Lemma 3.5.
Let $a, b, c \in \mathbb{N}$.
Let $3 \mid b$ and $3 \mid c$.
Let $a^3 + b^3 = c^3$.

Then $3 \mid \gcd(a, b, c)$.

Proof. By hypothesis we have that $3 \mid c^3 - b^3 = a^3$, which implies that $3 \mid a$, from which we can conclude that $3 \mid \gcd(a, b, c)$. □

Theorem 3.6.
To prove Theorem 3.66, it suffices to prove that

$$\forall a, b, c \in \mathbb{Z},\ \text{if } c \neq 0 \text{ and } 3 \nmid a \text{ and } 3 \nmid b \text{ and } 3 \mid c \text{ and } \gcd(a, b) = 1,\ \text{then } a^3 + b^3 \neq c^3.$$

Equivalently,

$$\forall a, b, c \in \mathbb{Z},\ \text{if } c \neq 0 \text{ and } 3 \nmid a \text{ and } 3 \nmid b \text{ and } 3 \mid c \text{ and } \gcd(a, b) = 1,\ \text{then } a^3 + b^3 \neq c^3$$

implies Theorem 3.66.

Proof. By contradiction we assume that

$$\exists a, b, c \in \mathbb{N} \setminus \{0\} \text{ such that } a^3 + b^3 = c^3.$$

By Lemma 1.22 we can assume that $\gcd(a, b, c) = 1$.
By Theorem 3.2 we can assume that $3 \mid abc$, from which it follows that

$$(3 \mid a) \vee (3 \mid b) \vee (3 \mid c).$$

We proceed by analysing each case:

- Case $3 \mid a$.
  Let $a' = -c$, $b' = b$, $c' = -a$, then $3 \mid c'$ and

  $$(a' \neq 0) \wedge (b' \neq 0) \wedge (c' \neq 0).$$

  Then $3 \nmid a'$ since otherwise by Lemma 3.4 we would have that $3 \mid \gcd(a, b, c) = 1$ which is absurd.
  Analogously, by Lemma 3.3 we have that $3 \nmid b'$.
  By contradiction we assume that $\gcd(a', b') \neq 1$ which, by basic divisibility properties, implies that there is a prime p such that $p \mid a'$ and $p \mid b'$. It follows that $p \mid b'^3 + a'^3 = b^3 - c^3 = -a^3$, which implies that $p \mid a$.
  Therefore $p \mid \gcd(a, b, c) = 1$ which is absurd.
  Moreover, we have that $a'^3 + b'^3 = -c^3 + b^3 = -a^3 = c'^3$ that contradicts our hypothesis.

- Case $3 \mid b$.
  Let $a' = a$, $b' = -c$, $c' = -b$.
  The rest of the proof is analogous to the first case using Lemma 3.3 and Lemma 3.5.

- Case $3 \mid c$. Let $a' = a$, $b' = b$, $c' = c$.
  The rest of the proof is analogous to the first case using Lemma 3.4 and Lemma 3.5.

Therefore, we can conclude that $a^3 + b^3 \neq c^3$. $\square$

Definition 3.7 (Solution')**.**
Let $a, b, c \in \mathcal{O}_K$ such that $c \neq 0$ and $\gcd(a, b) = 1$.
Let $\lambda \nmid a$, $\lambda \nmid b$ and $\lambda \mid c$.

A *solution'* is a tuple $S' = (a, b, c, u)$ satisfying the equation $a^3 + b^3 = uc^3$.

Definition 3.8 (Solution)**.**
Let $a, b, c \in \mathcal{O}_K$ such that $c \neq 0$ and $\gcd(a, b) = 1$.
Let $\lambda \nmid a$, $\lambda \nmid b$, $\lambda \mid c$ and $\lambda^2 \mid a + b$.

A *solution* is a tuple $S = (a, b, c, u)$ satisfying the equation $a^3 + b^3 = uc^3$.

Definition 3.9 (Multiplicity of Solution').
Let $S' = (a, b, c, u)$ be a *solution'*.

The *multiplicity* of S' is the largest $n \in \mathbb{N}$ such that $\lambda^n \mid c$.

Definition 3.10 (Multiplicity of Solution).
Let $S = (a, b, c, u)$ be a *solution*.

The *multiplicity* of S is the largest $n \in \mathbb{N}$ such that $\lambda^n \mid c$.

Definition 3.11 (Minimal Solution).
Let $S = (a, b, c, u)$ be a *solution*.

We say that S is *minimal* if for all solutions $S_1 = (a_1, b_1, c_1, u_1)$, the multiplicity of S is less than or equal to the *multiplicity* of S_1.

Lemma 3.12.
Let $S' = (a, b, c, u)$ be a *solution'*.

Then the multiplicity of S' is finite.

Proof. It directly follows from Lemma 2.10. □

Lemma 3.13.
Let S be a *solution* with multiplicity n.

Then there is a minimal solution S_1.

Proof. Straightforward since $n \in \mathbb{N}$ and $\mathbb{N}$ is well-ordered. □

Lemma 3.14.
Let $S' = (a, b, c, u)$ be a *solution'*.

Then $\lambda^4 \mid a^3 - 1 \wedge \lambda^4 \mid b^3 + 1$ or $\lambda^4 \mid a^3 + 1 \wedge \lambda^4 \mid b^3 - 1$.

Proof. Since $\lambda \nmid a$, then $\lambda^4 \mid a^3 - 1 \vee \lambda^4 \mid a^3 + 1$ by Lemma 2.23. Since $\lambda \nmid b$, then $\lambda^4 \mid b^3 - 1 \vee \lambda^4 \mid b^3 + 1$ by Lemma 2.23. We proceed by analysing each case:

- Case $\lambda^4 \mid a^3 - 1 \wedge \lambda^4 \mid b^3 - 1$. Since $\lambda \mid c$ we have that $\lambda \mid c^3 - (a^3 - 1) - (b^3 - 1) = 2$, which is absurd by Lemma 2.13.

- Case $\lambda^4 \mid a^3+1 \wedge \lambda^4 \mid b^3+1$. Since $\lambda \mid c$ we have that $\lambda \mid (a^3-1)+(b^3-1)-c^3 = 2$, which is absurd by Lemma 2.13.
- Case $\lambda^4 \mid a^3-1 \wedge \lambda^4 \mid b^3+1$. Trivial.
- Case $\lambda^4 \mid a^3+1 \wedge \lambda^4 \mid b^3-1$. Trivial.

□

Lemma 3.15.
Let $S' = (a, b, c, u)$ be a *solution'*.

Then $\lambda^4 \mid c^3$.

Proof. Apply Lemma 3.14 and then compute each case. □

Lemma 3.16.
Let $S' = (a, b, c, u)$ be a *solution'*.

Then $\lambda^2 \mid c$.

Proof. Apply Lemma 3.15. □

Lemma 3.17.
Let $S' = (a, b, c, u)$ be a *solution'* with multiplicity n.

Then $2 \leq n$.

Proof. It directly follows from Lemma 3.16. □

Lemma 3.18.
Let $S = (a, b, c, u)$ be a *solution* with multiplicity n.

Then $2 \leq n$.

Proof. It directly follows from Lemma 3.17. □

Lemma 3.19.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.

Let $S' = (a, b, c, u)$ be a *solution'*.

Then $a^3 + b^3 = (a + b)(a + \eta b)(a + \eta^2 b)$.

Proof. Straightforward calculation using Lemma 2.16 and Lemma 2.18. $\square$

Lemma 3.20.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $S' = (a, b, c, u)$ be a *solution'*.

Then $(\lambda^2 \mid a + b) \vee (\lambda^2 \mid a + \eta b) \vee (\lambda^2 \mid a + \eta^2 b)$.

Proof. By contradiction we assume that

$$(\lambda^2 \nmid a + b) \wedge (\lambda^2 \nmid a + \eta b) \wedge (\lambda^2 \nmid a + \eta^2 b).$$

Then, by definition, the multiplicity of λ in $a + b$, in $a + \eta b$ and in $a + \eta^2 b$ is less than 2. By properties of divisibility, Lemma 3.16 and Lemma 3.19, we have that

$$\lambda^6 \mid uc^3 = a^3 + b^3 = (a + b)(a + \eta b)(a + \eta^2 b).$$

Then, the multiplicity of λ in $(a + b)(a + \eta b)(a + \eta^2 b)$ is greater than or equal to 6. By Lemma 2.8 λ is prime, so we have that the multiplicity of λ in $(a+b)(a+\eta b)(a+\eta^2 b)$ is the sum of the multiplicities of λ in $a + b$, in $a + \eta b$ and in $a + \eta^2 b$, which is less than 6. This is a contradiction that forces us to conclude that

$$(\lambda^2 \mid a + b) \vee (\lambda^2 \mid a + \eta b) \vee (\lambda^2 \mid a + \eta^2 b).$$

$\square$

Lemma 3.21.
Let $S' = (a, b, c, u)$ be a *solution'*.

Then $\exists a_1, b_1 \in \mathcal{O}_k$ such that $S_1 = (a_1, b_1, c, u)$ is a *solution*.

Proof. By Lemma 3.20, we have that

$$(\lambda^2 \mid a + b) \vee (\lambda^2 \mid a + \eta b) \vee (\lambda^2 \mid a + \eta^2 b).$$

We proceed by analysing each case:

- Case $\lambda^2 \mid a+b$. Trivial using $a_1 = a$ and $b_1 = b$.
- Case $\lambda^2 \mid a+\eta b$. Let $a_1 = a$ and $b_1 = \eta b$.
  By Lemma 2.16, we have that $a^3 + (\eta b)^3 = a^3 + b^3 = uc^3$.
  By properties of coprimes and Lemma 2.17, we have that $\gcd(a, b) = 1$ implies that $\gcd(a, \eta b) = 1$.
  Since $a_1 = a$, we already know that $\lambda \nmid a = a_1$.
  By contradiction we assume that $\lambda \mid b_1 = \eta b$, which, by Lemma 2.16, it implies that $\lambda \mid \eta^2 \eta b = b$ that contradicts our assumption, forcing us to conclude that $\lambda \nmid b_1$.
- Case $\lambda^2 \mid a+\eta^2 b$. Let $a_1 = a$ and $b_1 = \eta^2 b$.
  By Lemma 2.16, we have that $a^3 + (\eta^2 b)^3 = a^3 + b^3 = uc^3$.
  By properties of coprimes and Lemma 2.17, we have that $\gcd(a, b) = 1$ implies that $\gcd(a, \eta^2 b) = 1$.
  Since $a_1 = a$, we already know that $\lambda \nmid a = a_1$.
  By contradiction we assume that $\lambda \mid b_1 = \eta^2 b$, which, by Lemma 2.16, it implies that $\lambda \mid \eta\eta^2 b = b$ that contradicts our assumption, forcing us to conclude that $\lambda \nmid b_1$.

Therefore, we can conclude that $\exists a_1, b_1 \in \mathcal{O}_k$ such that $S_1 = (a_1, b_1, c, u)$ is a *solution*. □

Lemma 3.22.
Let S' be a *solution*$'$ with multiplicity n.

Then there is a *solution* S with multiplicity n.

Proof. Let $S' = (a', b', c', u')$. Let a, b be the units given by Lemma 3.21. Then $S = (a, b, c', u')$ is a *solution*$'$ with multiplicity n. □

Lemma 3.23.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $S = (a, b, c, u)$ be a *solution*.

Then $a + \eta b = (a + b) + \lambda b$.

Proof. Trivial calculation. □

Lemma 3.24.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $S = (a, b, c, u)$ be a *solution*.

Then $\lambda \mid a + \eta b$.

Proof. Trivial since $\lambda \mid a + b$. □

Lemma 3.25.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $S = (a, b, c, u)$ be a *solution*.

Then $\lambda \mid a + \eta^2 b$.

Proof. Since $\lambda \mid a + b$, then $\lambda \mid (a + b) + \lambda^2 b + 2\lambda b = a + \eta^2 b$. □

Lemma 3.26.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $S = (a, b, c, u)$ be a *solution*.

Then $\lambda^2 \nmid a + \eta b$.

Proof. By contradiction we assume that $\lambda^2 \mid a + \eta b$, which implies that $\lambda^2 \mid a + b + \lambda b$ by Lemma 3.23. Since $\lambda^2 \mid a + b$, then $\lambda^2 \mid \lambda b$, which implies that $\lambda \mid b$, that contradicts Definition 3.8 forcing us to conclude that $\lambda^2 \nmid a + \eta b$. □

Lemma 3.27.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $S = (a, b, c, u)$ be a *solution*.

Then $\lambda^2 \nmid a + \eta^2 b$.

Proof. By contradiction using Lemma 2.18, we assume $\lambda^2 \mid a + \eta^2 b = a + b - b + \eta^2 b$. Since $\lambda^2 \mid a + b$, then $\lambda^2 \mid b(\eta^2 - 1) = \lambda b(\eta + 1)$. Since $\lambda \nmid b$, then $\lambda \mid \eta + 1 = \lambda + 2$, then $\lambda \mid 2$ which is absurd. □

Lemma 3.28.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $S = (a, b, c, u)$ be a *solution*.

Then $(\eta + 1)(-\eta) = 1$.

Proof. Trivial calculation using Lemma 2.18. □

Lemma 3.29.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $S = (a, b, c, u)$ be a *solution*.
Let $p \in \mathcal{O}_K$ be a prime such that $p \mid a + b$ and $p \mid a + \eta b$.

Then p is associated with λ.

Proof. We proceed by analysis each case:

- Case $p \mid \lambda$. It directly follows from Lemma 2.8.

- Case $p \nmid \lambda$.
  By hypothesis, we have that $p \mid a+b$ and $p \mid a+\eta b$. Then $p \mid (a+\eta b)-(a+b) = b(\eta-1) = b\lambda$, which implies that $p \mid b$ and we proceed analogously to show that $p \mid a$.
  Therefore $p \mid \gcd(a,b) = 1$ which is absurd.

Therefore, we can conclude that p is associated with λ. □

Lemma 3.30.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $S = (a,b,c,u)$ be a *solution*.
Let $p \in \mathcal{O}_K$ be a prime such that $p \mid a+b$ and $p \mid a+\eta^2 b$.

Then p is associated with λ.

Proof. We proceed by analysis each case:

- Case $p \mid \lambda$. It directly follows from Lemma 2.8.
- Case $p \nmid \lambda$.
  By hypothesis, we have that $p \mid a+b$ and $p \mid a+\eta^2 b$. By Lemma 2.16 and Lemma 2.17, we have that
  $$p \mid \eta((a+\eta^2 b)-(a+b)) = -(\eta^3-\eta)b = \lambda b,$$
  which implies that $p \mid b$ and we proceed analogously to show that $p \mid a$.
  Therefore $p \mid \gcd(a,b) = 1$ which is absurd.

Therefore, we can conclude that p is associated with λ. □

Lemma 3.31.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $S = (a,b,c,u)$ be a *solution*.
Let $p \in \mathcal{O}_K$ be a prime such that $p \mid a+\eta b$ and $p \mid a+\eta^2 b$.

Then p is associated with λ.

Proof. We proceed by analysis each case:

- Case $p \mid \lambda$. It directly follows from Lemma 2.8.
- Case $p \nmid \lambda$.
  By hypothesis, we have that $p \mid a + \eta b$ and $p \mid a + \eta^2 b$. Then $p \mid (a + \eta^2 b) - (a + \eta b) = \eta b(\eta - 1) = \eta b \lambda$, which, by Lemma 2.17, implies that $p \mid b$ and we proceed analogously to show that $p \mid a$.
  Therefore $p \mid \gcd(a, b) = 1$ which is absurd.

Therefore, we can conclude that p is associated with λ. ☐

Definition 3.32 (x, y, z, w)**.**
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $S = (a, b, c, u)$ be a *solution*.

We define $x \in \mathcal{O}_K$ such that $a + b = \lambda^{3n-2} x$.
We define $y \in \mathcal{O}_K$ such that $a + \eta b = \lambda y$.
We define $z \in \mathcal{O}_K$ such that $a + \eta^2 b = \lambda z$.
We define $w \in \mathcal{O}_K$ such that $c = \lambda^n w$.

Lemma 3.33.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let S be a *solution*.

Then $\lambda \nmid y$.

Proof. By contradiction we assume that $\lambda \mid y$, which implies that $\lambda^2 \mid \lambda y = a + \eta b$, that contradicts Lemma 3.26 forcing us to conclude that $\lambda \nmid y$. ☐

Lemma 3.34.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.

Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let S be a *solution*.

Then $\lambda \nmid z$.

Proof. By contradiction we assume that $\lambda \mid z$, which implies that $\lambda^2 \mid \lambda z = a + \eta^2 b$, that contradicts Lemma 3.27 forcing us to conclude $\lambda \nmid z$. □

Lemma 3.35.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $S = (a, b, c, u)$ be a *solution* with multiplicity n.

Then $\lambda^{3n-2} \mid a + b$.

Proof. By Definition 3.10 we have that $\lambda^n \mid c$. Since u is a unit, then by Lemma 3.19 we have that

$$\lambda^{3n} \mid uc^3 = a^3 + b^3 = (a + b)(a + \eta b)(a + \eta^2 b) = (a + b)(\lambda y)(\lambda z).$$

Then applying Lemma 3.33 and Lemma 3.34, we can conclude that $\lambda^{3n-2} \mid a + b$. □

Lemma 3.36.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let S be a *solution*.

Then $\lambda \nmid w$.

Proof. By contradiction we assume that $\lambda \mid w$, which implies $\lambda^{n+1} \mid \lambda^n w = c$ that contradicts Definition 3.10 forcing us to conclude that $\lambda \nmid w$. □

Lemma 3.37.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let S be a *solution*.

Then $\lambda \nmid x$.

Proof. By contradiction, if $\lambda \mid x$, then $\lambda^{3n-1} \mid \lambda^{3n-2}x = a + b$. Using Lemma 3.24 and Lemma 3.25, we have that $\lambda^{3n+1} \mid (a+b)(a+\eta b)(a+\eta^2 cdotb) = a^3 + b^3 = uc^3 = u\lambda^{3n}w^3$. Then $\lambda \mid w^3$ which implies that $\lambda \mid w$, that contradicts Lemma 3.36 forcing us to conclude $\lambda \nmid x$. □

Lemma 3.38.
Let S be a *solution* with multiplicity n.

Then $\gcd(x, y) = 1$.

Proof. Since $y \neq 0$ by Lemma 3.33, by the properties of PIDs it suffices to prove that $\forall p \in \mathcal{O}_K$ if p is prime and $p \mid x$, then $p \nmid y$. Let $p \in \mathcal{O}_K$ be prime and suppose by contradiction that $p \mid x$ and $p \mid y$ which implies that $p \mid \lambda^{3n-2}x = a + b$ and $p \mid \lambda y = a + \eta b$. Then by Lemma 3.29 we have that p is associated with λ, which implies that $\lambda \mid x$ that contradicts Lemma 3.37 forcing us to conclude that $p \nmid y$, which, as stated above, implies that $\gcd(x, y) = 1$. □

Lemma 3.39.
Let S be a *solution*.

Then $\gcd(x, z) = 1$.

Proof. Since $z \neq 0$ by Lemma 3.34, by the properties of PIDs it suffices to prove that $\forall p \in \mathcal{O}_K$ if p is prime and $p \mid x$, then $p \nmid z$. Let $p \in \mathcal{O}_K$ be prime and suppose by contradiction that $p \mid x$ and $p \mid z$ which implies that $p \mid \lambda^{3n-2}x = a + b$ and $p \mid \lambda z = a + \eta^2 b$. Then by Lemma 3.30 we have that p is associated with λ, which implies that $\lambda \mid x$ that contradicts Lemma 3.37 forcing us to conclude that $p \nmid z$, which, as stated above, implies that $\gcd(x, z) = 1$. □

Lemma 3.40.
Let S be a *solution*.

Then $\gcd(y, z) = 1$.

Proof. Since $z \neq 0$ by Lemma 3.34, by the properties of PIDs it suffices to prove that $\forall p \in \mathcal{O}_K$ if p is prime and $p \mid y$, then $p \nmid z$. Let $p \in \mathcal{O}_K$ be prime and suppose by contradiction that $p \mid y$ and $p \mid z$ which implies that $p \mid \lambda y = a + \eta b$ and $p \mid \lambda z = a + \eta^2 b$. Then by Lemma 3.31 we have that p is associated with λ, which implies that $\lambda \mid y$ that contradicts Lemma 3.33 forcing us to conclude that $p \nmid z$, which, as stated above, implies that $\gcd(y, z) = 1$. $\square$

Lemma 3.41.
Let S be a *solution* with multiplicity n.

Then $3n - 2 + 1 + 1 = 3n$.

Proof. It directly follows from Lemma 3.18 and calculations using ring properties. $\square$

Lemma 3.42.
Let $S = (a, b, c, u)$ be a *solution*.

Then $xyz = uw^3$.

Proof. It directly follows from Definition 3.32, Lemma 3.19, Lemma 2.9, Lemma 3.18 and calculations using ring properties. $\square$

Lemma 3.43.
Let S be a *solution*.

Then $\exists u_1 \in \mathcal{O}_K^\times$ and $\exists X \in \mathcal{O}_K$ such that $x = u_1 X^3$.

Proof. By the properties of PIDs, it suffices to prove that there exists a $k \in \mathcal{O}_K$ such that xk is a cube and $\gcd(x, k) = 1$. Let $k = yzu^{-1}$, then $xk = xyzu^{-1} = w^3$ by Lemma 3.42. Moreover, since $\gcd(x, y) = 1$ by Lemma 3.38 and $\gcd(x, z) = 1$ by Lemma 3.39, then $\gcd(x, yz) = 1$, which implies that $\gcd(x, k) = 1$. $\square$

Lemma 3.44.
Let S be a *solution*.

Then $\exists u_2 \in \mathcal{O}_K^\times$ and $\exists Y \in \mathcal{O}_K$ such that $y = u_2 Y^3$.

Proof. By the properties of PIDs, it suffices to prove that there exists a $k \in \mathcal{O}_K$ such that yk is a cube and $\gcd(y, k) = 1$. Let $k = xzu^{-1}$, then $yk = yxzu^{-1} = w^3$ by Lemma 3.42.

Moreover, since $\gcd(x, y) = 1$ by Lemma 3.38 and $\gcd(y, z) = 1$ by Lemma 3.40, then $\gcd(y, xz) = 1$, which implies that $\gcd(y, k) = 1$. $\square$

Lemma 3.45.
Let S be a *solution*.

Then $\exists u_3 \in \mathcal{O}_K^\times$ and $\exists Z \in \mathcal{O}_K$ such that $z = u_3 Z^3$.

Proof. By the properties of PIDs, it suffices to prove that there exists a $k \in \mathcal{O}_K$ such that zk is a cube and $\gcd(z, k) = 1$. Let $k = xyu^{-1}$, then $zk = zxyu^{-1} = w^3$ by Lemma 3.42. Moreover, since $\gcd(x, z) = 1$ by Lemma 3.39 and $\gcd(y, z) = 1$ by Lemma 3.40, then $\gcd(z, xy) = 1$, which implies that $\gcd(z, k) = 1$. $\square$

Definition 3.46 $(u_1, u_2, u_3, u_4, u_5, X, Y, Z)$**.**
Let S be a *solution*.

We define $u_1 \in \mathcal{O}_K^\times$ and $X \in \mathcal{O}_K$ such that $x = u_1 X^3$.
We define $u_2 \in \mathcal{O}_K^\times$ and $Y \in \mathcal{O}_K$ such that $y = u_2 Y^3$.
We define $u_3 \in \mathcal{O}_K^\times$ and $Z \in \mathcal{O}_K$ such that $z = u_3 Z^3$.
We define $u_4 = \eta u_3 u_2^{-1}$.
We define $u_5 = -\eta^2 u_1 u_2^{-1}$.

Lemma 3.47.
Let S be a *solution*.

Then $X \neq 0$.

Proof. By contradiction we assume that $X = 0$, then $x = 0$ by Definition 3.46. Therefore λ trivially divides x (as any number divides zero) which contradicts Lemma 3.37 forcing us to conclude that $X \neq 0$. $\square$

Lemma 3.48.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let S be a *solution*.

Then $\lambda \nmid X$.

Proof. By contradiction we assume that $\lambda \mid X$, then, by the properties of divisibility, $\lambda \mid u_1 X^3$, which implies, by Definition 3.46, that $\lambda \mid x$. However, this contradicts Lemma 3.37 forcing us to conclude that $\lambda \nmid X$. $\square$

Lemma 3.49.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let S be a *solution*.

Then $\lambda \nmid Y$.

Proof. By contradiction we assume that $\lambda \mid Y$, then, by the properties of divisibility, $\lambda \mid u_2 Y^3$, which implies, by Definition 3.46, that $\lambda \mid y$. However, this contradicts Lemma 3.33 forcing us to conclude that $\lambda \nmid Y$. $\square$

Lemma 3.50.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let S be a *solution*.

Then $\lambda \nmid Z$.

Proof. By contradiction we assume that $\lambda \mid Z$, then, by the properties of divisibility, $\lambda \mid u_3 Z^3$, which implies, by Definition 3.46, that $\lambda \mid z$. However, this contradicts Lemma 3.34 forcing us to conclude that $\lambda \nmid Z$. $\square$

Lemma 3.51.
Let S be a *solution*.

Then $\gcd(Y, Z) = 1$.

Proof. Since $Z \neq 0$ by Lemma 3.50, by the properties of PIDs it suffices to prove that $\forall p \in \mathcal{O}_K$ if p is prime and $p \mid Y$, then $p \nmid Z$. Let $p \in \mathcal{O}_K$ be prime and suppose by contradiction that $p \mid Y$ and $p \mid Z$ which implies that $p \mid u_2 Y^3 = y$ and $p \mid \lambda u_3 Z^3 = z$.

But this contradicts Lemma 3.40 forcing us to conclude that $p \nmid Z$, which, as stated above, implies that $\gcd(Y, Z) = 1$. $\square$

Lemma 3.52.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let S be a *solution* with multiplicity n.

Then $u_1 X^3 \lambda^{3n-2} + u_2 \eta Y^3 \lambda + u_3 \eta^2 Z^3 \lambda = 0$.

Proof. Applying Definition 3.46, Definition 3.32, Lemma 2.16 and Lemma 2.18, we have

$$\begin{aligned} u_1 X^3 \lambda^{3n-2} + u_2 \eta Y^3 \lambda + u_3 \eta^2 Z^3 \lambda &= x\lambda^{3n-2} + \eta y \lambda + \eta^2 z \lambda \\ &= (a+b) + \eta(a+\eta b) + \eta^2(a+\eta^2 b) \\ &= a(1+\eta+\eta^2) + b(1+\eta^4+\eta^2) \\ &= (a+b)(1+\eta+\eta^2) \\ &= (a+b)0 = 0 \end{aligned}$$

$\square$

Lemma 3.53.
Let S be a *solution*.

Then u_4 is a unit.

Proof. By Definition 3.46 $u_4 = \eta u_3 u_2^{-1}$, which is a product of units by Lemma 2.17. Since the product of units is a unit (multiplicative closure), it follows that u_4 must also be a unit. $\square$

Lemma 3.54.
Let S be a *solution*.

Then u_5 is a unit.

Proof. By Definition 3.46 $u_5 = -\eta^2 u_1 u_2^{-1}$, which is a product of units since $\eta^3 = 1$ by Lemma 2.16 and $-\eta(-\eta^2) = \eta^3$. Since the product of units is a unit (multiplicative closure), it follows that u_5 must also be a unit. $\square$

Lemma 3.55.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let S be a *solution* with multiplicity n.

Then $Y^3 + u_4 Z^3 = u_5(\lambda^(n-1)X)^3$.

Proof. Using Lemma 2.17, Lemma 2.9, it suffices to show that

$$\lambda\eta u_2(Y^3 + u_4 Z^3) = \lambda\eta u_2 u_5(\lambda^(n-1)X)^3$$

which can be proved by simple calculations involving Lemma 2.16, Lemma 3.18 and Lemma 3.52. □

Lemma 3.56.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let S be a *solution*.

Then $\lambda^2 \mid \lambda^4$.

Proof. Straightforward application of the definition of divisibility. □

Lemma 3.57.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let S be a *solution* with multiplicity n.

Then $\lambda^2 \mid u_5(\lambda^{n-1}X)^3$.

Proof. Using Lemma 3.18, we have that $\lambda^2 \mid \lambda^2 u_5 \lambda^{3n-5} X^3 = u_5(\lambda^{n-1}X)^3$. □

Lemma 3.58.
Let S be a *solution*.

Then $u_4 \in \{-1, 1\} \subset \mathcal{O}_K$.

Proof. Let $n \in \mathbb{N}$ be the multiplicity of the solution S.
By Theorem 2.4, it suffices to prove that

$$\exists m \in \mathbb{Z} \text{ such that } \lambda^2 \mid u_4 - m.$$

By Lemma 2.23 and Lemma 3.49, we have that

$$(\lambda^4 \mid Y^3 - 1) \vee (\lambda^4 \mid Y^3 + 1).$$

By Lemma 2.23 and Lemma 3.50, we have that

$$(\lambda^4 \mid Z^3 - 1) \vee (\lambda^4 \mid Z^3 + 1).$$

We proceed by analysing each case:

- Case $(\lambda^4 \mid Y^3 - 1) \wedge (\lambda^4 \mid Z^3 - 1)$.
  Let $m = -1$ and consider the fact that

  $$u_4 - m = Y^3 + u_4 Z^3 - (Y^3 - 1) - u_4(Z^3 - 1).$$

  By Lemma 3.55, we have that

  $$u_4 - m = u_5(\lambda^{n-1} X)^3 - (Y^3 - 1) - u_4(Z^3 - 1).$$

  Since, by Lemma 3.57, we know that

  $$\lambda^2 \mid u_5(\lambda^{n-1} X)^3$$

  and, by Lemma 3.56 and by assumption, we have that

  $$\lambda^2 \mid Y^3 - 1 \wedge \lambda^2 \mid Z^3 - 1,$$

  Then, we can conclude that

  $$\lambda^2 \mid u_4 - m.$$

- Case $(\lambda^4 \mid Y^3 - 1) \wedge (\lambda^4 \mid Z^3 + 1)$.
  Let $m = 1$ and proceed similarly to the first case.
- Case $(\lambda^4 \mid Y^3 + 1) \wedge (\lambda^4 \mid Z^3 - 1)$.
  Let $m = 1$ and proceed similarly to the first case.
- Case $(\lambda^4 \mid Y^3 + 1) \wedge (\lambda^4 \mid Z^3 + 1)$.
  Let $m = -1$ and proceed similarly to the first case.

□

Lemma 3.59.
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let S be a *solution* with multiplicity n.

Then $Y^3 + (u_4 Z)^3 = u_5(\lambda^{n-1}X)^3$.

Proof. By Lemma 3.58, we have that $u_4 \in \{-1, 1\}$, which implies that $u_4^2 = 1$. Therefore, by Lemma 3.55, we can conclude that

$$Y^3 + (u_4 Z)^3 = u_5(\lambda^{n-1}X)^3.$$

□

Definition 3.60 (Final Solution')**.**
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $S = (a, b, c, u)$ be a *solution* with multiplicity n.
Let $S'_f = (Y, u_4 Z, \lambda^{n-1}X, u_5)$.

Then S'_f is a *solution*$'$.

Lemma 3.61.
Let S be a *solution* with multiplicity n.

Then S'_f has multiplicity $n - 1$.

Proof. Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.

Let $(a', b', c', u') = S'_f$ be the final *solution'*, then $\lambda^{n-1} \mid \lambda^{n-1}X = c'$. By contradiction we assume that $\lambda^n \mid c'$ which implies that $\lambda \mid X$, that contradicts Lemma 3.48 forcing us to conclude that $\lambda^n \nmid c'$. Then S'_f has multiplicity $n-1$. □

Lemma 3.62.
Let S be a *solution* with multiplicity n.

Then S'_f has multiplicity $m < n$.

Proof. It directly follows from Lemma 3.61 since $m = n - 1 < n$. □

Theorem 3.63.
Let S be a *solution* with multiplicity n.

Then there is a *solution* with multiplicity $m < n$.

Proof. It directly follows from Lemma 3.61 and Lemma 3.62. □

Theorem 3.64 (Generalised Fermat's Last Theorem for Exponent 3)**.**
Let $K = \mathbb{Q}(\zeta_3)$ be the third cyclotomic field.
Let $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ be the ring of integers of K.
Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$.
Let $\zeta_3 \in K$ be any primitive third root of unity.
Let $\eta \in \mathcal{O}_K$ be the element corresponding to $\zeta_3 \in K$.
Let $\lambda \in \mathcal{O}_K$ be such that $\lambda = \eta - 1$.
Let $a, b, c \in \mathcal{O}_K$ and $u \in \mathcal{O}_K^\times$ such that $c \neq 0$ and $\gcd(a, b) = 1$.
Let $\lambda \nmid a$, $\lambda \nmid b$ and $\lambda \mid c$.

Then $a^3 + b^3 \neq uc^3$.

Proof. By contradiction we assume that there are $a, b, c \in \mathcal{O}_K$ and $u \in \mathcal{O}_K^\times$ such that $c \neq 0$, $\gcd(a, b) = 1$, $\lambda \nmid a$, $\lambda \nmid b$, $\lambda \mid c$ and $a^3 + b^3 = uc^3$. Then $S' = (a, b, c, u)$ is a *solution'*, which implies that there is a *solution* S by Lemma 3.22. Then, by Lemma 3.13, there is a minimal solution S_0 with multiplicity n. Hence, there is a *solution'* S'_1 with multiplicity $m < n$ by Theorem 3.63, which implies that there is a *solution* S_1 with multiplicity m by Lemma 3.22. However, this contradicts the minimality of S_0 forcing us to conclude that $a^3 + b^3 \neq uc^3$. □

Lemma 3.65.
To prove Theorem 3.66, it suffices to prove Theorem 3.64.
Equivalently, Theorem 3.64 implies Theorem 3.66.

Proof. Assume that $\forall a, b, c \in \mathcal{O}_K$, $\forall u \in \mathcal{O}_K^\times$ such that $c \neq 0$, $\gcd(a, b) = 1$, $\lambda \nmid a$, $\lambda \nmid b$ and $\lambda \mid c$, it holds that $a^3 + b^3 \neq uc^3$. Let $a, b, c \in \mathbb{Z}$ such that $a \neq 0$, $b \neq 0$ and $c \neq 0$. By Theorem 3.6, we can assume that $\gcd(a, b) = 1$, $3 \nmid a$, $3 \nmid b$, $3 \mid c$. By contradiction we assume that $a^3 + b^3 = c^3$ and let $u = 1$.

- By contradiction we assume that $\lambda \mid a$, which implies that the norm of λ divides a by Lemma 2.6, which implies that $3 \mid a$ by Lemma 2.5, that contradicts the assumption that $3 \nmid a$ forcing us to conclude that $\lambda \nmid a$.
- By contradiction we assume that $\lambda \mid b$, which implies that the norm of λ divides b by Lemma 2.6, which implies that $3 \mid b$ by Lemma 2.5, that contradicts the assumption that $3 \nmid b$ forcing us to conclude that $\lambda \nmid b$.
- $\lambda \mid 3$ by Lemma 2.7 and $3 \mid c$, then $\lambda \mid c$.

By our first assumption $a^3 + b^3 \neq uc^3 = 1c^3 = c^3 = a^3 + b^3$ which is absurd. □

3.3 Conclusion

Theorem 3.66 (Fermat's Last Theorem for Exponent 3)**.**
Let $a, b, c \in \mathbb{N}$.
Let $a \neq 0$, $b \neq 0$ and $c \neq 0$.

Then $a^3 + b^3 \neq c^3$.

Proof. By Lemma 3.65 and Theorem 3.64, we can conclude that

$$a^3 + b^3 \neq c^3.$$

□

Acknowledgements

I am immensely grateful to Riccardo Brasca for his exceptional supervision throughout the entire formalisation project. His guidance was pivotal in the coordination and execution of this work.

I extend my deepest appreciation to my colleagues Sanyam Gupta, Omar Haddad, David Lowry-Duda, Lorenzo Luccioli, Alexis Saurin, and Florent Schaffhauser. Their collaboration was essential in addressing the challenges we faced.

Special thanks are due to Floris van Doorn, whose expertise in the foundations of the Lean programming language was invaluable in order to debug and optimise the code for some of the most challenging formal proofs.

I would also like to acknowledge the organisers of the conference *Lean for the Curious Mathematician 2024*. Their efforts provided us with a wonderful platform to share our work and insights, fostering further dialogue and collaboration in the community.

This project would not have been possible without the collective effort and support of all mentioned, for which I am profoundly thankful.

References

[1] Jeremy Avigad. *Mathematical Logic and Computation.* Cambridge University Press, 2022. URL: http://dx.doi.org/10.1017/9781108778756.

[2] Jeremy Avigad. "Mathematics and the Formal Turn." In: *Bulletin of the American Mathematical Society* (2024). URL: http://dx.doi.org/10.1090/bull/1832.

[3] Jeremy Avigad. "Varieties of Mathematical Understanding." In: *Bulletin of the American Mathematical Society* (2021). URL: http://dx.doi.org/10.1090/bull/1726.

[4] Jeremy Avigad, Floris van Doorn, and Robert Lewis. *Logic and Proof.* URL: https://leanprover.github.io/logic_and_proof/.

[5] Jeremy Avigad and Patrick Massot. *Mathematics in Lean.* URL: https://leanprover-community.github.io/mathematics_in_lean/.

[6] Jeremy Avigad et al. *Theorem Proving in Lean 4.* URL: https://leanprover.github.io/theorem_proving_in_lean4/.

[7] Alexander Bentkamp et al. "Mechanical Mathematicians." In: *Communications of the ACM* (2023). URL: http://dx.doi.org/10.1145/3557998.

[8] Nicolas Bourbaki. "Algebraic Structures." In: *Algebra I: Chapters 1-3.* 1989. URL: http://dx.doi.org/10.1007/978-3-540-64243-5.

[9] Nicolas Bourbaki. "Description of Formal Mathematics." In: *Theory of Sets.* 2004. URL: http://dx.doi.org/10.1007/978-3-642-59309-3_2.

[10] Kevin Buzzard. *The Fermat's Last Theorem Project.* 2024.

[11] Kevin Buzzard, Johan Commelin, and Patrick Massot. "Formalising Perfectoid Spaces." In: *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs.* 2020. URL: http://dx.doi.org/10.1145/3372885.3373830.

[12] Mario Carneiro. *The Type Theory of Lean.* 2019. URL: https://github.com/digama0/lean-type-theory/releases/tag/v1.0.

[13] David Thrane Christiansen. *Functional Programming in Lean.* URL: https://lean-lang.org/functional_programming_in_lean/.

[14] The Mathlib Community. "The Lean Mathematical Library." In: *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs.* 2020. URL: http://dx.doi.org/10.1145/3372885.3373824.

[15] Floris van Doorn, Gabriel Ebner, and Robert Y. Lewis. "Maintaining a Library of Formal Mathematics." In: *Intelligent Computer Mathematics*. 2020. URL: http://dx.doi.org/10.1007/978-3-030-53518-6_16.

[16] Jesse Michael Han and Floris van Doorn. "A Formal Proof of the Independence of the Continuum Hypothesis." In: *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*. 2020. DOI: 10.1145/3372885.3373826. URL: http://dx.doi.org/10.1145/3372885.3373826.

[17] Marc Hindry. *Arithmetics*. Springer London, 2011. URL: http://dx.doi.org/10.1007/978-1-4471-2131-2.

[18] Jannis Limperg and Asta Halkjær From. "Aesop: White-Box Best-First Proof Search for Lean." In: *Proceedings of the 12th ACM SIGPLAN International Conference on Certified Programs and Proofs*. 2023. URL: http://dx.doi.org/10.1145/3573105.3575671.

[19] David Lowry-Duda. *FLT3 at Lean for the Curious Mathematician 2024*. 2024. URL: https://davidlowryduda.com/flt3-at-lftcm2024/.

[20] Heather Macbeth. *The Mechanics of Proof*. URL: https://hrmacbeth.github.io/math2001/.

[21] Daniel A. Marcus. *Number Fields*. Springer International Publishing, 2018. URL: http://dx.doi.org/10.1007/978-3-319-90233-3.

[22] Leonardo de Moura and Sebastian Ullrich. "The Lean 4 Theorem Prover and Programming Language." In: *Lecture Notes in Computer Science*. 2021. URL: https://doi.org/10.1007/978-3-030-79876-5_37.

[23] H. P. F. Swinnerton-Dyer. *A Brief Guide to Algebraic Number Theory*. Cambridge University Press, 2001. URL: http://dx.doi.org/10.1017/CBO9781139173360.

[24] Daniel Velleman. *How To Prove It With Lean*. URL: https://djvelleman.github.io/HTPIwL/.

[25] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer New York, 1997. URL: http://dx.doi.org/10.1007/978-1-4612-1934-7.