Fermat's Last Theorem Through a Geometric Lens

Alex Massarenti

Abstract

These notes are meant for a one-hour seminar aimed at early undergraduate students, with accessible windows for advanced high-school students. We introduce the projective plane, projective plane curves, and the genus of a smooth complex curve as the number of holes of its associated compact surface. We then interpret Fermat-type equations as questions about rational points on the Fermat curves, prove Fermat's Last Theorem for $n = 2, 4, 3$ (with fully explicit infinite descent for $n = 4$ and a full Eisenstein-integers/Euler descent for $n = 3$), and conclude with a roadmap of Wiles proof via modularity (Taniyama–Shimura–Weil), the Frey curve, and Ribet's theorem.

Contents

1 Projective geometry and projective plane curves

Definition 1.1. Let k be a field. The *projective plane over* k is

$$\mathbb{P}^2(k) \;=\; \big(k^3 \setminus \{(0,0,0)\}\big)/\sim$$

where $(X, Y, Z) \sim (\lambda X, \lambda Y, \lambda Z)$ for all $\lambda \in k^\times$. We denote the equivalence class of (X, Y, Z) by $[X : Y : Z]$ and call (X, Y, Z) *homogeneous coordinates*.

Remark 1.2. The sets $U_Z = \{Z \neq 0\}$, $U_X = \{X \neq 0\}$, $U_Y = \{Y \neq 0\}$ cover $\mathbb{P}^2$. On U_Z we normalize $Z = 1$ and identify $[X : Y : 1]$ with the affine point $(x, y) = (X/Z, Y/Z) \in \mathbb{A}^2$.

Definition 1.3. A *projective line* in $\mathbb{P}^2(k)$ is the zero locus of a nonzero linear homogeneous form

$$aX + bY + cZ = 0 \qquad (a, b, c \in k, \text{ not all } 0).$$

Proposition 1.4. *Any two distinct projective lines in $\mathbb{P}^2(k)$ intersect in exactly one point of $\mathbb{P}^2(k)$.*

Proof. Two distinct linear equations in X, Y, Z define a 1-dimensional solution space in k^3. Passing to projective classes gives a unique point of intersection. □

Definition 1.5. A *(plane) projective curve* over k is a subset

$$C = V(F) \subset \mathbb{P}^2$$

defined by a nonzero homogeneous polynomial $F(X, Y, Z) \in k[X, Y, Z]$. The *degree* of C is $\deg(F)$.

Definition 1.6. Let $C = V(F) \subset \mathbb{P}^2(k)$ where F is homogeneous. A point $P \in C$ is *singular* if

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0,$$

and *smooth* otherwise. The curve C is *smooth* if it has no singular points.

Remark 1.7 (Why smoothness matters). Over $\mathbb{C}$, a smooth projective curve is naturally a compact Riemann surface, hence a connected compact oriented topological surface. This is where the genus gets a vivid geometric meaning.

1.1 Genus as number of holes

Definition 1.8. Let S be a connected compact oriented surface. Its *genus* $g(S)$ is the number of handles (holes): $g = 0$ for a sphere, $g = 1$ for a torus, etc. Equivalently, the Euler characteristic satisfies

$$\chi(S) = 2 - 2g(S).$$

Definition 1.9. If $C/\mathbb{C}$ is a smooth projective curve, its *genus* $g(C)$ is the topological genus of the associated compact Riemann surface.

Theorem 1.10. *If $C \subset \mathbb{P}^2(\mathbb{C})$ is a smooth plane curve of degree $d \geq 1$, then*

$$g(C) = \frac{(d-1)(d-2)}{2}.$$

Example 1.11. A line ($d = 1$) has genus 0. A smooth conic ($d = 2$) has genus 0. A smooth cubic ($d = 3$) has genus 1 (these are elliptic curves).

Remark 1.12. Genus zero curves with a rational point often admit a rational parametrization (like the circle). Positive genus curves are typically much more rigid: rational parametrizations usually do not exist, and rational points become subtle.

2 Fermat curves and rational points

Fix an integer $n \geq 2$ and consider the *Fermat curve*

$$F_n : \quad (X^n + Y^n = Z^n) \subset \mathbb{P}^2.$$

Proposition 2.1. *There exists a nonzero integer triple $(x, y, z) \in \mathbb{Z}^3$ with $x^n + y^n = z^n$ if and only if $F_n(\mathbb{Q}) \neq \varnothing$. Moreover, solutions with $xyz \neq 0$ correspond to points $[X : Y : Z] \in F_n(\mathbb{Q})$ with $XYZ \neq 0$.*

Proof. If $(x, y, z) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ satisfies $x^n + y^n = z^n$, then $[x : y : z] \in \mathbb{P}^2(\mathbb{Q})$ lies on F_n. Conversely, if $[a : b : c] \in F_n(\mathbb{Q})$, choose representatives $a, b, c \in \mathbb{Q}$ with $a^n + b^n = c^n$. Multiplying by a common denominator d gives integers $A = da$, $B = db$, $C = dc$ with $A^n + B^n = C^n$. □

In characteristic zero, F_n is smooth, so Theorem 1.10 applies.

Proposition 2.2. *Over* $\mathbb{C}$*,*

$$g(F_n) = \frac{(n-1)(n-2)}{2}.$$

Thus $n = 2 \Rightarrow g = 0$, $n = 3 \Rightarrow g = 1$, $n \geq 4 \Rightarrow g \geq 3$.

Theorem 2.3 (Wiles–Taylor (Fermat's Last Theorem))**.** *For every integer* $n > 2$*, the Diophantine equation*

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

has no solution in nonzero integers x, y, z*.*

Equivalently, for $n > 2$ *the Fermat curve*

$$F_n : \ (X^n + Y^n = Z^n) \subset \mathbb{P}^2$$

has no $\mathbb{Q}$*-rational point with* $XYZ \neq 0$*.*

Remark 2.4 (Historical note). Fermat wrote the statement in the margin of his copy of Diophantus' *Arithmetica* around **1637**, claiming he had a truly marvelous proof but the margin was too small to contain.

Over the centuries, many partial results were proved:

- **Fermat (1640s; published posthumously)** proved the case $n = 4$ by *infinite descent* (essentially the argument given in Section 4.1).
- **Euler (1770)** proved the case $n = 3$ using what we would now call algebraic number theory (in the ring of Eisenstein integers).
- **Sophie Germain (1810s–1820s)** proved a major theorem covering infinitely many prime exponents, introducing what are now called "Sophie Germain primes" and a powerful descent strategy.
- **Dirichlet and Legendre (1825)** proved $n = 5$; **Lamé (1839)** proved $n = 7$.
- **Kummer (1847)** proved FLT for a large class of primes (the *regular primes*) by inventing "ideal numbers," a precursor of ideals in algebraic number theory.

The modern breakthrough came from linking FLT to elliptic curves and modular forms:

- **Taniyama and Shimura (1950s), refined by Weil (1960s)** formulated the modularity conjecture (now the Modularity Theorem) connecting elliptic curves over $\mathbb{Q}$ to modular forms.
- **Frey (1984)** suggested that a hypothetical Fermat solution would produce a special elliptic curve (the Frey curve).
- **Ribet (1986)** proved that such a Frey curve would contradict modularity (via the ε-conjecture), reducing FLT to a modularity statement.
- **Wiles (1993; with a crucial patch with Taylor in 1994; published 1995)** proved modularity for semistable elliptic curves over $\mathbb{Q}$, which (together with Ribet) implies Theorem 2.3.

Lemma 2.5 (Reduction)**.** *If there is a nontrivial integer solution to* $x^n + y^n = z^n$ *with* $n > 2$*, then:*

- *for any prime* $p \mid n$ *there is a nontrivial solution to* $x^p + y^p = z^p$*, and*
- *if* $4 \mid n$ *there is a nontrivial solution to* $x^4 + y^4 = z^4$*.*

Proof. If $p \mid n$ and $n = pm$, then from $x^n + y^n = z^n$ we get $(x^m)^p + (y^m)^p = (z^m)^p$. If $4 \mid n$ and $n = 4m$, similarly $(x^m)^4 + (y^m)^4 = (z^m)^4$. Nontriviality is preserved if $xyz \neq 0$. □

So proving FLT for $n = 4$ and for all odd primes p implies FLT for all $n > 2$.

3 The case $n = 2$: Pythagoras, the circle, and parametrization

The case $n = 2$ is the Pythagorean equation

$$x^2 + y^2 = z^2,$$

which is equivalent to the Pythagorean theorem in Euclidean geometry.

Definition 3.1. A *Pythagorean triple* is $(x, y, z) \in \mathbb{Z}^3$ with $x^2 + y^2 = z^2$. It is *primitive* if $\gcd(x, y, z) = 1$.

Theorem 3.2 (Euclid's parametrization)**.** *Every primitive Pythagorean triple is, up to swapping x and y, of the form*

$$x = m^2 - n^2, \qquad y = 2mn, \qquad z = m^2 + n^2,$$

for coprime integers $m > n > 0$ of opposite parity.

Consider the affine curve $X^2 + Y^2 = 1$. It has the rational point $(-1, 0)$. Any line through $(-1, 0)$ with rational slope $t \in \mathbb{Q}$ has equation $Y = t(X + 1)$. Substituting into $X^2 + Y^2 = 1$ and solving yields the rational parametrization

$$X(t) = \frac{1 - t^2}{1 + t^2}, \qquad Y(t) = \frac{2t}{1 + t^2}.$$

Clearing denominators gives Euclid's formula in Theorem 3.2.

Remark 3.3 (Genus viewpoint). The conic $X^2 + Y^2 = Z^2$ has genus 0, and the existence of one rational point forces infinitely many via lines and rational parametrization.

4 The case $n = 4$: Fermat's infinite descent

We prove a stronger statement than FLT for $n = 4$.

Theorem 4.1 (Fermat's right triangle theorem)**.** *There are no positive integers x, y, z such that*

$$x^4 + y^4 = z^2.$$

Corollary 4.2 (FLT for $n = 4$)**.** *There are no nonzero integers x, y, z such that $x^4 + y^4 = z^4$.*

Proof. If $x^4 + y^4 = z^4$, then $x^4 + y^4 = (z^2)^2$, contradicting Theorem 4.1. □

Lemma 4.3 (Primitive Pythagorean triples)**.** *Let $(A, B, C) \in \mathbb{Z}^3_{>0}$ satisfy $A^2 + B^2 = C^2$ and $\gcd(A, B, C) = 1$. Then exactly one of A, B is even. If A is even and B is odd, there exist coprime integers $m > n > 0$ of opposite parity such that*

$$A = 2mn, \qquad B = m^2 - n^2, \qquad C = m^2 + n^2.$$

Proof. Standard: from $(C - B)(C + B) = A^2$, show $\gcd(C - B, C + B) = 2$, write $C \pm B = 2(\text{square})$, and solve. □

Lemma 4.4 (Coprime factors of a square are squares)**.** *If $r, s \in \mathbb{Z}_{>0}$ are coprime and rs is a perfect square, then both r and s are perfect squares. More generally, if $r_1, \ldots, r_k$ are pairwise coprime and $r_1 \cdots r_k$ is a square, then each r_i is a square.*

Proof. Prime-exponent argument: if $p^e \| r$ with e odd, then p would appear to odd exponent in rs. □

Proof of Theorem 4.1. Assume, by contradiction, that solutions exist. Consider the nonempty set

$$\mathcal{Z} := \{\, z \in \mathbb{Z}_{>0} \mid \exists\, x, y \in \mathbb{Z}_{>0} \text{ with } x^4 + y^4 = z^2 \,\}.$$

By well-ordering, choose a solution (x, y, z) with z minimal in $\mathcal{Z}$.

Step 1: The solution is primitive. Let $d = \gcd(x, y)$. Then $d^4 \mid x^4 + y^4 = z^2$, so $d^2 \mid z$. Write $x = dx_1$, $y = dy_1$, $z = d^2 z_1$. Then $x_1^4 + y_1^4 = z_1^2$. By minimality, $d = 1$, hence $\gcd(x, y) = 1$.

Step 2: A primitive Pythagorean triple. We have $(x^2)^2 + (y^2)^2 = z^2$. Since $\gcd(x, y) = 1$, also $\gcd(x^2, y^2, z) = 1$. Thus (x^2, y^2, z) is a primitive Pythagorean triple. Exactly one of x^2, y^2 is even, hence exactly one of x, y is even. Assume x is even and y is odd.

By Lemma 4.3, there exist coprime integers $m > n > 0$ of opposite parity such that

$$x^2 = 2mn, \qquad y^2 = m^2 - n^2, \qquad z = m^2 + n^2. \tag{1}$$

Step 3: A second primitive Pythagorean triple. From $y^2 = m^2 - n^2$ we get $n^2 + y^2 = m^2$. Because $\gcd(m, n) = 1$ and $\gcd(n, y) = 1$, the triple (n, y, m) is primitive. Since y is odd, the even leg must be n; thus n is even.

Apply Lemma 4.3 again to (n, y, m): there exist coprime integers $r > s > 0$ of opposite parity such that

$$n = 2rs, \qquad y = r^2 - s^2, \qquad m = r^2 + s^2. \tag{2}$$

Step 4: Force squares. From $x^2 = 2mn$ and $n = 2rs$ we obtain

$$x^2 = 4mrs.$$

Hence $(x/2)^2 = mrs$ is a perfect square. We claim m, r, s are pairwise coprime: $\gcd(r, s) = 1$ by construction, and $\gcd(m, r) = \gcd(m, s) = 1$ because $\gcd(m, n) = 1$ and $n = 2rs$.

Therefore, by Lemma 4.4, each of m, r, s is a square:

$$m = w^2, \qquad r = u^2, \qquad s = v^2$$

for some $u, v, w \in \mathbb{Z}_{>0}$.

Step 5: Produce the smaller solution. From $m = r^2 + s^2$ we get

$$w^2 = u^4 + v^4.$$

So (u, v, w) is a positive integer solution of the same type $u^4 + v^4 = w^2$.

Step 6: Strict decrease. From (1) we have $z = m^2 + n^2$ with $m = w^2$ and $n = 2rs = 2u^2v^2 \neq 0$, hence

$$z = w^4 + (2u^2v^2)^2 > w^4 \geq w.$$

So $0 < w < z$, contradicting the minimality of z. Therefore no solutions exist. □

5 The case $n = 3$: Eisenstein integers (Euler's descent)

We prove that $x^3 + y^3 = z^3$ has no nontrivial integer solutions, in a symmetric form convenient for descent.

5.1 Eisenstein integers are Euclidean

Let

$$\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{i\sqrt{3}}{2}, \qquad \omega^2 + \omega + 1 = 0.$$

The *Eisenstein integers* are

$$\Lambda := \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Define the norm

$$N(a + b\omega) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2 \in \mathbb{Z}_{\geq 0}.$$

Then $N(\alpha\beta) = N(\alpha)N(\beta)$. The units are exactly the elements of norm 1: $\{\pm 1, \pm\omega, \pm\omega^2\}$.

Lemma 5.1 (Euclidean algorithm in Λ)**.** *For any $\alpha, \beta \in \Lambda$ with $\beta \neq 0$, there exist $q, r \in \Lambda$ such that $\alpha = \beta q + r$ and $N(r) < N(\beta)$. Hence Λ is a Euclidean domain, so a PID and a UFD.*

Proof. View $\alpha/\beta \in \mathbb{C}$. The lattice Λ tiles the plane by equilateral triangles of side 1, so there exists $q \in \Lambda$ with $|\alpha/\beta - q| \leq 1/\sqrt{3}$. Set $r = \alpha - \beta q$. Then

$$N(r) = |\alpha - \beta q|^2 = |\beta|^2 \, |\alpha/\beta - q|^2 \leq |\beta|^2 \cdot \frac{1}{3} < |\beta|^2 = N(\beta).$$

□

5.2 A crucial cube lemma

The identity $1 + 2\omega = i\sqrt{3}$ will be used repeatedly.

Lemma 5.2 (Cubes represented by $u^2 + 3v^2$)**.** *Let $u, v \in \mathbb{Z} \setminus \{0\}$ be coprime. The following are equivalent.*

(i) There exists $s \in \mathbb{Z}$ such that

$$u^2 + 3v^2 = s^3.$$

(ii) There exist $a, b \in \mathbb{Z}$ such that

$$u = a(a^2 - 9b^2), \qquad v = 3b(a^2 - b^2), \qquad s = a^2 + 3b^2.$$

(iii) There exist $a, b \in \mathbb{Z}$ such that

$$u + iv\sqrt{3} = (a + ib\sqrt{3})^3.$$

Proof. (iii) $\Rightarrow$ (ii) by direct expansion:

$$(a + ib\sqrt{3})^3 = a^3 + 3a^2(ib\sqrt{3}) + 3a(ib\sqrt{3})^2 + (ib\sqrt{3})^3 = \left(a^3 - 9ab^2\right) + i\sqrt{3}\left(3a^2b - 3b^3\right),$$

so $u = a^3 - 9ab^2 = a(a^2 - 9b^2)$ and $v = 3a^2b - 3b^3 = 3b(a^2 - b^2)$. Also

$$|a + ib\sqrt{3}|^2 = a^2 + 3b^2,$$

so taking absolute values gives $u^2 + 3v^2 = (a^2 + 3b^2)^3$, proving $s = a^2 + 3b^2$.

(ii) $\Rightarrow$ (i) is the same computation in reverse.

It remains to show (i) $\Rightarrow$ (iii). Assume $u^2 + 3v^2 = s^3$ with $\gcd(u, v) = 1$ and $uv \neq 0$.

Step 1: u and v have opposite parity. If u and v were both odd, then $u^2 + 3v^2 \equiv 1 + 3 \equiv 4 \pmod 8$, which cannot be a cube (mod 8, cubes are $0, \pm 1$). Thus they have opposite parity.

Step 2: u is not divisible by 3. If $3 \mid u$ then $3 \nmid v$ and $u^2 + 3v^2 \equiv 3 \pmod 9$, but cubes are $\equiv 0, \pm 1 \pmod 9$.

Step 3: $\gcd(2u, u^2 + 3v^2) = 1$. Since $u^2 + 3v^2$ is odd by Step 1 and $3 \nmid u$ by Step 2, any prime $p \mid 2u$ satisfies $p \notin \{2, 3\}$, so $p \mid u$ implies $p \nmid v$ and hence $p \nmid u^2 + 3v^2$.

Step 4: Coprimality in Λ. If $k, \ell \in \mathbb{Z}$ are coprime, then k and ℓ are coprime in Λ: if $x \in \Lambda$ satisfies $k/x, \ell/x \in \Lambda$, then $k^2/N(x), \ell^2/N(x) \in \mathbb{Z}$, so $N(x)$ divides both k^2 and ℓ^2, hence $N(x) = 1$ and x is a unit.

Step 5: Two Eisenstein integers are coprime. Consider

$$\alpha := u + v + 2v\omega = u + v(1 + 2\omega) = u + iv\sqrt{3} \in \Lambda, \qquad \overline{\alpha} = u - iv\sqrt{3} = u - v - 2v\omega \in \Lambda.$$

We claim α and $\overline{\alpha}$ are coprime in Λ. Indeed, if $x \in \Lambda$ divides both, then x divides their sum $2u$ and their product

$$\alpha\,\overline{\alpha} = u^2 + 3v^2.$$

By Step 3, $2u$ and $u^2 + 3v^2$ are coprime in $\mathbb{Z}$, hence coprime in Λ by Step 4. Thus x must be a unit.

Step 6: α is a cube up to a unit. We have $\alpha\,\overline{\alpha} = s^3$. Factor s into primes in the UFD Λ (Lemma 5.1). Since α and $\overline{\alpha}$ are coprime (Step 5), unique factorization implies

$$\alpha = \varepsilon\beta^3 \quad \text{for some } \beta \in \Lambda,\ \varepsilon \in \Lambda \text{ a unit.}$$

Step 7: The unit is real, hence $\varepsilon = \pm 1$. Write $\beta = k + \ell\omega$ with $k, \ell \in \mathbb{Z}$. If ε is non-real (i.e. $\pm\omega$ or $\pm\omega^2$), then writing $\alpha = \varepsilon\beta^3$ and converting to the $1, i\sqrt{3}$ basis forces both u and v to be even, contradicting Step 1. Hence $\varepsilon = \pm 1$.

Absorbing the sign into β if necessary, we may assume $\alpha = \beta^3$.

Step 8: Convert β to $a + ib\sqrt{3}$. Every element of Λ can be written uniquely as

$$\beta = a + ib\sqrt{3} \qquad (a, b \in \mathbb{Z}),$$

because $\omega = \frac{-1 + i\sqrt{3}}{2}$. Thus

$$u + iv\sqrt{3} = \alpha = \beta^3 = (a + ib\sqrt{3})^3,$$

which is (iii). This completes the proof. □

5.3 FLT for exponent 3 (full descent)

Theorem 5.3 (Fermat's Last Theorem for $n = 3$)**.** *The equation*

$$x^3 + y^3 + z^3 = 0$$

has no integer solution with $xyz \neq 0$. Equivalently, there are no nonzero integers x, y, z with $x^3 + y^3 = z^3$ and $xyz \neq 0$.

Proof. We argue by infinite descent using the well-ordering of $\mathbb{NN}$. Let

$$F := \left\{ |xyz| \in \mathbb{NN} \,\middle|\, x, y, z \in \mathbb{Z},\ xyz \neq 0,\ x^3 + y^3 + z^3 = 0 \right\}.$$

We prove F is empty by showing it has no minimal element. Assume for contradiction that $F \neq \varnothing$ and choose a triple (x, y, z) with $|xyz|$ minimal in F.

Step 1: x, y, z are pairwise coprime. If a prime p divides two of x, y, z, then it divides the third (from $x^3 + y^3 + z^3 = 0$). Dividing by p gives a smaller element of F, contradicting minimality.

Step 2: Exactly one of x, y, z is even. At most one is even by pairwise coprimality. At least one must be even because the sum of three odd cubes is odd. By permuting variables, assume z is even. Then x and y are odd.

Step 3: Define

$$u := \frac{x + y}{2}, \qquad v := \frac{x - y}{2}.$$

Then $u, v \in \mathbb{Z}$, $u \neq 0$, $v \neq 0$, $\gcd(u, v) = 1$, and u, v have opposite parity (since x, y are odd). Moreover,

$$-z^3 = x^3 + y^3 = (u + v)^3 + (u - v)^3 = 2u^3 + 6uv^2 = 2u(u^2 + 3v^2). \tag{3}$$

Step 4: u is divisible by 4, hence u is even and v is odd. Because z is even, $-z^3$ is divisible by 8. From (3), $2u$ is divisible by 8, so u is divisible by 4. Since u, v have opposite parity, v is odd.

Now we split into two cases depending on whether $3 \mid u$.

Case A: $3 \nmid u$. We claim that $2u$ and $u^2 + 3v^2$ are coprime. Indeed $u^2 + 3v^2$ is odd (since v is odd), so a common prime divisor p of $2u$ and $u^2 + 3v^2$ cannot be 2. Also $p \neq 3$ because $3 \nmid u$ and (mod 3) we have $u^2 + 3v^2 \equiv u^2 \not\equiv 0$. Thus $p \mid u$ and $p \mid 3v^2$ imply $p \mid v$, contradicting $\gcd(u, v) = 1$.

From (3), the product $(2u)(u^2 + 3v^2)$ is a cube (up to sign), and the two factors are coprime. Hence each factor is a cube up to sign:

$$2u = r^3, \qquad u^2 + 3v^2 = s^3 \tag{4}$$

for some nonzero integers r, s.

Apply Lemma 5.2 to the second equation in (4): there exist integers a, b such that

$$u = a(a^2 - 9b^2), \qquad v = 3b(a^2 - b^2). \tag{5}$$

Then $2u = r^3$ becomes

$$r^3 = 2a(a^2 - 9b^2) = 2a(a - 3b)(a + 3b). \tag{6}$$

Claim: the integers $2a$, $a - 3b$, $a + 3b$ are pairwise coprime. First, $\gcd(a, b) = 1$: any prime dividing both a and b would divide u and v via (5). Now if a prime p divides $a - 3b$ and $a + 3b$, then p divides their sum $2a$ and difference $6b$. If $p \neq 2, 3$, then $p \mid a$ and $p \mid b$, contradiction. A short parity check using that u is even and v is odd forces a odd and b even in (5), so 2 cannot divide both $a - 3b$ and $a + 3b$. Also 3 cannot divide both (else $3 \mid a$ and $3 \mid b$). Thus the gcd is 1. Similarly one checks $\gcd(2a, a \pm 3b) = 1$ using $\gcd(a, b) = 1$ and the parity conclusion. This proves pairwise coprimality.

Because the product (6) is a cube and the factors are pairwise coprime, each factor is a cube up to sign. Thus there exist nonzero integers k, ℓ, m such that

$$k^3 = -2a, \qquad \ell^3 = a - 3b, \qquad m^3 = a + 3b.$$

Summing gives

$$k^3 + \ell^3 + m^3 = (-2a) + (a - 3b) + (a + 3b) = 0.$$

Taking the product gives

$$|k\ell m|^3 = |2a(a^2 - 9b^2)| = |2u| = |x + y|.$$

Finally,

$$|x + y| \le |x| + |y| \le 2|x||y| \le |xyz| \quad \text{and} \quad |z| \ge 2,$$

so $|k\ell m| < |xyz|$. Hence $|k\ell m| \in F$ contradicts the minimality of $|xyz|$.

Case B: $3 \mid u$**.** Write $u = 3w$ with $w \in \mathbb{Z} \setminus \{0\}$. Then (3) becomes

$$-z^3 = 2(3w)\big((3w)^2 + 3v^2\big) = 18w\,(v^2 + 3w^2).$$

Because w is even (since u is divisible by 4 and 3) and v is odd, $v^2 + 3w^2$ is odd. Also v is not divisible by 3 (else $3 \mid x - y$ and $3 \mid x + y$ would force $3 \mid x, y$, contradicting coprimality), so $v^2 + 3w^2 \not\equiv 0 \pmod 3$. Hence $\gcd(18w,\ v^2 + 3w^2) = 1$.

Thus, as in Case A, each factor is a cube up to sign:

$$18w = r^3, \qquad v^2 + 3w^2 = s^3 \tag{7}$$

for some nonzero integers r, s.

Apply Lemma 5.2 to the second equation in (7) (with $(u, v) = (v, w)$): there exist integers a, b such that

$$v = a(a^2 - 9b^2), \qquad w = 3b(a^2 - b^2). \tag{8}$$

Then $18w = r^3$ becomes

$$r^3 = 54b(a^2 - b^2) = 54b(a - b)(a + b).$$

In particular $3 \mid r$; write $r = 3r_1$. Then

$$r_1^3 = 2b(a - b)(a + b).$$

A parity check from (8) shows a is odd and b is even, and $\gcd(a, b) = 1$. It follows that $2b$, $a - b$, and $a + b$ are pairwise coprime. Hence each is a cube up to sign: there exist nonzero integers k, ℓ, m such that

$$k^3 = -2b, \qquad \ell^3 = b - a, \qquad m^3 = b + a.$$

Then $k^3 + \ell^3 + m^3 = 0$, and

$$|k\ell m|^3 = |2b(a^2 - b^2)| = \left|\frac{6w}{9}\right| = \left|\frac{2u}{9}\right| = \left|\frac{x + y}{9}\right|.$$

Since $x + y \neq 0$ and $|x + y|/9 < |x + y| \le |xyz|$, we again get $|k\ell m| < |xyz|$, contradicting minimality.

Both cases contradict the existence of a minimal element of F. Therefore $F = \varnothing$, proving the theorem. □

6 From Fermat to Wiles: modularity and the modern proof

This section sketches the modern proof of FLT while keeping geometry in view: elliptic curves (genus 1), modular curves (moduli spaces), and maps between them.

6.1 Elliptic curves and their Galois representations

A (smooth) plane cubic over $\mathbb{Q}$ has genus 1. If it has a rational point, it can be written (after a change of variables) as

$$E: \quad y^2 = x^3 + Ax + B,$$

and $E(\mathbb{Q})$ carries a natural abelian group law (secant-and-tangent construction). One also gets, for each prime ℓ, an ℓ-adic Galois representation on the Tate module:

$$\rho_{E,\ell}: \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Reducing mod ℓ gives a representation $\overline{\rho}_{E,\ell}$ over $\mathbb{F}_\ell$.

6.2 Modular forms and modular curves $X_0(N)$

A weight-2 cusp form for $\Gamma_0(N)$ has a Fourier expansion

$$f(q) = \sum_{n \geq 1} a_n q^n, \qquad q = e^{2\pi i \tau}.$$

The *modular curve* $X_0(N)$ is a projective algebraic curve whose complex points parametrize elliptic curves together with a cyclic subgroup of order N. In other words, $X_0(N)$ is a geometric moduli space.

6.3 The Taniyama–Shimura–Weil (modularity) conjecture

An elliptic curve $E/\mathbb{Q}$ is called *modular* if it is associated to a weight-2 newform, equivalently if there exists a nonconstant morphism over $\mathbb{Q}$

$$X_0(N) \longrightarrow E$$

for some N (the conductor of E). Historically this was the Taniyama–Shimura conjecture (refined by Weil), and today it is the *Modularity Theorem*.

6.4 The Frey curve and Ribet's theorem

Assume for contradiction that there is a nontrivial primitive solution

$$a^p + b^p = c^p$$

for an odd prime p. Frey observed one can attach an elliptic curve (one convenient model is)

$$E_{a,b,p}: \quad y^2 = x(x - a^p)(x + b^p).$$

This curve is *semistable* and has very special behavior at primes dividing abc.

Ribet proved that such a hypothetical Fermat solution would force a failure of modularity:

Theorem 6.1 (Ribet (informal))**.** *If a nontrivial solution to $a^p + b^p = c^p$ exists for an odd prime p, then the associated Frey curve $E_{a,b,p}$ is not modular.*

So FLT would follow from modularity of the relevant class of elliptic curves.

6.5 Wiles–Taylor: semistable elliptic curves are modular

Wiles proved (with a crucial patching argument developed with Taylor) that semistable elliptic curves over $\mathbb{Q}$ are modular.

Theorem 6.2 (Wiles–Taylor (informal))**.** *Every semistable elliptic curve over $\mathbb{Q}$ is modular.*

Combining this with Ribet yields a contradiction: the Frey curve is semistable, hence modular by Wiles–Taylor, but non-modular by Ribet. Therefore no Fermat solution exists for odd primes p, and together with the $n = 4$ case and Lemma 2.5, this proves FLT for all $n > 2$.

6.6 The $R = T$ philosophy

Very roughly, Wiles compares:

- a deformation ring R parameterizing certain lifts of a residual Galois representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$, and
- a Hecke algebra T acting on modular forms (or on the cohomology of modular curves), encoding congruences between eigenforms.

The slogan is: *Galois representations should come from modular forms.* The technical centerpiece is to show an isomorphism

$$R \cong T.$$

The Taylor–Wiles method introduces auxiliary primes and a patching argument to prove R and T have matching size and structure, forcing $R = T$ and producing the desired modular form corresponding to the elliptic curve.

7 A bare bones summary

The Fermat curve F_n has genus $g(F_n) = \frac{(n-1)(n-2)}{2}$. Hence:

- $n = 2$ gives genus 0 and a rational parametrization $\Rightarrow$ infinitely many rational/integer solutions.
- $n = 3$ gives genus 1 (elliptic) $\Rightarrow$ rich arithmetic structure and classical descent.
- $n \geq 4$ gives genus > 1: deep theorems (e.g. Faltings' theorem) imply only finitely many rational points.

Wiles' proof does not directly enumerate $F_n(\mathbb{Q})$ for $n \geq 4$; instead it translates a hypothetical Fermat point into the existence of a certain elliptic curve and then uses the geometry/arithmetic of modular curves to rule it out.

References

[1] Dietmar A. Salamon, *Euler's proof of Fermat's Last Theorem for the exponent three*, preprint (March 2025).
`https://people.math.ethz.ch/~salamon/PREPRINTS/FERMAT.pdf`

[2] Pete L. Clark, *The Fermat Equation: Fermat's Last Theorem for* $n = 4$, notes.
`https://math.hawaii.edu/~mchyba/documents/syllabus/Math499/20thcentury/Fermat-Theorem.pdf`

[3] Kenneth Ireland and Michael Rosen, *A Classical Introduction to Modern Number Theory*, Springer.

[4] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer.

[5] Fred Diamond and Jerry Shurman, *A First Course in Modular Forms*, Springer.

[6] Andrew Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics **141** (1995), 443–551.

[7] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics **141** (1995), 553–572.