

Lemma 29.1. Let p be an odd prime. Then $x^p + y^p = z^p$ has no solutions $x, y, z \in \mathbb{Z}$ with $xyz \neq 0$ if it has no solutions $x, y, z \in \mathbb{N}$.

Theorem 29.2. (Euler) The equation $x^3 + y^3 = z^3$ has no solution with $x, y, z \in \mathbb{N}$.

Proof: Suppose $x, y, z \in \mathbb{N}^3$ a solution to $x^3 + y^3 = z^3$ with $z > 0$ minimal.

Step 1. There exist $p, q \in \mathbb{N}$ such that $\gcd(p, q) = 1$, $p \not\equiv q \pmod{2}$, $p < z$ such that $2p(p^2 + 3q^2)$ is a cube.

Step 2. $\gcd(2p, p^2 + 3q^2) = 1$ or 3 .

Step 3a. If $\gcd(2p, p^2 + 3q^2) = 1$ then get a solution to FLT with smaller z .

Step 3b. If $\gcd(2p, p^2 + 3q^2) = 3$ then get a solution to FLT with smaller z .

Exercise 29.3. Prove that the only solutions to $y^2 + 2 = x^3$ with $x, y \in \mathbb{Z}$ are $(3, \pm 5)$.

[Hint: Factor $y^2 + 2$ over $\mathbb{Q}(\sqrt{-2})$, which is a UFD. See pages 439–440 of Niven-Zuckerman-Montgomery (5th ed) for more details.]

Cyclotomic Fields: Let p be prime, $\zeta_p = e^{2\pi i/p}$. The p -th cyclotomic field is $\mathbb{Q}(\zeta_p)$.

Lemma 29.6. The minimal polynomial of ζ_p is

$$x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Lemma 29.7. The polynomial $x^p + y^p$ factors as

$$(x + y)(x + \zeta_p y) \cdots (x + \zeta_p^{p-1} y).$$

Lamé (1847) tried to generalise Euler's proof to all p using cyclotomic fields, but assumed unique factorisation in $\mathbb{Z}[\zeta_p]$. This is probably the most famous of the numerous flawed proofs of FLT.