

# AI Assisted Analysis of Fermat's Last Theorem

Charles Kelly

## AI Assistance

If the analyses generated by *deepai* (<https://deepai.org/chat/mathematics>) are correct, they confirm Fermat's conjecture.

## Introduction

Pierre de Fermat (1601-1665) was a lawyer, a member of the Parliament in Toulouse, and a mathematician. His conjecture is easy to explain: he said that there are no solutions to the following equation when X, Y, and Z are positive integers, and n is a positive integer greater than two:

$$X^n + Y^n = Z^n$$

Fermat created his conjecture in 1637 when he wrote in a copy of *Arithmetica* that he had a proof that was too large to fit in the margin. In 1995, professors Taylor<sup>1</sup> and Wiles<sup>2</sup> proved the conjecture.

## Limiting the Scope of the Problem to Prime Exponents

Professor Van der Poorten<sup>3</sup> shows that it is not necessary to prove Fermat's conjecture for any positive exponent n; rather, it is sufficient to prove it when the exponent p is prime and the greatest common divisor of X and Y equals 1:

$$X^p + Y^p = Z^p \tag{1}$$

## Variables

All variables represent integers.

## Change of Variables

These new variables represent the differences among the original variables:

$$i = Z - Y$$

$$k = Z - X$$

---

<sup>1</sup> Richard Taylor and Andrew Wiles, "Ring-theoretic properties of certain Hecke algebras", *Annals of Mathematics*, Vol. 141 (1995) pp 553-572.

<sup>2</sup> Andrew Wiles, "Modular elliptic curves and Fermat's Last Theorem", *Annals of Mathematics*, Vol. 141 (1995) pp 443-551

<sup>3</sup> Alf van der Poorten, "Notes on Fermat's Last Theorem", *Canadian Mathematical Society Series of Monographs and Advanced Texts*, Wiley Interscience, 1996, Page 8, note 1.9

$$r = X - i$$

These definitions imply:

$$X = r + i$$

$$Y = r + k$$

$$Z = r + i + k$$

If  $p > 2$ , then (1) can be written as:

$$(X + Y) \sum_{m=0}^{p-1} (-1)^m X^m Y^{p-m-1} = Z^p$$

This implies that:

$$(2r + i + k) \sum_{m=0}^{p-1} (-1)^m X^m Y^{p-m-1} = (r + i + k)^p$$

$$\sum_{m=0}^{p-1} (-1)^m X^m Y^{p-m-1} = \frac{(r + i + k)^p}{(2r + i + k)}$$

Similarly,

$$X^p + Y^p = Z^p$$

$$\frac{X^p + Y^p}{Z} = Z^{p-1}$$

$$\frac{(2r + i + k) \sum_{m=0}^{p-1} (-1)^m X^m Y^{p-m-1}}{r + i + k} = Z^{p-1}$$

Performing polynomial division on the left-hand side of this equation, using  $r$  as the reference variable, yields<sup>44</sup> a polynomial remainder of  $-(i^p + k^p)$ , which implies that

$$\frac{i^p + k^p}{r + i + k}$$

is an integer (because all the variables in the polynomial quotient are integers).

---

<sup>44</sup> <https://github.com/FermatAndAI/documents/blob/main/raw%20output%20from%20deepai/remainder.pdf>

Therefore, both of these expressions must (simultaneously) be integers:

$$\frac{(r+i+k)^p}{(2r+i+k)} \text{ and } \frac{i^p + k^p}{r+i+k}$$

If we use the following prompt:

given integers p, r, i, k, where p is prime and greater than 2, none of (i+k), r, i, k equal to zero, can the following expressions simultaneously be integers:  $(r+i+k)^p/(2r+i+k)$ ,  $(i^p + k^p)/(r+i+k)$

deepai responds with:

Conclusion. Except for the very special (and easily described) choice  $2r+i+k = \pm 1$ , there is no way to make both  $(r+i+k)^p/(2r+i+k)$  and  $(i^p + k^p)/(r+i+k)$  simultaneously integers once  $p > 2$  and none of r,i,k or i+k vanishes. (full response on github<sup>5</sup>)

Since the two fractions cannot simultaneously be integers, Fermat's conjecture is correct.

---

<sup>5</sup> [documents/raw output from deepai/simultaneous integers.pdf at main · FermatAndAI/documents](#)