Provability of the received Fermat's Last Theorem

Richard Wayte

29 Audley Way, Ascot, Berkshire SL5 8EE, England, UK

e-mail: rwayte@googlemail.com

Research article submitted to Algebra and Number Theory 7 February 2024

Abstract. The received Theorem is transformed into a new symmetrical expression, for it to be compared with a parallel all-integer expression. Differences in the configurations of the expressions prove that components of the Theorem cannot all be integers.

1. Introduction

Pierre de Fermat's Last Theorem was formulated around 1637 and not proved until Andrew Wiles [1] did so in 1995. Over the years, enthusiasts have been fascinated by the history of this simple theorem and tried proving it using elementary arithmetic [2].

Fermat's Last Theorem states: No three positive integers a, b, c, can satisfy the equation:

$$c^p = a^p + b^p \qquad (1)$$

if (p) is an integer greater than two.

2. Proof for (p = 3)

Given the equation

$$c^3 = a^3 + b^3, \qquad (2.0)$$

let (e) be a positive integer, and set up two expressions

$$[F(a,e) = c^3 - a^3 - e^3] \quad = \quad [b^3 - e^3 = F(b,e)]. \qquad (2.1)$$

For the F(a,e) term, substitute

$$c = (a + e), \text{ and } h = (3e), \qquad (2.2a)$$

then reduce to

$$F(a,e) = a(ha + 3e^2)\ . \qquad (2.2b)$$

For the F(b,e) term, let (q) and (m) be real positive numbers such that

$$b = (q + e)\ , \qquad (2.3)$$

$$m = (q + 3e) = (b + 2e), \qquad (2.3a)$$

then reduce to

$$F(b,e) = q(mq + 3e^2). \tag{2.3b}$$

Now, equate 4xF(a,e) to 4xF(b,e), and expand thus

$$(1/h) \times \{(2ha)(2ha + 6e^2)\} = (1/m) \times \{(2mq)(2mq + 6e^2)\}\,. \tag{2.4}$$

Substitute

$$X = (2ha + 3e^2), \tag{2.4a}$$

$$Y = (2mq + 3e^2), \tag{2.4b}$$

$$E = (3e^2), \tag{2.4c}$$

and reduce to a symmetrical equation which is equivalent to Eq.(2.1):

$$(1/h) \times \{(X - E)(X + E)\} = (1/m) \times \{(Y - E)(Y + E)\}. \tag{2.4d}$$

Tests on this could involve entering (a, X) as integers, then evaluating (b, Y) as non-integers, and vice-versa. There appears to be no vantage point, so the received Theorem is unprovable thus far.

Auspiciously, by engineering an independent *all-integer* expression to compare with this in detail, it can be deduced that Eq.(2.4d) could never be all-integer. One such expression can be derived from a simple statement like

$$\{12 \times 108\} = \{18 \times 72\}\,. \tag{2.5a}$$

Integers are being used here, for brevity. Calculate the arithmetic mean of each side and expand

$$\{(60 - 48) \times (60 + 48)\} = \{(45 - 27) \times (45 + 27)\}\,, \tag{2.5b}$$

then manipulate this into the form of Eq.(2.4d)

$$(1/27^2) \times \{(60 - 48)(60 + 48)\} = (1/48^2) \times \{(80 - 48)(80 + 48)\}, \tag{2.5c}$$

or reduced to

$$(1/81) \times \{(60 - 48)(60 + 48)\} = (1/256) \times \{(80 - 48)(80 + 48)\}. \tag{2.5d}$$

Here, factors analogous to Eq.(2.4d) are ($\tilde{X}$ = 60), ($\tilde{E}$ = 48), ($\tilde{Y}$ = 80). However, denominator value [$\tilde{h} = 27^2$] originates from the right side of Eq.(2.5b) and denominator value [$\tilde{m} = 48^2$] originates from the left side. This contrasts with Eq.(2.4d) which employs [h] from Eq.(2.4) on the left side and [m] on the right. So, ($\tilde{h}$,$\tilde{m}$) are not related to ($\tilde{X}$,$\tilde{Y}$) analogous to Eq.(2.4a,b). This is the vantage point from which progress is possible, as follows:-

Any proposed all-integer Eq.(2.4d) would be indistinguishable from an equation like Eq.(2.5d), and would have to satisfy its configuration. But such agreement would pose an insuperable problem with defining (e) uniquely. In this example: [$\tilde{h} = 81 \equiv 3e$] defines [$e = 27$], while [$\tilde{E} = 48 \equiv 3e^2$] defines [$e = 4$]. Every numerical example like this would have *two* ways of defining (e), one derived from the right side and one from the left. This is not compatible with the specific derivation of Eq.(2.4d). Further requirement in accordance with Eq.(2.4) would be that ($\tilde{h}$) must divide into ($\tilde{X} - \tilde{E}$), as well as ($\tilde{m}$) must divide into ($\tilde{Y} - \tilde{E}$). These conditions cannot be satisfied, therefore an all-integer equation (2.4d) could not exist.

This numerical example Eq.(2.5) implies that a general all-integer statement

$$\{F \times G\} = \{K \times L\}, \tag{2.6a}$$

is the only source of an all-integer equation of the form

$$(1/w) \times \{(X - E)(X + E)\} = (1/z) \times \{(Y - E)(Y + E)\}, \tag{2.6b}$$

which is not compatible with the structure of Eq.(2.4d).

In summary, by designing an all-integer equation (2.5d) for comparison with the undetermined equation (2.4d), it has been possible to deduce from their differing configurations that equation (2.4d) could not be all-integer. *This definitive result means that (a) and (b) cannot both be integers, which completes the proof of the Theorem for (p = 3).*

3. Proof for (p = 4)

Given the equation

$$c^4 = a^4 + b^4, \tag{3.0}$$

let (e) be a positive integer, then set up two equal expressions

$$[F(a,e) = c^4 - a^4 - e^4] = [b^4 - e^4 = F(b,e)]. \tag{3.1}$$

For F(a,e), substitute

$$c = (a + e), \text{ and } \quad H = (4ae + 6e^2), \tag{3.2a}$$

then reduce to

$$F(a,e) = a\{Ha + 4e^3\}. \tag{3.2b}$$

For F(b,e), substitute

$$b = (q + e), \tag{3.3}$$

$$M = (q^2 + 4eq + 6e^2), \tag{3.3a}$$

then reduce to

$$F(b,e) = q\{Mq + 4e^3\}\,. \tag{3.3b}$$

Now, equate 4xF(a,e) to 4xF(b,e) and expand thus

$$(1/H) \times \{\, 2Ha(2Ha + 8e^3)\ \} \ = \ (1/M) \times \{\, 2Mq(2Mq + 8e^3)\ \}\,. \tag{3.4}$$

Make this more symmetrical by substituting

$$X = (2Ha + 4e^3), \tag{3.4a}$$

$$Y = (2Mq + 4e^3), \tag{3.4b}$$

$$E = (4e^3), \tag{3.4c}$$

and reduce to

$$(1/H) \times \{(X - E)(X + E)\} \ = \ (1/M) \times \{(Y - E)(Y + E)\}. \tag{3.4d}$$

This equation is identical in form to Eq.(2.4d) although factors are defined differently; but the subsequent insuperable logic problem of defining (e) uniquely will lead to a similar conclusion that an all-integer equation (3.4d) could not exist. Here, factor (H) from Eq.(3.2a) contains (a) and (e) but the two ways remain of defining (e) through (H) and (E).

Thus, (a) and (b) cannot both be integers; *which means that the Theorem is proved for (p = 4).*

4. Proof for (p = 5)

Given the equation:

$$c^5 = a^5 + b^5, \tag{4.0}$$

let (e) be a positive integer then set up two equal expressions

$$[F(a,e) = c^5 - a^5 - e^5\,] = \ [\,b^5 - e^5 = F(b,e)]\,. \tag{4.1}$$

For F(a,e) substitute

$$c = (a + e), \text{ and } \quad H = (5a^2e + 10ae^2 + 10e^3)\,, \tag{4.2a}$$

then reduce to

$$F(a,e) = a\{Ha + 5e^4\}. \tag{4.2b}$$

For F(b,e), substitute

$$b = (q + e), \tag{4.3}$$

$$M = (q^3 + 5eq^2 + 10e^2q + 10e^3), \tag{4.3a}$$

then reduce to

$$F(b,e) = q\{Mq + 5e^4\}\,. \qquad (4.3b)$$

Now, equate 4xF(a,e) to 4xF(b,e), and expand thus

$$(1/H) \times \{\, 2Ha(2Ha + 10e^4)\,\} = \ (1/M) \times \{\, 2Mq(2Mq + 10e^4)\,\}\,. \qquad (4.4)$$

Make this more symmetrical by substituting

$$X = (2Ha + 5e^4), \qquad (4.4a)$$

$$Y = (2Mq + 5e^4), \qquad (4.4b)$$

$$E = (5e^4), \qquad (4.4c)$$

and reduce Eq.(4.4) to

$$(1/H) \times \{(X - E)(X + E)\} \ = \ (1/M) \times \{(Y - E)(Y + E)\}. \qquad (4.4d)$$

This equation is identical in form to Eq.(2.4d) although factors are defined differently; but the subsequent insuperable logic problem of defining (e) uniquely will lead to a similar conclusion that an all-integer equation (4.4d) could not exist.

Thus, (a) and (b) cannot both be integers; *which means that the Theorem is proved for (p = 5).*

5. Proof for (p > 2)

Proofs for (p = 7, 11, 13) have also been completed, so a general proof for (p > 2) can be proposed as follows. Given the equation

$$c^p = a^p + b^p, \qquad (5.0)$$

let (e) be a positive integer, then set up two equal expressions

$$[\, F(a,e) = c^p - a^p - e^p\,] = \ [\, b^p - e^p = F(b,e)]. \qquad (5.1)$$

For F(a,e), substitute

$$c = (a + e), \text{ and } \ H = [\{(a + e)^p - a^p - e^p\} - ape^{p-1}\,]/a^2, \qquad (5.2a)$$

then reduce to

$$F(a,e) = a\{Ha + pe^{p-1}\}. \qquad (5.2b)$$

For F(b,e), substitute

$$b = (q + e), \qquad (5.3)$$

$$M = [\{(q + e)^p - e^p\} - qpe^{p-1}\,]/q^2\,, \qquad (5.3a)$$

then reduce to

$$F(b, e) = q\{Mq + pe^{p-1}\}. \qquad (5.3b)$$

Now, equate 4xF(a,e) to 4xF(b,e), and expand thus

$$(1/H) \times \{2Ha(2Ha + 2pe^{p-1})\} \; = \; (1/M) \times \{2Mq(2Mq + 2pe^{p-1})\}. \qquad (5.4)$$

Make this more symmetrical by substituting

$$X = (2Ha + pe^{p-1}), \qquad (5.4a)$$

$$Y = (2Mq + pe^{p-1}), \qquad (5.4b)$$

$$E = (pe^{p-1}), \qquad (5.4c)$$

and reduce to

$$(1/H) \times \{(X - E)(X + E)\} \; = \; (1/M) \times \{(Y - E)(Y + E)\}. \qquad (5.4d)$$

This equation is identical in form to Eq.(2.4d) although factors are defined differently; but the subsequent insuperable logic problem of defining (e) uniquely will lead to a similar conclusion that an all-integer equation (5.4d) could not exist.

Thus, (a) and (b) cannot both be integers; *which means that the Theorem is proved for (p >2).*

By introducing (p = 4) and (p = 5) herein, it would be possible to make Sections 3 and 4 redundant.

6. Conclusion

A proof of Fermat's Last Theorem has been derived using elementary arithmetic in simple steps:

First, by substitution of variables, the original cubic equation was transformed into a balanced symmetrical format. The variables of this could not be made all-integer so the basic Theorem appeared to be unprovable. Second, independent of the Theorem, a designed equation containing all-integer variables in a balanced symmetrical format was generated. Third, by comparing the structures of these two expressions in detail, it became clear that the cubic equation could not be all-integer compatible. Fourth, the quartic, quintic, and general (p > 2) equations were also transformed into their own balanced symmetrical formats which could not be made compatible with designed all-integer expressions.

In conclusion, for each value of (p), the received Theorem needed to be transformed into a symmetrical equation, for comparison with a designed all-integer symmetrical equation; then a proof by deduction was possible.

References

[1] Wiles, A.J. (1995) *"Modular elliptic curves and Fermat's Last Theorem".* Annals of Mathematics 141, No.3, pp 443-551

[2] Wikipedia. https://en.wikipedia.org/wiki/Fermat%27s_Last_Theorem