On Fermat's Last Theorem and Gödel's Incompleteness Theorem

Richard Wayte
29 Audley Way, Ascot, Berkshire SL5 8EE, England, UK
e-mail: rwayte@googlemail.com

Research article **4 February 2022**

Abstract. Fermat's Last Theorem is proved using elementary arithmetic. Connection of this proof to Gödel's Incompleteness Theorem is mentioned.

1. Introduction

Fermat's Last Theorem was formulated in 1637 and not proved until Andrew Wiles [1] did so in 1995. Over the years, enthusiasts have been encouraged by the simplicity of the theorem to prove it using elementary arithmetic [2]. A proof compatible with Gödel's Incompleteness Theorem is given.

Fermat's Last Theorem: 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 numbers such that

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

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

then reduce to

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

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

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

Make this expression more symmetrical by substituting

$$\mathrm{X} = (2\mathrm{ha} + 3\mathrm{e}^2), \qquad (2.4b)$$

$$\mathrm{Y} = (2\mathrm{mq} + 3\mathrm{e}^2), \qquad (2.4c)$$

then substitute ($E = 3e^2$), and reduce to

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

This is equivalent to Eq.(2.1), so for any integer (X) the left side will evaluate to an integer, and for any integer (Y) the right side will evaluate to a *different* integer if Eq.(1) is true. By specifying integers (q) and (e), this expression invariably yields a non-integer (X), so at this stage the Theorem is looking unprovable.

An idea is required to strengthen the system in order to determine whether (X) and (Y) can ever both be integers. Auspiciously, *a balanced all-integer* equation of this same format can be conceived via an auxiliary theorem which does not include Eqs.(2.4b,c). It is easy to demonstrate by using an arbitrary numerical example like

$$\{12 \times 108\} = \{18 \times 72\}\,, \qquad (2.5a)$$

then calculate the arithmetic mean of each side and expand

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

and express this in the same format as Eq.(2.4d)

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

which simplifies to

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

Here, those factors *analogous* to Eq.(2.4d) are ($\tilde{X} = 60$), ($\tilde{E} = 48$), ($\tilde{Y} = 80$). However, denominator [$\tilde{h} = 81$] employs factor [27^2] from the right side of Eq.(2.5b) and denominator [$\tilde{m} = 256$] employs [48^2] from the left side. This is *in stark contrast* to Eq.(2.4d) which employs [h] from Eq.(2.2a) on the left side and [m] from Eq.(2.3a) on the right. Therefore, these ($\tilde{h}$, $\tilde{m}$) cannot be related to ($\tilde{X}$, $\tilde{Y}$) in the way given by Eq.(2.4b,c). Accordingly, Eq.(2.5a) is the *unique format* necessary to produce an *all-integer* equation (2.5d) which contains an integer ($\tilde{Y}$) with an integer ($\tilde{X}$), but it is totally incompatible with the derivation of Eq.(2.4d) from Eq.(2.1) via Eqs.(2.4b, c). That is, Eq.(2.4d) can never be all-integer because it did not derive from a format like Eq.(2.5a). Founding relationships like Eq.(2.2b), and Eq.(2.3b) do not contribute to an all-integer equation like Eq.(2.5d). Given this, further proof is not necessary.

This *lemma* regarding Eqs.(2.5) could be stated in general: An *all-integer* equation of the form

$$(1/w^2) \times \{(\mathrm{X} - \mathrm{E})(\mathrm{X} + \mathrm{E})\} = (1/z^2) \times \{(\mathrm{Y} - \mathrm{E})(\mathrm{Y} + \mathrm{E})\}, \qquad (2.6a)$$

can only be derived from an initial *all-integer* equation of the form

$$\{\mathrm{F} \times \mathrm{G}\} = \{\mathrm{K} \times \mathrm{L}\}. \qquad (2.6b)$$

Hence, within the system of Fermat's Last Theorem for (p = 3), transformation of Eq.(2.1) to the format of Eq.(2.4d) has revealed that Eq.(1) may be true but unprovable, thereby satisfying Gödel's Incompleteness Theorem. But, a stronger system, containing a lemma Eq.(2.6a,b) invoking the uniqueness of Eqs.(2.5), has now made Eq.(1) provable by deduction. This logical jump might frustrate the resources of an autonomous computing machine.

Consequently, Eq.(2.4d) can never be all-integer *and (b) is not an integer if (a) is an integer; meaning that Eq.(1) is proved for (p = 3).*

3. Proof for (p = 4)

Given the equation

$$\mathrm{c}^4 = \mathrm{a}^4 + \mathrm{b}^4, \qquad (3.0)$$

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

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

For F(a,e), substitute

$$\mathrm{c} = (\mathrm{a} + \mathrm{e}), \text{ and } \quad \mathrm{H} = (4\mathrm{ae} + 6\mathrm{e}^2)\ , \qquad (3.1a)$$

then reduce to

$$F(a, e) = a\{Ha + 4e^3\}\ . \tag{3.1b}$$

For F(b,e), substitute

$$b = (q + e), \tag{3.2}$$

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

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

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

Make this more symmetrical by substituting

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

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

then substitute ($E = 4e^3$) 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 format to Eq.(2.4d) although factors are defined differently; but the logical argument which followed Eq.(2.4d) will lead to the same conclusion.

Thus, Eq.(3.4d) cannot be all-integer so *(b) cannot be an integer if (a) is an integer; which means that Eq.(1) 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

$$c = (a + e),\ \text{and}\quad H = (5a^2e + 10ae^2 + 10e^3)\ , \tag{4.1a}$$

then reduce to

$$F(a, e) = a\{Ha + 5e^4\}. \tag{4.1b}$$

For F(b,e), substitute

$$b = (q + e), \tag{4.2}$$

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

then reduce to

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

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

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

Make this more symmetrical by substituting

$$X = (2Ha + 5e^4), \tag{4.4b}$$

$$Y = (2Mq + 5e^4), \tag{4.4c}$$

then substitute ($E = 5e^4$) and reduce Eq.(4.4a) to

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

This equation is identical in form to Eq.(2.4d) although factors are defined differently; but the logical argument following Eq.(2.4d) will lead to the same conclusion.

Thus, Eq.(4.4d) cannot be all-integer so *(b) cannot be an integer if (a) is an integer; which means that Eq.(1) 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

$$c^p = a^p + b^p, \tag{5.0}$$

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

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

For F(a,e), substitute

$$c = (a + e), \text{ and } H = [\{(a + e)^p - a^p - e^p\} - ape^{p-1}]/a^2, \tag{5.1a}$$

then reduce to

$$F(a, e) = a\{Ha + pe^{p-1}\}. \tag{5.1b}$$

For F(b,e), substitute

$$b = (q + e), \tag{5.2}$$

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

then reduce to

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

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

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

Make this more symmetrical by substituting

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

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

then substitute ($E = pe^{p-1}$) 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 logical argument following Eq.(2.4d) will lead to the same conclusion.

Thus, Eq.(5.4d) cannot be all-integer so *(b) cannot be an integer if (a) is an integer; which means that Eq.(1) 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.

First, by substitution of variables, the original cubic equation was transformed into a balanced symmetrical format. In worked examples, the variables could not all be integers, so the Theorem had the appearance of being true but unprovable, like a candidate for Gödel's Incompleteness Theorem.

Then, the idea of a new auxiliary theorem was conceived which stipulated *all-integer* variables fitted into the same balanced symmetrical format.

By comparing configurations of these two balanced symmetrical expressions, it became clear why the cubic equation could never be all-integer compatible.

The quartic, quintic and general (p > 2) equations were also transformed into balanced symmetrical formats which could not be compatible with fitted all-integer expressions.

In conclusion, the stronger system containing the new lemma enabled Fermat's Last Theorem to be proved by deduction. Thus, from 1637 the Theorem was true but required a stronger system to prove it.

References

[1] Wiles, A.J. (1995) Annals of Mathematics 141, No.3, pp 443-551

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