On Fermat's Last Theorem (revised)

Richard Wayte

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

e-mail: rwayte@googlemail.com

Research article submitted to **Advances in Mathematics 6 Dec 2017.**

Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declarations of interest: none

Abstract. A solution of Fermat's Last Theorem is given, using elementary function arithmetic and inference from worked examples.

Keywords: Fermat's last theorem. 11D41

1. Introduction

Fermat's Last Theorem was formulated in 1637 and apparently not proved successfully until 1995, when Andrew Wiles [1] did so using the latest high level number theory. Over the years, enthusiasts have been encouraged by the simplicity of the conjecture to try and prove it using elementary function arithmetic [2]. This is one such attempt using inference from worked examples.

Theorem

No three positive integers a, b, c, can satisfy the equation:

$$a^p + b^p = c^p \tag{1.1}$$

if (p) is an integer greater than two.

2. Proof for (p = 3)

Given the equation:

$$a^3 + b^3 = c^3, \tag{2.0}$$

let (c = a + e) for (e) a positive integer. Set up two equal expressions:

$$\left[f(a,e) = \frac{c^3 - a^3 - e^3}{3e} \right] = \left[\frac{b^3 - e^3}{3e} = f(b,e) \right]. \tag{2.1}$$

In the first expression, substitute for (c) and also let (a = se), then simplify to get:

$$f(a,e) = a(ka + e) = s(ks + 1) \times e^2, \tag{2.1a}$$

where in this case,

$$k = 1. \tag{2.1b}$$

Here, f(a,e) will be an integer when (a) is an integer.

In the second expression, f(b,e) will be an integer for selected values of integer (b) such as:

$$b_n = (3n - 2)e, \quad \text{for } e = 2, 5, 7, ...28 \quad , \tag{2.2a}$$

or $$b_n = ne, \text{ for } e = 3, 6 \quad , \tag{2.2b}$$

or $$b_n = (n + 3)e/4, \quad \text{for } e = 24 \quad , \tag{2.2c}$$

where integer ($n \geq 1$). Other selected (b_n) values are produced by other (e) values. Now, for f(b,e), substitute

$$b_n = (q + 1)e \ , \text{ and } \ u = (q/3 + 1), \tag{2.3a}$$

and simplify to get:

$$f(b,e) = qe(uqe + e). \tag{2.3b}$$

Let potential integer f(a,e) from Eq.(2.1a) be equated to this actual integer f(b,e), thus:

$$(1/k)\{(ka) \times (ka + e)\} \ = \ (1/u)\{(uqe) \times (uqe + e)\} \ . \tag{2.4a}$$

The aim is to prove that (a) cannot really be an integer in this equation.

Make this more symmetrical by substituting:

$$x = (2ka + e), \tag{2.4b}$$

and

$$y = (2uqe + e) \ , \tag{2.4c}$$

then Eq.(2.4a) simplifies to:

$$(1/k)\{(x - e) \times (x + e)\} \ = \ (1/u)\{(y - e) \times (y + e)\} \ . \tag{2.4d}$$

In practise examples, (y) and (u) have always been calculated after choosing (e) and (b_n) values, and then (x) has been derived as a non-integer every time. However, by reversing this procedure and starting with chosen integers (a), (e) and (x), one is led towards (u) and (y) values unconstrained by (b_n). Auspiciously, this reveals the exact reason why (x) was never an integer in the former procedure.

Lemma: The general format of Eq.(2.4d) would allow numerical examples possessing an integer (x) if (y) is not related to (u) through Eq.(2.4c).

Proof: Develop a simple arbitrary expression which has the form of Eq.(2.4d) without reference to (b_n). For example, let:

$$\{15\times 49\}=\{21\times 35\}=735\ , \tag{2.5a}$$

then expand:

$$\{(32-17)\times(32+17)\}=\{(28-7)\times(28+7)\}\ , \tag{2.5b}$$

or

$$\{(32-17)\times(32+17)\}=(7/17)^2\{(68-17)\times(68+17)\}\ . \tag{2.5c}$$

Here, (x ≡ 32), (e ≡ 17), and (y ≡ 68), while u/k ≡ $(17/7)^2$ employs 17 and 7 from previous terms. Given this straightforward derivation, it appears that Eq.(2.5c) may be the simplest and unique format for getting an integer (x), albeit integer (y) does not satisfy Eq.(2.4c), which would require (y ≈ 2963.57) when using this (u/k) value. **QED.**

Now, compare this result with an arbitrary real example of Eq.(2.4d), wherein (e = 28, b_{16} = 1288, q = 45, u = 16, k = 1), and (y = 40348) satisfies Eq.(2.4c). Thus Eq.(2.4d) becomes directly:

$$(x-28)\times(x+28)=(1/16)\{(40348-28)\times(40348+28)\}\ , \tag{2.6a}$$

which could be simplified:

$$(x-28)\times(x+28)=\{(10087-7)\times(10087+7)\}=101747520\ , \tag{2.6b}$$

or expanded:

$$(x-28)\times(x+28)=(7/28)^2\{(40348-28)\times(40348+28)\}\ , \tag{2.6c}$$

where substituted u ≡ $(28/7)^2$ employs 28 and 7 from previous terms, as in Eq.(2.5c). Predictably, (x) evaluates to a non-integer (10087.036), so modify this expression in order to make (x) equal to a nearby integer, say (10089). First, factorise the final product in Eq.(2.6b) differently:

$$101747520 = 9888 \times 10290, \qquad (2.7a)$$

then calculate the arithmetic mean [(9888+10290)/2 = 10089] which will represent *integer* (x) in expressions similar to Eq.(2.6b, c):

$$\{(10089-201)\times(10089+201)\} = \{(10087-7)\times(10087+7)\} = 101747520\ , \qquad (2.7b)$$

or $$\{(10089-201)\times(10089+201)\} = (7/201)^2\{(289641-201)\times(289641+201)\}. \qquad (2.7c)$$

Here, (e = 201) is new, and new u/k = $(201/7)^2$ employs 201 and 7 from previous terms, just as the substituted (u) did in Eq.(2.6c). However, the new value of (y = 289641) is not related to new (u/k) through Eq.(2.4c), which would require (y ≈ 818865236).

This situation will exist for every real example of Eq.(2.4d), so values of (y) defined correctly by Eq.(2.4c) will never occur in expressions constructed like Eq.(2.7c), or Eq.(2.5c), which have the unique and necessary format for allowing an integer (x). Put another way: every example like Eq.(2.7c) with integer (x) will not be an expression of Eq.(2.4d).

Clearly, these examples prove that (a) can never be an integer if (b) is first selected to be an integer. This is equivalent to the proof of Eq.(1.1) for (p = 3).

3. Proof for (p = 4)

Given the equation:

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

let (c = a + e) for (e) a positive integer. Set up two equal expressions:

$$\left[f(a,e) = \frac{c^4 - a^4 - e^4}{2e} \right] = \left[\frac{b^4 - e^4}{2e} = f(b,e) \right]. \qquad (3.1)$$

In the first expression, substitute for (c) and also let (a = se), then simplify to get:

$$f(a,e) = a\left\{a(2a+3e) + 2e^2\right\} = s\{Ks+2\}\times e^3, \qquad (3.1a)$$

where,

$$K = (2s+3)\ . \qquad (3.1b)$$

Here, f(a,e) will be an integer when (a) is an integer.

In the second expression, f(b,e) will be an integer for selected values of integer (b) such as:

$$b_n = (2n-1)e, \qquad \text{or} \qquad b_n = ne, \quad \text{or} \qquad b_n = (n+3)e/4, \qquad (3.2)$$

where integer (n ≥ 1). Other selected (b_n) values are produced by other (e) values. Now, for f(b,e), substitute

$$b_n = (q+1)e \ , \quad \text{and} \quad U = \left(q^2/2 + 2q + 3\right), \tag{3.3a}$$

and simplify to get:

$$f(b,e) = q\{Uq + 2\} \times e^3 . \tag{3.3b}$$

Let f(a,e) from Eq.(3.1a) be equated to this f(b,e), thus:

$$(1/K)\{Ka(Ka + 2e)e\} = (1/U)\{Uqe(Uqe + 2e)e\} \ . \tag{3.4a}$$

Make this more symmetrical by substituting:

$$x = (Ka + e) , \tag{3.4b}$$

and

$$y = (Uqe + e) , \tag{3.4c}$$

then Eq.(3.4a) simplifies to:

$$(1/K)\{(x-e)\times(x+e)\} \ = \ (1/U)\{(y-e)\times(y+e)\} \ . \tag{3.4d}$$

This equation is identical in form to Eq.(2.4d) even though (U, K, x, y) are defined differently. It is expected that (s) and (K) in Eq.(3.1b) will often be fractions rather than integers, in which case every term in Eq.(3.4d) would need to be multiplied by (e) and replaced, eg. ($e' = e^2$), ($x' = xe$), ($K' = Ke$), ($y' = ye$), ($U' = Ue$). Consequently, the logical argument which followed Eq.(2.4d) will apply and lead to the same conclusion. That is, genuine values of (y) calculated from Eq.(3.4c) do not occur in expressions of the form Eq.(2.5c) and Eq.(2.7c) which have the format necessary for getting an integer (x) or (x'). *Therefore (a) can never be an integer if (b) is selected to be an integer. This is equivalent to the proof of Eq.(1.1) for (p = 4).*

4. Proof for (p = 5)

Given the equation:

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

let (c = a + e) for (e) a positive integer. Set up two equal expressions:

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

In the first expression, substitute for (c) and also let (a = se), then simplify to get:

$$f(a,e) = s\{ks + 1\} \times e^4 , \tag{4.1a}$$

where,

$$k = \left(s^2 + 2s + 2\right). \tag{4.1b}$$

Again, f(a,e) will be an integer when (a) is an integer.

In the second expression, f(b,e) will be an integer for selected values of integer (b) such as:

$$b_n = (5n-4)e, \quad \text{or} \quad b_n = ne, \quad \text{or} \quad b_n = (n+3)e/4, \tag{4.2}$$

where integer ($n \geq 1$). Other selected (b_n) values are produced by other (e) values. Now, for f(b,e), substitute

$$b_n = (q+1)e \ , \ \text{and} \ \ u = \left(q^3/5 + q^2 + 2q + 2\right), \tag{4.3a}$$

and simplify to get:

$$f(b,e) = q\{uq+1\} \times e^4. \tag{4.3b}$$

Let f(a,e) from Eq.(4.1a) be equated to this f(b,e), thus:

$$(1/k)\left\{k\,a\,(k\,a+e)e^2\right\} = (1/u)\left\{u\,q\,e\,(u\,q\,e+e)e^2\right\} \ . \tag{4.4a}$$

This equation is identical in form to Eq.(2.4a) even though (u, k) are defined differently. It is expected that (s) and (k) in Eq.(4.1b) will often be fractions rather than integers, then some factors in Eq.(4.4a) would need to be multiplied by the (e^2) term, and replaced, ie. ($k' = ke^2$), ($u' = ue^2$), ($e' = ee^2$), thus:

$$(1/k')\left\{k'\,a\,(k'\,a+e')\right\} = (1/u')\left\{u'\,q\,e\,(u'\,q\,e+e')\right\} \ . \tag{4.4b}$$

Consequently, the logical argument following Eq.(2.4a) will apply and lead to the same conclusion. *Therefore (a) can never be an integer if (b) is selected to be an integer. This is equivalent to the proof of Eq.(1.1) for (p = 5).*

5. Proof for (p = prime number ≥ 3)

Proofs for (p = 7, 11, and 13) have been performed to confirm that they follow the format of (p = 5) given above. Therefore a general proof for all prime numbers will be proposed as follows.

Given the equation:

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

let (c = a + e) for (e) a positive integer. Set up two equal expressions:

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

In the first expression, substitute for (c) and also let (a = se), then simplify to get:

$$f(a,e) = s\{ks+1\}\times e^{p-1}, \tag{5.1a}$$

where,

$$k = \left[(s+1)^p - \left(s^p + ps + 1\right)\right] / \left(ps^2\right). \tag{5.1b}$$

Again, f(a,e) will be an integer when (a) is an integer.

In the second expression, f(b,e) will be an integer for selected values of integer (b) such as:

$$b_n = [p(n-1)+1]e, \quad \text{or} \quad b_n = ne, \quad \text{or} \quad b_n = (n+3)e/4, \tag{5.2}$$

where integer ($n \geq 1$). Other selected (b_n) values are produced by other (e) values. Now, for f(b,e), substitute

$$b_n = (q+1)e \ , \ \text{and} \ \ u = \left[(q+1)^p - (pq+1)\right] / \left(pq^2\right), \tag{5.3a}$$

and simplify to get:

$$f(b,e) = q\{uq+1\}\times e^{p-1}. \tag{5.3b}$$

Let f(a,e) from Eq.(5.1a) be equated to this f(b,e), thus:

$$(1/k)\left\{ka(ka+e)e^{p-3}\right\} = (1/u)\left\{uqe(uqe+e)e^{p-3}\right\}. \tag{5.4a}$$

This equation is identical in form to Eq.(2.4a) even though (u, k) are defined differently, It is expected that (s) and (k) in Eq.(5.1b) will often be fractions rather than integers, then some factors in Eq.(5.4a) would need to be multiplied by the (e^{p-3}) term, and replaced, ie. ($k' = ke^{p-3}$), ($u' = ue^{p-3}$), ($e' = ee^{p-3}$), thus:

$$(1/k')\{k'a(k'a+e')\} = (1/u')\{u'qe(u'qe+e')\} \ . \tag{5.4b}$$

Consequently, the logical argument following Eq.(2.4a) will apply and lead to the same conclusion. *Therefore (a) can never be an integer if (b) is selected to be an integer. This is equivalent to the proof of Eq.(1.1) for any prime number $p \geq 3$.*

6. Conclusion

The simplicity of Fermat's conjecture implied that there might be a proof available using only basic algebra. Thus, to remove the (c^3) term, (c) was replaced by the sum of integer (a) and an arbitrary constant integer (e). This allowed the cubic equation to be split into two parts f(a,e) and f(b,e), for separate development. The aim was to show that each part could evaluate numerically to an integer, but never the same

integer for both. The first part was factorised in terms of integers (a, k) and (e). The second part was factorised after integer (b) was replaced using new variables (q, u), and (e). Both parts were then reformulated with new variables (x) and (y) in order to get an expression of simplistic symmetry. After extensive calculations confirming that (x) appeared destined to be a non-integer at all times, a search outside of the cubic problem was made for an analogous expression *possessing all integers*. Examples were found involving integers equivalent to (x), (e), with corresponding integers (y), (u), which were independent of the cubic expression. It transpired that the basic format of these new *all-integer expressions* was unique and would never be satisfied by the complicated (y)(u) numerical relationship in the prized symmetric cubic expression. That is, Fermat's theorem was solved for the cubic case.

The quartic equation was reduced to the symmetric expression of the cubic equation, but with more complicated (k, u). Again, the format of the equivalent *all-integer expression* could never be satisfied by the complicated (y)(u) relationship of a quartic expression. The quintic equation was then reduced to the symmetric expression, and could not satisfy the format of the *all-integer expression.* Finally, the analysis was performed for a general power (p = prime number) equation to show that there was no apparent restriction on (p).

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