FERMAT'S

LAST

THEOREM

REVISITED

AGAIN

© Colin Newton 18/04/2018

FERMAT'S LAST THEOREM

When Fermat wrote a note in the margin of his copy of Bachet's Arithmetica to the effect that he had a marvellous proof that $x^n + y^n \neq z^n$ where n is any integer greater than 2, perhaps he was thinking along the following lines. The argument is based on the proof that if y and z are nth powers then x is not an nth power, conversely if both x and y are nth powers then z is not an nth power. The proofs investigate powers of $4n$, $4n + 2$ and $4n \pm 1$ for all $n > 0$.

Definition 1 Define a **Pythagorean Triple** (PT) as $x^2 + y^2 = z_p^2$, and all three are integers.

Definition 2 Define a **Diophantine Triple** (DT) as $y^2 - x^2 = z_d^2$, and all three are integers.

Theorem 1 Any integer $x > 2$ with $(1 \leq w_p < x) \mid x^2$ generates all Pythagorean Triples.

Proof $x^2 + y^2 = z_p^2$ and without loss of generality assume $x < y$

then $x^2 = z_p^2 - y^2 = (z_p - y)(z_p + y)$ since $(z_p - y)(z_p + y) = z_p^2 + z_p y - y z_p - y^2 = z_p^2 - y^2$.

Let $z_p - y = w_p$ then $z_p = y + w_p$ and $x^2 = w_p (y + w_p + y)$

therefore $x^2 = w_p (2y + w_p) = 2yw_p + w_p^2$ hence $2yw_p = x^2 - w_p^2$

and $$y = \frac{x^2 - w_p^2}{2w_p} \text{ and } z_p = y + w_p = \frac{x^2 - w_p^2}{2w_p} + \frac{2\,w_p^2}{2w_p} = \frac{x^2 + w_p^2}{2w_p}$$

For $x > 2$, $w_p \mid x^2$ and for y to be positive, $1 \leq w_p < x$. ❑

Notes for Theorem 1.

1 If x is even, w odd or even, then y, and hence z, may be fractions with the denominator equal to 2. e.g. for $x = 4$, $y = 15/2$ and $z = 17/2$ with $w = 1$, multiplying by 2 gives the Triple (8, 15, 17). $x = 10$ produces (10, 24, 26) with w = 2, but also (10, 21/2, 29/2) with $w = 4$ and (10, 15/2, 25/2) with $w = 5$. Multiply by 2 to obviate the problem.

For all Primitive Pythagorean Triples GCD (x, y) = 1 : –

2 For $x > 2$ there always exists a Pythagorean Triple, for x odd let $w = 1$, x even let $w = 2$.
3 If x is odd, w is odd since the numerators of both y and z must be even to be divisible by 2.
4 If x is even, and w is even then the numerators of both y and z are divisible by 4.
5 If x is odd, w is odd and y is even, if x is even, w is even and y is odd, in both cases z is odd.

Theorem 2 Any integer $x > 2$ with $(1 \leq w_d < x) \mid x^2$ generates all Diophantine Triples.

Proof $y^2 - x^2 = z_d^2$. For z_d to be positive and without loss of generality assume $x < y$

then $x^2 = y^2 - z_d^2 = (y - z_d)(y + z_d)$ since $(y - z_d)(y + z_d) = y^2 + y z_d - z_d y - z_d^2 = y^2 - z_d^2$.

Let $y - z_d = w_d$ then $y = z_d + w_d$ and $x^2 = w_d (z_d + w_d + z_d)$

hence $x^2 = w_d (2z_d + w_d) = 2z_d w_d + w_d^2$ therefore $2z_d w_d = x^2 - w_d^2$

and $$z_d = \frac{x^2 - w_d^2}{2w_d} \text{ and } y = z_d + w_d = \frac{x^2 - w_d^2}{2w_d} + \frac{2\,w_d^2}{2w_d} = \frac{x^2 + w_d^2}{2w_d}$$ ❑

Note For Theorem 3 below, the x and y in Theorem 1 are equal to the x and y in Theorem 2.

Theorem 3 Any integer $x > 2$ and w such that $(1 \le w < x) \mid x^2$ cannot generate both a Pythagorean Triple and a Diophantine Triple simultaneously.

Proof.

Assume 1 that $x^2 + y^2 = z_p{}^2$ is a PT, then to generate a DT requires that $y^2 - x^2 = z_d{}^2$, hence

$$z_d{}^2 = \frac{(x^2 - w_p^2)^2}{4\,w_p^2} - x^2 = \frac{(x^2 - w_p^2)^2 - 4w_p^2x^2}{4\,w_p^2} \qquad w_p = z_p - y \text{ from Theorem 1}$$

and $z_d = \frac{1}{2w_p}\sqrt{x^4 - 6x^2w_p^2 + w_p^4} \Rightarrow z_d \neq$ an integer. To be square the expression under the $\sqrt{\ }$ must be of the form $x^4 - 2x^2w_p{}^2 + w_p{}^4 = (x^2 - w_p{}^2)^2$ by the Binomial Theorem, i.e. the coefficients of the expansion of $(x^2 - w_p{}^2)^2$ are given by the 2nd row of Pascal's Triangle.

Assume 2 that $y^2 - x^2 = z_d{}^2$ is a DT, then to generate a PT requires that $x^2 + y^2 = z_p{}^2$ hence

$$z_p{}^2 = \frac{(x^2 + w_d^2)^2}{4w_d^2} + x^2 = \frac{(x^2 + w_d^2)^2 + 4w_d^2x^2}{4\,w_d^2} \qquad w_d = y - z_d \text{ from Theorem 2}$$

and $z_p = \frac{1}{2w_d}\sqrt{x^4 + 6x^2w_d^2 + w_d^4} \Rightarrow z_p \neq$ an integer. To be square the expression under the $\sqrt{\ }$ must be of the form $x^4 + 2x^2w_d{}^2 + w_d{}^4 = (x^2 + w_d{}^2)^2$ by the Binomial Theorem, i.e. the coefficients of the expansion of $(x^2 + w_d{}^2)^2$ are given by the 2nd row of Pascal's Triangle. ❑

Before proceeding, a couple of Lemmas (Lemmata?) and also a couple of identities.

Lemma 1 The product of two squares is also a square.

Proof $x^2 \times y^2 = (x\,y)^2$ for all x and y greater than 0. ❑

Lemma 2 The product of two numbers, where one or both are non-square is not a square.

Proof $x^2 \times y^2 = (x\,y)^2 \Rightarrow x \times y \neq$ square for one or both x and $y > 1$ and $\neq$ square. ❑

Identity 1 $(x + y)^n = c_0x^n + c_1x^{n-1}y + c_2x^{n-1}y^2 + \ldots + c_1xy^{n-1} + c_0y^n$ by the Binomial Theorem where the coefficients $c_0, c_1, c_2, \ldots c_2, c_1, c_0$ are the values of the corresponding numbers in the nth row of Pascal's Triangle and $c_0 = 1$.

Identity 2 $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \ldots + x^2y^{n-3} + xy^{n-2} + y^{n-1})$ where all the coefficients are 1. It is left to the reader to multiply it out to prove it.

Theorem 4 **Fermat's Last Theorem** for $x^4 + y^4 \neq$ a fourth power.

Proof The proof is for x or y not being a fourth power, hence $x^4 + y^4 \neq z^4$.
Assume for a contradiction, $x^4 + y^4 = z^4$ then
$x^{2\times2} = z^{2\times2} - y^{2\times2} = (z^2 - y^2)(z^2 + y^2)$ where both $(z^2 - y^2)$ and $(z^2 + y^2)$ require to be square by Lemma 1. However, by Theorems 1, 2 and 3, if $(z^2 - y^2) =$ a square then $(z^2 + y^2) \neq$ a square and vice-versa, hence $(z^2 - y^2)(z^2 + y^2) \neq$ a square by Lemma 2, therefore x is not a square and not equal to a fourth power since $x^4 = (x^2)^2$, this proves $x^4 \neq z^4 - y^4$ hence the equation $x^4 + y^4 \neq z^4$ is true. Exchanging x and y produces the same result ❑

Theorem 5 Fermat's Last Theorem for $4n$, i.e. $x^{4n} + y^{4n} \neq z^{4n}$ for all $n > 1$.

The proof is by induction on n.

For $n = 1 \Rightarrow x^4 + y^4 = z^4 \Rightarrow x^4 = z^4 - y^4 = (z^2 - y^2)(z^2 + y^2) \neq x^4$ by Theorems 1, 2 and 3, and already proven by Theorem 4.

For $4n$ $\quad x^{4n} + y^{4n} = z^{4n} \Rightarrow x^{4n} = z^{4n} - y^{4n} = z^{2\times 2n} - y^{2\times 2n} = (z^{2n} - y^{2n})(z^{2n} + y^{2n})$

$= (Z^2 - Y^2)(Z^2 + Y^2)$ where $Z = z^n$ and $Y = y^n$

but $\quad (Z^2 - Y^2)(Z^2 + Y^2) \neq$ a fourth power by Theorems 1, 2, 3 and 4.

For $4(n + 1)$ $\quad x^{4(n+1)} + y^{4(n+1)} = z^{4(n+1)} \Rightarrow x^{4(n+1)} = z^{4(n+1)} - y^{4(n+1)}$

$= z^{2\times 2(n+1)} - y^{2\times 2(n+1)} = (z^{2(n+1)} - y^{2(n+1)})(z^{2(n+1)} + y^{2(n+1)})$

$= ({Z_1}^2 - {Y_1}^2)({Z_1}^2 + {Y_1}^2)$ where $Z_1 = z^{(n+1)}$ and $Y_1 = y^{(n+1)}$

but $\quad ({Z_1}^2 - {Y_1}^2)({Z_1}^2 + {Y_1}^2) \neq$ a fourth power by Theorems 1, 2, 3 and 4. ❑

Theorems 4 and 5 prove that the equation $x^{4n} + y^{4n} \neq z^{4n}$ is true for all $n > 0$.

Theorem 6 Fermat's Last Theorem for $4n + 2$ where $n = 1$, i.e. $x^6 + y^6 \neq z^6$.

Assume for a contradiction that $x^6 + y^6 = z^6 \Rightarrow x^6 = y^6 - z^6$.

then $\quad x^6 = (z^2 - y^2)(z^4 + z^2y^2 + y^4)$. To be a sixth power, the first bracket requires to be a square which it may be by Theorem 2, but also the second bracket requires to be a fourth power, which is impossible since to be so, it requires to be of the form $(z^4 + 2z^2y^2 + y^4)$ by the Binomial Theorem as per Identity 1. Hence x is not a sixth power and the equation $x^6 + y^6 \neq z^6$ is true. ❑

Theorem 7 Fermat's Last Theorem for $4n + 2$ where n is any integer > 1.

The proof is by induction on n, the case for $n = 1$ is proven by Theorem 6 but for $n > 1$

$4n + 2$ $\quad x^{4n+2} + y^{4n+2} = z^{4n+2} \Rightarrow x^{4n+2} = z^{4n+2} - y^{4n+2}$

therefore $\quad x^{4n+2} = (z^2 - y^2)(z^{4n} + z^{4n-2}y^2 + \ldots + x^2y^{4n-2} + y^{4n})$ where the first bracket may be square by Theorem 2, however all the coefficients of the second bracket are 1, but for a fourth power should be the coefficients of the $4n$th row of Pascal's Triangle by the Binomial Theorem as per Identity 1. Hence x is not a $(4n + 2)$th power and the equation $x^{4n+2} + y^{4n+2} \neq z^{4n+2}$ is true for all $n > 1$.

$4(n + 1) + 2$ $\quad x^{4(n+1)+2} + y^{4(n+1)+2} = z^{4(n+1)+2} \Rightarrow x^{4(n+1)+2} = z^{4(n+1)+2} - y^{4(n+1)+2}$ therefore $x^{4(n+1)+2} = (z^2 - y^2)(z^{4(n+1)} + z^{4(n+1)-2}y^2 + \ldots + x^2y^{4(n+1)-2} + y^{4(n+1)})$ where the first bracket may be square by Theorem 2, however all the coefficients of the second bracket are 1, but for a fourth power, require to be the coefficients of the $(4n + 1)$th row of Pascal's Triangle by the Binomial Theorem as per Identity 1. Hence x is not a $(4(n + 1) + 2)$th power and the equation $x^{4(n+1)+2} \neq z^{4(n+1)+2} - y^{4(n+1)+2} \Rightarrow x^{4(n+1)+2} + y^{4(n+1)+2} \neq z^{4(n+1)+2}$ is true for all $n > 1$. ❑

Theorems 1 to 7 prove Fermat's Last Theorem is true for all even powers of n greater than 2.

Theorem 8 Fermat's Last Theorem for $4n - 1$ where n is any integer > 0.

The proof is by induction on n.

For $n = 1$ $4n - 1 = 3 \Rightarrow x^3 + y^3 = z^3 \Rightarrow x^3 = z^3 - y^3 = (z - y)(z^2 + zy + y^2)$ by Identity 2. The only two factors that satisfy this equation are x and x^2 but $(z^2 + zy + y^2) \neq$ square since, by the Binomial Theorem it must be of the form $(z^2 + 2zy + y^2) = (z + y)^2$. Hence, by Lemma 2, $x^3 \neq z^3 - y^3$ i.e. $x^3 + y^3 \neq z^3$. Note $(z - y)(z^2 + zy + y^2) = z^3 + z^2y + zy^2 - z^2y - zy^2 - y^3 = z^3 - y^3$.

For $4n - 1$ $x^{4n-1} + y^{4n-1} = z^{4n-1} \Rightarrow x^{4n-1} = z^{4n-1} - y^{4n-1}$ and by Identity 2 $= (z - y)(z^{4n-2} + z^{4n-3}y + \ldots + zy^{4n-3} + y^{4n-2})$ where the second bracket may be the expansion of several factors. The only two factors that satisfy this equation are x and x^{4n-2}. The second bracket cannot be a $(4n - 2)$th power, since it is of the form of Identity 2 and not of the form of Identity 1, hence $x^{4n-1} + y^{4n-1} \neq z^{4n-1}$ and therefore equation $x^{4n-1} + y^{4n-1} \neq z^{4n-1}$ is true.

$4(n + 1) - 1$ $x^{4(n+1)-1} + y^{4(n+1)-1} = z^{4(n+1)-1} \Rightarrow x^{4(n+1)-1} = z^{4(n+1)-1} - y^{4(n+1)-1}$ and by Identity 2 $= (z - y)(z^{4(n+1)-2} + z^{4(n+1)-3}y + \ldots + zy^{4(n+1)-3} + y^{4(n+1)-2})$ where the second bracket may be the expansion of several factors. The only two factors that satisfy this equation are x and $x^{4(n+1)-2}$. The second bracket cannot be a $(4(n+1)-2)$th power, since by the Binomial Theorem, it must be of the form of Identity 1. Therefore x is not a $4((n + 1) - 1)$th power and the equation $x^{4(n+1)-1} \neq y^{4(n+1)-1} + z^{4(n+1)-1} \Rightarrow x^{4(n+1)-1} + y^{4(n+1)-1} \neq z^{4(n+1)-1}$ is true. ❑

Theorem 9 Fermat's Last Theorem for $4n + 1$ where n is any integer > 0.

The proof is by induction on n.

For $n = 1$ $4n + 1 = 5 \Rightarrow x^5 + y^5 = z^5 \Rightarrow x^5 = z^5 - y^5 = (z - y)(z^4 + z^3y + z^2y^2 + zy^3 + y^4)$. The only two factors that satisfy this equation are x and x^4 but $(z^4 + z^3y + z^2y^2 + zy^2 + y^4) \neq$ a fourth power since to be so requires that $(z^4 + 4z^3y + 6z^2y^2 + 4zy^3 + y^4) = (z + y)^4$ by the Binomial Theorem. Hence $x^5 \neq z^5 - y^5$ and therefore equation $x^5 + y^5 \neq z^5$ is true.

For $4n + 1$ $x^{4n+1} + y^{4n+1} = z^{4n+1} \Rightarrow x^{4n+1} = z^{4n+1} - y^{4n+1}$ and by Identity 2 $= (z - y)(z^{4n} + z^{4n-1}y + \ldots + zy^{4n-1} + y^{4n})$ where the second bracket may be the expansion of several factors. The only two factors that satisfy this equation are x and x^{4n}. The second bracket cannot be a $4n$th power, since it is of the form of Identity 2 and not of the form of Identity 1, and therefore $x^{4n+1} \neq y^{4n+1} - z^{4n+1}$ and hence equation $x^{4n+1} + y^{4n+1} \neq z^{4n+1}$ is true.

$4(n + 1) + 1$ $x^{4(n+1)+1} + y^{4(n+1)+1} = z^{4(n+1)+1} \Rightarrow x^{4(n+1)+1} = z^{4(n+1)+1} - y^{4(n+1)+1}$ $= (z - y)(z^{4(n+1)} + z^{4(n+1)-1}y + z^{4(n+1)-2}y^2 \ldots + zy^{4(n+1)-1} + y^{4(n+1)})$ where the second bracket may be the expansion of several factors. The only two factors that satisfy this equation are x and $x^{4(n+1)}$. The second bracket cannot be a $4(n + 1)$th power, since it is of the form of Identity 2 and not of the form of Identity 1, hence $x^{4(n+1)+1} \neq z^{4(n+1)+1} - y^{4(n+1)+1}$ which implies that the equation $x^{4(n+1)+1} + y^{4(n+1)+1} \neq z^{4(n+1)+1}$ is true. ❑

Theorems 8 and 9 prove Fermat's Last Theorem is true for all odd powers of n greater than 2.