ALGEBRAIC PROOF OF LAST THEOREM OF P.FERMAT

(1601-1665 AD)

Ramesh Chandra Ray
Professor of Electrical Engineering
Chittagong University of Engineering and Technology (CUET)
Bangladesh.
E-mail: ramesh_ray2003@yahoo.com, rameshchandraray@yahoo.com
www.rameshcray.wordpress.com

Abstract: An elementary proof of the last theorem of P. Fermat, the famous French Mathematician is shown in this paper. The proof has been given by algebraic method using algebraic equations.

Key words: Integral values, Partial differentiation, Minimum value-$f_{\min}$.

AMS Subject Classification No: 11D41

Introduction: The famous French mathematician P. Fermat has invented and solved many theorems in his life time (1601-1665 AD). At the last part of his lifetime, he proposed this theorem, that is known as "Fermat's Last Theorem (FLT)". He did not show any solution of this theorem. It comes to know that he has written comment in the margin of a book -- "I have got a fine solution of this problem, but due to want of space in the margin, I cannot state there".

Theorem: The equation, $x^n+y^n=z^n$ has no positive integral solution for $n>2$.

Solution: We can write, $2^ny^n=2^nz^n-2^nx^n$

$$=\{(z+x)+(z-x)\}^n-\{(z+x)-(z-x)\}^n=(z-x)^n\{(\frac{z+x}{z-x}+1)^n-(\frac{z+x}{z-x}-1)^n\}.$$

Let, $\{(\frac{z+x}{z-x}+1)^n-(\frac{z+x}{z-x}-1)^n\}=\{(\frac{z+x}{z-x}\pm k)^n$, where $k\neq 1$. Then,

$$2^nz^n-2^nx^n=(z-x)^n(\frac{z+x}{z-x}\pm k)^n=\{(z+x)\pm k(z-x)\}^n=(z+x+kz-kx)^n,$$

or, $$(z+x+kz-kx)^n+2^nx^n-2^nz^n=f(k,x,z) \qquad (1)$$

And, $$(z+x-kz+kx)^n+2^nx^n-2^nz^n=f(k,x,z) \qquad (2)$$

Let, $z=(r^n+s^n)$, $x=(r^n-s^n)$ or $y=(r^n-s^n)$, $r>s$. Then we get from the equations (1) and (2),

$$2^n(r^n+ks^n)^n+2^n(r^n-s^n)^n-2^n(r^n+s^n)^n=f(k,r,s) \qquad (3)$$

And, $$2^n(r^n-ks^n)^n+2^n(r^n-s^n)^n-2^n(r^n+s^n)^n=f(k,r,s) \qquad (4)$$

…………………………………………

Again we can write, $2^ny^n=2^nz^n-2^nx^n$

$$=\{(z+x)+(z-x)\}^n-\{(z+x)-(z-x)\}^n=(z+x)^n\{(1+\frac{z-x}{z+x})^n-(1-\frac{z-x}{z+x})^n\}.$$

Let, $\{(1+\frac{z-x}{z+x})^n-(1-\frac{z-x}{z+x})^n\}=(c\pm\frac{z-x}{z+x})^n$, where $c\neq 1$. Then,

$$2^nz^n-2^nx^n=(z+x)^n(c\pm\frac{z+x}{z-x})^n=\{c(z+x)\pm(z-x)\}^n=(cz+cx+z-x)^n,$$

or, $$(cz+cx+z-x)^n+2^nx^n-2^nz^n=f(c,x,z) \qquad (5)$$

And, $$(cz+cx-z+x)^n+2^nx^n-2^nz^n=f(c,x,z) \qquad (6)$$

……………………………………

Again we can write, $2^n x^n = 2^n z^n - 2^n y^n$

$={(z+y)+(z-y)}^n - {(z+y)-(z-y)}^n = (z-y)^n \{(\frac{z+y}{z-y}+1)^n - (\frac{z+y}{z-y}-1)^n\}$.

Let, $\{(\frac{z+y}{z-y}+1)^n - (\frac{z+y}{z-y}-1)^n\} = (\frac{z+y}{z-y} \pm h)^n$, where $h \neq 1$. Then,

$2^n z^n - 2^n y^n = (z-y)^n (\frac{z+y}{z-y} \pm h)^n = \{(z+y) \pm h(z-y)\}^n = (z+y+hz-hy)^n$,

or, $(z+y+hz-hy)^n + 2^n y^n - 2^n z^n = f(h,y,z)$ (7)

And, $(z+y-hz+hy)^n + 2^n y^n - 2^n z^n = f(h,y,z)$ (8)

……………………………………..

Again we can write, $2^n x^n = 2^n z^n - 2^n y^n$

$=\{(z+y)+(z-y)\}^n - \{(z+y)-(z-y)\}^n = (z+y)^n \{(1+\frac{z-y}{z+y})^n - (1-\frac{z-y}{z+y})^n\}$.

Let, $\{(1+\frac{z-y}{z+y})^n - (1-\frac{z-y}{z+y})^n\} = (m \pm \frac{z-y}{z+y})^n$, where $m \neq 1$. Then,

$2^n z^n - 2^n y^n = (z+y)^n (m \pm \frac{z-y}{z+y})^n = \{m(z+y) \pm (z-y)\}^n = (mz+my+z-y)^n$,

or, $(mz+my+z-y)^n + 2^n y^n - 2^n z^n = f(m,y,z)$ (9)

And, $(mz+my-z+y)^n + 2^n y^n - 2^n z^n = f(m,y,z)$ (10)

……………………………………….

Again we can write, $2^n z^n = 2^n x^n + 2^n y^n$

$=\{(x+y)+(x-y)\}^n + \{(x+y)-(x-y)\}^n = (x-y)^n \{(\frac{x+y}{x-y}+1)^n + (\frac{x+y}{x-y}-1)^n\}$.

Let, $\{(\frac{x+y}{x-y}+1)^n + (\frac{x+y}{x-y}-1)^n\} = (\frac{x+y}{x-y} \pm g)^n$, where $g \neq 1$. Then,

$2^n x^n + 2^n y^n = (x-y)^n (\frac{x+y}{x-y} \pm g)^n = \{(x+y) \pm g(x-y)\}^n = (x+y+gx-gy)^n$,

or, $(x+y+gx-gy)^n - 2^n x^n - 2^n y^n = f(g,x,y)$ (11)

And, $(x+y-gx+gy)^n - 2^n x^n - 2^n y^n = f(g,x,y)$ (12)

……………………………………..

Again we can write, $2^n z^n = 2^n x^n + 2^n y^n$

$=\{(x+y)+(x-y)\}^n + \{(x+y)-(x-y)\}^n = (x+y)^n \{(1+\frac{x-y}{x+y})^n + (1-\frac{x-y}{x+y})^n\}$.

Let, $\{(1+\frac{x-y}{x+y})^n + (1-\frac{x-y}{x+y})^n\} = (b \pm \frac{x-y}{x+y})^n$, where $b \neq 1$. Then,

$2^n x^n + 2^n y^n = (x+y)^n (b \pm \frac{x-y}{x+y})^n = \{b(x+y) \pm (x-y)\}^n = (bx+by+x-y)^n$,

or, $(bx+by+x-y)^n - 2^n x^n - 2^n y^n = f(b,x,y)$ (13)

And, $(bx+by-x+y)^n - 2^n x^n - 2^n y^n = f(b,x,y)$ (14)

……………………………………

Now, we differentiate partially the equation (1) with respect to k, x, z respectively and considering the differentiated equations are equal to 0 for obtaining minimum value, we get a suitable value, that is, $k=\frac{z^{n-1}+x^{n-1}}{z^{n-1}-x^{n-1}}$, or, $z=x(\frac{k+1}{k-1})^{1/(n-1)}$, or, $x=z(\frac{k-1}{k+1})^{1/(n-1)}$

Putting the value of k in the equation (1) and get

$$\{z+x+(z-x)(\frac{z^{n-1}+x^{n-1}}{z^{n-1}-x^{n-1}})\}^n+2^nx^n-2^nz^n=f_{\min}$$

Now we put $f_{\min}=0$ and obtain the relation of x and z of this equation when n>2,

$$(z/x)^{n-1}+(z/x)=2$$

Again, putting the value of $z=x(\frac{k+1}{k-1})^{1/(n-1)}$ in the equation (1) and get

$$x^n[\{1-k+(k+1)(\frac{k+1}{k-1})^{1/(n-1)}\}^n+2^n-2^n(\frac{k+1}{k-1})^{n/(n-1)}]=f_{\min} \qquad (15)$$

Then $f_{\min}=0$ for n=2 of the equation (15) when k=0.

Also putting the value of $x=z(\frac{k-1}{k+1})^{1/(n-1)}$ in the equation (1) and get

$$z^n[\{1+k-(k-1)(\frac{k-1}{k+1})^{1/(n-1)}\}^n+2^n(\frac{k-1}{k+1})^{n/(n-1)}-2^n]=f_{\min} \qquad (16)$$

Then $f_{\min}=0$ for n=2 of the equation (16) when k=0.

Some other values of k, x, z are obtained from the equations (1) and (2) for n=2 and $f(k,x,z)=0$. Then, $k=\{2(\frac{z+x}{z-x})^{1/2}-(\frac{z+x}{z-x})\}$ and $k=\{\left(\frac{z+x}{z-x}\right)-2(\frac{z+x}{z-x})^{1/2}\}$

[Examples: (i) For $f_{\min}=0$, the minimum values are x=3, y=4, z=5, k=0, n=2.

(ii) Some other values are obtained such as, x=21, y=20, z=29, k=±(5/4), n=2.]

Again, we differentiate partially the equation (3) with respect to k, r, s respectively and obtain the suitable results by the above way such as,

$$k=-(r^n/s^n), \quad r^n=s^n\{\frac{1+(-1)^{1/(n-1)}}{1-(-1)^{1/(n-1)}}\}, \quad r^n=s^n\{\frac{(-1)^{1/(n-1)}+1}{(-1)^{1/(n-1)}-1}\}, \quad k=\pm\{\frac{1+(-1)^{1/(n-1)}}{1-(-1)^{1/(n-1)}}\},$$

Putting these values in the equation (3) and get

$$2^n(s^n)^n[\{\frac{(-1)^{1/(n-1)}}{1-(-1)^{1/(n-1)}}\}^n-\{\frac{1}{1-(-1)^{1/(n-1)}}\}^n]=f_{\min} \qquad (17)$$

And, $$2^n(s^n)^n[\{\frac{1}{(-1)^{1/(n-1)}-1}\}^n-\{\frac{(-1)^{1/(n-1)}}{(-1)^{1/(n-1)}-1}\}^n]=f_{\min} \qquad (18)$$

Then we find that $f_{\min}=0$ of the equations (17) and (18) when n=2.

Similarly, we can derive by the same way as described before and get several equations for n>2 and $f_{\min}=0$. The equations are listed below:

From the equation (1), $(z/x)^{n-1}+(z/x)=2$ (19)

From the equation (2), $(z/x)^{n-1}+(z/x)=2$ (20)

From the equation (5), z=x, (but z>x) (21)

From the equation (6), $2(z^{n-1}+z^{n-2}x+\ldots+x^{n-1})-(z^{n-2}x+z^{n-3}x^2+\ldots+zx^{n-2})=0$ (22)

From the equation (7), $(z/y)^{n-1}+(z/y)=2$ (23)

From the equation (8), $(z/y)^{n-1}+(z/y)=2$ (24)

From the equation (9), $z=y$, (but $z>y$) (25)

From the equation (10), $2(z^{n-1}+z^{n-2}y+\ldots.+y^{n-1})-(z^{n-2}y+z^{n-3}y^2+\ldots.+zy^{n-2})=0$ (26)

From the equation (11), $x^{n-2}+y^{n-2}=0$ (27)

From the equation (12), $x^{n-2}+y^{n-2}=0$ (28)

From the equation (13), $(x/y)^{n-1}-(x/y)=2$ (29)

From the equation (14), $(y/x)^{n-1}-(y/x)=2$ (30)

From the equation (3), collect the equations (17) and (18).

There are more equations, similar to (3), (4), (15), (16), (17), (18). Those are not derived here.

So, x or y or z will have no integral values from the above equations when $f_{\min}=0$.

Then we conclude that $z^n-x^n-y^n=f_{\min}\neq 0$, or, $x^n+y^n-z^n=f_{\min}\neq 0$ for the positive integral values of x, y, z and $n>2$. [Examples: (i) $7^3-6^3-5^3=2=f_{\min}\neq 0$, (ii) $9^3+10^3-12^3=1=f_{\min}\neq 0$.]

Hence x, y, z will have no positive integral solution for $n>2$.

It is completing the proof of Last Theorem of P. Fermat by algebraic method.

References:

1. G. H. Hardy & E. M. Wright, An Introduction to the Theory of Numbers, Fifth Edition, 1979, Oxford Science Publications.
2. P. Ribenboim, Recent Results on Fermat's Last Theorem, Canad. Math. Bull. 20(2) (1977), 229-242.
3. P. Ribenboim, Kummer's Ideas on Fermat's Last Theorem, Enseign. Math. (2) 29 (1-2) (1983), 165-167.
4. Andrew J. Wiles, Modular Elliptic Curves and Fermat's Last Theorem, Annals of Mathematics, 141 (1995), 443-551.

GEOMETRICAL SOLUTION OF LAST THEOREM OF P.FERMAT (1601-1665 AD)

Ramesh Chandra Ray
Professor of Electrical Engineering
Chittagong University of Engineering and Technology (CUET)
Bangladesh.
E-mail: ramesh_ray2003@yahoo.com, rameshchandraray@yahoo.com
www.rameshcray.wordpress.com

Abstract:
An elementary proof of the last theorem of the French Mathematician P. Fermat, $x^n + y^n = z_n{}^n$, has been discussed in the paper by geometrical method. For n = 2, the equation $x^2 + y^2 = z_2{}^2$, represents right angle triangle. For any value of n, it is obtained that $z_{n+2} < z_{n+1} < z_n < z_{n-1} < z_{n-2} ...... < z_2$, or $z_2 > z_3 > z_4 > z_5$...etc (proof is given below). These are shown in fig.1(a) and fig.1(b). [Example:- $20^2 + 21^2 = 29^2$. Then, $20^3 + 21^3 = 17261 < 29^3$.]

AMS Subject Classification No: 11D41

Theorem: In the equation, $x^n + y^n = z_n{}^n$, there is no solution when x, y, z_n and n > 2 are positive integers.

Proof of $z_{n+2} < z_{n+1} < z_n < z_{n-1} < z_{n-2} ... < z_2$, or $z_2 > z_3 > z_4 > z_5$....etc(stated in abstract):

Let, $z_2 = (x^2 + y^2)^{1/2}$, $z_3 = (x^3 + y^3)^{1/3}$,....$z_n = (x^n + y^n)^{1/n}$, $z_{n+r} = (x^{n+r} + y^{n+r})^{1/(n+r)}$, $z_{n+s} = (x^{n+s} + y^{n+s})^{1/(n+s)}$, r > s and $z_{n+r} < z_{n+s}$, or,

$$(x^{n+r} + y^{n+r})^{1/(n+r)} < (x^{n+s} + y^{n+s})^{1/(n+s)}.$$

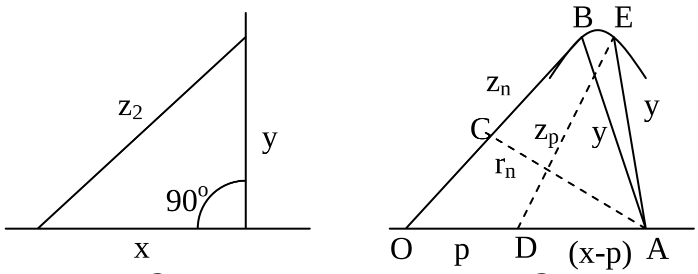
Then $(x^{n+r} + y^{n+r})^{(n+s)} < (x^{n+s} + y^{n+s})^{(n+r)}$............(a)

As x < y or y < x or y = x, let x = my or y = mx and m < 1 or m = 1. Then it is obtained from (a) that, $(1 + m^{n+r})^{(n+s)} < (1 + m^{n+s})^{(n+r)}$, or,

$$0 < \{{}^{(n+r)}C_1 m^s - {}^{(n+s)}C_1 m^r\} + m^n\{{}^{(n+r)}C_2 m^{2s} - {}^{(n+s)}C_2 m^{2r}\} + m^{2n}\{{}^{(n+r)}C_3 m^{3s} - {}^{(n+s)}C_3 m^{3r}\} + ...(b)$$

So it is obtained from (b) for m < 1 or m = 1 and any value of n, r, s, r > s that, LHS < RHS. Hence, $z_{n+2} < z_{n+1} < z_n < z_{n-1} < ... < z_2$, or $z_2 > z_3 > z_4 > z_5$…etc.

Proof of the theorem: As it is proved that $z_{n+2} < z_{n+1} < z_n < z_{n-1} < ... < z_2$, or $z_2 > z_3 > z_4 > z_5$ ...etc, then the following fig.1(a) and fig.1(b) can be drawn. Let OA= x, OD = p, DA = (x - p), BE arc, AB = AE = y, OB = z_n, OC = CB = $z_n/2$, DE = z_p, CA = r_n and the angles $\angle OAB < 90^o$, $\angle DAE < 90^o$ (for n > 2). Considering various values of p, it can be represented in accordance



n=2 n>2
(a) Fig.1 (b)

with the Fermat's theorem, $x^n + y^n = z_n{}^n$ from the triangle ΔOAB and also $(x - p)^n + y^n = z_p{}^n$ from the triangle ΔDAE.

Then $z_p < z_n$ and $z_p > y$. By applying Apollonius theorem to the triangle ΔOAB, it is obtained that, $x^2 + y^2 = 2r_n^2 + z_n^2/2 = z_2^2$…………(i)

Again by using 'square rule', $[A^2 + B^2 = C^2, A = (R^2 - S^2), B = 2RS, C = (R^2 + S^2), R > S]$, the following relations can be written from (i):

$x = (R_1^2 - S_1^2)$, $y = 2R_1S_1$, $R_1 > S_1$, $z_n = (R_2^2 - S_2^2)\sqrt{2}$, $r_n\sqrt{2} = 2R_2S_2$, $R_2 > S_2$, $z_2 = (R_1^2 + S_1^2) = (R_2^2 + S_2^2)$, or $(R_1^2 - R_2^2) = (S_2^2 - S_1^2) = g$, or $R_1^2 = (R_2^2 + g)$ and $S_1^2 = (S_2^2 - g)$.

Then $x = (R_1^2 - S_1^2) = (R_2^2 - S_2^2) + 2g = 2g + z_n/\sqrt{2}$,.……(1)

or, $2g = x - z_n/\sqrt{2}$.............(1).

Putting this value of (1), it is obtained that

$$(2g + z_n/\sqrt{2})^n + y^n = z_n^n \text{……….(2)}$$

So it is determined by the value of 2g from (1) and (2) whether x, y, n and z_n will be simultaneously integers or not.

To obtain the possible integral values of x and z_n from (1), there may be a value of $2g = (p - q/\sqrt{2})$, where p and q are integers.

Then it is obtained from the equation (1) that, $(x - p) = (z_n - q)/\sqrt{2}$………….(ii)

$(p \rightarrow x, z_n \rightarrow z_p, z_p \rightarrow y), (p = x, z_n = z_p = y = q)$

When $p = x$ and $q = z_n$ at (ii), then $(x - p)^n + y^n = z_p^n$, or $0 + y^n = z_p^n$, or, $z_p = y$. But $z_p > y$ for validity of Fermat's equations.

So $x > p$ and $z_n > q$. Then z_n will not be integer from (ii) for $x > p$.

[Example:- Let x = 3, y = 5 and p = 1, 2, 3. Then it can be written,

$3^n + 5^n = z_n^n$ and $(3 - p)^n + 5^n = z_p^n$.

For p = 1, the Fermat's equation, $(3 - 1)^n + 5^n = z_p^n$, or, $2^n + 5^n = z_p^n$ is valid, $z_p > y$.

For p = 2, the Fermat's equation, $(3 - 2)^n + 5^n = z_p^n$, or, $1^n + 5^n = z_p^n$ is valid, $z_p > y$.

For p = 3, the Fermat's equation, $(3 - 3)^n + 5^n =z_p^n$, or, $0 + 5^n = z_p^n$ is invalid. Then $z_p = 5 = y$.

Again let (x - p) = 3, 4, 5,.....etc. Then $3^n + 5^n = z_p^n$, $4^n + 5^n = z_p^n$, $5^n + 5^n = z_p^n$, $6^n + 5^n = z_p^n$,.....etc.

So $x > p$ and $z_n > z_p > y$ for validity of the Fermat's equations.]

Hence x or y or z_n or $n > 2$ is not integer from the equations (1) and (2) for any value of 2g. It proves the last theorem of P. Fermat by geometrical method.

References:

[1] G. H. Hardy & E. M. Wright—An Introduction to the Theory of Numbers, Fifth Edition,1979, Oxford Science Publications.

[2] P. Ribenboim, Recent Results on Fermat's Last Theorem, Canad. Math. Bull.20(2)(1977), 229-242.

[3] P. Ribenboim, Kummers Ideas on Fermat's Last Theorem, Enseign. Math. (2) 29(1-2)(1983),165-167.

[4] Andrew J. Wiles, Modular Elliptic Curves and Fermat's Last Theorem, Annals of Mathematics, 141, (1995), 443-551.