MAY BE FERMAT'S OWN PROOF

By

RAMASWAMY KRISHNAN

B-7/203, VIJAY PARK, THANE (W), INDIA - 400615

Email ID – ramasa421@gmail.com ; mobile - +91 93202 94848

SYNOPSIS

Many times a great problem has a simple solution. A simple solution for Fermat's Theorem is presented here. In the first two pages, after going through well known facts, using nothing but The elementary formula $(x+y)^n$, it is derived

$$2^p p^{p\propto} p_1^p p_2^p p_3^p p_4^p$$
$$= 4abc \sum_1^{(p-1)/2} pC_{2r}\, a^{p-2r-1} \left\{ \sum_0^{r-1} pC_{2s+1}\, b^{2r-2s-2} c^{2s} \right\}$$

Where a = (x+y), b = (z-y), c = (z-x). This equation itself shows why the Theorem is true. In the next three pages, taking 'y' as the smallest of the three, it is proved that

$\boldsymbol{p\ is\ a\ divisor\ of\ z, x, or\ (z-x)\ and\ p_4 = 1}$. This proves the theorem for all values of $\boldsymbol{p \geq 5}$.

RAMASWAMY KRISHNAN

01/01/2022

PREFACE

I assure Mathematicians that it will not take more than 15 minutes to go through the proof.
I am a graduate engineer and not a mathematician. My knowledge of Mathematics probably does not go beyond 1850. In 1965 while I was browsing through the 'Elementary Theory Of Numbers' by Hardy and Wright to find what Number Theory is all about, in a British council library, I came across The Fermat's Theorem.

I just wondered why is it so difficult to prove. A year later in my college library, in 'Theory of numbers and Diophantine analysis' by Carmichael I again came across the Theorem and understood the enormity of proving it. These two are my only reference books. I first felt that I have to read a lot of Mathematics before even attempting to solve it. But by the time I reached home I changed my mind. My I.Q. may not be as good as Fermat's but my knowledge is higher than him. Hence if he has proved it, I can try to prove it without using any knowledge not known to him.
That is why I have titled it as MAY BE FERMAT'S OWN PROOF. I have not used anything that is not known to him.

R. KRISHNAN

01-01-2022

THE PROOF OF FERMAT'S THEOREM

$$1.\,(x+y-z)^p$$

It is well known that Fermat's Theorem can be divided in to two parts.

PART 1 :-- If 'p' is an odd prime , x, y, z are positive integers such that, p, x, y, z are prime to each other and

$x^p + y^p = z^p$ ----------(1)

there exist positive integers $p_1, p_2, p_3, q_1, q_2, q_3$ and

$$x = p_1q_1, y = p_2q_2, z = p_3q_3 \quad and$$

$$z-y = p_1^p,\ z-x = p_2^p,\ x+y = p_3^p$$ ----------(2)

PART 2 : - If 'p' is a divisor of x or y or z say 'z' then there exist an integer 'α' so that z = $p^\alpha p_3 q_3$ and $x+y = p^{p\alpha-1}\, p_3^p$ ----------(3)

Let 'q' be a prime factor of q_3 . Let q – 1 = pk + r

Hence $x^p \equiv (-y)^p$ mod (q) ----------(4)

But $x^{pk+r} \equiv y^{pk+r}$ mod (q) ----------(5)

So $x^r \equiv (-y)^r$ mod (q) ----------(6)

From (4) & (6) it is obvious that if r $\neq$ 0, $x + y \equiv 0\ mod\ (q)$

So $q \equiv 1\ mod(p), hence\ q_3 \equiv 1\ mod(p)$ & $so\ q_3^p \equiv 1 \bmod(p^2)$

Similarly, $q_1^p \equiv q_2^p \equiv q_3^p \equiv 1\ mod(p^2)$ ----------(7)

(5)

It is possible to prove $q_1 \equiv q_2 \equiv q_3 \equiv 1\, mod(p^2)$

From (7), we get $p_1^p + p_2^p \equiv p_3^p\, mod(p^2)$ & so

$$x + y - z \equiv 0\, mod\ (p^2) \quad \text{----------(8)}$$

Therefore $x + y - z = p^{\alpha} p_1 p_2 p_3 p_4\, where\ \alpha \geq 2$ and

p_4 is prime to x, y, z ----------(9)

Let $x + y = a\ ;\ z - y = b;\ z - x = c$

Then $2(x + y - z) = a - (b + c); 2z = a + (b + c)$

$$2x = a + (b - c);\ 2y = a - (b - c)$$

So $(2p^{\propto} p_1 p_2 p_3 p_4)^p = [2(x + y - z)]^p + (2z)^p - (2x)^p - (2y)^p$

$$= (a - b - c)^p + (a + b + c)^p - (a - b + c)^p - (a + b - c)^p$$

Therefore $2^p p^{p\propto} p_1^p p_2^p p_3^p p_4^p$

$= 4abc \sum_1^{(p-1)/2} pC_{2r}\, a^{(p-2r-1)} \left\{\sum_o^{r-1} pC_{2s+1}\, b^{(2r-2s-2)} c^{2s}\right\}$---(10)

2. *THE PROOF*

'z', 'x' are two positive integers prime to each other

and z-x $< x < z$, ----------(11)

& $y^p = z^p - x^p$ ----------(12)

Assumption 1 :-- y is an integer ----------(13)

From the above assumption we get

$$y \equiv (z - x)\ mod(p)$$

Therefore $y^p \equiv (z - x)^p\ mod(p^2)$ and hence

$z^p - x^p \equiv (z - x)^p\ mod(p^2)$ ----------(14)

Assumption 2 :--

$'p' is\ not\ a\ prime\ of\ z, x, or (z - x)$ ----------(15)

From (14) and (15) we get

$$A = \frac{(z^p - x^p) - (z-x)^p}{(z-x)^p} \equiv 0\ mod(p^2)$$ ----------(16)

Assumption 3 :-- $p_4 \neq 1$ ----------(17)

First, an analysis of assumption 2 :-

From (11) : $A > 1$

Let $B = \frac{A}{p} \equiv 0\ mod(p)$

So let,

$\frac{1}{p}C_r = \frac{1}{r!}\frac{1}{p}\left(\frac{1}{p}-1\right)---\left(\frac{1}{p}-r+1\right)$ ----------(18)

$\frac{1}{p}C_r A^r = \frac{1}{r!}(1-p)(1-2p)--(1-rp+p)\frac{A^r}{p^r}$

$\frac{1}{p}C_r A^r = \frac{1}{r!}(1-p)(1-2p)--(1-rp+1)\,B^r$ ----------(19)

We know that if 'y' is an integer then

$y \equiv z-x\ mod(p);\ \ So\ \frac{y}{z-x} \equiv 1\ mod(p)$

So let $\frac{y}{z-x} = 1+pk_1$ ----------(20)

So $(\frac{y}{z-x})^p = \frac{y^p}{(z-x)^p} = \frac{z^p-x^p}{(z-x)^p} = A+1$

So $A+1 = (1+pk_1)^p \equiv 1+p^2k_1\ mod(p^3)$

So $pk_1 \equiv \frac{A}{p}\ mod(p^2)$

So now let $\frac{y}{z-x} = 1+B+p^2k_2$ ----------(21)

Hence $A+1 \equiv 1+pB+pC_2B^2+p^3k_2 mod(p^4)$

So now, $\frac{y}{z-x} = 1+B+\frac{1}{2!}(1-p)B^2+p^3k_3$ ----------(22)

and so on. But $(p^s)!$ in the denominator will increase the number of terms required.

But $\frac{A^{p^s}}{(p^s)!} \equiv omod(p\ to\ the\ power\ of\ \frac{p^{s+1}-2p^s+1}{p-1})$

As Lt $s\ tends\ to\ \infty$, $\frac{p^{s+1}-2p^s+1}{p-1}\ tends\ to\ \infty.$

So $\frac{y}{z-x} = \sum_0^\infty \frac{1}{p}C_r A^r$

Or $+ve\ value\ 0f\ \left(\frac{y}{z-x}\right) tends\ to\ \infty$. Therefore, if 'y' is

an integer then our assumption (2) is incorrect.

Hence 'p' is a divisor of z, x, or (z-x).

THIS PROOVES HALF OF FERMAT'S THEOREM.

And in equation (10), $abc = p^{p\propto-1}p_1^p p_2^p p_3^p$ ----------(23)

Now coming to <u>assumption 3</u>

As $p_4 \neq 1\ let$ 'q' be a prime of p_4.

Then $\frac{y}{Z-X} \equiv 1\ mod\ (q)\ and\ so\ let \frac{y}{z-x} = 1 + qk_1$ ----------(24)

As 'q' is not a divisor of z, x, or (z-x), by repeating

the process done for 'p' we arrive

That $+ve\ value\ of\ \frac{y}{z-x} = \infty$ ----------(25)

Therefore, our assumption 3 is wrong.

Hence, $p_4 = 1$.

Now, $2^3 p^{p\propto} p_1^p p_2^p p_3^p = 8 \times 3abc\ for\ prime\ 3\ \ in\ eqn\ (10).$

If $x \neq z$, for p ≥ 5 , $RHS > LHS$ in equation (10).

Therefore, Fermat's Theorem is proved for $p \geq 5$

As for p = 3 and p = 4, proofs already exist, so

FERMAT'S THEOREM STANDS PROOVED FOR ALL VALUES OF 'p'.

Explanation And Conclusion :--

$$\frac{y^p}{(z-x)^p} = 1 + \frac{y^p-(z-x)^p}{(z-x)^p} = 1 + \frac{z^p-x^p-(z-x)^p}{(z-x)^p} = 1 + A$$

So, $\frac{y}{(z-x)} = (1+A)^{\frac{1}{p}}$. But RHS cannot be expanded

into an infinite series because $A > 1$. But if 'p' is not a prime of

z, x, or (z-x) and $p_4 \neq 1$, then it results in this invalid expansion.

Thus, we get the proof of the theorem for all primes that are

greater than or equal to '5'.

I don't have any references other than what I have given in the preface. I have not used anything not known to Fermat. So, I have named it as MAY BE FERMAT'S OWN PROOF.