Beal Conjecture & Fermat's Last Theorem

Shubhankar Paul

Abstract— **In this paper we will prove two problems :**

1) **Beal Conjecture**
2) **Fermat's Last Theorem**

First we will show Beal Conjecture is true.
Then we will show Fermat's Last Theorem is true.

Index Terms— **Beal Conjecture, Fermat's Last Theorem**

I. Beal Conjecture Problem

The banker and poker player Andrew Beal has conjectured that there are no solutions to the equation

$a^x + b^y = c^z$

if a, b, and c are co-prime integers, and x, y, and z are all integers > 2.

The problem is to prove the Beal Conjecture, or find a counter-example.

Solution

1) a, b, c all cannot be even as they are co-prime.
2) a, b, c all cannot be odd otherwise Left hand Side will become even and Right Hand side will become odd.
3) Two of them cannot be even. Let's say a and c are even then b must be even. (Contradiction). Let's say a and b are even then c must be even (Contradiction).
4) So, two of them are odd and one is even. We will consider this case.

Either a or b may be even from LHS. Let's say a even b and c odd.

Case 1 : y, z are even.

Implies z/2 and y/2 are integers.

So, a^x = (c²)^(z/2) – (b²)^(y/2) ....eqn (1)

Now, c ≡ ±1 (mod 4)

⇨ c² ≡ 1 (mod 4)

Similarly, b² ≡ 1 (mod 4)

So, we can write, c² = 4m+1 and b² = 4n + 1

Now, putting into eqn (1) we get,

a^x = (4m+1)^(z/2) – (4n+1)^(y/2)

Breaking RHS into Binomial expansion, we get,

a^x = (4m)^(z/2) +(z/2)C_1*(4m)^(z/2-1) + ...+(z/2)*4m + 1 – (4n)^(y/2) – (y/2)C_1*(4n)^(y/2-1) - ....- (y/2)*4n – 1

Manuscript received November 03, 2013.

Shubhankar Paul, Passed BE in Electrical Engineering from Jadavpur University in 2007. Worked at IBM as Manual Tester with designation Application Consultant for 3 years 4 months. Worked at IIT Bombay for 3 months as JRF.

⇨ a^x = 4[2k + {(z/2)*m – (y/2)*n}]

Now, x is minimum 3. Implies 2³ is a factor of a^x. So, RHS should be divisible by 8.

⇨ {(z/2)*m – (y/2)*n}/2 = integer

⇨ (z/2²)*m – (y/2²)*n = integer

z/2 and y/2 are odd according to our case.

⇨ m = 2p ; n = 2q

If z/2 is not odd then z/2² also integer and y/2 is not odd then y/2² also integer.

z/2² integer means c_1 ≡ 1 (mod 8) and b_1 ≡ 1 (mod 8)

So, either (m = 2p and n = 2q) OR z/2² and y/2² are integers.

Whatever be the case we end up with the equation (1) as,

a^x = (8p+1)^r - (8q+1)^s ....equation (A)

Breaking it into binomial expansion, we get,

a^x = (8p)^r +rC_1(8p)^(r-1) + ...+ r*8p + 1 – (8q)^s – sC_1(8q)^(s-1) - .... – s*8q – 1

⇨ a^x = 8[2k_1 + (rp – sq)]

⇨ RHS is divisible by 16 as (rp-sq) is even. But LHS ≡ 8 (mod 16).

Here is the contradiction.

Now, there can be two more conditions hovering into mind.

1) We take x = 4
2) Either p or q must be even. Let's say p = 2t.

Case 1 : Then right hand side is divisible by 16. And we can change x = 4.

In that case say r = 2g and s = 2h or p=2g and q=2h or r=2g and q=2h or p=2g and s = 2h

In either case we can form equation (1) as a^x = (16g+1)^r – (16h+1)^s

⇨ a^x = (16g)^r + rC_1*(16g)^(r-1) + ... + r*16g +1 – (16h)^s - sC_1*(16h)^(s-1) - ...... – s*16h – 1

⇨ a^x = 16{ 2k + (rg – sh)}

⇨ Again the same equation and same procedure if followed it will go on infitely. So, we choose the contradiction case.

Case 2 : Equation (1) becomes

a^x =(16t+1)^r – (8q+1)^s ....equation (C)

Breaking into Binomial expansion, we get,

a^x = (16t)^r + rC_1*(16t)^(r-1) + ... + r*16t + 1 – (8q)^s – sC_1*(8q)^(s-1) - .... – s*8q – 1

Now, if we divide (16t+1)^r by 16 the quotient is odd as r*t is odd. If we divide (8q+1)^s by 16 the quotient is even if (sq+1) is divisible by 4 and odd if (sq+1) is divisible by 2.

Let's take (sq+1) is divisible by 2.

Then, on dividing RHS by 16 gives even quotient as rt + (sq+1)2 is even.

⇨ a_1 = 4i+1 form. (if a_1= 4i+3 form then gives odd quotient on division by 16)

Now, dividing both sides by 32, RHS gives even quotient if rt+(sq+1)/2 is divisible by 4 and gives odd quotient if rt+(sq+1)/2 is divisible by 2.
LHS = $8*a_1^3$ = $8*(4i+1)^3$ = $8(64i^3+48i^2+12i +1)$ = $32(16i^3+12i^2+3i) + 8$
⇨ LHS gives odd quotient on division by 32 if i is odd and gives even quotient if i is even.

Again it will go on increasing the math giving no solution.
Similarly it will go on increasing if (sq+1)/2 is divisible by 4.
⇨ y, z cannot be both even.

Case 2 : y odd, z even.
Now, a^x = c^z – b^y
Z even => z/2 = integer .
Now, c ≡ ± (mod 4)
⇨ $c^2 \equiv 1$ (mod 4)

So, c^z = (4m+1)^(z/2)
Now, b^y must be of the form (4n+1)^y to get RHS divided by 4.
Now, RHS = (4m+1)^(z/2) – (4n+1)^y .... equation (B)
Breaking into Binomial expansion we get,
(4m)^(z/2) + $(z/2)C_1$(4m)^(z/2-1)+ .... + (z/2)*4m + 1 – (4n)^y – yC_1*(4n)^(y-1) -. .... – y*4n – 1
= 4 [2k + {(z/2)*m – y*n}]
But x is minimum 3. Implies LHS has a factor of 8.
So, RHS should get divided by 8.
⇨ (z/2)(m/2) – y*(n/2) = integer.

So, either m=2p or $z/2^2$ is an integer and n = 2q
In either of the case of m=2p or $z/2^2$ = integer we end up with the equation (1)
a^x = (8p+1)^z_1 - (8q+1)^y
Now, this is similar to equation (A)
Therefore no solution.
⇨ y odd , z even gives no solution.

Case 3 : y even, z odd.
a^x = c^z – b^y
⇨ a^x = c^z – (b^2)^(y/2)

Now, b ≡ 1(mod 4)
⇨ $b^2 \equiv 1$ (mod 4)

RHS = c^z – (4n+1)^(y/2)
Now c must be of theform 4m+1 to get divided by 4.
Now RHS = (4m+1)^z – (4n+1)^(y/2)
This equation is similar to equation (B)
Implies no solution.
Case 4 : y,z both odd.
a^x =c^z – b^y
= c*(c^2)^(z-1)/2 – b*(b^2)^(y-1)/2
= c*(8m+1)^(z-1)/2 – b*(8n+1)^(y-1)/2
= c*[(8m)^(z-1)/2 + (z-1)/$2C_1$*(8m)^{(z-1)/2 -1} + ... +8m*(z-1)/2 + 1] - b*[(8n^(y-1)/2 + (y-1)/$2C_1$(8n)^{(y-1)/2 -1} + ... +8n*(y-1)/2 + 1]

Dividing both sides by 8, LHS = 0 as x is minimum 3
RHS = (c-b)
Now, c-b ≡ 0
⇨ c ≡ b

Dividing both sides by 16 we get,
LHS ≡ $8a_1$ (mod 16)
RHS ≡ c*{(z-1)/2}*8m – b{(y-1)/2}*8n + (c-b)
Now $8a_1$ ≡ c*{(z-1)/2}*8m – b*{(y-1)/2}*8n + (c-b)
⇨ a_1 ≡ c*{(z-1)/2}*m – b*{(y-1)/2}*n + i (odd integer)

Now we can write, z = 4t+1 and y = 2u+1 (say)
Let's say, b = 8m+1 then c = 8m+1 (as b ≡ c (mod 8))
Now RHS = (8m+1)^(4t+1) – (8n+1)^(2u+1)
= (8m)^(4t+1) + $(4t+1)C_1$ *(8m)^(4t) + ... + (4t+1)*8m + 1 – (8n)^(2u+1) - $(2u+1)C_1$ *(8n)^(2u) - .... – (2u+1)*8n – 1
= 8*[$2k_1$ + {(4t+1)*m – (2u+1)*n}]
= 8*[$2k_1$ + 2(2mt-un) + (m-n)]
Now (m-n) is even which we will not continue to infinite process as shown in red colour up. So, we will make either m or n even.
Let's putting 2m in place of m.
Now the equation becomes : (16m+1)^z_1 - (8n+1)^y_1
Same as equation (C).
Similarly it can be proved for the set of values (b = 8m+3, c =8n+3); (b=8m+5, c=8m+5); (b=8m+7, c=8m+7).
So, no solution for y, z, both odd.

<u>c even and a & b are odd</u>
Case 1 : If x,y both even.
a^x + b^y = c^z
(a^2)^(x/2) + (b^2)^(y/2)
= (4m+1)^(x/2) +(4n+1)^(y/2)
= (4m)^(x/2) +$(x/2)C_1$(4m)^(x/2 -1) + ... + (x/2)*4m + 1 + (4n)^(y/2) + $(y/2)C_1$(4n)^(y/2 -1) + ... + (y/2)*4n + 1
= $4k_1$ + 2
Divisible by 2 and not 4. But z is at lease 3 i.e. RHS has got a minimum factor of 8.
So, in this case solution is not possible.
Case 2 : x odd, y even.
a^x + b^y
= (2m+1)^x + (4n+1)^(y/2)
= (2m)^x + xC_1*(2m)^(x-1) + ... + x*2m + 1 + (4n)^(y/2) + $(y/2)C_1$*(4n)^(y/2 -1) + ... +(y/2)*4n + 1
= $2k_1$ + 2
= $2(k_1+1)$
As per the above case no solution.
Case 3 : x even , y odd
Same as Case 2.
Case 4 : x,y both odd
a^x + b^y
= a*(a^2)^(x-1)/2 + b*(b^2)^(b-1)/2
= a*(8m+1)^(x-1)/2 + b*(8n+1)^(y-1)/2
= a[(8m)^(x-1)/2 + ...+8m*(x-1)/2 +1] + b[(8n)^(y-1)/2 + ... + 8n*(y-1)/2 + 1]
= $8k_1$ + (a+b)
Now dividing both sides by 8, RHS ≡ (a+b) and LHS ≡ 0 (mod 8)
⇨ (a+b) ≡ 0 (mod 8)

So, the set of values of a and b can be
(a=8m+3, b=8n-3); (a=8m+1, b = 8n-1)
Taking the first set of values,
LHS = (8m+3)^x + (8m-3)^y
= [(8m)^x +xC_1 *(8m)^(x-1)*3 + ... + x*8m*3^(x-1) + 3^x] +[(8n)^y - yC_1 *(8n)^(y-1)*3 + ... + y*8n*3^(y-1) – 3^y]
= 8*2k + (3^x – 3^y)

Now, dividing both sides by 16,
$(3^x - 3^y) \equiv 8$ or 0
If we take 8 then, z=3
Now, $c = 2*c_1$
$c^3 = 2^3*c_1^3$
$c^3 \equiv 8c_1$ or $72\, c_1 \pmod{16}$
⇨ $c^3 \equiv 8c_1 \pmod{16}$

Now, LHS $\equiv 8 \pmod{16}$
⇨ $8c_1 \equiv 8 \pmod{16}$
⇨ $c_1 \equiv 1 \pmod{16}$
⇨ $c_1 = 16j+1$

RHS $= 8*(16j+1)^3$
$= 8*(16^3*j^3 + 3*16^2*j + 48j^2 + 1)$
Now, RHS $\equiv 8 \pmod{32}$
LHS $\equiv 8*\{mx*3^{(x-1)} + ny*3^{(y-1)}\} + (3^x - 3^y) \pmod{32}$
Now $(3^x - 3^y) \equiv 8 \pmod{16}$
⇨ $(3^x - 3^y) \equiv \pm 8 \pmod{32}$

Now, m and n cannot be both even or both odd otherwise LHS will be divisible by 16.
⇨ $mx*3^{(x-1)} + ny*3^{(y-1)}$ is odd.
⇨ $8*\{mx*3^{(x-1)} + ny*3^{(y-1)}\} \equiv \pm 8 \pmod{32}$
⇨ LHS $\equiv \pm 8 \pm 8 \pmod{32}$
⇨ LHS cannot be $\equiv 8 \pmod{32}$

So here is the contadiction. So no solution.
Now, we take $(3^x - 3^y) \equiv 0 \pmod{16}$
⇨ z = 4.

Then, it will go on increasing z infinitely giving no solution as stated in the coloured portion.
Similarly, we can prove for (a =8m+1, b = 8n-1
So, no solution when x, y both odd.

Conclusion

From the above cases we see that no solution exists for the equation $a^x + b^y = c^z$ when a, b, c are co-prime and x,y,z > 2.

Result

Beal Conjecture is true.

II. Fermat's Last Theorem Problem

In 1637, Pierre de Fermat claimed to have a proof that there are no solutions to the equation

$a^n + b^n = c^n$

if a, b, c, and n are integers, and n>2.

Andrew Wiles proved this theorem in 1994, but using many areas of mathematics completely unknown in Fermat's day.

The problem is to prove Fermat's Last Theorem, using only techniques available to mathematicians in the seventeenth century.

Solution

1) Three of a. b, c cannot be even otherwise there is a factor of 4 by which it will get divided until two odd occurs.
2) Three of them cannot be odd because otherwise $(a^n + b^n)$ will be even and c^n will be odd.
3) Two of them cannot be even. Let's say a, b even then (a^n+b^n) is even and c cannot be odd.
4) Two of them are odd and one is even. We will consider this case.

Case 1 : a even, b and c are odd.
Let's take n odd.
The equation is $a^n + b^n = c^n$
Let's say $a = (2^t)\{(2^{nt})*p + 1\}$
$b = \{2^{(nt)}\}*q + 1$
$c = \{2^{(nt)}\}*m+1$
Now, $c^n - b^n = [\{2^{(nt)}\}*m+1]^n - [\{2^{(nt)}\}*m+1]^n$
Expanding in binomial expansion,
$= [\{2^{(tn)}\}*m]^n + nC_1 [\{2^{(tn)}*m]^{(n-1)} + \ldots + n*\{2^{(tn)}\}*m + 1 - [\{2^{(tn)}\}*q]^n - nC_1 [\{2^{(tn)}*q]^{(n-1)} - \ldots - n*\{2^{(nt)}\}*q - 1$
$= \{2^{(tn)}\}[2k + n(m-q)]$ where 2k = taken all terms except nm and nq
Now n is odd. Left hand side is divisible by $2^{(tn)}$. So, either m or q must be even and another must be odd otherwise right hand side will be divisible by $2^{(nt+1)}$
Let's put 2m in place of m.
Now, $c^n - b^n = [\{2^{(nt+1)}\}*m+1]^n - [\{2^{(nt)}\}*m+1]^n$
Expanding in binomial expansion,
$= [\{2^{(tn+1)}\}*m]^n + nC_1 [\{2^{(nt+1)}\}*m]^{(n-1)} + \ldots + n*\{2^{(nt+1)}\}*m + 1 - [\{2^{(nt)}\}*q]^n - nC_1 [\{2^{(nt)}\}*q]^{(n-1)} - \ldots - n*\{2^{(tn)}\}*q - 1$
Now, if we divide it (RHS) by $2^{(nt+1)}$ we get $-nq\{2^{(nt)}$
Now, $a^n = 2^{tn}[\{2^{(tn)}\}*p + 1]^n$
Expanding in binomial expansion,
$a^n = 2^{tn}[\{\{2^{(tn)}\}*p\}^n + nC_1 \{\{2^{(tn)}\}*p\}^{(n-1)} + \ldots + n*2^{(tn)}*p + 1$
Clearly LHS gives $2^{(nt)}$ as remainder when divided by $2^{(nt+1)}$
⇨ $2^{(nt)} - [-nq\{2^{(nt)}\}] \equiv 0 \pmod{2^{(nt+1)}}$
⇨ $\{2^{(nt)}\}(1+nq) \equiv 0 \pmod{2^{(nt+1)}}$

As n is odd this equation is true for any value of q where q is odd (previously defined)
⇨ It is not an equation rather an identity of q independent of the value of n, t, p, m.

But they are connected by an equation. => They are dependent on each other.
Here is the contradiction.
So, when n is odd Case 1 fails.
Now n is even.
Let's say n/2 is odd.
Then the equation can be written as $(a^2)^{(n/2)} + (b^2)^{(n/2)} = (c^2)^{(n/2)}$
Putting $a^2 = x$, $b^2 = y$, $c^2 = z$ and n/2 = m we get,
$X^n + y^m = z^m$
Which is similar to the previous equation. So it will fail.
Let's say $n/2^2$ is odd.
Again putting $a_1 = x$, $b_1 = y$, $c_1 = z$ and n/4 = m
We get the previous equation.
So, for n even it fails.

Similarly we can prove when,
a = (2^t){(2^nt)*p + 3}
b ={2^(nt)}*q +3
c = {2^(nt)}*m+3
and also other cases.

Case 2 : a, b odd. c even

Dividing both sides by 8, we get, RHS ≡ 0 (mod8) as n is minimum 3.
LHS ≡ a + b (as any odd square number ≡ 1 (mod 8))
⇨ a+b ≡ 0 (mod 8)

Let's take the below combination :
a = {2^(nt)}*m+1
b ={2^(nt)}*q -1
c = (2^t){(2^nt)*p + 1}
Now, a^n + b^n = [{2^(nt)}*m+1]^n + [{2^(nt)}*q -1]^n
Expanding in binomial expansion we get,
[{2^(nt)}*m]^n + nC_1[{2^(nt)}*m]^(n-1) + ... + n*{2^(nt)*m} + 1 – [{2^(nt)}*q]^n + nC_1[{2^(nt)}*q]^(n-1) -.......+n*{2^(nt)}*q – 1
= {2^(t)}[2k + n(m+q)] where 2k is all term together except nm and nq.
Now, either of m or q must be odd and another must be even.
Let's put 2m in place of m
Now, a^n + b^n = [{2^(nt+1)}*m + 1]^n + [{2^(nt)}*q -1]^n
= [{2^(nt+1)}*m]^n + nC_1[{2^(nt+1)}*m]^(n-1) + ...+ n*{2^(nt+1)}*q + 1 - [{2^(nt)}*q]^n + nC_1[{2^(nt)}*q]^(n-1) - ....+ n{2^(nt))*q – 1
Dividing this by 2^(nt+1) we get, n{2^(nt))*q
Now, c^n = {2^(nt)} {(2^nt)*p + 1}^n
= {2^(nt)}[{{2^(nt)}*p}^n + nC_1 {{2^(nt)}*p}^(n-1) + ... + n*{2^(nt)}*p + 1]
Clearly it fives 2^(nt) as remainder when divided by 2^(nt+1)
⇨ 2^(nt) – nq{2^(nt)} ≡ 0 (mod 2^(nt+1))
⇨ {2^(nt)}(1-nq) ≡ 0 (mod 2^(nt+1))

This is again the same case as in case 1.
As n is odd this equation is true for any value of q where q is odd (previously defined)
⇨ It is not an equation rather an identity of q independent of the value of n, t, p, m.

But they are connected by an equation. => They are dependent on each other.
Here is the contradiction.
So, when n is odd Case 2 fails.
Now, n is even.
We can write the equation as (a²)^(n/2) + (b²)^(n/2) = c^n
Now as n is minimum 3 so RHS congruent to 0 mod 8.
But a² ≡ 1 (mod 8) also b² ≡ 1 (mod 8)
⇨ (a²)^(n/2) ≡ 1 (mod 8) and (b²)^(n/2) ≡ 1 (mod 8)
⇨ a^n + b^n ≡ 2 (mod 8)

whereas RHS ≡ 0 (mod 8)
Here is the contradiction.
So case 2 fails for n even.

Conclusion

There is no such combination of n, a, b, c exists.

Result

Fermat's Last Theorem is true.

References

[1] Al Shenk, Cálculo e geometria analítica, translationby Anna Amália Feijó Barroso,Rio de Janeiro: Campus, 1983-1984.
[2] J. L. Boldrini, S. I. R. Costa, V. L. Figueiredo, H. G. Wetzler, Álgebra linear, 3 ed., São Paulo: Harper &Row do Brasil, 1980.
[3] M. L. Crispino, Variedades lineares e hiperplanos, Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.
[4] K. Michio, Hiperespaço, translationby Maria Luiza X. de A. Borges, technicalreviewby Walter Maciel, Rio de Janeiro: Rocco, 2000.
[5] Euclides, Os elementos, translationandintroductionby Irineu Bicudo, São Paulo: Unesp, 2009.

Shubhankar Paul, Passed BE in Electrical Engineering from Jadavpur University in 2007. Worked at IBM as Manual Tester with designation Application Consultant for 3 years 4 months. Worked at IIT Bombay for 3 months as JRF. Published 2 papers at International Journal.