DISCOVERY ON BEAL'S CONJECTURE

Idriss Olivier BADO[1]

[1]STATISTIC AND ECONOMY, ENSEA, Abidjan, IVORY COAST

Abstract

.

In this paper we give a proof for Beal's conjecture . Since the discovery of the proof of Fermat's last theorem by Andre Wiles, several questions arise on the correctness of Beal's conjecture. By using a very rigorous method we come to the proof. Let $\mathbf{G} = \{(x, y, z) \in \mathbf{N}^3 : \min(x, y, z) \geq 3\}$ $\Omega_n = \{p \in \mathbf{P} : p \mid n, p \nmid z^y - y^z\}$,

$$\mathbf{T} = \{(x, y, z) \in \mathbf{N}^3 : x \geq 3, y \geq 3, z \geq 3\}$$

$\forall (x, y, z) \in \mathbf{T}$ consider the function $f_{x,y,z}$ be the function defined as :

$$\begin{array}{llll} f_{x,y,z} & : \mathbf{N}^3 & \to & \mathbf{Z} \\ & (X, Y, Z) & \mapsto & X^x + Y^y - Z^z \end{array}$$

Denote by

$$\mathbf{E}^{x,y,z} = \{(X, Y, Z) \in \mathbf{N}^3 : f_{x,y,z}(X, Y, Z) = 0\}$$

and $\mathbf{U} = \{(X, Y, Z) \in \mathbf{N}^3 : \gcd(X, Y) \geq 2, \gcd(X, Z) \geq 2, \gcd(Y, Z) \geq 2\}$ Let $x = \min(x, y, z)$. The obtained result show that :if $A^x + B^y = C^z$ has a solution and $\Omega_A \neq \emptyset$, $\forall p \in \Omega_A$,

$$Q(B, C) = \sum_{j=1}^{x-1} [\binom{y}{j} B^j - \binom{z}{j} C^j]$$

has no solution in $(\frac{\mathbf{Z}}{p^x \mathbf{Z}})^2 \setminus \{(\overline{0}, \overline{0})\}$ Using this result we show that Beal's conjecture is true since

$$\bigcup_{(x,y,z) \in \mathbf{T}} \mathbf{E}^{x,y,z} \cap \mathbf{U} \neq \emptyset$$

.

Then $\exists (\alpha, \beta, \gamma) \in \mathbf{N}^3$ such that $\min(\alpha, \beta, \gamma) \leq 2$ and $\mathbf{E}^{\alpha,\beta,\gamma} \cap \mathbf{U} = \emptyset$ The novel techniques use for the proof can be use to solve the variety of Diophantine equations . We provide also the solution to Beal's equation . Our proof can provide an algorithm to generate solution to Beal's equation

2010 AMS Classiftcation:11A05, 11A41, 11D09, 11D41, 11D61, 11N32

Keywords and phrases:Lemma; Theorem; Beal; Fermat ; Conjecture

1 Introduction

Mathematicians have long been intrigued by Pierre Fermat's famous assertion that $A^n+B^n = C^n$ is impossible and the remark written in the margin of his book that he had a demonstration . This became known as Fermat's Last Theorem despite the lack of a proof. Andrew Wiles proved the relationship in 1994, though everyone agrees that Fermat's proof could not possibly have been the proof discovered by Wiles. Number theorists remain divided when speculating over whether or not Fermat actually had a proof, or whether he was mistaken. This mystery remains unanswered though the prevailing wisdom is that Fermat was mistaken. This conclusion is based on the fact that thousands of mathematicians have cumulatively spent many millions of hours over the past 350 years searching unsuccessfully for such a proof. It is easy to see that $A^n + B^n = C^n$ then either A B, and C are co-prime or, if not co-prime that any common factor could be divided out of each term until the equation existed with co-prime bases. We could then restate Fermat Last Theorem by saying that $A^n + B^n = C^n$ is impossible with co-prime bases. Beyond Fermat's Last Theorem $A^n + B^n = C^n$ No one suspected that might also be impossible with co-prime bases until a remarkable discovery in 1993 by a Dallas, Texas number theory enthusiast by the name of D. Andrew "Andy" Beal . Andy Beal was working on Fermat Last Theorem when he began to look at similar equations with independent exponents. He constructed several algorithms to generate solution sets but the very nature of the algorithms he was able to construct required a common factor in the bases. He began to suspect that coprime bases might be impossible and set out to test his hypothesis by computer. Andy Beal and a colleague programmed 15 computers and after thousands of cumulative hours of operation had checked all variable values through 99. Many solutions were found: all had a common factor in the bases. While certainly not conclusive, Andy Beal now had sufficient reason to share his discovery with the world. In the fall of 1994, Andy Beal wrote letters about his work to approximately 50 scholarly mathematics periodicals and number theorists. Among the replies were two considered responses from respected number theorists. Many invegestions have been made without success . The announcement of year 1993 the Fermat's Last Theorem was an exciting event for the entire mathematics community. This Introduction was to discuss the mathematical history of Fermat's Last Theorem , broken up into the following periods 1. Diophantus to Euler 2. Euler to Frey 3. Frey to Wiles . I hope that the Introduction succeeds in conveying the flavor of this truly wonderful mathematics. Hence the basic claim of FLT is that the equation $x^n + y^n = z^n$ has no solutions when x,y,z are non-zero integers and $n \geq 3$ In 1983, faltings proved the Mordell's conjecture which implies that a polynomial equation with rational coefficients $Q(X, Y) = 0$ has only finitely many rational solutions when the curve has genus over 2.Serre and Rabbet shows that the conjecture of The Taniyama – Shimura which states that all elliptic curves over rational numbers are modular implies Fermat Last theorem .It is in this way all researchs have been focus in proving that conjecture . Richard K. Guy in [1] settled all the original works in Beal's conjecture. In our paper based on the existing Litterature Thomas Barnet-Lamb, Toby Gee, and David Geraghty in [2] , H. Riesel in [4],Elkies ND (2007) in [5], Mauldin RD (1997) [6], P.A. Clement in [7], P. Ribenboim in [8],H.L. Montgomery and R.C Vaughan in [9], Waldschmidt M (2004) in [10] a rigourous proof of Beal conjecture .

2 PRINCIPLE OF THE PROOF

Let

$$\mathbf{T} = \{(x, y, z) \in \mathbf{N}^3 : x \geq 3, y \geq 3, z \geq 3\}$$

$\forall (x, y, z) \in \mathbf{T}$ consider the function $f_{x,y,z}$ be the function defined as :

$$\begin{array}{llcl} f_{x,y,z} & : \mathbf{N}^3 & \to & \mathbf{Z} \\ & (X, Y, Z) & \mapsto & X^x + Y^y - Z^z \end{array}$$

Denote by

$$\mathbf{E}^{x,y,z} = \{(X, Y, Z) \in \mathbf{N}^3 : f_{x,y,z}(X, Y, Z) = 0\}$$

and $\mathbf{U} = \{(X, Y, Z) \in \mathbf{N}^3 : \gcd(X, Y) \geq 2, \gcd(X, Z) \geq 2, \gcd(Y, Z) \geq 2\}$

2.1 LEMMA1

If

$$\bigcup_{(x,y,z)\in \mathbf{T}} \mathbf{E}^{x,y,z} \cap \mathbf{U} \neq \emptyset$$

Then $\exists(\alpha,\beta,\gamma) \in \mathbf{N}^3$ such that $\min(\alpha,\beta,\gamma) \leq 2$ and $\mathbf{E}^{\alpha,\beta,\gamma} \cap \mathbf{U} = \emptyset$

2.2 LEMMA 1 PROOF

Suppose that

$$\bigcup_{(x,y,z)\in \mathbb{T}} \mathbb{E}^{x,y,z} \cap \mathbb{U} \neq \emptyset$$

and let $(A_1, A_2, A_3) \in \bigcup_{(x,y,z)\in\mathbb{T}} \mathbb{E}^{x,y,z} \cap \mathbb{U}$ then $\exists(x_1, x_2, x_3) \in \mathbb{T}$ such that

$$(A_1, A_2, A_3) \in \mathbb{E}^{(x_1,x_2,x_3)} \cap \mathbb{U}$$

So we can find (d_1, d_2, d_3) with $\gcd(d_i, d_j) = 1, \forall i \neq j \in \{1,2,3\}$ and $d_i \mid A_i, \forall i \in \{1,2,3\}$ such that $A_i = \prod_{j=1}^{3} d_j^{\theta_j^i}$ Where θ_j^i will be determined by the following relation

$$\prod_{j=1}^{3} d_j^{x_1\theta_j^1} + \prod_{j=1}^{3} d_j^{x_2\theta_j^2} = \prod_{j=1}^{3} d_j^{x_3\theta_j^3}$$

Pulling

$$\theta_1^1 = \frac{\alpha + x_2x_3\theta_1}{x_1}, \theta_2^1 = x_3\theta_2, \theta_3^1 = x_2\theta_3$$
$$\theta_2^2 = \frac{\beta + x_1x_3\theta_2}{x_2}, \theta_1^2 = x_3\theta_1, \theta_3^2 = x_1\theta_3$$
$$\theta_3^3 = \frac{\gamma + x_1x_2\theta_3}{x_3}, \theta_1^3 = x_2\theta_1, \theta_2^3 = x_1\theta_2$$

Let Find $\theta_1, \theta_2, \theta_3$ such that $x_1 \mid \alpha + x_2x_3\theta_1, x_2 \mid \beta + x_1x_3\theta_2, x_3 \mid \gamma + x_1x_2\theta_3$ Consider the following equation

$$x_2x_3\theta_1 \equiv x_1 - \alpha[x_1]$$
$$x_1x_3\theta_2 \equiv x_2 - \beta[x_2]$$
$$x_1x_2\theta_3 \equiv x_3 - \gamma[x_3]$$

Hence

$$(x_2x_3)^{\phi(x_1)}\theta_1 \equiv (x_1 - \alpha)(x_2x_3)^{\phi(x_1)-1}[x_1]$$
$$(x_1x_3)^{\phi(x_2)}\theta_2 \equiv (x_2 - \beta)(x_1x_3)^{\phi(x_2)-1}[x_2]$$
$$(x_1x_2)^{\phi(x_3)}\theta_3 \equiv (x_3 - \gamma)(x_1x_2)^{\phi(x_3)-1}[x_3]$$

Looking for $\alpha < x_1, \beta < x_2, \gamma < x_3$ by the Euler theorem we have :

$$\theta_1 \equiv (x_1 - \alpha)(x_2x_3)^{\phi(x_1)-1}[x_1]$$

$$\theta_2 \equiv (x_2 - \beta)(x_1x_3)^{\phi(x_2)-1}[x_2]$$

$$\theta_3 \equiv (x_3 - \gamma)(x_1x_2)^{\phi(x_3)-1}[x_3]$$

In obvious manner we can assert that $\min(\alpha, \beta, \gamma) \leq 2$ if not the process will continue until to obtain this bound By construction

$$\mathbf{E}^{\alpha,\beta,\gamma} = \{(d_1, d_2, d_3) : d_1^{\alpha} + d_2^{\beta} = d_3^{\gamma}\}$$

then

$$\mathbf{E}^{\alpha,\beta,\gamma} \cap \mathbf{U} = \emptyset$$

2.3 LEMMA 2

$\mathbf{G} = \{(x, y, z) \in \mathbf{N}^3 : \min(x, y, z) \geq 3\}$ $\Omega_n = \{p \in \mathbf{P} : p \mid n, p \nmid z^y - y^z\}$ Let $x = \min(x, y, z)$. if $A^x + B^y = C^z$ has a solution then if $\Omega_A \neq \emptyset$, $\forall p \in \Omega_A$

$$Q(B, C) = \sum_{j=1}^{x-1} [\binom{y}{j} B^j - \binom{z}{j} C^j]$$

has no solution in $(\frac{\mathbf{Z}}{p^x\mathbf{Z}})^2 \setminus \{(\overline{0}, \overline{0})\}$

2.4 PROOF

Suppose that $A^x + B^y = C^z$ has a solution Let $p \in \Omega_A$ Then

$$Q(B, C) = Q(B, \sqrt[z]{A^x + B^y})$$

By the hypothesis we have

$$Q(\overline{B}, \sqrt[z]{\overline{B^y}}) \equiv 0[p^x]$$

Pulling $\overline{B} = \overline{\theta^z}$

$$\sum_{j=1}^{x-1} [\binom{y}{j} \overline{\theta^{zj}} - \binom{z}{j} \overline{\theta^{yj}}] \equiv 0[p^x]$$

Let

$$\Gamma = \{j \in \{1, 2, ..x - 1\} : \binom{y}{j} \overline{\theta^{zj}} - \binom{z}{j} \overline{\theta^{yj}} \equiv 0[p^x]\}$$

In the following we are going to prove that $\Gamma^c = \emptyset$ Assume that $\Gamma^c \neq \emptyset$ Then

$$\sum_{j \in \Gamma^c} [\binom{y}{j} \overline{\theta^{zj}} - \binom{z}{j} \overline{\theta^{yj}}] \equiv 0[p^x]$$

Let Assume $\theta^z = p^x q + r, \theta^y = p^x q' + r'$ and

$$f_n(r, r') = \sum_{j \in \Gamma^c} [\binom{y}{j} r^j - \binom{z}{j} r'^j] - p^x n$$

Assume the existence of the integer root r'_0 and the existence of the integer n_0 such that $\sum_{j\in\Gamma^c}\binom{y}{j}r^j = a_{n_0}$ Where $a_n = np^x + \sum_{j\in\Gamma^c}\binom{z}{j}r_0'^j$ Hence $r^{\min(\Gamma^c)} \mid a_{n_0}$ .Also we have $a_{n_0} \mid \sum_{j\in\Gamma^c}\binom{y}{j}r^{j-\min(\Gamma^c)}$ or $a_{n_0} \mid r^{\min(\Gamma^c)}$ .Suppose that $a_{n_0} \mid \sum_{j\in\Gamma^c}\binom{y}{j}r^{j-\min(\Gamma^c)}$ then

$$r^{\min(\Gamma^c)} \leq a_{n_0} \leq \sum_{j\in\Gamma^c}\binom{y}{j}r^{j-\min(\Gamma^c)}$$

So

$$\frac{r^{\min(\Gamma^c)}}{p^x} \leq n + \frac{\sum_{j\in\Gamma^c}\binom{z}{j}r_0'^j}{p^x} \leq \frac{\sum_{j\in\Gamma^c}\binom{y}{j}r^{j-\min(\Gamma^c)}}{p^x}$$

which is equivalent to

$$\frac{r^{\min(\Gamma^c)}}{p^x} \leq \frac{\sum_{j\in\Gamma^c}\binom{y}{j}r^j}{p^x} \leq \frac{\sum_{j\in\Gamma^c}\binom{y}{j}r^{j-\min(\Gamma^c)}}{p^x}$$

. Suppose that $a_{n_0} \mid r^{\min(\Gamma^c)}$ Hence $a_{n_0} = r^{\min(\Gamma^c)}$ As

$$\sum_{j\in\Gamma^c}\binom{y}{j}r^j = a_{n_0} \geq 1 + r^{\min(\Gamma^c)}$$

.So $\Gamma^c = \emptyset$ We have now:

$$\forall j \in \{1,2,...,x-1\}, \binom{y}{j}r^j - \binom{z}{j}r'^j \equiv 0[p^x]$$

Pulling $R(X) = \binom{y}{j}X^j - \binom{z}{j}$ Since the existence of r'' such that $r''r' \equiv 1[p^x]$ we have $\forall j, R(rr'') \equiv 0[p^x]$ for $j=1$ we have $rr'' = zy'$ and

$$\forall j, \binom{y}{j}z^j - \binom{z}{j}y^j \equiv 0[p^x]$$

Then $r = z_0, r' = y_0$ where $z \equiv z_0[p^x]$ and $y \equiv y_0[p^x]$ So $\overline{B} = z_0$ and $\overline{C} = y_0$ then $z_0^y \equiv y_0^z[p^x]$ .Using this result we have $z^y - y^z \equiv [p^x]$ which is in contradictory with our hypothesis . The Lemma is thus proved

2.5 LEMMA 3

Let $\mathbf{G} = \{(x,y,z) \in \mathbf{N}^3 : x = \min(x,y,z) \geq 3, y \neq z\}$ if $\mathbf{E}^{x,y,z} \cap \mathbf{U} = \emptyset$ then $\mathbf{E}^{x,y,z} = \emptyset$

LEMMA 3 PROOF

Suppose that $x = \min(x,y,z)$ Then $\Omega_A \neq \emptyset$. Indeed if $\exists p$ such that $y^z - z^y \equiv 0[p]$ then $y^z \equiv z^y[p]$ $z\log_z(y) \equiv y[p]$ and $y\log_y(z) \equiv z[p]$ As $z \neq y$ then $\log_y(z) \in \mathbf{N}, \log_z(y) \in \mathbf{N}$ if $\exists a,b$ such that $z = y^a, y = z^b$ then $z = z^{ab}$ so $y = z$ which is in contradictory with our hypothesis . Hence $\Omega_A \neq \emptyset$ Consider now $p \in \Omega_A$ and suppose that $\mathbf{E}^{x,y,z} \neq \emptyset$ and $\mathbf{E}^{x,y,z} \cap \mathbf{U} = \emptyset$ then Pulling $d_1 = \gcd(A,B), d_2 = \gcd(A,C), d_3 = \gcd(B,C)$ if $\forall i \in \{1,2,3\}, d_i \geq 2$ the result will be in contradictory with our hypothesis ,so $\exists i \in \{1,2,3\}$ such that $d_i = 1$ Without loss of generality we can suppose that $d_1 = 1$ .Using the relation $A^x = C^z - B^y$ then $d_3 \mid A^x$ so $d_3 = 1$. Using the same idea we have $d_2 = 1$ $C^z - B^y \equiv 0[p]$ As $d_1 = 1$ Now with the fact that $p \not| C, p \not| B$
We can write : $C = pk + r$ where $1 \leq r \leq p-1$ and $B = pk' + r'$,$1 \leq r' \leq p-1$, $r^z - r'^y \equiv 0[p]$ Hence $\overline{r^z} = \overline{r^y}$ in $\frac{\mathbf{Z}}{p\mathbf{Z}}$ let $\overline{r^y} = p - j$ for a certain $j \in [1, p-1]$ Pulling $P(r) = r^y - p + j$ the zero of the polynomial function over the ring $\frac{\mathbf{Z}}{p\mathbf{Z}}$ is $r_k = \sqrt[y]{p-j}\zeta^{\frac{k}{y}}$, $\forall 0 \leq k \leq y-1$ where $\zeta = e^{2i\pi}$ .Using the that r_k is integer then $j = p-1$ and $k = 0$ Beal equation becomes :

$$p^x K^x + \sum_{j=1}^{y} \binom{y}{j} p^j K'^j = \sum_{j=1}^{z} \binom{z}{j} p^j K''^j$$

$$\sum_{j=1}^{x-1} \binom{y}{j} p^j K'^j \equiv \sum_{j=1}^{x-1} \binom{z}{j} p^j K''^j [p^x]$$

Let

$$Q(X,Y) = \sum_{j=1}^{x-1} [\binom{y}{j} X^j - \binom{z}{j} Y^j] p^j$$

By the Lemma 2 $Q(A,B) = Q(K',K'') = 0$ has no solution in $(\frac{\mathbf{Z}}{p^x\mathbf{Z}})^2 \setminus \{(\overline{0},\overline{0})\}$ .The Lemma is thus proved

3 THEOREM

Let x,y,z a given integers . Let $(A,B,C) \in \mathbf{N}^3 \setminus \{(0,0,0)\}$ such that the Beal's equation

$$A^x + B^y = C^z$$

is satisfied then $\gcd(A,B,C) \geq 2$

3.1 PROOF OF THE THEOREM

Let x,y,z a given integers . Let $(A,B,C) \in \mathbf{N}^3 \setminus \{(0,0,0)\}$ such that the Beal's equation

$$A^x + B^y = C^z$$

is satisfied . If $x = y = z$ by Last theorem of Fermat the result yields . Suppose that $y \neq z$ by the Lemma 3 we have :

$$\gcd(A,B) \geq 2, \gcd(B,C) \geq 2, \gcd(A,C) \geq 2$$

then $\gcd(A,B,C) \geq 2$

3.2 DISCUSSION

Before our result , it appears that there has not been found a general proof of Beal's conjecture. Only the particular case was proved and this was proved by Crandall and Pomerance [11]. There are a number of such cases [12]-[13] where partial proofs was given . As-well, there are cases where computer searchers are made . If Beal's is true as we have shown here, then, all computer searches will never find a counter-example and the best way to resolved this would be via general proof as we have done In our paper . Our thrust has been on a direct proof and just as the proof presented here , the proof provided is simple with all the clarity , general and all-encompassing. It covers all possible cases.

4 CONCLUSION

In our article gives us a proof of the conjecture of Beal. Our proof is of a very understandable clarity. Although she uses both analytical methods but it is purely arithmetical proof.

Acknowledgement

We are grateful to Mr Jean Toupouvogui and Professor Tanoe for their appreciation.

References

[1] Richard K. Guy, Unsolved problems in number theory, Third Edition, Springer- Verlag, Berlin (2004).

[2] Thomas Barnet-Lamb, Toby Gee, and David Geraghty. Congruences between Hilbert modular forms: constructing ordinary lifts. Duke Math. J., 161(8):1521– 1580, 2012.

[3] Thomas Barnet-Lamb, Toby Gee, and David Geraghty. Congruences between Hilbert modular forms: constructing ordinary lifts, II. Math. Res. Lett., 20(1): 67–72, 2013. .

[4] H. Riesel, Prime numbers and computer methods for factorization, Progress in Mathematics Vol, 126, Birkh¨auser Boston, Boston, MA, 1994.

[5] Elkies ND (2007). The ABC's of Number theory. The Havard College mathematics Review 1(1)

[6] Mauldin RD (1997). A Generalization of Fermat's last theorem: Beal's conjecture and the Prize Problem. Notices of The AMS 44(11):1436-1437

[7] P.A. Clement, Congruences for sets of primes, AMM 56 (1949), 23–25

[8] P. Ribenboim, The new book of prime number records, Springer, 1996

[9] H.L. Montgomery and R.C. Vaughan, On the distribution of reduced residues, Annals of Math., 2nd series 123 (1986), no. 2, 311–333.

[10] Waldschmidt M (2004). Open Diophantine problems. Moscow mathematics 4:245- 305.

[11] Crandall, R. and Pomerance, C. (2000) Prime Numbers: A Computational Per- spective. Spinger Science Business Media, Berlin, 147.

[12] Siksek, S. and Stoll, M. (2014) The Generalised Fermat Equation $x^2 + y^3 = z^7$.Archiv der Mathematik, 102, 411-421.

[13] Darmon, H. and Granville, A. (1995) On the Equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. Bulletin of the London Mathematical Society, 27, 513-543