Note for the Beal's Conjecture

Frank Vega

May 15, 2024

Article

Note for the Beal's Conjecture

Frank Vega [1]

[1] GROUPS PLUS TOURS INC., 9611 Fontainebleau Blvd, Miami, FL, 33172, USA; vega.frank@gmail.com

Abstract: This work explores two famous conjectures in number theory: Fermat's Last Theorem and Beal's Conjecture. Fermat's Last Theorem, posed by Pierre de Fermat in the 17th century, states that there are no positive integer solutions for the equation $a^n + b^n = c^n$, where n is greater than 2. This theorem remained unproven for centuries until Andrew Wiles published a proof in 1994. Beal's Conjecture, formulated in 1997 by Andrew Beal, generalizes Fermat's Last Theorem. It states that for positive integers A, B, C, x, y, and z, if $A^x + B^y = C^z$ (where x, y, and z are all greater than 2), then A, B, and C must share a common prime factor. Beal's Conjecture remains unproven, and a significant prize is offered for a solution. This paper provides a concise introduction to both conjectures, highlighting their connection and presenting a short proof of the Beal's Conjecture.

Keywords: Generalized Fermat Equation; prime numbers; binomial theorem; coprime numbers

MSC: 11D41

---

1. Introduction

Around 1637, Pierre de Fermat, a French mathematician, scribbled a now-famous remark in the margin of a book he was reading. He claimed to have discovered a proof for the equation $a^n + b^n = c^n$ having no solutions in positive integers for n greater than 2 [1]. However, he didn't provide the details of his proof [1]. Mathematicians like Leonhard Euler and Sophie Germain made significant contributions years later [2] [3]. In the 20th century, mathematicians like Ernst Kummer proved the theorem for a specific class of numbers [4]. However, a complete solution remained out of reach. Finally, in 1994, Andrew Wiles, a British mathematician, announced a proof for Fermat's Last Theorem. The proof was incredibly complex, drawing on advanced areas of mathematics like elliptic curves. After some initial errors were addressed, Wiles' work was accepted as the long-awaited solution to the theorem [5].

In 1993, Andrew Beal, an amateur mathematician and banker, formulates the Beal's Conjecture while investigating generalizations of Fermat's Last Theorem. The conjecture is stated publicly for the first time where Beal offers a prize of $5,000 for a proven solution or disproof of the conjecture [6]. This prize was later increased several times, reaching its current value of $1 million held by the American Mathematical Society (AMS). The Beal's Conjecture says that if $A^x + B^y = C^z$, where A, B, C, x, y, and z are all positive integers, and x, y, and z are greater than 2, then A, B, and C must share a common prime factor [6]. In other words, there are no solutions where A, B, and C are completely coprime numbers [6]. This conjecture has occasionally been referred to as a generalized Fermat equation. Indeed, Fermat's Last Theorem can be seen as a special case of the Beal's Conjecture restricted to $x = y = z$. New important advances for this problem have emerge in the last years [7], [8], [9].

The proof of Fermat's Last Theorem was described as a "stunning advance" in the citation for Wiles's Abel Prize award in 2016. It also proved much of the Taniyama-Shimura conjecture, subsequently known as the modularity theorem, and opened up entire new approaches to numerous other problems and mathematically powerful modularity lifting techniques [10]. However, the Beal's Conjecture remains unsolved. In this note, using only simple arguments, we show that the Beal's Conjecture is true. Wiles' proof is very far for being close to Fermat's claimed theorem due to its long extension, complexity and tools that were only available during the 20th century. A trustworthy and short proof for Beal's

Conjecture could considerably impact pure mathematics and spur new advances in number theory. Besides, this work unveils the long known mystery about the possible existence of Fermat's claimed theorem. Certainly, this work could be closer to Fermat's claimed proof.

2. Materials and methods

According to the binomial theorem, the expansion of any nonnegative integer power n of the binomial $x + y$ is a sum of the form

$$(x+y)^n = \binom{n}{0} \cdot x^n \cdot y^0 + \binom{n}{1} \cdot x^{n-1} \cdot y^1 + \ldots + \binom{n}{n} \cdot x^0 \cdot y^n,$$

where each $\binom{n}{k}$ is a positive integer known as a binomial coefficient, defined as

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} = \frac{n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot (k-2) \cdot \ldots \cdot 2 \cdot 1}.$$

This formula is also referred to as the binomial formula or the binomial identity [11]. The expression $d \mid n$ means the integer d divides n. We denote by $gcd(\ldots)$, the greatest common divisor.

Proposition 1. *A natural number p is prime if and only if $p \mid \binom{p}{k}$ for all integers $0 < k < p$ [12].*

Proposition 2. *Let a, b and c be natural numbers greater than 1. If a and b are coprime numbers and $a = b \cdot c$, then we necessarily obtain that $a \mid c$ [13].*

Putting all together yields the proof of the Beal's Conjecture.

3. Results

This is a main insight.

Lemma 1. *The integer solutions (x, y) for the equation*

$$a \cdot x + b \cdot y = c \cdot x + d \cdot y$$

are in the form of

$$(x, y) = \left(k \cdot \frac{(d-b)}{gcd(d-b, a-c)}, k \cdot \frac{(a-c)}{gcd(d-b, a-c)}\right)$$

under the assumption that $(d-b)$ and $(a-c)$ are nonzero values and a, b, c and d are integers which are not equal to 0.

Proof. If the equation

$$a \cdot x + b \cdot y = c \cdot x + d \cdot y$$

holds, then $(x, y) = (k \cdot X, k \cdot Y)$ is also a solution for any choice of real k where $(x, y) = (X, Y)$ is some particular solution. We know that $X = d - b, Y = a - c$ is a particular solution. So, the real solutions are $(x, y) = (k \cdot (d-b), k \cdot (a-c))$ for any choice of real k. Since we are studying solely the integer solutions, then $x = k \cdot (d-b)$, $y = k \cdot (a-c)$ that is $\frac{x}{y} = \frac{(d-b)}{(a-c)}$ which means that the rational $\frac{x}{y}$ in its lowest form is

$$\frac{\left(\frac{(d-b)}{g}\right)}{\left(\frac{(a-c)}{g}\right)}$$

where $g = gcd(d-b, a-c)$. That also means that $x = k \cdot \frac{(d-b)}{g}$, $y = k \cdot \frac{(a-c)}{g}$ for any choice of integer k. Therefore, the integer solutions are in the form of

$$(x, y) = \left(k \cdot \frac{(d-b)}{gcd(d-b, a-c)}, k \cdot \frac{(a-c)}{gcd(d-b, a-c)}\right)$$

for any integer k. □

The following is a key Lemma.

Lemma 2. *Let a, b and c be three distinct natural numbers greater than 1 and p, q and r be three different prime numbers. If we have $p \mid (a+b)$, $q^2 \mid (c-b)$, $r^2 \mid (c-a)$, $p \mid c$, $q^2 \mid a$ and $r^2 \mid b$, then this implies that $c = (a+b)$ or $gcd(a, b, c) > 1$.*

Proof. We can rewrite the same statement as

$$\begin{aligned} a + b &= p \cdot u, \\ c - b &= q \cdot v, \\ c - a &= r \cdot w, \\ c &= p \cdot U, \\ a &= q \cdot V, \\ b &= r \cdot W, \end{aligned}$$

such that u, v, w, U, V and W are natural numbers. Now, we would have

1. First, substituting a and c in

$$\begin{aligned} q \cdot V + b &= p \cdot u \\ p \cdot U - b &= q \cdot v, \end{aligned}$$

   gives
$$p \cdot U + q \cdot V = p \cdot u + q \cdot v.$$

2. Again, substituting b and c in

$$\begin{aligned} a + r \cdot W &= p \cdot u \\ p \cdot U - a &= r \cdot w, \end{aligned}$$

   gives
$$p \cdot U + r \cdot W = p \cdot u + r \cdot w.$$

There are two cases to consider: case (i): $u = U$, $v = V$ and $w = W$ and $c = (a+b)$; case (ii): $(v - V)$, $(w - W)$ and $(u - U)$ are nonzero values and $gcd(a, b, c) > 1$. The case (i) is supported by the fact that if any of these values $(v - V)$, $(w - W)$ or $(u - U)$ is equal to zero, then that necessarily forces $u = U$, $v = V$ and $w = W$. Indeed, if $u = U$, then $v = V$ and $w = W$. For example, this is derived from the equation

$$p \cdot U + r \cdot W = p \cdot u + r \cdot w$$

and so $u = U$ implies $r \cdot W = r \cdot w$, hence $W = w$. The same happens if $v = V$ or $w = W$. Let's assume that $u = U$, $v = V$ and $w = W$ and $c \neq (a+b)$. That would mean that

$$a = q \cdot V = q \cdot v = c - b.$$

which implies that $c = (a+b)$ and so, we show the case (i) is true using a proof by contradiction. Suppose that $(v-V)$, $(w-W)$ and $(u-U)$ are nonzero values and $gcd(a,b,c) = 1$ (i.e. we assume that the case (ii) is false). By Lemma 1, we know that necessarily

$$p = k \cdot \frac{(v-V)}{gcd(v-V, U-u)} = k' \cdot \frac{(w-W)}{gcd(w-W, U-u)}$$

for some integers k and k' whenever $(v-V)$, $(w-W)$ and $(u-U)$ are nonzero values and $gcd(a,b,c) = 1$. Suppose that $\mid k \mid = \mid k' \mid = 1$ or $\mid k \mid = \mid k' \mid = p$ since p is prime and therefore,

$$\frac{(v-V)}{gcd(v-V, U-u)} = \frac{(w-W)}{gcd(w-W, U-u)}$$

which is

$$gcd(w-W, U-u) \cdot (v-V) = gcd(v-V, U-u) \cdot (w-W)$$

where $\mid \ldots \mid$ is the absolute value function. Since we know that

$$p \cdot U - p \cdot u = q \cdot v - q \cdot V$$
$$p \cdot U - p \cdot u = r \cdot w - r \cdot W,$$

then

$$q \cdot (v-V) = r \cdot (w-W).$$

Putting both equations together become into $q = gcd(w-W, U-u)$ and $r = gcd(v-V, U-u)$. That would be the same as $q = gcd(w-W, v-V, U-u)$ and $r = gcd(w-W, v-V, U-u)$ since $q \mid (v-V)$ and $r \mid (w-W)$ due to $q^2 \mid (c-b)$, $r^2 \mid (c-a)$, $q^2 \mid a$ and $r^2 \mid b$. Certainly, we deduce that $q \mid v$, $q \mid V$, $r \mid w$ and $r \mid W$ whenever $q^2 \mid (c-b)$, $r^2 \mid (c-a)$, $q^2 \mid a$ and $r^2 \mid b$. Since this implies that $q = r$ which means that $gcd(a,b,c) > 1$, we reach a contradiction. Consequently, by reductio ad absurdum, we conclude that the Lemma 2 is true. □

This is the main theorem.

Theorem 1. *The Beal's Conjecture is true.*

Proof. Suppose that the Beal's Conjecture is false. Hence, there would exist an equation $A^x + B^y = C^z$, where A, B, C, x, y, and z are all positive integers, and x, y, and z are greater than 2, and A, B, and C are coprime numbers. We can confirm that $A, B, C > 1$ according to the Catalan solution [14]. Let's take three different prime numbers p, q and r such that $p \mid C^z$, $q^2 \mid A^x$ and $r^2 \mid B^y$ (we assume that p is odd otherwise we could take q or r in the next step and obtain the same result). Putting together the binomial theorem and Proposition 1, we can rewrite the equation $A^x + B^y = C^z$ as

$$a + b + p \cdot a \cdot b \cdot k = c$$
$$a = c - b + p \cdot c \cdot b \cdot n$$
$$b = c - a + p \cdot c \cdot a \cdot m$$

such that $a = A^{x \cdot p}$, $b = B^{y \cdot p}$ and $c = C^{z \cdot p}$ where k, m and n are natural numbers (in case of taken into account q or r as a possible odd prime candidate instead of p, then we should readjust into an equivalent statement as either ($a' = -C^{z \cdot q}$, $b' = B^{y \cdot q}$ and $c' = -A^{x \cdot q}$) or ($a'' = A^{x \cdot r}$, $b'' = -C^{z \cdot r}$ and $c'' = -B^{y \cdot r}$), respectively). After that, we substitute the previous values of a, b, c, p, q and r inside of Lemma 2. Certainly, we deduce that $p \mid (a+b)$, $q^2 \mid (c-b)$, $r^2 \mid (c-a)$, $p \mid c$, $q^2 \mid a$ and $r^2 \mid b$, because of $q^2 \mid n$, $r^2 \mid m$ and $p \mid (p \cdot a \cdot b \cdot k)$ whenever

$$a + b - c = p \cdot c \cdot b \cdot n = p \cdot c \cdot a \cdot m$$

such that $a \mid n$ and $b \mid m$ by Proposition 2. By the Fermat's Last Theorem, we know that $c \neq (a+b)$ using p as an integer exponent greater than 2 due to p is an odd prime [5]. In general, we can show that there is a contradiction under the assumption that $c \neq (a+b)$ and $gcd(a,b,c) = 1$ according to the Lemma 2. Since this implies that the natural numbers A, B, and C cannot be coprimes, then we prove that the Beal's Conjecture is true. □

References

1. Fermat, P.d. *Oeuvres de Pierre de Fermat*; Vol. 1, Gauthier-Villars, 1891.
2. Euler, L. *Elements of Algebra*; Springer Science & Business Media, 2012.
3. Germain, S. *Oeuvres philosophiques de Sophie Germain*; Collection XIX, 2016.
4. Kummer, E.E. Zur Theorie der complexen Zahlen **1847**.
5. Wiles, A. Modular elliptic curves and Fermat's Last Theorem. *Annals of mathematics* **1995**, *141*, 443–551. https://doi.org/10.2307/2118559.
6. Beal, A. A Generalization of Fermat's Last Theorem: The Beal Conjecture and Prize Problem. *Notices of the AMS* **1997**, *44*.
7. Anni, S.; Siksek, S. Modular elliptic curves over real abelian fields and the generalized Fermat equation $x^{2l} + y^{2m} = z^p$. *Algebra & Number Theory* **2016**, *10*, 1147–1172. https://doi.org/10.2140/ant.2016.10.1147.
8. Rahimi, A.M. An Elementary Approach to the Diophantine Equation $ax^m + by^n = z^r$ Using Center of Mass. *Missouri Journal of Mathematical Sciences* **2017**, *29*, 115–124. https://doi.org/10.35834/mjms/1513306825.
9. Freitas, N.; Naskręcki, B.; Stoll, M. The generalized Fermat equation with exponents 2, 3, n. *Compositio Mathematica* **2020**, *156*, 77–113. https://doi.org/10.1112/S0010437X19007693.
10. Ribet, K.A. Galois representations and modular forms. *Bulletin of the American Mathematical Society* **1995**, *32*, 375–402. https://doi.org/10.1090/S0273-0979-1995-00616-6.
11. Abramowitz, M.; Stegun, I.A. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*; Vol. 55, US Government printing office, 1968.
12. Irwin, K. Toward the Unification of Physics and Number Theory. *Reports in Advances of Physical Sciences* **2019**, *3*, 1950003. https://doi.org/10.1142/S2424942419500038.
13. Hardy, G.H.; Wright, E.M. *An Introduction to the Theory of Numbers*; Oxford University Press, 1979.
14. Mihăilescu, P. Primary cyclotomic units and a proof of Catalans conjecture. *J. Reine Angew. Math* **2004**, *572*, 167–195. https://doi.org/10.1515/crll.2004.048.

Short Biography of Authors

Frank Vega is essentially a Back-End Programmer and Mathematical Hobbyist who graduated in Computer Science in 2007. In May 2022, The Ramanujan Journal accepted his mathematical article about the Riemann hypothesis. The article "Robin's criterion on divisibility" makes several significant contributions to the field of number theory. It provides a proof of the Robin inequality for a large class of integers, and it suggests new directions for research in the area of analytic number theory.