A Note on the Beal Conjecture

Frank Vega

July 3, 2024

A NOTE ON THE BEAL CONJECTURE

FRANK VEGA

Abstract. Around 1637, Pierre de Fermat famously scribbled, and claimed to have a proof for, his statement that equation $a^n + b^n = c^n$ has no positive integer solutions for exponents $n > 2$. The theorem stood unproven for centuries until Andrew Wiles' groundbreaking work in 1994, with a notable caveat: Wiles' proof, while successful, relied on modern tools far beyond Fermat's claimed approach in terms of complexity. Combining short and basic tools, we were able to prove the Beal conjecture, a well-known generalization of Fermat's Last Theorem. The present work potentially offers a solution which is closer in spirit to Fermat's original idea.

1. Introduction

Fermat's Last Theorem, first stated by its namesake Pierre de Fermat in the 17^{th} century, it claims that there are no positive integer solutions to the equation $a^n + b^n = c^n$, whenever $n \in \mathbb{N}$ is greater than 2. In a margin note left on his copy of Diophantus' *Arithmetica*, Fermat claimed that he had a proof which the margin was too small to contain. [1]. Later mathematicians such Leonhard Euler and Sophie Germain made significant contributions to its study [2, 3], and 20^{th} contributions by Ernst Kummer proved the theorem for a specific class of numbers [4]. However, a complete solution remained out of reach.

Finally, in 1994, British mathematician Andrew Wiles announced a proof for Fermat's Last Theorem. His was a complex and multifaceted work, drawing on advanced areas of mathematics such as elliptic curves which were beyond the purview prevalent in Fermat's heyday. After some initial errors were addressed, Wiles' work was hailed as the long-awaited proof of the Theorem [5] and 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 [6]. The techniques used by Wiles are ostensibly far from Fermat's claimed proof in terms of extension, complexity and novelty of tools used—many of which were only available during the 20^{th} century.

In 1993, Andrew Beal, an American amateur mathematician and banker, formulated a conjecture while exploring generalizations of Fermat's Last Theorem. Beal first publicly presented the conjecture, along with a $5000 prize for a proof or counterexample. This prize has since been raised several times and is currently held by the American Mathematical Society (AMS) at $1 million. The Beal conjecture

Date: July 3, 2024.

2020 *Mathematics Subject Classification.* Primary 11D41, 11A41; Secondary 11D04, 11B65.

Key words and phrases. Fermat's Equation, Prime Numbers, Linear Diophantine Equations, Binomial Theorem.

states that if the equation $A^x + B^y = C^z$ holds, where A, B, C, x, y, and z are all positive integers with x, y, and z greater than 2, then A, B, and C must share a common prime factor − in other words, there are no solutions to the aforementioned equation if A, B, and C are pairwise coprime [7]. The statement generalizes Fermat's, which arises as a special case whenever $x = y = z$.

Recent years have witnessed significant advancements in tackling the Beal conjecture, as evidenced by works such as [8, 9, 10]. For instance, Peter Norvig, a Google research director, performed a computational search for counterexamples and ruled out their existence for $x, y, z \leq 7$ and $A, B, C \leq 250000$, as well as for $x, y, z \leq 100$ and $A, B, C \leq 10000$ [11]. Our proposed proof of the Beal conjecture precludes any counterexamples from existing regardless of the range considered. Consequently, we present what we contend is a a correct and short proof for Fermat's Last Theorem. The degree of actual closeness it might have with Fermat's own can only be speculated upon, but in our view simplicity was of paramount importance and we have deliberately eschewed techniques and results that were not available in the 17^{th} century.

2. Background and ancillary results

Notation 2.1. As usual, $\binom{n}{k}$ stands for the binomial coefficient; $d \mid n$ stands for *integer d divides integer n* while $d \nmid n$ means the opposite; and we denote by $\gcd(a, b)$, the *greatest common divisor* of a, b, i.e. the positive generator of the ideal $(a, b) \subset \mathbb{Z}$ or equivalently the common divisor of a, b that is divided by all common divisors thereof.

The following results are immediate. Firstly we have the Binomial Theorem [12], which for every $n \in \mathbb{Z}_{\geq 0}$ describes the distributive expansion of the n^{th} power of the binomial $x + y$ in any commutative ring $(R, +, \cdot)$:

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

Proposition 2.2 ([13])**.** *$p \in \mathbb{N}$ is prime if and only if $p \mid \binom{p}{k}$ for all integers $0 < k < p$.*

$\mathbb{Z}$ is trivially an integral domain (e.g. [14, Ch. II §1]) hence:

Proposition 2.3 (Cancellation property on $\mathbb{Z}$)**.** *For any $a, b, c \in \mathbb{Z}$, $a \neq 0$ and $a \cdot b = a \cdot c$ imply $b = c$.*

Proposition 2.4 ([15])**.** *Let $a, b, c \in \mathbb{N}$ greater than 1. If a, b are coprime (i.e. $\gcd(a, b) = 1$) and $a = b \cdot c$, then $a \mid c$.*

Lemma 2.5. *The solutions (x, y) for the Diophantine equation*

$$a \cdot x + b \cdot y = c \cdot x + d \cdot y, \tag{2}$$

where the integer coefficients satisfy $d \neq b$, $a \neq c$ and $a \cdot b \cdot c \cdot d \neq 0$, are

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

Proof. It is well known and very easily proven [16, Theorem 2.1.1] that if (x_0, y_0) is a particular solution to Diophantine equation $Ax + Bx = C$, then the general solution of this equation is

$$x = x_0 + k \cdot \frac{B}{\gcd(A,B)}, \quad y = y_0 - k \cdot \frac{A}{\gcd(A,B)}, \qquad k \in \mathbb{Z}.$$

In the equation resulting from (2), we have $A = a - c$, $B = b - d$, $C = 0$ and particular solution $(x_0, y_0) = (0, 0)$, and the Lemma follows immediately. $\square$

3. Main Result

Lemma 3.1. *Let a, b, c be pairwise distinct integers such that*

$$\{\pm 1, 0\} \cap \{a, b, c, a-b, a-c, c-b, a+b\} = \varnothing$$

and p, q and r be three prime integers, not necessarily distinct. If

$$p^2 \nmid (c - (a+b)), \quad p \mid \gcd(a+b, c), \quad q^3 \mid \gcd(c-b, a), \quad r^3 \mid \gcd(c-a, b),$$

then $\max\{\gcd(a,b), \gcd(a,c), \gcd(b,c)\} > 1$.

Proof. Our hypotheses can be written as

$$a + b = p \cdot u, \tag{3}$$
$$c - b = q^2 \cdot v, \tag{4}$$
$$c - a = r^2 \cdot w, \tag{5}$$
$$c = p \cdot U, \tag{6}$$
$$a = q^2 \cdot V, \tag{7}$$
$$b = r^2 \cdot W, \tag{8}$$

with $u, v, w, U, V, W \in \mathbb{N}$. Two immediate conditions linking these numbers arise. Firstly, (7) combined with (3) (resp. (6) combined with (4)) yield

$$q^2 \cdot V + b = p \cdot u, \qquad p \cdot U - b = q^2 \cdot v,$$

which added together become

$$p \cdot U + q^2 \cdot V = p \cdot u + q^2 \cdot v \Rightarrow p \cdot (u - U) + q^2 \cdot (v - V) = 0. \tag{9}$$

Secondly, and similarly, (8) combined with (3) (resp. (6) combined with (5)) yield

$$a + r^2 \cdot W = p \cdot u, \qquad p \cdot U - a = r^2 \cdot w,$$

thus

$$p \cdot U + r^2 \cdot W = p \cdot u + r^2 \cdot w \Rightarrow p \cdot (u - U) + r^2 \cdot (w - W) = 0. \tag{10}$$

Subtracting (10) from (9) entails

$$q^2 \cdot |v - V| = r^2 \cdot |w - W| = p \cdot |u - U|, \tag{11}$$

which will come handy later on.

Let $G = \{\gcd(a,b), \gcd(a,c), \gcd(b,c)\}$. At this juncture, we claim:

(i) $0 \in \{u - U, v - V, w - W\}$ if and only if $\{u - U, v - V, w - W\} = \{0\}$;
(ii) $u = U$, $v = V$ and $w = W$ if and only if $c = a + b$ (which implies a contradiction under the assumption that $p^2 \nmid (c - (a+b))$);
(iii) $(u - U) \cdot (v - V) \cdot (w - W) \neq 0$ implies $\max G > 1$.

Let us prove these statements. (i) is the easiest to address: an identity between any of u, v, w and its upper-case counterpart yields trivial cancellations of terms in (9) and (10) and thus the remaining two required identities, on account of the fact that $\mathbb{Z}$ is an integral domain. The other implication is trivial.

Let us prove (ii). Necessity is obvious: $a+b=c$ and (3), (6) imply $p \cdot U = p \cdot u$ and the remaining identities $v = V, w = W$ follow from (i). Sufficiency holds because $v = V$ implies $a = q \cdot V = q \cdot v = c - b$, thus $c = a + b$.

Let us prove (iii). Assume that $u - U, v - V, w - W \neq 0$ and $\max G = 1$, and we will arrive to a contradiction. Lemma 2.5 and (9), (10) imply the existence of $k, k' \in \mathbb{Z}$ such that

$$p = k \cdot \frac{v - V}{\gcd(v - V, U - u)} = k' \cdot \frac{w - W}{\gcd(w - W, U - u)}, \tag{12}$$

$$q^2 = -k \cdot \frac{u - U}{\gcd(v - V, U - u)}, \tag{13}$$

$$r^2 = -k' \cdot \frac{u - U}{\gcd(w - W, U - u)}, \tag{14}$$

Primality and (12) imply $|k|, |k'| \in \{1, p\}$ which leads to four cases.

Case 1: $|k| = |k'| = p$. (13) and (14) imply p divides, hence equals, q, r, absurd.
Case 2: $|k| = 1$, $|k'| = p$. (14) implies $p \mid r$, thus $p = r$, contradiction.
Case 3: $|k| = p$, $|k'| = 1$. (13) implies $p \mid q$, thus $p = q$, contradiction again.
Case 4: $|k| = |k'| = 1$. Then (12), (13), (14) become

$$|v - V| \cdot \gcd(w - W, u - U) = |w - W| \cdot \gcd(v - V, u - U) \tag{15}$$

$$|u - U| = q^2 \cdot \gcd(v - V, u - U) = r^2 \cdot \gcd(w - W, u - U), \tag{16}$$

$$|v - V| = p \cdot \gcd(v - V, u - U), \tag{17}$$

$$|w - W| = p \cdot \gcd(w - W, u - U), \tag{18}$$

Domain cancellation Proposition 2.3 and our hypothesis $u - U, v - V, w - W \neq 0$ imply that (15) and (11) result in

$$q^2 \mid \gcd(w - W, U - u), \quad r^2 \mid \gcd(v - V, U - u).$$

Since $q^3 \mid \gcd(c - b, a)$ and $r^3 \mid \gcd(c - a, b)$, we can infer that $q^2 \mid v - V$ and $r^2 \mid w - W$. Certainly, we can further deduce that if q^2 divides both v and V, and r^2 divides both w and W, then these conditions ($q^3 \mid \gcd(c - b, a)$ and $r^3 \mid \gcd(c - a, b)$) necessarily imply that $q^2 \mid v - V$ and $r^2 \mid w - W$. So, we could show that

$$(q \cdot r)^2 \mid \gcd(w - W, v - V, U - u) \tag{19}$$

under the assumption that $q \neq r$ ($q = r$ implies a contradiction). Then,

$$\frac{|v - V|}{p \cdot r^2} = \frac{|w - W|}{p \cdot q^2} = \frac{|u - U|}{(q \cdot r)^2}. \tag{20}$$

after dividing both sides of (11) by $p \cdot (q \cdot r)^2$. According to (19), $\frac{|u-U|}{(q \cdot r)^2}$ would be a positive integer. This implies $p \mid v - V$ and $p \mid w - W$ by (20). We only need to show that

$$(p \cdot q^2 \cdot r^2) \mid \gcd(w - W, v - V, U - u). \tag{21}$$

That is equivalent to

$$\frac{|v-V|}{p^2\cdot r^2}=\frac{|w-W|}{p^2\cdot q^2}=\frac{|u-U|}{p\cdot q^2\cdot r^2}. \tag{22}$$

after dividing both sides of (11) by $(p\cdot q\cdot r)^2$. According to (21), $\frac{|u-U|}{p\cdot q^2\cdot r^2}$ would be a positive integer. This implies $p^2 \mid v-V$ and $p^2 \mid w-W$ by (22). Hence, it is enough to show that

$$p^2 \mid r^2\cdot(w-W)$$

which implies that

$$p^2 \mid (c-(a+b))$$

under the assumption that $p\neq r$ ($p=r$ implies a contradiction) and

$$r^2\cdot(w-W)=r^2\cdot w-r^2\cdot W=(c-(a+b)).$$

Since $p^2 \nmid (c-(a+b))$ is an initial precondition of this Lemma, we reach our final contradiction.

Condition (ii) and the hypothesis in (iii) are all-encompassing and mutually exclusive on account of (i). □

Theorem 3.2. *The Beal conjecture is true.*

Proof. Assume otherwise, i.e. identity $A^x+B^y=C^z$ holds for some $A,B,C,x,y,z\in\mathbb{N}$ such that $x,y,z>2$ and A,B,C are pairwise coprime. We can assume that $A,B,C>1$ in virtue of the already-proven Catalan conjecture [17]. Let p,q,r be different prime numbers such that $p\mid C$, $q\mid A$ and $r\mid B$

CASE 1: p is odd. Binomial formula (1) and Proposition 2.2 allow us to rewrite the equation $A^x+B^y=C^z$ as

$$(A^x+B^y)^p=C^{pz} \quad\Rightarrow\quad a+b+p\cdot A^x\cdot B^y\cdot k=c, \tag{23}$$

$$(C^z-B^y)^p=A^{px} \quad\Rightarrow\quad a=c-b+p\cdot C^z\cdot B^y\cdot n, \tag{24}$$

$$(C^z-A^x)^p=B^{py} \quad\Rightarrow\quad b=c-a+p\cdot C^z\cdot A^x\cdot m, \tag{25}$$

where $a=A^{x\cdot p}$, $b=B^{y\cdot p}$ and $c=C^{z\cdot p}$ and $k,m,n\in\mathbb{Z}$. This implies that $k>0$ because all the binomial summands that it arises from are strictly positive; this in turn entails $n,m\neq 0$. Thus $a+b-c$ is divisible by p on account of (23). We have $p\mid a+b$ (due to (23) and $p\mid c$) and (24), (25) and Proposition 2.4 imply

$$a+b-c=p\cdot C^z\cdot B^y\cdot n=p\cdot C^z\cdot A^x\cdot m \quad \text{hence } A^x\mid n \text{ and } B^y\mid m, \tag{26}$$

which in turn implies $q^3\mid c-b$ from (24) (because $q^3\mid n$ from (26), $x>2$ and $q^3\mid a$) and $r^3\mid c-a$ from (25) (because $r^3\mid b$ and $r^3\mid m$ due to (26) and $y>2$). Moreover, $p^2\nmid(c-(a+b))$ (due to (23), $p^2\mid c$ and $p\nmid A^x\cdot B^y\cdot k$ by Proposition 2.2 since $p\mid A^x\cdot B^y\cdot k$ would necessarily imply that p^2 should be a prime number which is not the case). Natural numbers a,b,c,p,q,r thus fulfill the hypotheses of Lemma 3.1. Thus by a simple deduction Lemma 3.1 implies $\max\{\gcd(a,b),\gcd(a,c),\gcd(b,c)\}>1$, but this contradicts our hypothesis that A,B,C, hence a,b,c, are pairwise coprime.

CASE 2: $p = 2$. Then q, r are odd, and (23)–(25) can be replaced by

$$(A^x + B^y)^q = C^{qz} \quad \Rightarrow \quad -a' = -c' + b' + q \cdot A^x \cdot B^y \cdot k', \tag{27}$$

$$(B^y - C^z)^q = -A^{zq} \quad \Rightarrow \quad c' = a' + b' + q \cdot B^y \cdot C^z \cdot n', \tag{28}$$

$$(C^z - A^x)^q = B^{qy} \quad \Rightarrow \quad b' = -a' + c' + q \cdot C^z \cdot A^x \cdot m', \tag{29}$$

for $a' = -C^{z \cdot q}$, $b' = B^{y \cdot q}$ and $c' = -A^{x \cdot q}$. The rest of the proof is similar to that of CASE 1. Again, $k' > 0$ because it arises from a binomial sum with positive summands, hence $n', m' \neq 0$ as well. Thus $a' + b' - c'$ is divisible by q on account of (27). $q \mid a' + b'$ due to (28) and $q \mid c'$, and (27) and (29) imply

$$a' + b' - c' = -q \cdot A^x \cdot B^y \cdot k' = q \cdot C^z \cdot A^x \cdot m' \quad \text{hence } C^z \mid k' \text{ and } B^y \mid m', \tag{30}$$

which in turns imply $p^3 \mid k'$ and $r^3 \mid m'$, hence $p^3 \mid c' - b'$ (because of (27), $z > 2$ and $p^3 \mid a'$) and $r^3 \mid c' - a'$ (because of (29), $y > 2$ and $r^3 \mid b'$). Furthermore, $q^2 \nmid (c' - (a' + b'))$ (due to (28), $q^2 \mid c'$ and $q \nmid B^y \cdot C^z \cdot n'$ by Proposition 2.2 since $q \mid B^y \cdot C^z \cdot n'$ would necessarily imply that q^2 should be a prime number which is not the case). All in all, a', b', c', p', q', r' (i.e. $p' = q$, $q' = p$ and $r' = r$) once again fulfill the hypotheses of Lemma 3.1 and the exact same argument used in CASE 2 ensues.

In conclusion, assuming the given natural numbers A, B, and C are pairwise coprime leads to a contradiction. □

4. CONCLUSION

This paper presents a short and concise proof of the Beal conjecture. We have shown that if equation

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

holds with integer exponents $x, y, z > 2$, then A, B, C must share a nontrivial common factor. This had remained an open problem ever since it was first proposed by Andrew Beal in 1993. This successful proof of his eponymous conjecture vindicates the aforementioned potential of simple tools as applied to difficult problems.

This accomplishment contributes to resolves a longstanding problem in Number Theory (i.e. Fermat's Last Theorem), first posed by Pierre de Fermat nearly 387 years ago. Our proof leverages the vast history of mathematical attempts to tackle this Theorem, offering a simpler and shorter approach compared to previous methods.

This is the bona fide confirmation that the wealth of tools available in Fermat's days was indeed enough to prove his seminal result, and it opens exciting avenues for further exploration. The techniques developed here show promise for application to similar Diophantine equations and other problems in Number Theory and, by extension, Abstract Algebra.

REFERENCES

[1] Pierre de Fermat. *Oeuvres de Pierre de Fermat*, volume 1. Gauthier-Villars, 1891. URL: https://archive.org/details/oeuvresdefermat02ferm.

[2] Leonhard Euler. *Elements of Algebra*. Springer Science & Business Media, 2012. doi:10.1007/978-1-4613-8511-0.

[3] Sophie Germain. *Oeuvres philosophiques de Sophie Germain*. Collection XIX, 2016. URL: https://gallica.bnf.fr/ark:/12148/bpt6k2032890/f13.image.

[4] Ernst Eduard Kummer. Zur theorie der complexen zahlen. 1847. doi:10.1007/BF01212902.

[5] Andrew Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of mathematics*, 141(3):443–551, 1995. doi:10.2307/2118559.
[6] Kenneth A Ribet. Galois representations and modular forms. *Bulletin of the American Mathematical Society*, 32(4):375–402, 1995. doi:10.1090/S0273-0979-1995-00616-6.
[7] Andrew Beal. A Generalization of Fermat's Last Theorem: The Beal Conjecture and Prize Problem. *Notices of the AMS*, 44(11), 1997. URL: https://www.ams.org/notices/199711/beal.pdf.
[8] Samuele Anni and Samir Siksek. Modular elliptic curves over real abelian fields and the generalized Fermat equation $x^{2l} + y^{2m} = z^p$. *Algebra & Number Theory*, 10(6):1147–1172, 2016. doi:10.2140/ant.2016.10.1147.
[9] Amir M Rahimi. An Elementary Approach to the Diophantine Equation $ax^m + by^n = z^r$ Using Center of Mass. *Missouri Journal of Mathematical Sciences*, 29(2):115–124, 2017. doi:10.35834/mjms/1513306825.
[10] Nuno Freitas, Bartosz Naskręcki, and Michael Stoll. The generalized Fermat equation with exponents 2, 3, n. *Compositio Mathematica*, 156(1):77–113, 2020. doi:10.1112/S0010437X19007693.
[11] Peter Norvig. Beal's Conjecture: A Search for Counterexamples. *Norvig.com*, July 2017. Accessed 10 June 2024. URL: http://norvig.com/beal.html.
[12] Milton Abramowitz and Irene A Stegun. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, volume 55. US Government printing office, 1968. URL: https://personal.math.ubc.ca/~cbm/aands/abramowitz_and_stegun.pdf.
[13] Klee Irwin. Toward the Unification of Physics and Number Theory. *Reports in Advances of Physical Sciences*, 3(01):1950003, 2019. doi:10.1142/S2424942419500038.
[14] Serge Lang. Algebra. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002. xvi+914 pp. ISBN: 978-0-387-95385-4 doi:10.1007/978-1-4613-0041-0.
[15] Godfrey Harold Hardy and Edward Maitland Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1979. ISBN: 978-0-1985-3171-5 URL: https://books.google.com.cu/books?id=FlUj0Rk_rF4C.
[16] Titu Andreescu, Dorin Andrica and Ion Cucurezeanu. An Introduction to Diophantine Equations. A Problem-Based Approach. Birkhäuser Verlag, New York, 2010. xii+345 pp. ISBN: 978-0-8176-4548-9 doi:10.1007/978-0-8176-4549-6.
[17] Preda Mihăilescu. Primary cyclotomic units and a proof of Catalans conjecture. *J. Reine Angew. Math*, 572:167–195, 2004. doi:10.1515/crll.2004.048.

Information Physics Institute, Miami, Florida, United States
Email address: vega.frank@gmail.com