The Bulletin of Society for Mathematical Services and Standards *Online: 2013-09-02*
ISSN: 2277-8020, Vol. 7, pp 17-22
doi:10.18052/www.scipress.com/BSMaSS.7.17

An All-Inclusive Proof of Beal's Conjecture

Stephen M. Marshall

Senior Engineer and Mathematician

Abstract

This paper presents a complete and exhaustive proof of the Beal Conjecture. The approach to this proof uses the Fundamental Theorem of Arithmetic as the basis for the proof of the Beal Conjecture. The Fundamental Theorem of Arithmetic states that every number greater than 1 is either prime itself or is unique product of prime numbers. The prime factorization of every number greater than 1 is used throughout every section of the proof of the Beal Conjecture. Without the Fundamental Theorem of Arithmetic, this approach to proving the Beal Conjecture would not be possible.

Introduction

In 1997 an amateur mathematician and Texas banker named Andrew Beal discovered the Beal Conjecture. The Beal Conjecture states that the only solutions to the equation $A^x + B^y = C^z$, when A, B, C, are positive integers, and x, y, and z are positive integers greater than 2, are those in which A, B, and C have a common prime factor. The truth of the Beal Conjecture implies Fermat's Last Theorem, which states that there are no solutions to the equation $a^n + b^n = c^n$ where a, b, and c are positive integers and n is a positive integer greater than 2. More than three hundred years ago, Pierre de Fermat claimed he had a proof but did not leave a record of it. The theorem was finally proved in the 1990s by Andrew Wiles, together with Richard Taylor. Both the Beal Conjecture and Fermat's Last Theorem are typical of many statements in number theory: easy to say, but extremely difficult to prove.

The Proof

The Beal Conjecture states the following:

If $A^x + B^y = C^z$, where A, B, C, x, y and z are positive integers and x, y and z are all greater than 2, then A, B and C must have a common prime factor.

We will prove for every positive integer for A, B, and C and for every x, y and z that are greater than

2 that the Beal Conjecture is true. This proof is based on the Fundamental Theorem of Arithmetic; therefore we will begin the proof of Beal's Conjecture with a proof (WIKIPEDIA®) of the Fundamental Theorem of Arithmetic below:

Proof of Fundamental Theorem of Arithmetic

In Number Theory the **fundamental theorem of arithmetic**, also called the **unique factorization theorem** or the **unique-prime-factorization theorem**, states that every number greater than 1 is either prime itself or is the product of prime numbers, and that, although the order of the primes in the second case is arbitrary, the primes themselves are not. For example,

$$1200 = 2^4 \times 3^1 \times 5^2 = 3 \times 2 \times 2 \times 2 \times 2 \times 5 \times 5 = 5 \times 2 \times 3 \times 2 \times 5 \times 2 \times 2 = \cdots \text{etc.}$$

The theorem is stating two things: first, that 1200 *can* be represented as a product of primes, and second, no matter how this is done, there will always be four 2s, one 3, two 5s, and no other primes in the product.

The requirement that the factors be prime is necessary: factorizations containing composite numbers may not be unique (e.g. $12 = 2 \times 6 = 3 \times 4$).

The proof uses Euclid's lemma *Elements* VII, 30): if a prime p divides the product of two natural numbers a and b, then p divides a or p divides b (or both).

Existence

By induction: assume it is true for all numbers less than n. If n is prime, there is nothing more to prove. Otherwise, there are integers a and b, where $n = ab$ and $1 < a \leq b < n$. By the induction hypothesis, $a = p_1p_2...p_n$ and $b = q_1q_2...q_m$ are products of primes. But then $n = ab = p_1p_2...p_nq_1q_2...q_m$ is the product of primes. In the base case, 2 is a trivial product of primes.

Uniqueness

Assume that $s > 1$ is the product of prime numbers in two different ways:

$$s = p_1p_2 \ldots p_m = q_1q_2 \ldots q_n$$

We must show $m = n$ and that the q_j are a rearrangement of the p_i.
By Euclid's lemma p_1 must divide one of the q_j; relabeling the q_j if necessary, say that p_1 divides q_1. But q_1 is prime, so its only divisors are itself and 1. Therefore, $p_1 = q_1$, so that

$$\frac{s}{p_1} = p_2 \ldots p_m = q_2 \ldots q_n$$

Reasoning the same way, p_2 must equal one of the remaining q_j. Relabeling again if necessary, say $p_2 = q_2$. Then

$$\frac{s}{p_1p_2} = p_3 \ldots p_m = q_3 \ldots q_n$$

This can be done for all m of the p_i, showing that $m \leq n$. If there were any q_j left over we would have

$$\frac{s}{p_1p_2 \ldots p_m} = 1 = q_k \ldots q_n$$

which is impossible, since the product of numbers greater than 1 cannot equal 1. Therefore $m = n$ and every q_j is some p_i.

Elementary proof of uniqueness

The fundamental theorem of arithmetic can also be proved without using Euclid's lemma, as follows: Assume that $s > 1$ is the smallest positive integer which is the product of prime numbers in two different ways. If s were prime then it would factor uniquely as itself, so there must be at least two primes in each factorization of s:

$$s = p_1p_2 \ldots p_m = q_1q_2 \ldots q_n$$

If any $p_i = q_j$ then, by cancellation, $s/p_i = s/q_j$ would be a positive integer greater than 1 with two distinct factorizations. But s/p_i is smaller than s, meaning s would not actually be the smallest such integer. Therefore every p_i must be distinct from every q_j.

Without loss of generality, take $p_1 < q_1$ (if this is not already the case, switch the p and q designations.) Consider

$$t=(q_1-p_1)(q_2\ldots q_n)$$

and note that $1 < q_2 \leq t < s$. Therefore t must have a unique prime factorization. By rearrangement we see,

$$t=q_1(q_2-p_n)-p_1(q_2\ldots q_n)$$
$$=s- p_1(q_2\ldots q_n)$$
$$=p_1((p_2\ldots p_m)-(q_2\ldots q_n))$$

Here $u = ((p_2 \ldots p_m) - (q_2 \ldots q_n))$ is positive, for if it were negative or zero then so would be its product with p_1, but that product equals t which is positive. So u is either 1 or factors into primes. In either case, $t = p_1u$ yields a prime factorization of t, which we know to be unique, so p_1 appears in the prime factorization of t.
If $(q_1 - p_1)$ equaled 1 then the prime factorization of t would be all q's, which would preclude p_1 from appearing. Thus $(q_1 - p_1)$ is not 1, but is positive, so it factors into primes: $(q_1 - p_1) = (r_1 \ldots r_h)$. This yields a prime factorization of

$$t=(r_1-r_h)(q_2\ldots q_n)$$

which we know is unique. Now, p_1 appears in the prime factorization of t, and it is not equal to any q, so it must be one of the r's. That means p_1 is a factor of $(q_1 - p_1)$, so there exists a positive integer k such that $p_1k = (q_1 - p_1)$, and therefore

$$p_1(k+1)=q_1$$

But that means q_1 has a proper factorization, so it is not a prime number. This contradiction showsthat s does not actually have two different prime factorizations. As a result, there is no smallest positive integer with multiple prime factorizations, hence all positive integers greater than 1 factor uniquely into primes.

Proof of Beal's Conjecture

First we shall assume that the Beal Conjecture is false, specifically:
If $A^x + B^y = C^z$, where A, B, C, x, y and z are positive integers and x, y and z are all greater than 2, then A, B and C cannot have a common prime factor.

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

Factoring the left side, $A^x(1 + B^y/A^x) = C^z$
Since A, B, and C are all positive integers then A^x, B^y, and C^z then for C^z to be a positive integer $(1+ B^y/A^x)$ must be a positive integer (**first possibility)** or a fraction that has a factor of A^x in its denominator so by reducing $A^x(1 + B^y/A^x)$ it is equal to the integer C^z (**second possibility)**.

Proof of first Possibility

For the first case if $(1 + B^y/A^x)$ = positive integer
Then, B^y/A^x must be an integer, which implies that B^y and A^x have a common prime factors in accordance with (IAW) the Fundamental Theorem of Arithmetic. Furthermore, B^y must be

divisible by A^x since B^y/A^x is an integer, then A^x must be reduced to 1 for B^y/A^x to be reduced to a positive integer.

Proof that B^y/A^x do not have any common prime factors using our assumption that Beal's Conjecture is false

Factoring B^y/A^x, then

$$B^y/A^x = \frac{(B_1)(B_2)(B_3) \ldots\ldots\ldots (By\text{-}_2)(By\text{-}_1)(By)}{(A_1)(A_2)(A_3) \ldots\ldots\ldots (Ax\text{-}_2)(Ax\text{-}_1)(Ax)}$$

Since $B = B_1 = B_2 = By\text{-}_1 = By$ and $A = A_1 = A_2 = Ax\text{-}_1 = Ax$, then none of the series of B's or A's have common prime factors since in our assumption we assumed that Beal's Conjecture was false and A, B and C cannot have a common prime factor. Therefore, B^y and A^x do not have any common prime factors.

However, IAW the **Fundamental Theorem of Arithmetic** every integer > 1 must be a unique series of prime factors, therefore B^y/A^x can only be an integer if A and B have common prime factors. Therefore since B^y/A^x cannot be an integer according to our assumption that Beal's Conjecture is false and A, B and C cannot have a common prime factor. However B^y/A^x must be an integer, therefore B^y and A^x must have common prime factors and our assumption that A, B, and C cannot have a common prime factor is false and Beal's Conjecture must be true for this first possibility.

Proof of second Possibility

The only other possibility is for $(1 + B^y/A^x)$ to be a fraction that has a factor of A^x in its denominator so by reducing $A^x(1 + B^y/A^x)$ it is equal to the integer C^z.

Let A^x_F = a factor of A^x

Therefore, $(1 + B^y/A^x) = N/A^x_F$ where N is a positive integer

Reducing, $A^x_F + (B^yA^x_F)/A^x = N$

A^x_F is a positive integer since it is a factor of A^x which is a positive integer.

Therefore, $(B^yA^x_F)/A^x$ must be an integer, then rearranging, $(B^yA^x_F)/A^x = (B^y)/(A^x/A^x_F)$

Let A^{X-R} = the multiplication of series of prime factors remaining for A^x after reducing A^x/A^x_F to an integer.

Let A^x_r = the multiplication of series of prime factors remaining for A^x_F after reducing A^x/A^x_F to an integer.

A^x_r cannot have a prime factor with B^y since the prime factors for A^x_r is a subset of the prime factors for A^x and according to our assumption and earlier proof that B^y and A^x do not have any common prime factors, then A^x_r cannot have any common prime factors with B^y. Using the same logic, A^{X-R} cannot have a prime factor with B^y since the prime factors for A^{X-R} is a subset of the prime factors for A^x and according to our assumption and earlier proof that B^y and A^x do not have any common prime factors, then $A^{X-R}A^x_r$ cannot have any common prime factors with B^y.

More specifically,

$$(B^y)/(A^{X-R})(A^x_r) = \frac{(B_1)(B_2)(B_3) \ldots\ldots\ldots (By\text{-}_2)(By\text{-}_1)(B_y)}{(A_1)(A_2)(A_3) \ldots\ldots\ldots (Ax\text{-}_{R-1})(Ax\text{-}_R)(A^x_r)}$$

None of the A's 1 through X-R have a common prime factor with any of the B's 1 through Y since $B = B_1 = B_2 = B_y$ and $A = A_1 = A_2 = Ax\text{-}_R$ and according to our assumption A, B, and C do not have any common prime factors. Since $A^x{}_r$ is a factor of A^x which has no common factors with B^y according to our first proof. Therefore, $A^x{}_r$ has no common prime factors with B^y, finally B^y and $(A^{X-R})(A^x{}_r)$ have no common prime factors.

However, for our second and final possibility, we have shown earlier that $(B^y)/(A^x/A^x{}_F)$ must be integer. Since $(B^y)/(A^x/A^x{}_F) = (B^yA^x{}_F)/A^x = (B^y)/(A^{X-R})(A^x) =$ integer. Therefore, since:

$$(B^y)/(A^{X-R})(A^x{}_r) = \frac{(B_1)(B_2)(B_3)\ \ldots\ldots\ldots (By\text{-}_2)(By\text{-}_1)(B_y)}{(A_1)(A_2)(A_3)\ \ldots\ldots\ldots (Ax\text{-}_{R-1})(Ax\text{-}_R)(A^x{}_r)} = \text{integer}$$

Therefore, since $B = B_1 = B_2 = B_y$ and $A = A_1 = A_2 = Ax\text{-}_R$ then A and B must have common prime factors for $(B^y)/(A^{X-R})(A^x{}_r)$ to be an integer. Furthermore, by the **Fundamental Theorem of Arithmetic** every integer > 1 must be a unique series of prime factors, therefore $(B^y)/(A^{X-R})(A^x{}_r)$ is a unique series of prime factors that can only be an integer if A and B have common prime factors.

Now we shall address the case when either A, B, or C are equal to 1. For $A^x + B^y = C^z$ let A = 1, then $1 + B^y = C^z$, then $1 = C^z - B^y$, since Y and Z are both > 2, then since B and C > 1 it is only possible for $C^z - B^y$ to be greater than 1, or equal to 0 only if $C^z = B^y$. For example, the smallest number possible for either B or C is 2. Since Y and Z are both > 2, then the lowest integer for Y or Z is 3. Then if lowest integer for C or B is 2, then say B = 2, then $B^3 = 2^3 = 8$, which is > 1. If $C^z \neq B^y$ then the lowest integer C can be is 3, then $C^3 = 3^3 = 27$, and $C^z - B^y = 27 - 8 = 19 > 1$, so there is no solution for $A^x + B^y = C^z$ when A = 1.

Following the same logic we can show that if B = 1, then there is no solution for $A^x + B^y = C^z$.

For $A^x + B^y = C^z$ let B = 1, then $A^x + 1 = C^z$, then $1 = C^z - A^x$, since X and Z are both > 2, then since A and C >1 it is only possible for $C^z - A^x$ to be greater than 1, or equal to 0 only if $C^z = A^x$. For example, the smallest number possible for either A or C is 2.Since X and Z are both > 2, then the lowest integer for X or Z is 3. Then if lowest integer for C or B is 2, then say A = 2, then $A^x = 2^3 = 8$, which is > 1. If $C^z \neq A^x$ then the lowest integer C can be is 3, then $C^3 = 3^3 = 27$, and $C^z - A^x = 27 - 8 = 19 > 1$, so there is no solution for $A^x + B^y = C^z$ when B = 1.

Following similar logic, if C = 1, then $A^x + B^y = 1$, but the lowest integers that A and B can be is A= B = 1, but then $A^x + B^y = 1$ can be reduced to 1 + 1 = 1, since $2 \neq 1$, then we have shown that there is no solution for $A^x + B^y = C^z$ when C = 1. This also shows that if A = B = C = 1, then that there is no solution for $A^x + B^y = C^z$ when A = B = C = 1. Also if two of A, B, or C are equal to 1, then let A = B = 1. Then $A^x + B^y = C^z$ can be reduced to $1 + 1 = C^z$ and Z > 2, then the lowest integer Z can be is Z = 3. Then $1 + 1 = C^3$ but if C = then 2 = 1, but $2 \neq 1$. If C = 2 then $1 + 1 = 2^z$. Again, the smallest integer for Z is Z – 3, then $1 + 1 = 2^3 = 8$. But $1 + 1 = 2 \neq 8$, and following the same logic for all C integers, C > 2 will not have solutions either. We have shown there is no solution for $A^x + B^y = C^z$ when A =B = 1.

Following similar logic as above for A = B =1, if any two of A, B, or C are equal to 1, then it can easily be shown that there is no solution for $A^x + B^y = C^z$ when any two combinations of A, B, or C are equal to 1.

The only remaining proof to completely prove that Beal's Conjecture is true is to show that C has a common prime factor with A and B. We have already proven that A and B have a common prime factor and have show that B^y and A^x have a common prime factor.

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

Let p be a common prime factor of B^y and A^x
Then $p(A^x/p + B^y/p) = C^z$
Reducing, $(A^x/p + B^y/p) = C^z/p$
Since p is a common prime factor of B^y and A^x, then A^x/p and B^y/p can both be reduced to integers. Therefore, since A^x/p and B^y/p are both integers then C^z/p is an integer, which is only possible if p is a common prime factor of C^z. Therefore, we have thoroughly proven that A, B, and C have common prime factors.

Conclusion

Our assumption that A, B, and C cannot have a common prime factor is false and Beal's Conjecture must be true for this second possibility. Beal's Conjecture has already been proven for the first possibility, therefore Beal's Conjecture is proven true for all possibilities and for all A, B, and C positive integers and all x, y, $z > 2$.

References

[1] A Classical Introduction to Modern Number Theory, Authors: Kenneth Ireland and Michael Rosen

[2] An Introduction to the Theory of Numbers, Authors: G. H. Hardy, Edward M. Wright, and Andrew Wiles

[3] Wikipedia, the free encyclopedia, the Fundamental Theorem of Arithmetic