A Possible Approach to Fermat's Last Theorem

Sylvain Bernier

April 25, 2025 *(finalized April 30)*

Abstract

Inspired by the world of Pythagorean triples, we imagine that valid triples could exist for other prime powers. Then we figure out what properties the terms in the triple would need to possess.

Euclid's formula can be used to generate Pythagorean triple, but there is an alternate, equivalent, formula. It looks like something similar would need to happen for other prime powers if triples were to exist for them. In this case, no single formula can generate triples, obviously. But having two partial formulas gives us the potential to find conflict, because they would also need to be equivalent.

To this, we add a simple independent reference value, which connects the terms together without using exponents. Despite the simplicity, it adds a number of additional restrictions.

Taken together, this seems to be a possible way to approach the problem which doesn't require very advanced methods.

1 Introduction

This problem is nearly four hundred years old and has been tackled by a lot of people better qualified than me. The only solution so far, by Andrew Wiles in the 1990's, is out of reach for most, including me. For me and others, hope remains for something more accessible.

I've been playing with this as a brainteaser every now and then for decades. There were countless "false positives" over the years, when I thought I had a solution but found a flaw later... Then in spring 2023, a discovery convinced me that I had everything needed for a solution, if I only could organize it properly... This hasn't happened yet. The latest "false positive" was part of the initial version of the current document.

I have removed the flawed conclusion, but I do believe that my approach to the problem is interesting. Therefore I am sharing its origin here in more details than initially. Maybe some will find it useful.

I'm among those who believe that Fermat did have a valid proof and that we just haven't rediscovered it yet, however unlikely that seems to many. If my little two cents can help with that, I would be happy.

I have included some background information to help with modular arithmetic and other prerequisites. Feel free to skip the parts that you don't need.

2 The Problem Itself

Fermat's last theorem can be expressed in a very compact manner:

> the equation $A^X + B^X = C^X$ has no solution where A, B, C, X are all positive integers and $X > 2$.

3 Trimming to the Essential

3.1 Primitive and Prime

To cover the problem entirely, it is enough to work within the notion of "primitive triples", those that can't be simplified. If such triples can exist, then all others can. Reciprocally, if they can't exist, others can't either. It's exactly like when $X = 2$, where real triples exist and are called "Pythagorean". For example, $(3, 4, 5)$ is the simplest primitive Pythagorean triple. It creates $3^2+4^2 = 5^2$, thus allowing $6^2+8^2 = 10^2$ and all other multiples to exist.

For the exponents, it's similar. Working with prime powers is enough. If we have $A^{15} + B^{15} = C^{15}$, we can focus on proving that either the 3^{rd} or the 5^{th} power is impossible. This is sufficient to cover the 15^{th} power, because $A^{15} + B^{15} = (A^5)^3 + (B^5)^3 = (A^3)^5 + (B^3)^5$.

These simplifications allow us to use powerful tools that would otherwise be inaccessible. There's just one exception...

3.2 The Case of $X = 4$

There's an infinite number of possible triples for $X = 2$.

Because triples do exist in that case, we need a way to cover other exponents that are themselves powers of 2 (4, 8, 16 and so on), as they have no other prime factors than 2 itself. This is why the 4^{th} power needs to be dealt with, despite not being a prime power. It takes care of the other powers of 2.

I have my own original proof that the theorem is true for $X = 4$. I quite like it, but it would take extra space and bring nothing, really. There already exist various historical proofs of this, which are well documented, including Fermat's own. Let's just take for granted that the theorem is true for $X = 4$, for the sake of brevity and to avoid distractions from the core concept used here, which only covers odd powers.

3.3 Refocusing

We can restate the problem like this then:

> try finding a solution to $A^P + B^P = C^P$, with A, B, C three positive integers that are pairwise coprime and with P a prime number, $P > 2$.

4 Foundation from $P = 2$

My work is a sort of extension of what makes things possible in the world of squares. Starting with this may help to better understand the process for $P > 2$ later on.

4.1 Making Triples

With Pythagorean triples, we have groups of three integers (A, B, C) that satisfy $A^2 + B^2 = C^2$, or Pythagoras' theorem. They can be viewed as right triangles with integer sides. Some more examples:

$$15^2 + 8^2 = 17^2 \qquad 21^2 + 20^2 = 29^2 \qquad 91^2 + 60^2 = 109^2$$

There are various methods to generate them. The main one is Euclid's formula, which can be used to generate all possible triples. To generate a random one, it tells us to start with two integers, usually identified as M, N. One of them must be odd and the other even. Then we can generate A, B, C like this:

$$A = M^2 - N^2, \qquad B = 2MN, \qquad C = M^2 + N^2, \qquad M > N$$

If M, N are coprime this will generate a primitive triple with A, C odd and B even. For example, $(3, 4, 5)$ is obtained with $M = 2, N = 1$. The three examples above are generated with $(M, N) = (4, 1), (5, 2)$ and $(10, 3)$ respectively.

4.2 Another Way

There's an alternate version of Euclid's formula. Curiously, that's the one I figured out first on my own. This time we use F, G to distinguish this version from the other one. They must both be odd and we generate a triple like this:

$$A = FG, \qquad B = \tfrac{1}{2}(F^2 - G^2), \qquad C = \tfrac{1}{2}(F^2 + G^2), \qquad F > G$$

Just like the main version, primitive triples will be generated if F, G are coprime. We get the same A, C odd and B even. To get $(3, 4, 5)$ again, we need $F = 3, G = 1$. Our three other examples require $(F, G) = (5, 3), (7, 3)$ and $(13, 7)$.

4.3 $(C - A)$ and $(C - B)$

We have two different, but equivalent, ways of expressing any triple. This gives us an interesting approach for $P > 2$. We won't have two ways to produce an eventual whole triple, but it will be possible to connect A with a partial Euclid-like formula and B with its alternate. This may have potential to create conflict.

To achieve this, we will use $C - A$ and $C - B$. Let's look at them now for $P = 2$ in order to better understand what will be done for $P > 2$:

Substituting with M, N from the main version of Euclid's formula:

$$C - A = (M^2 + N^2) - (M^2 - N^2) = 2N^2$$

$$C - B = (M^2 + N^2) - 2MN = (M - N)^2$$

Then substituting with F, G from the alternate version:

$$C - A = \tfrac{1}{2}(F^2 + G^2) - FG = \tfrac{1}{2}(F - G)^2$$

$$C - B = \tfrac{1}{2}(F^2 + G^2) - \tfrac{1}{2}(F^2 - G^2) = G^2$$

The simplest results are: G^2 for $(C - B)$ and $2N^2$ for $(C - A)$.

One of them must be an odd square and the other twice a square. The values can take two simple forms, and we must have one of each.

Also important is that while $G^2 = (C - B)$, we have $G \mid A$.[1]

Similarly, $2N^2 = (C - A)$ while $N \mid B$.

The root of the square divides the complementary term.

5 Prerequisites for $P > 2$

Before going further, the following elements must be understood.

5.1 Pascal's Triangle and Binomials

Pascal's triangle has many interesting properties. Some of them will be very useful to us.

Let's look at the first few rows of it:

0	·	·	·	·	·	·	·	1				
1	·	·	·	·	·	·	1		1			
2	·	·	·	·	·	1		2		1		
3	·	·	·	·	1		3		3		1	
4	·	·	·	1		4		6		4		1
5	·	·	1		5		10		10		5		1
6	·	1		6		15		20		15		6		1

When expanding a binomial such as $(A + B)^X$, the coefficients for the terms can be obtained from Pascal's triangle. If the single "1" at the top is on row number "zero", then any row number X provides the coefficients needed. For example, row 3 gives us (1,3,3,1), the coefficients for expanding $(A + B)^3$ into $A^3 + 3A^2B + 3AB^2 + B^3$.

The most important property for our needs, however, is about prime numbers. If you look at the rows where X is prime and ignore the 1's at both ends, the other coefficients are all multiples of that prime number. You can see this in rows 2, 3 and 5 above, which are primes, while it doesn't work in row 4 with the central "6", or in row 6 with the three central values.[2]

When X is prime, it corresponds to our P. This property of prime rows is present in all the possible cases that concern us and will be taken for granted from here on.

5.2 Modular Arithmetic

If you need a quick refresher, modular arithmetic can be seen as an extension of the common notion of "odd" and "even" numbers, but with regards to divisibility by other numbers than 2. When dividing any integer by 2, you either get 1 as remainder, or there is no remainder. Dividing by 3, you can get 1, 2 or none, and so on.

Let's look at a simple odd number like 3. In the context of modular arithmetic, "odd" means that "*3 is congruent to 1, modulo 2*" and is written: $3 \equiv 1 \pmod 2$. We can also say that $3 \equiv 5 \pmod 2$ because 3 and 5 being both odd, they both have the same remainder when divided by 2.

This is not very useful when dividing by 2... But it is when the divisor increases, because "odd" and "even" do not cover all the options. For example: $5 \equiv 8 \pmod 3$, $17 \equiv 10 \pmod 7$. In the first case, they both have a remainder of 2 when divided by 3. In the second case, they both have a remainder of 3 when divided by 7.

This notation is useful when we don't care about the numbers themselves, but only their relationships. If you are not familiar with this at all, please look it up as it is essential from now on. You must understand the basic properties.

The rest of this document is always about $(\text{mod } P)$ only, even if I may omit or forget to specify it a times...

[1] A vertical line "|" means "divides" (is a factor of).

[2] For this and much more about Pascal's triangle, Wikipedia has a good article.

5.3 Help from Fermat Himself

An important tool that we need is Fermat's own "little" theorem.[3] It is in good part why we need modular arithmetic. Being one of Fermat's own findings and necessary here, this was a most interesting requirement when it appeared...

Fermat's little theorem states two important things:

$$\text{if we have a prime number } P \text{ and an integer } A, \text{ then } A^P \equiv A \pmod{P}$$

$$\text{if } A \text{ is coprime with } P, \text{ then we also have } A^{P-1} \equiv 1 \pmod{P}$$

An important way that it is useful to us now is this:

$$A^P + B^P = C^P \quad \Rightarrow \quad A^P + B^P \equiv C^P \pmod{P} \quad \Rightarrow \quad A + B \equiv C \pmod{P}$$

It works because P is prime, therefore $A^P \equiv A$, $B^P \equiv B$ and $C^P \equiv C \pmod{P}$.

This is an extension of what happens for $P = 2$, where an odd number produces an odd square and an even number produces an even square. The difference is that there's more than two options if $P > 2$, and a lot more as P grows...

6 Potential Triples for any P

Attempting to find Euclid-like formulas for any P requires $C - A$ and $C - B$ again. We use $C - A$ as model for both, but first we introduce D, such that $D = C - A$.

Because A and C must be coprime to have a primitive triple, D is necessarily coprime with both C and A.

We then have $C = A + D$ and we can do this:

$$A^P + B^P = C^P = (A + D)^P = A^P + PA^{P-1}D + \ldots + PAD^{P-1} + D^P$$

Subtracting A^P, then rearranging:

$$B^P = PA^{P-1}D + \ldots + PAD^{P-1} + D^P$$

$$B^P - D^P = PAD(A^{P-2} + \ldots + D^{P-2}) \tag{6.1}$$

Example with $P = 5$:

$$A^5 + B^5 = C^5 = (A + D)^5 = A^5 + 5A^4D + 10A^3D^2 + 10A^2D^3 + 5AD^4 + D^5$$

$$\Rightarrow \quad B^5 = 5A^4D + 10A^3D^2 + 10A^2D^3 + 5AD^4 + D^5$$

$$\Rightarrow \quad B^5 - D^5 = 5AD\left(A^3 + 2A^2D + 2AD^2 + D^3\right)$$

6.1 Scaling Down the Options

Back to general equation (6.1), the left side must be divisible by P, which means that $B^P \equiv D^P \pmod{P}$. But using Fermat's little theorem, we can say that:

$$B^P \equiv D^P \equiv B \equiv D \pmod{P}$$

We must also be able to factor out D from $B^P - D^P$ on the left, so we need $D \mid B^P$ and it's D^1 only, a single D. That's because the unseen terms in "$+\ldots+$" are all multiples of D. A and D are coprime so A^{P-2} makes $(A^{P-2} + \ldots + D^{P-2})$ coprime with D. Therefore, only D^1 is available on the right and the left must be the same.[4] Let's have $B^P = DH$ and substitute in (6.1):

$$DH - D^P = PAD(A^{P-2} + \ldots + D^{P-2})$$

Then dividing all by D:

$$H - D^{P-1} = PA(A^{P-2} + \ldots + D^{P-2}) \tag{6.2}$$

$$P \mid H - D^{P-1} \quad \Rightarrow \quad H \equiv D^{P-1} \pmod{P}.$$

[3] You can find many different styles of proofs of it on math reference sites.

[4] Unless $P = D$, handled indirectly in the next section. $D \mid B^P$ is still a basic need.

(6.2) copied over: $H - D^{P-1} = PA(A^{P-2} + \ldots + D^{P-2})$

The left side must be divisible by P, with only two possible scenarios:

1. if $D \equiv 0 \Rightarrow H \equiv 0 \pmod{P}$
2. if $D \not\equiv 0 \;\Rightarrow\; D^{P-1} \equiv 1 \;\Rightarrow\; H \equiv 1 \pmod{P}$, using Fermat's little theorem.

We can ignore all other possible modulo values that would exist for generic non-prime exponents. This makes $P > 2$ similar to $P = 2$ where only even and odd exist. Whenever $P > 2$, we could interpret "odd" as meaning "any D where $P \nmid D$".

6.2 Detailed View

$B^P = DH$, so DH must be a P^{th} power.

D and H can each be P^{th} powers individually, or they share prime factors with a total (or multiple) of P of each factor inside DH overall. A simple example will be clearer: 25×36 vs 20×45. Both equal $30^2 = 900$ but only the first version is a product of two squares. Internally, however, it's the same group of prime factors at play and they can produce either version.

Let's look at what happens with each of the two possible scenarios:

1. If both $D, H \equiv 0 \pmod{P}$, then they cannot both be P^{th} powers. In equation (6.2), if both D, H contain more than P^1 each, only P^1 would be canceled by the single P on the right side and A would need to be divisible by P. Then $P \mid A$ and $P \mid B$ and (A, B, C) is not a primitive triple. This is not affected by $(A^{P-2} + \ldots + D^{P-2})$, because $D \equiv 0$ and only A^{P-2} inside is not divisible by D. Therefore, because $A \not\equiv D$, $P \nmid A$ and $P \nmid (A^{P-2} + \ldots + D^{P-2})$.
   So if $D, H \equiv 0$, then $B \equiv 0 \pmod{P}$ and to have A, B, C pairwise coprime we need $A \not\equiv 0$. The only way for this to be possible is to have $P \mid H$ once, with $P^{P-1} \mid D$, so that $B^P = DH$ works as a P^{th} power. Then $P^1 \mid (H - D^{P-1})$, with no P factor remaining after.
   Except for this shared P^1, they must be coprime, or any other factor that they share would also need to be shared by A. By introducing M and N, we can imagine the possibility of generating these partial, but plausible values:
   $C - A = D = P^{P-1}N^P, \quad H = PM^P, \quad B = PMN$ with M, N coprime and $P \nmid M$ for a primitive triple.[5]

2. If $D \not\equiv 0$ and $H \equiv 1 \pmod{P}$, then to generate primitive triples they must be coprime, or A will share their common factor again. Both need to be P^{th} powers already. In this case we can create plausible values more simply. We can use F and G as parameters to distinguish from the other option:
   $C - A = D = G^P, \; H = F^P, \; B = FG, \; F \equiv 1, G \not\equiv 0 \pmod{P}, \; F, G$ coprime.

6.3 $P = 2$ vs $P > 2$

I used M, N in the first scenario and F, G in the second because they are related to the same variables used for $P = 2$. Indeed, if you go through the process for $P = 2$, you will end up with Euclid's formula and it's alternate.

When $P = 2$, we can find two formulas which both can generate identical triples in slightly different ways. They are interchangeable. You can easily verify that if a triple is generated using M, N in the main formula, then you will get the same triple by using $F = M + N$, $G = M - N$ in the alternate version.

When $P > 2$, we do not have a single formula to generate triples. But we can imagine that what we have are pieces of two formulas, one giving us some information about A and the other about B. Though incomplete, we can assume that if triples were possible, the two complete formulas would have to be equivalent, just like for Pythagorean triples. We will never know.

[5] Cf footnote 3: $P = D$ is only possible for $P = 2, N = 1$. Not our concern here.

However, if A and B want a chance to exist at all for $P > 2$, then we can be sure that there are only two simple forms that they can take, similarly to $P = 2$.

Also similar to $P = 2$, $(C - A)$ and $(C - B)$ must take the form $P^{P-1}N^P$ or G^P. This means that the root of the P^{th} power in a difference divides the complementary term, just like for Pythagorean triples.

7 The Magic Key

7.1 Overview

When exploring some more, something else shows up.

In equation (6.1), we have $B^P - D^P$ on the left side. Instead of substituting like we did then, let's look at the standard expansion of this difference of same powers[6]:

$$B^P - D^P = (B - D)(B^{P-1} + B^{P-2}D + \ldots + BD^{P-2} + D^{P-1})$$

Let's focus on $B - D$:

$$B - D = B - (C - A) = A + B - C$$

If we had used $C - B$ as model instead of $C - A$, we would have obtained:

$$A - D = A - (C - B) = A + B - C$$

Both give an identical result, which means that the expression $A + B - C$ really showcases the interchangeability of A and B. This looks important, so let's give it a name, K, such that $K = A + B - C$. K is automatically a positive integer because all the others are integers and $(A + B) > C$.
We have seen that if $A^P + B^P = C^P$, then $A + B \equiv C \pmod{P}$.

Therefore $(A + B) - C \equiv 0 \pmod{P}$ and $P \mid K$, for any P.
This is the most basic property of K.

7.2 K^P divisible by $(A + B)$

We have $K^P = (A + B - C)^P$. We can group A and B together, then expand the result as a binomial :

$$K^P = [(A + B) - C]^P = (A + B)^P - P(A + B)^{P-1}C + \ldots + P(A + B)C^{P-1} - C^P$$

All the terms have an $(A + B)$ factor, except C^P at the far right.
However, if $A^P + B^P = C^P$ we can substitute C^P with $A^P + B^P$:

$$K^P = (A + B)^P - P(A + B)^{P-1}C + \ldots + P(A + B)C^{P-1} - (A^P + B^P)$$

Because $P > 2$ is always odd, there is a way to factorize $A^P + B^P$ for all the cases that concern us:[7]:

$$A^P + B^P = (A + B)(A^{P-1} - A^{P-2}B + \ldots - AB^{P-2} + B^{P-1})$$

This means that if $A^P + B^P = C^P$ with P odd, then K^P must be divisible by $(A + B)$ because each term in the expression has $A + B$ as a factor.

[6] Basically, an extension of the regular identity for a difference of two squares. Proof easily found on any math reference website.

[7] This identity can be found on Wikipedia or at The Problem Site, among others.

7.3 K^P is divisible by both $(C-A)$ and $(C-B)$

As seen in section 7.1, K^P can also be expressed like this:

$$K^P = [A-(C-B)]^P \qquad \text{and} \qquad K^P = [B-(C-A)]^P$$

It works similarly than for $(A+B)$. Instead of replacing the last term in each expansion, we replace the first one.

Let's do one:

$$K^P = [A-(C-B)]^P = A^P - PA^{P-1}(C-B) + \ldots + PA(C-B)^{P-1} - (C-B)^P$$

All the terms are divisible by $(C-B)$, except the first one, A^P. Again, if $A^P+B^P = C^P$ is true, this time we can replace A^P with $(C^P - B^P)$:

$$K^P = (C^P - B^P) - PA^{P-1}(C-B) + \ldots + PA(C-B)^{P-1} - (C-B)^P$$

$(C^P - B^P)$ is a difference of two same powers, which can be expressed as:

$$C^P - B^P = (C-B)(C^{p-1} + C^{P-2}B + \ldots + CB^{P-2} + B^{P-1})$$

We have the global $(C-B)$ factored out. The same thing will happen when we do this for $(C-A)$. Therefore we can be certain that if $A^P + B^P = C^P$, then K^P must be divisible by both $(C-B)$ and $(C-A)$.

We can also be certain that $(C-A), (C-B)$ can be extracted concurrently. That's because they must be coprime, otherwise A, B cannot be coprime and this is not a primitive triple. Remember that $(C-A)$ shares a factor with B and the same goes for $(C-B)$ and A. This means that we can safely write this: $K^P = (C-A)(C-B)[\ldots]$.

7.4 Summary

For $(A+B)$ we only can cover odd powers. The general conclusion for the three factors must be limited to that too. Still, we can state with confidence that:

> if $A^P + B^P = C^P$ and P is odd, then $(A+B)$, $(C-A)$ and $(C-B)$ must all be factors of $K^P = (A+B-C)^P$.

The simplest situation is when $P = 3$. In this case, only the three factors above appear, plus an extra factor $P = 3$:

$$K^3 = (A+B-C)^3 = 3(A+B)(C-A)(C-B)$$

Again, that's what must be possible IF $A^3 + B^3 = C^3$.

You can also verify that $(A+B)$ is not a factor when $P = 2$.

You will get $K^2 = 2(C-A)(C-B)$.

Because the $A+B$ factor is not present when $P = 2$ while it is for any other prime power, exploring it could potentially be useful.

In particular, there is this other way to rewrite the identity for K: $A+B = C+K$. This is something that can be explored in various ways too. $A+B$ and $C+K$ can substitute each other anywhere that they are present.

8 Closing Thoughts

There is more to it, but this would stray too far from the initial version of this document.

For instance, there is actually a way to visualize everything geometrically for any P. I will most likely prepare a document about this when I can. This is what got me spending more time on the problem these past couple of years. Having some visual tool to see what's going on is really nice, even if so far that's all it has allowed, just nice visuals, no proof yet.