SGC2, An Infinitude of P Factors

Origin: 2024-08-08 D. Ross Randolph

Abstract-Hypothesis:

For Sophie Germain Case 2: one of the 3 variables **A, B or C $\equiv 0$ Mod P^{∞}**
These intricate ideas will be elucidated in depth on the following pages.

While FLT was proved quite some time ago by Wiles/Taylor, it remains out of reach for the vast majority of mathematicians, due to the need of a strong background in modularity theory for *elliptic* curves, and other arcane branches of Number Theory. Thus most mathematicians are hoping for a proof that is a little easier to comprehend using Diophantine equations. This paper is intended to satisfy that need.

I have tried hard to making the writing light and entertaining. Writing this paper was like writing a book, a tremendous amount of blood, sweat and tears went into it's construction. Thousands of hours of math work. Do not feel the need to try to rush thru it, three subsequent readings of perhaps an hour each should allow complete absorption of this creative work of mathematics art.

Separate proofs will be presented for Sophie Germain Case 1 and Sophie Germain Case 2. For those uneducated in Sophie Germain's work, the two cases are rather simple to understand. For the formula $A^P + B^P = C^P$,

Case 1: None of the coprime variables A, B or C will have a factor of P.
Case 2: One of the coprime variables A, B or C will have a factor of P.

In my lexicon SGC1 represents Sophie Germain Case 1, and SGC2 represents Sophie Germain Case 2.

For SGC1, I will use an approach using magnitude inequality, and then indivisibility by P^2 to show one of the variables A, B or C must contain a factor P, which then essentially merges the proof with the SGC2 solution. This will be presented in a separate paper.

For SGC2, the proof will be iterative, showing an infinite number of factors of P in one of the three variables A, B or C

It is noted here, that from what I gather reading historical records Pierre Fermat favored an iterative proof method in many of his proofs. Of course anyone well versed in FLT (*Fermat's Last Theory*) is aware that the proof for the case N=4, used the iterative method referred to as Infinite Descent, as the 3 variables A, B and C descend with each iteration towards zero. We may consider the SGC2 proof in this exposition perhaps as a proof by Infinite Ascent, as one of the variables A, B and C must approach infinity.

In my earlier 9th proof attempt, which I wrote up several months ago, I used a metaphor of climbing Mount Everest liberally throughout the proof in various places, and I will reuse much of that proof in this new document. I hope you find the reading of this proof entertaining and sparkling. Or at least you may find it more entertaining and sparkling than your average Diophantine proof you may find on arXiv. For quite certainly, it is highly conceivable that others could have discovered a similar proof years before, but due to an inability to promote their ideas to the world at large, a proof would have gone unnoticed. Note, mathematics manipulation is only a way to pass the time for me, my true skills lie in music creation and engineering, thus you may find my notations somewhat arcane, for which I apologize in advance.

Basic knowledge regarding the exponent value. For any case of $A^N + B^N = C^N$, where N is >=3, it is relatively easy to show that it is only necessary to prove FLT for prime number exponents. Additionally, it is only necessary to prove FLT for A, B and C being coprime for obvious reasons. For even number value exponents, any that are composite and have an odd number factor will be provable by the odd number having a prime number factor, and if N = 4, 8, 16, 32 etcetera, Fermat's proof for N =4 by Infinite Descent serves as the simple basis of a proof. I will not elaborate on the statements in this paragraph, as the proofs are very simple and can be viewed on a 1000 different web portals.

INDEX

-1- Abstract-Hypothesis

-2- Conventions used in this Paper

-3- Foundational Knowledge, Explained using the Mount Everest metaphor

-4- Sophie Germain Case 2, Iterative Proof Method

-5- Synopsis

Addendum:

A) Foundational Knowledge, Expansions of Fermat's Little Theorem
B) References and Suggested reading
C) Email Contact information

Change Log located at the end of the paper.

Conventions used in this Paper:

Please note that instead of using the congruence operator of 3 parallel lines, I will instead be using a standard equality operator, for all modulus equations, as was the practice used regularly in the somewhat distant past. This will save me considerable mouse clicks during the creation of this document.

The abbreviation FLT will be used to indicate Fermat's Last Theory.

In the last 20 years of working on this theory, I have become accustomed to using a Symmetrical Form of the presentation of FLT, as follows: $A^P + B^P + C^P = 0$, this form has the benefit of reducing the amount of analysis when dealing with a symmetrical problem such as FLT. It should be mentioned the first Mathematician to seriously do some work on this problem other than Pierre Fermat himself was Leonard Euler, and he wrote his proof for the case N = 3 in the Symmetrical form as well. At times I may switch over to the non-symmetrical standard form of $A^P + B^P = C^P$, when the NSF (*non-Symmetrical Form*) may yield better clarity in an explanation.

Finally, the variables A, B and C are broken down into factors A_1, A_2, B_1, B_2, C_1 and C_2. The subscripts help to organize the factoring and memorizing of these 6 variables.

FOUNDATION THEORY, Necessary to Gain Basic Skills to understanding Fermat's Last Theorem

Note, there is a certain amount of repetition in this section, and some of the final forms referred to as "Presentation of D", may be not actually be required to be absorbed for a clear understanding of the two final SGC proofs, but are of interest in gaining a solid foothold into the fundamentals, none-the-less.

These next few pages will give the basic equational tools and gear necessary for climbing to the peak of the Mount Everest of math problems. Note the Himalaya's peaks are many and this Sherpa can only explore a limited number of them. I have found two routes to the summit, from which an inspiring view and feeling well being may spring. The climb is not without ardor, and to try to push to quickly to the summit may find one out of breath, and a fuzzy mind. Thus it is essential to accumulate these basic equational tools and commit them to memory. In further documents in this proof, the level of detail that will be expressed DEPENDS on a deep internal mathematics absorption of this foundational base.

At the completion of this portion of the proof we will be at Base Camp, and prepared to ascend to the heights of Everest.

The starting point will be defining the problem. It is normally defined as follows:

$$X^N + Y^N = Z^N$$

With X, Y and Z being positive integer values, and N being an integer value >= 3. That
there exist no possible solutions.

A proof for the case for N = 4 was shown by Fermat in a margin of his copy of Arithmetica, and later published by his son, after his death. Adjacent to the short detailed proof which makes use of the technique of Infinite Descent, is a comment that there are no solutions for any other higher exponent than 2, and that the margin of the paper is to small to hold this proof. Hard to say one way or another if he had a rock solid proof.

Anyway moving on, if N is any power of 2 >= 4 the proof would also hold, based upon simple algebraic use of exponent rules. Using similar reasoning, we can prove that any odd number exponent which is a composite number, will also hold true, if we can establish a proof for either of the factors for that composite number. And of course any even number which is a product of an odd prime number or odd composite number will also be “covered” by a proof for prime numbers which are >=3.

Based upon the above, and my personal preferences, we may rewrite the starting point equation as:

$$A^P + B^P = C^P$$

In this presentation, the exponent P represents a prime number >=3, and A, B and C as coprime integers.
The fundamental reasoning that A, B and C are considered as coprime, is that if A and B had a common factor, then C would also, and then we could remove this factor from all 3 variables, and rewrite.

Again based upon personal preference we may rewrite the equation in the symmetrical form as:

$$A^P + B^P + C^P = 0$$

In this presentation, we presume one of the 3 variables A, B and C must be negative. For convenience sake we will assume that C has a negative value. It should be noted that Euler was the first mathematician to find a proof for the case P = 3, and his proof used the symmetrical form. In other words, good historical precedent to proceed along this approach vector to the solution.

At this point maybe good to throw in some philosophy (*OH NOOOOOOO!*) Oh yes, consider the following.

This proof could also be for two negative numbers and one positive number, and be equally valid. And if we conveniently ignore the trivial solution aspect, the potential values and polarities of ***negative, zero and positive*** sort of make up a spectrum analogy of the human race coloration and sexual orientation. (*Note, this paper may be burned in "Fahrenheit 451ish fashion" in some fundamentalist republic provinces, and produce lots of heat, and additional CO_2 for our sky*.) So much for my comedic relief, back to reality.

Sophie Germain around the year 1800 was working on a number of mathematical and physics problems, her work on Fermat's Last Theorem has had a profound effect on the understanding of the underlying aspects of the problem. And her definition of Case 1 and Case 2 analysis of the famous equation is a starting point in understanding the two fundamental analysis approaches which must be employed.

Case 1, is when **none** of the integer variables A, B or C contains a factor of P.

Case 2, is when **one** of the integer variables A, B or C contains a factor of P.

Other than this simple branching aspect of the proof definition, no other aspects of Sophie Germain's extensive work on Fermat's Last Theory are utilized, in this exposition.

FACTORING $A^P + B^P + C^P = 0$

Consider $G^P + H^P$ and $G^P - H^P$ each consists of two factors as follows:

$G^P + HP = (G + H)(G^{P-1} - G^{P-2}H + G^{P-3}H^2 - \dots\dots\dots + G^2H^{P-3} - GH^{P-2} + H^{P-1})$

Note, alternating sign polarities in factor 2

$G^P - H^P = (G - H)(G^{P-1} + G^{P-2}H + G^{P-3}H^2 + \dots\dots\dots + G^2H^{P-3} + GH^{P-2} + H^{P-1})$

Note, same polarities in factor 2

Note, writing out the above right side factor 2 is time consuming to write, so as a shortcut, we may consider using the following functions instead:

$f_a(G, H, P) = (G^{P-1} - G^{P-2}H + G^{P-3}H^2 - \dots\dots\dots + G^2H^{P-3} - GH^{P-2} + H^{P-1})$

(f_a being the additive function factor of $G^P + H^P$)

$f_s(G, H, P) = (G^{P-1} + G^{P-2}H + G^{P-3}H^2 + \ldots\ldots\ldots + G^2H^{P-3} + GH^{P-2} + H^{P-1})$
(f_s being the subtractive function factor of $G^P - H^P$)

While working in the symmetrical presentation of Fermat's Last Theory I do not show the subscript "a" or "s", since all factoring work is from an additive point of view.

We may now expand the presentation form for Sophie Germain Case 1, using the above factoring Concepts.

> **Please bear in mind that G + H, may only divide once into $G^N + H^N$, and that for SGC1 there can be no common factors that exist between G + H and $f_a(G, H, P)$. This is shown in Lemma T3 on page 12. Regarding SGC2, this T3 Lemma also shows that if G + H contains one or more P factors then $f_a(G, H, P)$ must contain exactly one factor of P.**

$A_1^PA_2^P + B_1^PB_2^P + C_1^PC_2^P = 0$ (*Specific to SGC1*)
where $A_1^P = - (B + C)$ and $A_2^P = f (B, C, P)$
and $B_1^P = - (A + C)$ and $B_2^P = f (A, C, P)$
and $C_1^P = - (A + B)$ and $C_2^P = f (A, B, P)$

Similarly, we may expand the presentation for Sophie Germain Case 2:

$A_1^PA_2^P + B_1^PB_2^P + \mathbf{P_1^P}C_1^PC_2^P = 0$ (*Specific to SGC2*)
where $A_1^P = - (B + C)$ and $A_2^P = f (B, C, P)$
and $B_1^P = - (A + C)$ and $B_2^P = f (A, C, P)$
and $\mathbf{P^{P-1}}C_1^P = - (A + B)$ and $\mathbf{P}C_2^P = f (A, B, P)$

At this point, I suppose a simple presentation that can be written out on a blackboard for the class is needed. Let's look at the simpler case of SGC1 first, for P=5.

$A^5 + B^5 + C^5 = 0 = (A+B)(A^4 – A^3B + A^2B^2 -A^3B + B^4) + C^5$

and we could rewrite this as $(A+B)(A^4 – A^3B + A^2B^2 -A^3B + B^4) = -C^5$

The above form looks pretty basic, of course if we used the typical non-symmetrical presentation form instead of $-C^5$ we would simply have C^5. At this point you may wonder, why deal with a symmetrical form at all, which has positive and negative integer variables. Well, when the algebraic juggling gets super complex, using a somewhat simpler form helps to keep the polarity errors from creeping in to the analysis. Of course at this point in the exposition, everything is pretty simple. When we get to the trinomial expansion of $(A + B + C)^P$, the symmetrical form starts to look more appealing.

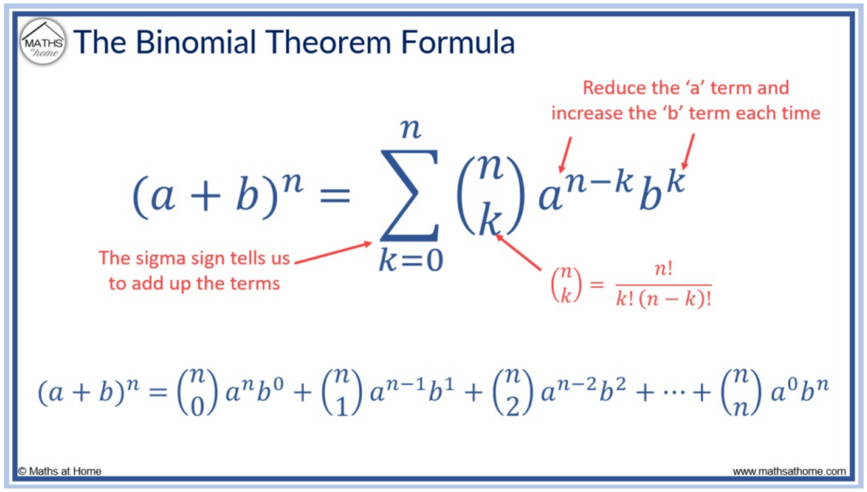
Binomial Expansion of $(a+b)^P$

When $(a+b)^P$ goes thru binomial expansion, the expanded form may be presented/condensed as:

$a^P + P\,(f(a,b)) + b^P$ *(with P (f(a,*b)) *representing the sum of all center terms)*

Basically, all of the center term coefficients will have a prime factor of P.

This may be understood by absorbing the basic standard formula for Binomial Expansion which is noted to the right:


The Binomial Theorem Formula
Reduce the 'a' term and increase the 'b' term each time
$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$
The sigma sign tells us to add up the terms
$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$
$(a+b)^n = \binom{n}{0} a^n b^0 + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n} a^0 b^n$
© Maths at Home
www.mathsathome.com

Maybe a little too abstract? Let's try a few prime exponent examples to add light to the concept.

$(a+b)^3 = a^3 + 3a^2b + 3\,ab^2 + b^3$
$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$

If you study the coefficient formula for a bit (*shown in Red Text above*), it will make sense, that all of the center term coefficients must have a prime factor of P, since a prime factor of n occurs in the numerator and can not occur in the denominator for all center term coefficients.

Below is Pascal's triangle from Wiki which shows all of the term coefficients up to exponent 7:
(*It's a classic math diagram!*) The center term coefficient prime factors are obvious for 3, 5 and 7.

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1

Trinomial Expansion of $(A+B+C)^P$

Now for Trinomial Expansion, pretty much the same applies, but we will now have to start thinking somewhat geometrically, but with supportive algebraic logic.

$(A + B + C)^3 =$ *(first diagrams, exponent = 3)*

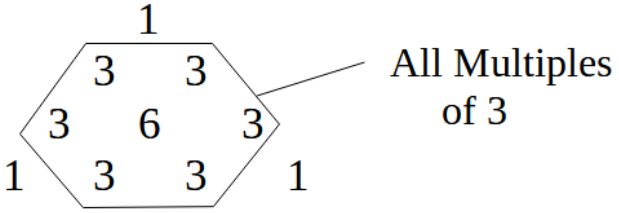
$(A + B + C)^5 =$ *(following diagram, exponent = 5)*

$$C^3$$

$$3AC^2 + 3BC^2$$

$$3A^2C + 6ABC + 3B^2C$$

$$A^3 + 3A^2B + 3AB^2 + B^3$$



$$C^5$$

$$5AC^4 + 5BC^4$$

$$10A^2C^3 + 20ABC^3 + 10B^2C^3$$

$$10A^3C^2 + 30A^2BC^2 + 30AB^2C^2 + 10B^3C^2$$

$$5A^4C + 20A^3BC + 30A^2B^2C + 20AB^3C + 5B^4C$$

$$A^5 + 5A^4B + 10A^3B^2 + 10A^2B^3 + 5AB^4 + B^5$$

NOTE, all of the coefficients (*shown in brown text*) for the P=5 trinomial expansion are divisible by 5.

For the general case of any prime number equal to 3 or greater this must also be true, since the center terms of the Binomial expansion are all multiples of the prime exponent factor, when expanded.

From the above rather un-artistic graphics we can gain a foothold into Trinomial expansion coefficients, that they all appear to be multiples of the prime exponent.

Formulaically expressed as:

$(A + B + C)^P = A^P + B^P + C^P + P\,(f(A,B,C,P))$

Where $P\,(f(A,B,C,P))$ is a unique positive integer value function representing the sum of all center terms.

Thus we observe the 3 corner terms have coefficients of 1, and all of the center coefficients are multiples of prime exponent value P.

The graphical view is nice, maybe algebraically you may understand that since all non-corner ***perimeter*** binomial expansions have factors of prime P, when we can multiply any horizontal binomial center row coefficients by the outer perimeter angled vertical row coefficients then all interior term coefficients must also contain a factor of prime P.

Perhaps at this point a more tangible proof of the center none-perimeter coefficients is needed. Supposing we rewrite the starting point equation in this analysis as follows:

$(A + B + C)^P = ((A+B) + C)^P$ and next simply apply Binomial Expansion to (A+B) and C.

In this case, if we consider P = 5, and the second row from the bottom, we will see that the coefficient elements will all be multiples of 5. Then once we expand (A+B), all of these coefficients will be multiplied by the factor 5. QED.

Since the summation of A^P, B^P and C^P is supposedly zero, we may now remove the 3 corner elements from the isosceles matrix.

With the 3 Corner Values of A^P, B^P and C^P removed, we find that all remaining elements are divisible by P, additional a careful analysis of a typical binomial expansion shows that the sum of the center terms are also divisible by a + b, therefore we can now show that the expansion of $(A + B + C)^P$ has the following 4 factors:

P (A+B) (B+C) and (C+A)

And bearing in mind the previous work from page 6: $A+B = -C_1^P$, $B+C = -A_1^P$, $C+A = -B_1^P$

Then based upon the knowledge that (A + B + C) must have an initial value which can be raised to the P exponent to $(A + B + C)^P$, we may determine that (A + B + C) must have an alternate form of:

$$A + B + C = P\,A_1\,B_1\,C_1\,K$$

with K being an arbitrary integer value which is related to the remaining factor of the division of $(A+B+C)^P$ *by* $P(A+B)(B+C)(C+A)$

For the case P = 3, K is easily determined for SGC2 and SGC1. However for higher order prime exponents the computation of K as a formula derived from A, B and C becomes more and more difficult as the exponent P increases. Yet we do not need to know the exact value of K, only that it is an integer if there would exist a counter-example solution to FLT.

Additionally, the various presentations of A + B + C may be given a single variable designation of **D** to simplify reference to this important variable in the FLT analysis.

Restating:

$$D = A + B + C = P\,A_1\,B_1\,C_1\,K$$

Still there are many more Presentations of D, which we will be required to be fluent in, as we forge our way to Base Camp.

<u>Presentations of D:</u>

Perhaps the **most important presentation of D** is as follows, thru substitution:

$$A + B + C \;=\; \frac{(A + B) + (B + C) + (A + C)}{2} \;=\; \frac{C_1^P \;+\; A_1^P \;+\; B_1^P}{-\,2}$$

(*Note, above form specific to SGC1*)

Although the -2 in the denominator of the far right presentation, appears out of place, it’s required to be a negative. Not too hard to show that, if you go back to the beginning of the proof.

This particular form is instrumental to the final proof for SGC2 since it is factorable, and after factoring new transforms are possible which lead directly to the actual proofs, which will be explored in later sections of this document.

These forms can also be expressed in relation to SGC2 as:

$$A + B + C \;=\; \frac{(A + B) + (B + C) + (A + C)}{2} \;=\; \frac{\mathbf{P^{P-1}}C_1^P \;+\; A_1^P \;+\; B_1^P}{-\,2}$$

It may be noted that this form is less factorable, than the form for SGC1, however $A_1^P + B_1^P$ can be factored!

And there yet remain a few more forms of D, which will be useful gear as we approach Base Camp:

$A_1^P = -(B + C)$ **$A + (B + C) = A - A_1^P$** **Similar substitutions for B and C arrive at:**

$A + B + C = A - A_1^P = B - B_1^P = C - C_1^P$ *This form for **SGC1***

and

$A + B + C = A - A_1^P = B - B_1^P = C - \mathbf{P^{P-1}}C_1^P$ *This form for **SGC2***

Now these last forms have a use of proving some detail about A_2, B_2 and C_2 for SGC1 as follows:

$A - A_1^P = A_1 (A_2 - A_1^{P-1})$ *Of course same considerations for B and C*

Based upon a complete understanding of Fermat's Little Theorem, we can show that:

$A^P = A$ Mod P and less well expounded: $A^{P-1} = 1$ Mod P

From the above we can prove for SGC1 that A_2, B_2 and $C_2 = 1$ Mod P, and for SGC2 if we assume C has the factor P then A_2 and $B_2 = 1$ Mod P and C_2 is an undefined Modulus of P, which is not 0 Mod P.

Below supporting lemma was written abut 18 months ago, and demonstrates that no common factors can exist between A_1 and A_2 other than P, and similarly for variables B and C. It also shows that if P is a factor of A_1, then it must also be a factor of A_2.

It is somewhat intuitive that A_1 can not be divided into A_2, this lemma helps to show this from a fundamental level.

T3 lemma

Binomial Expansion & Subduction of $J^P + K^P$

It is generally well known in number theory, proper factoring of $J^P + K^P$, and limits of prime cofactors when J and K are coprime. However this common knowledge is repeated below in a somewhat abbreviated form. I use the term Subduction here, as an indication of the application of subtractive and deductive reasoning processes.

And obviously, the same method of proof would apply to $J^P – K^P$

Similar to the form on pages 1 to 4, $J^{P-1} – J^{P-2} K + J^{P-3} K^2 \ldots K^{P-1}$ is simply represented by $f(J,K)$.

For the case P=5 as an example, it is given

$J^P + K^P$ Factors Into:

$$(J+K)(J^4 – J^3K + J^2K^2 – JK^3 + K^4)$$

However $(J+K)$ can not have any prime co-factor within $(J^4 –J^3K +J^2K^2 –JK^3 +K^4)$ except P as follows,

If attempting to divide J+K into $(J^4 –J^3K +J^2K^2 –JK^3 +K^4)$, *(this detailed on pg 6 to right)*

J+K Long Division	Coefficients only shown				
	1	-1	1	-1	1
Subtr $J^3(J+K)$* 1	1	1			

	0	-2			
Subtr $J^2K(J+K)$* -2		-2	-2		

		0	3		
Subt $JK^2(J+K)$* 3			3	3	

			0	-4	
Subt K3(J+K)* -4				-4	-4

				0	5

Here the remainder (*AKA residue*) is $5K^4$. Similarly, by successive J+K factor subtraction (*long division*), the remaining may be shown alternately as $5J^4$ or $5J^2K^2$.

The remainder is not fully divisible into J+K.

However it is easy to show any prime cofactors would need to exist between J+K and (*with symmetrical form*) $5J^2K^{2.}$,

Thus $\frac{5J^2K^2}{J+K}$ would have to have these cofactors.

The only cofactor can be P (*or 5 in this case*).
J^2 and K^2 can not contain any cofactors to J+K, by reciprocity.
Such that $\frac{J + K}{JK}$ can not have any cofactors since
it can be rewritten/understood that K is stated to be relatively prime (*coprime*) to J.

Then due to the simplicity of the subduction process:

$\frac{PJK}{J+K}$ may only have a single cofactor of P.

Thus J^P+K^P can only be factored as:

Case 1: $(J+K) \cdot f(J,K)$ with no common factor P
Or Case 2: $(J+K) \cdot f(J,K)$ with a common factor P

With $f(J,K)$ only able to contain a single factor of P

Detailed example of long division by J+K shown below, for clarity of understanding:

$$J^4 – J^3K +J^2K^2 – JK^3 +K^4 \ / \ (J + K)$$

$$\begin{array}{rl}
& J^4 – J^3K + J^2K^2 – JK^3 + K^4 \\
– & J^3 (J+K) \\
\hline
& – 2J^3K +J^2K^2 \\
+ & 2J^2K (J+K) \qquad \textit{(note, -1 * -1 = +1)} \\
\hline
& 3J^2K^2 – JK^3 \\
– & 3JK^2 (J+K) \\
\hline
& – 4JK^3 + K^4 \\
+ & 4K^3 (J+K) \qquad \textit{(note, -1 * -1 = +1)} \\
\hline
& 5K^4
\end{array}$$

Thus showing that P, in this case 5, is the only remainder when divided by J + K, similarly if dividing right to left the remainder will be $5J^4$, and if dividing symmetrically from both ends simultaneously, the result will be $5J^2K^2$. In all 3 cases, the only possible cofactor to J +K is 5 in essence P.

This T3 Lemma is fundamentally written to show that there are no possible common factors between A_1, A_2, B_1, B_2, C_1 and C_2 except the possibility of a factor of P.

I coined the term "Subduction" as being Subtraction/Deduction combined.

It should be somewhat obvious from the above analysis that if $J^P + K^P$ can not have a *single* factor of P, since both factors of it must contain a factor of P. Of course J + K could contain multiple factors of P, but $f_A(J,K,P)$ may only contain a single factor of P.

The long division presented above, dividing J + K into $f_A(J,K,P)$, can be done from left to right, right to left or may simultaneously be approached from both left and right sides. Although it is clearly intuitively obvious that J+K can not divided into $f_A(J,K,P)$ with the exception of factor P, this Lemma drives the point home using Long Division.

My first writeup on this in my NoteBook was for the case P = 7, with the Long division approached from both left and right sides simultaneously. Quite naturally, the residue was $7J^3K^{3.}$

Identification of Solutions of Fermat's Last Theorem

<u>Proof of Fermat's Last Theory, Iterative Proof for Sophie Germain Case 2</u>

Since we stipulate that one of the 3 variables A, B or C has a factor of P for the SGC2 (*Sophie Germain Case 2*) proof to FLT, the formula's below are adapted to that form. We will assume that variable C contains the factor P, and that it is distributed as follows, $\mathbf{C = P\, C_1\, C_2}$, thus:

$$A^P + B^P + C^P = 0$$

$$A_1^P = -(B + C) \qquad B_1^P = -(A + C) \qquad \mathbf{P^{P-1}}C_1^P = -(A + B)$$

$$A_2^P = f(B, C, P) = (B^{P-1} - B^{P-2}C + B^{P-3}C^2 - \ldots\ldots\ldots + B^2C^{P-3} - BC^{P-2} + C^{P-1})$$
$$B_2^P = f(A, C, P) = (A^{P-1} - A^{P-2}C + A^{P-3}C^2 - \ldots\ldots\ldots + A^2C^{P-3} - AC^{P-2} + C^{P-1})$$
$$\mathbf{P}\, C_2^P = f(A, B, P) = (A^{P-1} - A^{P-2}B + A^{P-3}B^2 - \ldots\ldots\ldots + A^2B^{P-3} - AB^{P-2} + B^{P-1})$$

$$A + B + C = P\, A_1\, B_1\, C_1\, K = \frac{(A + B) + (B + C) + (A + C)}{2} = \frac{\mathbf{P^{P-1}}C_1^P + A_1^P + B_1^P}{-2}$$

Keeping in our mind the proof for SGC1 previously studied, we may recall that in the denominator of the following presentation of D we have a factor of 2. I have additionally, shown the SGC2 presentation of it to the right of it:

$$\frac{C_1^P \quad + \quad A_1^P \quad + \quad B_1^P}{-\,2} \qquad\qquad \frac{P^{P-1}C_1^P \quad + \quad A_1^P \quad + \quad B_1^P}{-\,2}$$

The factor of P, will be shown to be infinite within C_1 …...

OK, now let us proceed: $$\frac{P^{P-1}C_1^P \quad + \quad A_1^P \quad + \quad B_1^P}{-\,2}$$

We note that $A_1^P + B_1^P$ will be divisible by $A_1 + B_1$, and this is the first step in the proof which may be referred to as an Infinitude of P Factors proof.

Next we may understand that $A_1 + B_1$ must contain the factor P. (*At this point I might suggest that any presentation use the case of P = 5, for clarity of thought. This could be written out on a classroom blackboard, whiteboard, or on a pad of paper, if you are working independently.)*

Since $A_1 + B_1$ must have a factor of P, then indeed $A_1^P + B_1^P$ divided by $A_1 + B_1$ must also contain a factor of P, as explained in our *foundational work* document on FLT, regarding SGC2.

Thus $A_1^P + B_1^P$ can not have a single factor of P, it must contain 2 factors of P at a minimum.

Note:
$A_1^{P-1} - A_1^{P-2}B_1 + A_1^{P-3}B_1^2 - \ldots\ldots\ldots + A_1^2B_1^{P-3} - A_1B_1^{P-2} + B_1^{P-1}$
will have P addend products, and will thus have a factor of P, since $A_1 = - B_1$ Mod P
A simple example of $2^5 + 3^5$ will demonstrate this 32 + 243 = 275, which is divisible by 25.
You may need to think this thru a few times before you absorb the 2 factors of P concept completely.

Since we have established now that D must contain 2 factors of P, we can look at other presentations of D as: $P A_1 B_1 C_1 K$ and $A_1A_2 + B_1B_2 + PC_1C_2$

Clearly $P A_1 B_1 C_1 K$ must necessarily contain 2 factors of P, with C_1 having one factor and P having the other factor.
(*Please see pg 18 Lemma T4 for further elucidation of this statement.*)

However inspection of $A_1A_2 + B_1B_2 + PC_1C_2$ yields an interesting concept which is that $A_1A_2 + B_1B_2$ must also contain 2 factors of P. The significance of this is that since A_2 and B_2 must be equal to 1 Mod P which is explained in the SGC1 proof, and thus we may present the following formula:

$$A_1A_2 + B_1B_2 = (A_1 + B_1)(1 \text{ Mod } P)$$

From this equation we may observe and conclude that $A_1 + B_1$ must have 2 factors of P, in other words must have the factor $P^{2.}$,

If we iterate this new understanding into the formulaic presentation of D:

$$\frac{P^{P-1}C_1^P \quad + \quad A_1^P \quad + \quad B_1^P}{-\ 2}$$

We now find that there are 3 factors of P present within it.

As we apply this looping iteration between the three presentations of D noted below:

$$\frac{P^{P-1}C_1^P \quad + \quad A_1^P \quad + \quad B_1^P}{-\ 2} \qquad P\ A_1\ B_1\ C_1\ K \qquad \text{and} \qquad A_1A_2 + B_1B_2 + PC_1C_2$$

We must come to the only logical conclusion, which is that we may loop Ad Infinitum, and with each loop another power of P will present itself, thus completing the proof for SGC2, using the Iterative Powers of P Method.

CLARIFICATION NOTE:
The "driving function" that makes the loop iterate, will be explained here.

The fact that $A_1^P + B_1^P$ always has an additional factor of P in the f (A_1, B_1, P) factor of the $A_1^P + B_1^P$ expansion, in comparison to the formula $A_1A_2 + B_1B_2$, means that there can never be a balance in the two presentations of D, thus shifting from the one presentation and back to the other presentation of D continually advances the number of iterations of the factor P, which must ultimately present itself within the variable C_1.

T4 lemma

Analysis of Presentation D_2 (P A_1 B_1 C_1 K)
P factors within C_1 and K for SGC2

The statement “Clearly P A_1 B_1 C_1 K must necessarily contain 2 factors of P, with C_1 having one factor and P having the other factor” has a simple proof as follows which shows K cannot contain a factor of P, using presentation of form D_{4C}.

P A_1 B_1 C_1 K => A + B + C => (A + B) + C => $- P^{P-1}C_1^P + PC_1C_2 \Rightarrow PC_1(C_2 – P^{P-2}C_1^{P-1})$ (*Form D_{4C}*)

$D_{4C} = PC_1(C_2 – P^{P-2}C_1^{P-1})$ *(this form from top of page 11 SGC2 development, note C = PC_1C_2 for SGC2)*

From inspection of Presentation form D_{4C} it is apparent that if there are two factors of P, then one of the factors must reside within C_1. Ergo, K can not contain the extra factor of P. QED

Synopsis

This sparse approach to proving Fermat’s Last Equation may be broken into 3 segments. The first of which shows by purely Diophantine algebraic methods that the summation of the 3 variables A, B and C may be presented in 7 different forms, which are referred to as Presentations of D.

Presentations D_1, D_2, D_3, D_{4A}, D_{4B} and D_{4C} are described in the section titled Foundational Knowledge, and these forms are presented both for Sophie Germain Case 1 as well as Sophie Germain Case 2.

In the second section of the proof, the Diophantine algebra use is steered towards the use of the Modulus operator instead. Analysis using the Modulus of exponent P dominates this last segment. Use of iterative looping thru the SGC2 equation sets, show that an infinite number of factors must reside within the integers used for A, B and C.

For the SGC2 proof, we start with form $\mathbf{D_3}$ and then inspect as form $\mathbf{D_2}$ and then analyze as form $\mathbf{D_1}$, and then back to form $\mathbf{D_3}$ to restart the process. The iteration restated below as:

$\mathbf{D_3} \rightarrow D_2 \rightarrow D_1 \rightarrow \mathbf{D_3} \rightarrow D_2 \rightarrow D_1 \rightarrow \mathbf{D_3} \rightarrow D_2 \rightarrow D_1$ **...** ad infinitum.

We can therefore show that this infinite iteration will result in the following infinity state: **A, B or C $\equiv$ 0 Mod P^{∞}**

ADDENDUM

-A- STATEMENTS of EXPANSIONS of FERMAT'S LITTLE THEOREM:

$A^P = A \text{ Mod } P$, is a typical way of writing Fermat's Little Theorem, it therefore thru induction it holds that $A^{P-1} = 1 \text{ Mod } P$.
And now since $A^0 = 1 \text{ Mod } P$ and $A^{P-1} = 1 \text{ Mod } P$, we can determine the periodicity which is P-1, thus we may write

$$A^{K(P-1) + 1} = A \text{ Mod } P$$

If we look at a simplified case of P = 5, we can understand that A Mod P will occur at N = 0, 5, 9, 13, 17 … as K is incremented. The best way to attain great clarity of this concept is to observe some "output" from a few Libre Office worksheets, presented below:

Modulus of Prime Number 3

Periodicity is 3 - 1

N = 13	0	**1**	**2**
N = 12	0	1	1
N = 11	0	**1**	**2**
N = 10	0	1	1
N = 9	0	**1**	**2**
N = 8	0	1	1
N = 7	0	**1**	**2**
N = 6	0	1	1
N = 5	0	**1**	**2**
N = 4	0	1	1
N = 3	0	**1**	**2**
N = 2	0	1	1
N = 1	0	**1**	**2**
N = 0	0	1	1

Modulus of Prime Number 5

Periodicity is 5 - 1

N = 13	0	**1**	**2**	**3**	**4**
N = 12	0	1	1	1	1
N = 11	0	1	3	2	4
N = 10	0	1	4	4	1
N = 9	0	**1**	**2**	**3**	**4**
N = 8	0	1	1	1	1
N = 7	0	1	3	2	4
N = 6	0	1	4	4	1
N = 5	0	**1**	**2**	**3**	**4**
N = 4	0	1	1	1	1
N = 3	0	1	3	2	4
N = 2	0	1	4	4	1
N = 1	0	**1**	**2**	**3**	**4**
N = 0	0	1	1	1	1

Modulus of Prime Number 7

Periodicity is 7 - 1

N = 13	0	**1**	**2**	**3**	**4**	**5**	**6**
N = 12	0	1	1	1	1	1	1
N = 11	0	1	4	5	2	3	6
N = 10	0	1	2	4	4	2	1
N = 9	0	1	1	6	1	6	6
N = 8	0	1	4	2	2	4	1
N = 7	0	**1**	**2**	**3**	**4**	**5**	**6**
N = 6	0	1	1	1	1	1	1
N = 5	0	1	4	5	2	3	6
N = 4	0	1	2	4	4	2	1
N = 3	0	1	1	6	1	6	6
N = 2	0	1	4	2	2	4	1
N = 1	0	**1**	**2**	**3**	**4**	**5**	**6**
N = 0	0	1	1	1	1	1	1

Modulus of Prime Number 11

Periodicity is 11 - 1

N = 21	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
N = 20	0	1	1	1	1	1	1	1	1	1	1
N = 19	0	1	6	4	3	9	2	8	7	5	10
N = 18	0	1	3	5	9	4	4	9	5	3	1
N = 17	0	1	7	9	5	3	8	6	2	4	10
N = 16	0	1	9	3	4	5	5	4	3	9	1
N = 15	0	1	10	1	1	1	10	10	10	1	10
N = 14	0	1	5	4	3	9	9	3	4	5	1
N = 13	0	1	8	5	9	4	7	2	6	3	10
N = 12	0	1	4	9	5	3	3	5	9	4	1
N = 11	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
N = 10	0	1	1	1	1	1	1	1	1	1	1
N = 9	0	1	6	4	3	9	2	8	7	5	10
N = 8	0	1	3	5	9	4	4	9	5	3	1
N = 7	0	1	7	9	5	3	8	6	2	4	10
N = 6	0	1	9	3	4	5	5	4	3	9	1
N = 5	0	1	10	1	1	1	10	10	10	1	10
N = 4	0	1	5	4	3	9	9	3	4	5	1
N = 3	0	1	8	5	9	4	7	2	6	3	10
N = 2	0	1	4	9	5	3	3	5	9	4	1
N = 1	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
N = 0	0	1	1	1	1	1	1	1	1	1	1

Modulus of Prime Number 13

Periodicity is 13 - 1

N = 25	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
N = 24	0	1	1	1	1	1	1	1	1	1	1	1	1
N = 23	0	1	7	9	10	8	11	2	5	3	4	6	12
N = 22	0	1	10	3	9	12	4	4	12	9	3	10	1
N = 21	0	1	5	1	12	5	5	8	8	1	12	8	12
N = 20	0	1	9	9	3	1	3	3	1	3	9	9	1
N = 19	0	1	11	3	4	8	7	6	5	9	10	2	12
N = 18	0	1	12	1	1	12	12	12	12	1	1	12	1
N = 17	0	1	6	9	10	5	2	11	8	3	4	7	12
N = 16	0	1	3	3	9	1	9	9	1	9	3	3	1
N = 15	0	1	8	1	12	8	8	5	5	1	12	5	12
N = 14	0	1	4	9	3	12	10	10	12	3	9	4	1
N = 13	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
N = 12	0	1	1	1	1	1	1	1	1	1	1	1	1
N = 11	0	1	7	9	10	8	11	2	5	3	4	6	12
N = 10	0	1	10	3	9	12	4	4	12	9	3	10	1
N = 9	0	1	5	1	12	5	5	8	8	1	12	8	12
N = 8	0	1	9	9	3	1	3	3	1	3	9	9	1
N = 7	0	1	11	3	4	8	7	6	5	9	10	2	12
N = 6	0	1	12	1	1	12	12	12	12	1	1	12	1
N = 5	0	1	6	9	10	5	2	11	8	3	4	7	12
N = 4	0	1	3	3	9	1	9	9	1	9	3	3	1
N = 3	0	1	8	1	12	8	8	5	5	1	12	5	12
N = 2	0	1	4	9	3	12	10	10	12	3	9	4	1
N = 1	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
N = 0	0	1	1	1	1	1	1	1	1	1	1	1	1

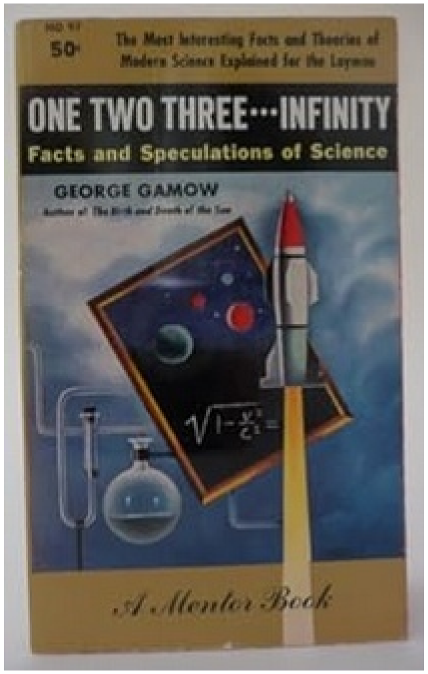
Now Let's consider the composite number 5 x 7 = 35
You may note that periodicity is the lowest common denominator of 5-1 and 7-1, which is 12. And that for the 12th and 24th rows that the Modulus of 35 is only **1** if the input parameter **A** is coprime to both 5 and 7.

N																																			
37	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**																										
36	1	1	1	1	15	1	21	1	1																										
35	1	18	12	9	10	6	28	22	4																										
34	1	9	4	11	30	1	14	29	16																										
33	1	22	13	29	20	6	7	8	29																										
32	1	11	16	16	25	1	21	1	11																										
31	1	23	17	4	5	6	28	22	9																										
30	1	29	29	1	15	1	14	29	1																										
29	1	32	33	9	10	6	7	8	4																										
28	1	16	11	11	30	1	21	1	16																										
27	1	8	27	29	20	6	28	22	29																										
26	1	4	9	16	25	1	14	29	11																										
25	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**0**
24	1	1	1	1	15	1	21	1	1	15	1	1	1	21	15	1	1	1	1	15	21	1	1	1	15	1	1	21	1	15	1	1	1	1	0
23	1	18	12	9	10	6	28	22	4	5	16	3	27	14	15	11	33	2	24	20	21	8	32	19	30	31	13	7	29	25	26	23	17	34	0
22	1	9	4	11	30	1	14	29	16	25	11	9	29	21	15	16	4	4	16	15	21	29	9	11	25	16	29	14	1	30	11	4	9	1	0
21	1	22	13	29	20	6	7	8	29	20	1	27	13	14	15	1	27	8	34	20	21	22	8	34	15	6	27	28	29	15	6	22	13	34	0
20	1	11	16	16	25	1	21	1	11	30	16	11	1	21	15	11	16	16	11	15	21	1	11	16	30	11	1	21	1	25	16	16	11	1	0
19	1	23	17	4	5	6	28	22	9	10	11	33	27	14	15	16	3	32	19	20	21	8	2	24	25	26	13	7	29	30	31	18	12	34	0
18	1	29	29	1	15	1	14	29	1	15	1	29	29	21	15	1	29	29	1	15	21	29	29	1	15	1	29	14	1	15	1	29	29	1	0
17	1	32	33	9	10	6	7	8	4	5	16	17	13	14	15	11	12	23	24	20	21	22	18	19	30	31	27	28	29	25	26	2	3	34	0
16	1	16	11	11	30	1	21	1	16	25	11	16	1	21	15	16	11	11	16	15	21	1	16	11	25	16	1	21	1	30	11	11	16	1	0
15	1	8	27	29	20	6	28	22	29	20	1	13	27	14	15	1	13	22	34	20	21	8	22	34	15	6	13	7	29	15	6	8	27	34	0
14	1	4	9	16	25	1	14	29	11	30	16	4	29	21	15	11	9	9	11	15	21	29	4	16	30	11	29	14	1	25	16	9	4	1	0
13	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**0**
12	1	1	1	1	15	1	21	1	1	15	1	1	1	21	15	1	1	1	1	15	21	1	1	1	15	1	1	21	1	15	1	1	1	1	0
11	1	18	12	9	10	6	28	22	4	5	16	3	27	14	15	11	33	2	24	20	21	8	32	19	30	31	13	7	29	25	26	23	17	34	0
10	1	9	4	11	30	1	14	29	16	25	11	9	29	21	15	16	4	4	16	15	21	29	9	11	25	16	29	14	1	30	11	4	9	1	0
9	1	22	13	29	20	6	7	8	29	20	1	27	13	14	15	1	27	8	34	20	21	22	8	34	15	6	27	28	29	15	6	22	13	34	0
8	1	11	16	16	25	1	21	1	11	30	16	11	1	21	15	11	16	16	11	15	21	1	11	16	30	11	1	21	1	25	16	16	11	1	0
7	1	23	17	4	5	6	28	22	9	10	11	33	27	14	15	16	3	32	19	20	21	8	2	24	25	26	13	7	29	30	31	18	12	34	0
6	1	29	29	1	15	1	14	29	1	15	1	29	29	21	15	1	29	29	1	15	21	29	29	1	15	1	29	14	1	15	1	29	29	1	0
5	1	32	33	9	10	6	7	8	4	5	16	17	13	14	15	11	12	23	24	20	21	22	18	19	30	31	27	28	29	25	26	2	3	34	0
4	1	16	11	11	30	1	21	1	16	25	11	16	1	21	15	16	11	11	16	15	21	1	16	11	25	16	1	21	1	30	11	11	16	1	0

3	1	8	27	29	20	6	28	22	29	20	1	13	27	14	15	1	13	22	34	20	21	8	22	34	15	6	13	7	29	15	6	8	27	34	0
2	1	4	9	16	25	1	14	29	11	30	16	4	29	21	15	11	9	9	11	15	21	29	4	16	30	11	29	14	1	25	16	9	4	1	0
1	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**
N																																			

It’s quite mind numbing I suppose. But we can understand the basics of Composite number Exponential Modulus when simply inspecting the above table, and we can thru induction state the extend these concepts to other composite scenarios.

-B- References and Suggested Reading


50¢
The Most Interesting Facts and Theories of Modern Science Explained for the Layman
ONE TWO THREE···INFINITY
Facts and Speculations of Science
GEORGE GAMOW
A Mentor Book

George Gamow, “One Two Three, Infinity”, 1959
A plain look at the outer-universe, the inner-universe, the expansion of space time, and infinity. Out-of-print, for quite a few years now, good luck finding a copy.

Mathematicians thru history whose work is foundational to this exposition.
Wikipedia Links:

Diophantus

Euclid

Pythagoras of Samos

Al-Khwarizmi

Pierre Fermat

Blaise Pascal

Leonard Euler

Sophie Germain

-C- For the near future, I may be contacted by email at: D.Ross.Randolph345@Gmail.com Feel free to establish contact.

CHANGE LOG:

2024-7-6, Green Bold text statements added at the top of page 6, to clarify that C_1 and C_2 are coprime.

2024-7-14, Improved graphics on page 8. Added some clarifications and cleanups on page 9 regarding origin of K factor.

2024-7-15, Cleared away some of the fog at the bottom of pg 9 and top of pg 10, re derivation of $PA_1B_1C_1K$.

2024-7-16, For SGC2 iterative proof, a Lemma T4 was added to prove the extra factor of P occurs in C_1 not K.

2024-7-18, Synopsis section added at end of SGC2 proof. 2024-7-19, added further elucidation to the Synopsis.

2024-7-21, Ripped out the flawed SGC1 proof, and several other non-essential sections not related to the proof. The SGC1 proof will be presented in a separate paper, which will merge it into the SGC2 proof.

2024-8-8, Fixed exponent error in Lemma T4