Sophie Germain's Theorems with some detours

The famous Fermat's Last Theorem claims that for natural numbers A, B, C, and $n > 2$,

$$A^n + B^n \neq C^n .$$

I am a mathematician who never looked closely at this theorem up until quite recently.
Set Theory, Logic, Effectivity and Randomness were my interests.
This "New Math" receives a deserved criticism from many classical mathematicians.
Indeed, it became a "legend in its own mind", defying its original goal to clean up mathematics.
I believed and still do, that New Math has a future, that it will go back to its destination.
In New Math, I became convinced that everything can be explained crystal clearly.
Mathematics is common sense applied with uncommon exactness. But when common sense and plausibilities are overgrown by the weed of formalism, then it becomes Formalism.
But this internal definition corresponds to a very human external one. Formalism is simply lying. Either not telling what we see, or talking about things we do not see. This duality of lies, this definition of Formalism is ruling not only mathematics, but our whole modern civilization.
The yearly circus and bread of the Romans became the continuous entertainment and consumption of the present. The joy of understanding, seeing things clearly and the joy of spreading this joy, became replaced by vanity and greed. Fame and fortune are our goals.
This is not a new shift. It started thousands of years ago and yoga predicted the shift to become worse and worse. This worsening is due to the social accommodation and re-inforcement of the wrong side of humans, leaving almost no room for the good.
We are on the brink. And yet, there is no hope for change.
I offer my help to anybody who will be changed by my words to see this dark present.
Maybe we can work together to alter the future.
And now, back to my new interest in Fermat's Last Theorem.
My surprise was how Formalism appears in a condensed way in this subject.
The simplicity and beauty was hidden in even more bizarre way as usual.
Number Theory's relation to New Math has a special twist.
New Math's second stage started with Gödel's Incompleteness Theorem. In this, it was crucial to show that all effectively definable relations are explicit from addition and multiplication. This is very surprising already for exponentiation. To explain this more clearly, I'll make a little detour.
Addition is repeated counting that is adding merely 1. Multiplication is repeated addition of a same member. And finally, exponentiation is a repeated multiplication of a same member.
So the naïve definitions are:

$$x + \underbrace{1 + 1 + \ldots + 1}_{y \text{ many}} = x + y$$

$$\underbrace{x + x + x + \ldots + x}_{y \text{ many}} = x \bullet y$$

$$\underbrace{x \bullet x \bullet x \bullet \ldots \bullet x}_{y \text{ many}} = x^y$$

These are not perfect, because they use dots for the unmentioned members, so are not truly explicit formulas. Peano realized the rule systems that can give these operations in closed forms without dots. But a weed was already growing in these systems, namely the use of functions.
The pure way to explain the truth, is to regard consecutiveness as a relation $x \lhd y$, meaning:
$1 \lhd 2$, $2 \lhd 3$, $3 \lhd 4$, . . . This is what we know, what we accept only as given.
Then, we'll tell the relations $x + y = z$, $x \bullet y = z$, $x^y = z$ by the following rules:

Addition:

$x \lhd z \quad \rightarrow \quad x + 1 = z$

$x + v = w \text{ and } v \lhd y \text{ and } w \lhd z \quad \rightarrow \quad x + y = z$

Multiplication:

$\rightarrow \quad x \bullet 1 = x$

$x \bullet v = w \text{ and } v \lhd y \text{ and } w + x = z \quad \rightarrow \quad x \bullet y = z$

Exponentiation:

$\rightarrow \quad x^1 = x$

$x^v = w \text{ and } v \lhd y \text{ and } w \bullet x = z \quad \rightarrow \quad x^y = z$

The blank left sides before the arrows above in multiplication's and exponentiation's first rules mean that we don't need any condition and can use the right side for any cases.
Now we can derive all numerical cases of the three operations from the infinite many given consecutiveness cases: $1 \lhd 2$, $2 \lhd 3$, . . . plus the three rule systems.
For example, to derive $4 + 3 = 7$ observe:

$4 \lhd 5 \quad \rightarrow \quad 4 + 1 = 5$

$4 + 1 = 5 \text{ and } 1 \lhd 2 \text{ and } 5 \lhd 6 \quad \rightarrow \quad 4 + 2 = 6$

$4 + 2 = 6 \text{ and } 2 \lhd 3 \text{ and } 6 \lhd 7 \quad \rightarrow \quad 4 + 3 = 7$

Observe that on the left sides, we only used either cases of $\lhd$, or already derived cases of $+$.
Using derived cases of $+$ we can derive cases for $\bullet$. For example $4 \bullet 3 = 12$:

$\rightarrow \quad 4 \bullet 1 = 4$

$4 \bullet 1 = 4 \text{ and } 1 \lhd 2 \text{ and } 4 + 4 = 8 \quad \rightarrow \quad 4 \bullet 2 = 8$

$4 \bullet 2 = 8 \text{ and } 2 \lhd 3 \text{ and } 8 + 4 = 12 \quad \rightarrow \quad 4 \bullet 3 = 12$

These rule systems are not explicit definitions. The reason is simple. Namely, we allowed the target relation of the right to be on the left side too.
It would be explicit if we only used accepted relations on the left to derive a new on the right.
In these cases by custom, we reverse the order and start with the target. Also instead of a one directional arrow we use two directional. Same as the "if and only if" logical symbol but with an added : to indicate that we don't claim rather introduce this logical relation the first time.
A simplest example could be the basic relations, if we only use a fix given number of repetitions in the naïve definitions. Indeed then, we don't need dots. But to use relations and no functions, we still need more variables. For example:

$x + 3 = z \quad :\leftrightarrow \quad x \lhd u \text{ and } u \lhd v \text{ and } v \lhd z$

$x \bullet 3 = z \quad :\leftrightarrow \quad x + x = u \text{ and } u + x = v \text{ and } v + x = z$

$x^3 = z \quad :\leftrightarrow x \bullet x = u \text{ and } u \bullet x = v \text{ and } v \bullet x = z$

These explicit definitions should actually use Logical symbols on the right.
Above we were still not really exact, because the used u , v variables were not specified.
There are only two meanings for such variables.
Either we mean them to be true for all values or true for some values. These two meanings are abbreviated in Logic as the two quantors $\forall$ and $\exists$. Here above it was obviously this second, so the precise explicit formulas as definitions are:

$x + 3 = z \;\; :\leftrightarrow \;\; \exists u \, \exists v \; (x \lhd u \text{ and } u \lhd v \text{ and } v \lhd z)$

$x \bullet 3 = z \;\; :\leftrightarrow \;\; \exists u \, \exists v \; (x + x = u \text{ and } u + x = v \text{ and } v + x = z)$

$x^3 = z \;\; :\leftrightarrow \;\; \exists u \, \exists v \; (x \bullet x = u \text{ and } u \bullet x = v \text{ and } v \bullet x = z)$

The definition of being a composite number is also explicit by multiplication.
Indeed, it means having factors that none of them is 1:

$x \text{ composite} \;\; :\leftrightarrow \;\; \exists u \, \exists v \; (u \neq 1 \text{ and } v \neq 1 \text{ and } u \bullet v = x)$

The formal symbol of negating, to replace such crossing over, is $\neg$. So, $u \neq v$ is $\neg (u = v)$.
Negation can be used for the two quantors too. To see its use, lets observe that being a prime means not being composite nor 1. So, the definition is:

$x \text{ prime} \;\; :\leftrightarrow \;\; \neg \, \exists \, u \, \exists \, v \; [\neg (u = 1) \text{ and } \neg (v = 1) \text{ and } u \bullet v = x] \text{ and } \neg (x = 1)$

A rule of Logic that already Aristotle collected in his formal logic is:

$$\neg \, \exists \, u \; . \; . \; . \leftrightarrow \; \forall \, u \, \neg \; . \; . \; .$$

Indeed, a non existent u for $. \; . \; .$ means that for all u $. \; . \; .$ is not true, that is, $\neg \; . \; . \; .$ is true.
This rule allows to change the definition of prime into an other form:

$x \text{ prime} \;\; :\leftrightarrow \;\; \neg \, \exists \, u \, \exists \, v \; [\neg (u = 1) \text{ and } \neg (v = 1) \text{ and } u \bullet v = x] \text{ and } \neg (x = 1)$

$$\updownarrow$$

$$\forall u \neg \, \exists \, v \; [\neg (u = 1) \text{ and } \neg (v = 1) \text{ and } u \bullet v = x] \text{ and } \neg (x = 1)$$

$$\updownarrow$$

$$\forall u \; \forall \; v \; \neg \; [\neg (u = 1) \text{ and } \neg (v = 1) \text{ and } u \bullet v = x] \text{ and } \neg (x = 1)$$

An other logical rule is that $\neg$ of "and"-s is the "or"-s of the $\neg$-s :
Indeed, not being happy and beautiful means not being happy or not being beautiful.
Using for our definition, we can continue:

$\forall u \; \forall \; v \; [\neg \neg (u = 1) \text{ or } \neg \neg (v = 1) \text{ or } \neg (u \bullet v = x)] \;\; \text{and} \;\; \neg (x = 1)$

Of course, a trivial rule is that $\neg \neg$ cancels each other, so we get:

$\forall u \; \forall \; v \; [(u = 1) \text{ or } (v = 1) \text{ or } \neg (u \bullet v = x)] \;\; \text{and} \;\; \neg (x = 1)$

Or to change the order of "or"-s:
$\forall u \; \forall \; v \; [\neg (u \bullet v = x) \text{ or } (u = 1) \text{ or } (v = 1)] \;\; \text{and} \;\; \neg (x = 1)$

And indeed, an x is prime if for all u , v their product is not x unless u or v are 1.
The word “unless” of course simply means “only if”.
Indeed, x is prime if it is not a product $u \bullet v$ only if $u = 1$ or $v = 1$.
So the word “if” appears in this version of “or” with the first member negated.
This is not accidental. “if then”, that is the implication $\rightarrow$ is always simply this meaning:
$A \rightarrow B \;:\leftrightarrow\; \neg A$ or B
So a new form or formula for x being prime is:

$\forall u \; \forall v \; [(u \bullet v = x) \rightarrow ((u = 1) \text{ or } (v = 1))]$ and $\neg (x = 1)$

This is the most common sense form for an exact meaning of x being prime as:
If x is a product, then one of the members is 1, and x itself is not 1.
An easy way to exclude the number to be 1 could be to specify that only one member is 1:
An x is prime means : If x is a product, then exactly one of the members is 1.
Of course this was not the reason to exclude 1 as prime, rather to be able to claim Unique Prime Factorization of all numbers except 1.
This world of formulas is the exactification of math.
The few strange facts that we encountered are indicating the whole story of Logic.
The defining of the $\rightarrow$ implication by “or” and in general all other logical connections also to be replaced by only the “and” and “or” is the newest purification, accepted in the modern version of Logic as Proof Theory. This emphasizes even more that the $\rightarrow$ arrows in derivation systems are different. They are “inferences”.
To use inferences in Logic itself was the crucial story of new math.
This could only happen because of the above so “naturally” introduced method of the two quantors as $\exists$ u and $\forall$ u. This is not natural at all. To drag a variable into the front and indicate its existence or universality this way was a huge step. This is what Aristotle didn’t know and thus his Formal Logic remained detached from even mathematical reality. So the really crucial point is the correct use of variables. Even mathematics used Latin abbreviations and a mixture of letter combinations till slowly the variables and formulas crystallized. The concrete numbers as opposed to the variables are names. The obvious important relation of quantors and names is that if something is true for a name then it is existent too and if something is true universally then it must be true for all names too. But this is not enough! We derive existences without producing concrete cases that is finding the names for them. The trivial and today hidden method due to Formalism is that we can create artificial names. Hilbert realized that the new clear use of variables allows to avoid such introduction of created names and instead use variables.
So the Hilbert rules of the two quantors were born, using variables and implication.
But this is the unimportant side. The important fact is that we have to widen the rules from fully quantized meaningful statements to only partially quantized forms that is formulas.
We derive formulas so that in the end the statements will be among them too. This the trick, the formal price to be totally exact. This derivability of the Logical truths obviously resembles the derivable relations of Peano. Rule systems are all essentially the same. Among numbers we derive cases of relations that is number triplets or tuples in general, while in Logic we derive formulas and the statements among them too. This was the real important realization of Gödel to show that an axiom system that can derive arithmetic, will always derive its own derivabilities too in disguise. This then implies that some statements must remain undecidable. Neither being derivable statement that is theorem nor negative of a theorem. The underlying deeper reason is actually expressible by derivabilities alone. Namely:
If a rule system is complex enough then the non derivable cases are not merely non derivable by this particular system but in general too. Not derivable by any rule system.
So one single complex system can create a set, namely the left over or complement set of the derived cases, that is a totally underivable set for ever and by any imaginable rule system.
This at once explains undecidability! If a complex enough axiom system derives the A, B, C, . . statements then it is impossible that every S statement or its negative is among these.

First of all, if the system is truthful it should not derive contradictions. We shouldn't have both an S and $\neg S$ among these. So the optimal would be to have all S or $\neg S$ in the derived ones.
But this would mean that the non derivable statements are derivable too. Not by the axiom system which gives the A, B, C, . . list, rather by the system followed with a formal negating.
So the universal non derivability is the reason that non theorems can not be simply the negated theorems. These are a derivable set but the non theorems are a universally non derivable.
A rule system fully determines this complement set of its derivabilities and this gives us the false impression that this complement must be similar to the derivabilities. But a closer look at even everyday rule systems shows the difference.
The chess rules tell exactly how the possible situations on the board go. The complement set is all situations that are not obtainable by fair steps. In chess we have some simple giveaways that a situation is impossible, like one players two bishops being on same color. But these don't tell all impossibilities. The set of all impossibilities is more complex than the ruled possibilities.
Not only is this more complex complement set determined by the system but many times even explicitly expressible too in the language that the axiom system uses. Indeed, if the system can express its own derivable statements translated as cases of an explicit formula $F(x)$, then the negated formula $\neg F(x)$ determines the non derivable statements.
So $F(x)$ gives derivabilities of the system itself, namely for every concrete n name that is natural number, $F(n)$ is a statement that expresses that a statement coded by n is derivable.
Also, the true $\neg F(n)$ cases are a universally non derivable set by any rule system.
This also gives the claimed undecidable statement in a more concrete form and so I repeat the argument for undecidability from non derivability:
Namely for some natural numbers n neither $F(n)$ nor $\neg F(n)$ are theorems.
This must be so, again if the system is truthful at least, that is wouldn't derive an $F(n)$ if the coded statement by n is not derivable.
Then the derivable $F(n)$ cases can maximum be exactly the truthful cases that is when the n coded statements are derivable. But this optimal derivability of the F cases is impossible. Some true F cases that is derivable statements must be underivable. That is, the system can not recognize its own derivabilities fully through this F. The reason is simple. If this was the case then the $\neg F(n)$ cases were derivable too. Not by the system itself of course, rather using the system for $F(n)$ and then using negating as an extra step. So the universal non derivability of $\neg F(n)$ defies this and so indeed already $F(n)$ couldn't be fully derived.
When this crucial point came and Gödel proved that addition and multiplication are such complex enough system, it was old fashioned number theory that showed how all rule systems like Peano's rules above, can be turned into explicit formulas.
So amazingly, $x^y = z$ can be replaced by an explicit formula too, using of course logical symbols including $\exists$, $\forall$ but only $+$ and $\bullet$ as basic non logical relations.
This is amazing, but didn't really alter the role of the $x^y = z$ exponentiation in classical math.
The most crucial usage of exponentiation is of course Fermat's Last Theorem, claiming that:
$A^n + B^n \neq C^n$ if $n > 2$.
New Math culminated in the result of Paul Cohen, by showing that the basic puzzle of Set Theory, the so called continuum problem is unsolvable.
In a formal sense, exponentiation or power is involved here too.
The power set is always a bigger set than the exponent: $2^S > S$. Even the meaning of 2^S is similar to 2^n for n numbers. But the $>$ of course is crucially infinite.
The mentioned continuum problem was whether there are infinites between S and 2^S.
You can't ask a simpler question and yet Set Theory is unable to answer.
Not long after Cohen's shocking result, a bombshell came in classical math too.
Fermat's Last Theorem was proved. So everything is over. The two power problems are closed.
But in truth, these results show that everything is open. To see this, we have to know the details how they claimed to close the problems. And indeed, both of them were unsatisfactory.
This, I don't want to go into now. Rather, I show some simple and crystal clear facts to see why Fermat's Last Theorem is so special.

The A , B , C natural numbers are an n-Fermat triple if $A < B$ and $A^n + B^n = C^n$.
This of course means $A < B < C$.
The 1-Fermat triples are simply the $A + B = C$ sum cases with $A < B$, like $2 + 3 = 5$.
The 2-Fermat triples are the old Pythagorean triples. Simplest case is $3^2 + 4^2 = 5^2$.
Fermat's Last or as it should be called, Fermat's Lost Theorem claims:

There are no n-Fermat triples if $n > 2$.

Already, the smallest $n = 3$ case is difficult to prove.
But most importantly, the $4 , 3 , 5 , 14 , 7$ cases, which are in order of difficulty, were all proved in their own particular ways.
The first person who had a plan for proving the claim for all $n > 2$ together, was a woman Sophie Germain. Usually the suppressive male scientific environment is mentioned to elevate her importance. The deeper Formalist environment of course is not even recognized. She had simple and crystal clear ideas for her plan that failed in the end. A side result of her plan is what today is presented as her theorems. A total distortion and degradation of her role.
She couldn't forge an anti-Formalist view. In that early stage of the mathematical formalism, influenced mostly by Gauss, the malicious side was not evident. Yet, the mathematical rubbish found on the internet, especially on Wikipedia, is a direct consequence of this late classical math initiated by Gauss.

Basic Facts of Fermat Triples

1.)
If a p prime divides two of A , B , C then p divides the n powers of those two too.
Thus, $A^n + B^n = C^n$ means that p divides two members of these three and thus, it has to divide the third, because sums or differences keep the common dividers. Finally, if p divides the third power too, then p must divide the base too.
This final third step is where p has to be a prime.
Indeed for example, 4 divides $6^2 = 36$, but 4 doesn't divide the base 6. This could only happen because 4 was not a prime. Its two 2 factors were able to divide the two appearance of 6 in 36. To see why it can't happen for a p prime, we can go other ways too.
So suppose, p divides a B^n power, but p would not divide the B base. Then, B has an r remainder to p, that is, $B = m p + r$. We can calculate the powers of B with this:
For example, $B^2 = (m p + r)^2 = (m p)^2 + 2 m p r + r^2$. Here, all members contain p except r^2.
This same goes for higher powers or repeated multiplications with $(m p + r)$, so:
$B^n = M p + r^n$ and thus, p can only divide this if it divides r^n.
Now it seems quite obvious, that since $r < p$, this smaller number multiplied together n times, can not be dividable by p.
If we accept the Unique Prime Factorization, then it is instantly proved too, because p's factorization is itself the single p and r^n can contain only smaller primes than p. So the two can not be equal. This special case could be proved without UPF too.
I mentioned this remainder argument as a first appearance for remainders being in general the true, behind the scene causes of Fermat's Theorem. Their role becomes more and more apparent.
The simple end result here is that for A , B , C Fermat triples, any p factor of two has to be of the third too. So, if any two have no such p factor, that is are so called relative primes, then the third is relative prime too, with any of the two. So, for these Fermat triples, we can simply say that they are relative primes or "simple". This name is logical from the followings:
First of all, not having p prime common factor, means also not having any $d \neq 1$ common divider at all, because d would have some prime factors itself.
Having a d common divider means: $A = a d$, $B = b d$, $C = c d$ and so we have:

$A^n + B^n = (a\,d)^n + (b\,d)^n = d^n\,(a^n + b^n) = C^n = (c\,d)^n = d^n\,c^n$.
Thus, dividing with d^n we get $a^n + b^n = c^n$.
Doing such divisions or simplifications repeatedly or at once for a greatest possible d divider, $a^n + b^n = c^n$ will become true with a, b, c relative primes that is simple.
So the simple triples are actually the totally simplified triples. And the simplification process proves that: Having n-Fermat triples means also having simple ones. Or negatively:

If there are no simple n-Fermat triples, then there are none in general.

2.)
Not only the A, B, C base can be reduced to simple a, b, c but the n exponent can be simplified too. Indeed, if one of n's factors is f, that is $n = m\,f$, then we have:

$a^n + b^n = a^{m\,f} + b^{m\,f} = (a^m)^f + (b^m)^f = c^n = c^{m\,f} = (c^m)^f$

So, a^m, b^m, c^m is an f-Fermat triple. Or again negatively:

If there are no f-Fermat triples, then there are no $m\,f$ –Fermat triples either.

Since all numbers are built from primes, we might jump to the following consequence:

If there are no simple p-Fermat triples, then there are none in general.

This reduction though is true as claim, unfortunately not useful because we do know that there are 2-Fermat triples for example $3^2 + 4^2 = 5^2$. But all $n > 2$ numbers have either an odd prime factor or 4, so a less beautiful reduction is still useful:

If there are no simple n-Fermat triples for $n = 4$ or odd primes, then there are none for all $n > 2$.

And indeed, the $n = 4$ impossibility was the easiest, already proven by Fermat.
The simplest odd prime 3 was much harder and I explain that story in an other article.

3.)
A special fact is that for any A, B, C n-Fermat triple, at least one of them must be even.
Indeed, all three can't be odds, because powers of odds are odds too, but sums or differences of odds are even. So, $A^n + B^n$ or $C^n - A^n$ or $C^n - B^n$ would be even, contradicting the third.
For relative prime, or simple a, b, c triples of course, no two of them can be even. So here:

There is exactly one even in the triple, either a or b or c.

Sometimes we can tell more about this even member. Such is the famous $n = 2$ case:

4.)
Among the simple 2-Fermat triples or so called Pythagorean triples, the even can not be c.
Indeed, if c is even, then it is $c^2 = (2\,k)^2 = 4\,k^2$, so is dividable by 4.
Since a, b would be odds, their squares are $(2\,k + 1)^2 = 4\,k^2 + 4\,k + 1$ so have 1 remainder to 4. Thus, $a^2 + b^2$ would have 2 remainder to 4, that is not dividable by 4 as the other side.
For these existing Pythagorean triples, the main concern was to tell exactly what they are.
The Babylonians already found the solution.
Amazingly, by the biggest c member as variable, we can tell the exact rule of existing a and b.
Namely, the c^2 can be a sum of squares of relative primes if and only if c itself can.

$$\exists\, a\ \exists\, b\quad c^2 = a^2 + b^2 \quad\leftrightarrow\quad \exists\, u\ \exists\, v\quad c = u^2 + v^2$$

We omitted the condition of being relative primes because we already agreed to use these only.
Both directions can be proved by explicit formulas, but the Babylonians only found the ones that proved $\leftarrow$. First of all $u = v$ would mean even c, so we can assume that $u < v$.
Then the two formulas for a , b are:

$$a = v^2 - u^2 \quad , \quad b = 2\,u\,v$$

Indeed, $(v^2 - u^2)^2 + (2\,u\,v)^2 = (u^2 + v^2)^2$ can be verified by squaring the sums.
For the reverse formulas, that is proving $\rightarrow$, we have to specify which of a , b is the even.
So we give up the earlier $a < b$ convention and rather accept that a is the odd and b is the even.
Then the formulas of u , v are:

$$u = \sqrt{\frac{c-a}{2}} \quad , \quad v = \sqrt{\frac{c+a}{2}}$$

Amazingly, $u^2 + v^2 = c$ becomes trivial, because the squaring cancels the roots and
$\frac{c-a}{2} + \frac{c+a}{2} = c$ .The easiness of this suggests that something was wrong.
We didn't even use the $a^2 + b^2 = c^2$ condition. What we forgot about is that our u , v square root formulas are not necessarily whole numbers. To prove that they are, we need the condition.
The oddness of c and a proves that the two fractions under the square roots are whole.
But why are they squares? Multiplying them together $\frac{c-a}{2} \bullet \frac{c+a}{2} = \frac{c^2-a^2}{4} = \frac{b^2}{4} = \left(\frac{b}{2}\right)^2$.
Indeed, b was even so it is a square. But why does this mean that $\frac{c-a}{2}$ and $\frac{c+a}{2}$ are square too? Because, they are relative primes. Indeed, first of all they are relative primes, because their sum and difference is c and a. So, any common prime factor of them would be common of these too, but these two are relative primes. Secondly, since they are relative primes, they have no common prime factors. $\left(\frac{b}{2}\right)^2$ has all prime factors with even occurrence and $\frac{c-a}{2}$ and $\frac{c+a}{2}$ containing different prime factors will contain also even occurrences. So they are squares.
Why the Babylonians missed this, I don't get into now, but more shocking is the following:
You can go on the internet and enter "Pythagorean triples" and you'll find a flood of rubbish, except the above simple and straight forward proof for the two directions.

5.)
For the $n > 2$ cases where we believe there are no Fermat triples, we still argue the same way as above for the Pythagorean triples, that is assuming as if they exist.
A new feature in these arguments is the re-occurring role of remainders. Usually, to a new bigger P number than the p exponent. The remainders to P can be $1, 2, 3, \ldots, P-1$.
If a number is dividable by P, then we say that the remainder is 0.
This is a very natural extension of the naturals and we will be careful not to abuse it and stick with naturals, except among these P remainders.
Sums, products and powers give remainders that can be calculated from the remainders of the numbers already.
For example, 7's remainder to 5 is 2, so 7^2 should have remainder $2^2 = 4$ and indeed, 49 has 4 remainder to 5.
But if the remainder calculations become P, we again regard it as 0 and if we go above P, we use the new remainders.
For example, 7's remainder to 5 is 2 again, and 8's remainder is 3.

So, $7 \bullet 8$ should give $2 \bullet 3 = 6$ which overflows 5 and so becomes only 1.
And indeed, 56 has 1 remainder to 5.
All this can be precisely written if we use $[\ ]$ for remainders to P.
For example, the aboves with $P = 5$:
$[7 \bullet 8] = [\,[\,7\,] \bullet [\,8\,]\,] = [\,2 \bullet 3\,] = [6] = 1$. Similarly, for the Fermat triples:
If $a^p + b^p = c^p$ then we also have: $[\,a^p + b^p\,] = [\,[\,a^p\,] + [\,b^p\,]\,] = [\,c^p\,]$
So if this is impossible, then we know that the Fermat triple was impossible too.
Or if the remainders can allow only special "Fermat triples" among them then the originals must be correspondingly special.
The reverse, that is solutions among remainders of course don't guarantee solutions for the full triples. Luckily, in our subject of the Fermat triples, we are striving for impossibilities. So, using remainders is a perfect tool.
The simplest practical case is for the $p = 3$ and 5 triples.
We claim that if they exist, it can only be if 3 or 5 divides one of a , b , c.
Lets show first 3 and try $P = 3$ itself as a divider. To see why this doesn't work is easy.
The remainders to 3 are $1 , 2 , 0$. The cubes therefore have remainders: $1 , [8] = 2 , 0$ again.
This is bad because we have too many choices and indeed we have $1 + 1 = 2$ as a solution.
This solution avoids the remainder 0, so we can not conclude from this alone what we want.
The trick is to use a different P, namely $P = p^2 = 3^2 = 9$.
Indeed, to this, the basic remainders are:
$1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 0$ which are much more, but checking the cubes' remainders to 9:

$[1^3] = 1$

$[2^3] = 8$

$[3^3] = [27 = 3 \bullet 9] = 0$

$[4^3] = [64 = 7 \bullet 9 + 1] = 1$

$[5^3] = [125 = 13 \bullet 9 + 8\ ] = 8$

$[6^3] = [216 = 24 \bullet 9\ ] = 0$

$[7^3] = [343 = 38 \bullet 9 + 1\ ] = 1$

$[8^3] = [512 = 56 \bullet 9 + 8\ ] = 8$

As we see, in spite of the many original remainders, the cubes have only $0 , 1$ and 8 .
Thus, we can not satisfy $[\,a^3\,] + [\,b^3\,] = [\,c^3\,]$ without using 0, that is one of the powers must be dividable by 9 and so one of the a , b , c must be dividable by 3.
For $p = 5$, again we can regard the remainders to $P = 25$ to see that 0 must be used.
And so, for all 5-Fermat triples, 5 must divide one of the members.
It would be quite a task to calculate all cube remainders to 25.
For the next $p = 7$, this idea doesn't even work. So this simple $P = 7^2$ divider doesn't prove that 49 divides one of the powers. And yet 7 must divide a member by other arguments.
This suggests that the main "easily" provable feature is that p must divide a member.
And the hard part would be "only" to prove the impossibility for triples containg a p multiple.
On the other hand, the use of P above as trick also indicates that maybe we should regard associated P values to p in general. Then the task is dual:
A P association to p, with a reduction system of the non P multiple cases to P multiples.
Deal with the P multiple cases.

6.)
Sophie Germain's plan was to combine these two. To cut the Gordian knot with one slash.
With hindsight, it was too grand to be true. But her idea was amazing:
She turned the first part, the reduction to the P multiple cases into an instantaneous self elimination of the second part, the P multiple cases themselves. Namely:
Suppose we can find infinite many P_1 , P_2 , . . . for every single p, that for every p-Fermat triple a , b , c , every P_1 , P_2 , . . . must divide one of the a , b , c bases.
Then we are finished at once. Indeed:
The dividers of thee numbers a , b , c when combined are merely finite many.
What's more, she had quite a concrete idea what these P_1 , P_2 , . . . should be for any p.
Namely, some of the $2 k p + 1$ prime numbers.
Obviously, there are infinite many $2 k p + 1$ numbers for every p.
Not obviously at all, we can assume that there are infinite many primes among these.
But this is still not enough. We have to screen these even further. Only some of them qualify, even as candidates to be P dividers. That is, forming remainder equations to P, so that the 0 exclusion makes the Fermat solutions already impossible among these remainders.
The plan failed. Not only the P division could not be forced, but it turned out that there are only finite many such P candidates for a given p. What remained is a reversal, that is a p division guaranteed from a single existing P with three conditions.
The obvious condition is the original goal, that P must divide a member. In other words, among the P remainders, all Fermat triples must use 0. The second condition is that P is prime too.
The third crucial condition was stumbled on by Germain's perfect instinct, connecting p with these remainders.
This theorem is far from the grand solution but it is still a useful tool for reduction, if a P with the three conditions can be guaranteed. As I said Germain knew that some of the $2 k p + 1$ primes are the P-s and yet the first two mentioned conditions and the crucial third that she stumbled upon don't require this $2 k p + 1$ form.
A second theorem of Germain proves that in the particular case, if $P = 2 p + 1$ is a prime, then it at once satisfies the two other conditions (beside being prime).
She also knew that $P = 8 p + 1$, $10 p + 1$, $14 p + 1$, $16 p + 1$ being primes, are also qualifying, but the exact proofs were given by Legendre.
The missing $6 p + 1$, $12 p + 1$ are not accidental. They can never qualify as P.
The reason why only such $2 k p + 1$ form primes can qualify as P, can be seen easily.
This Form Restriction Theorem will be shown right after her second theorem.

Basic Facts of All Remainders to a P Prime

As we saw, the power remainders are not all possible values, that's why sometimes we can claim impossible triples. To examine these, first we have to look at the original non powered, that is full remainders $1 , 2 , 3 , . . . , P - 1 , 0$.
The fundamental fact is that if P is a prime then multiplying these with each other, we can only get 0 if 0 itself is multiplied. That is: $r , s \neq 0 \rightarrow [r s] \neq 0$.
This is so, because $r , s < P$ so by Unique Prime Factorization, $[r s]$ can not be P.
The consequence of this is that an $r \neq 0$ remainder multiplied by two different s , t can not become the same: $r \neq 0$, $s \neq t \rightarrow [r s] \neq [r t]$.
Indeed, suppose $s < t$ then $[r s] = [r t]$ would mean $[r (t - s)] = 0$. But, $r \neq 0$ and $t - s \neq 0$.
The consequence of this is that multiplying r with all possible $1 , 2 , 3 , . . . , P - 1 , 0$ remainders, we get P many different results. Some we know for sure, like $r \bullet 1 = r , r \bullet 0 = 0$.
But that's not important now, rather that we have P many of them.
Indeed, this means that we must obtain all possible remainders as results. So:
Every t remainder can be obtained from an $r \neq 0$ with a suitable s as: $t = [r s]$.

In short, division can be defined as this suitable s: $s = \left[\frac{t}{r}\right]$

As we see, just like among normal numbers, the $r \neq 0$ was the condition of having a division.

The big difference is that to calculate $\left[\frac{t}{r}\right]$ is not possible easily, like among numbers.

Multiplication was quite simple, we merely have to watch the overflow.
Division is mostly a trial and error game.
Already, the product values with a fix r are pretty erratic due to the overflow.
Division is even more unpredictable. But, it does exist uniquely.

The basic concept to understand the theorems of Sophie Germain is the
"P-list of a p power sequence" abbreviated as $\{p : P\}$ and defined as follows:

$1^p , 2^p , 3^p , \ldots$ is a p power sequence.
The Fermat triples in it are three members A^p , B^p , C^p so that $A^p + B^p = C^p$.
We already knew this. Rather our belief that these can't exist if $p > 2$.
Now, instead of this problem, lets regard the remainders of every member of the p power sequence to P. That is : $[1^p] , [2^p] , [3^p] , \ldots$
We can be sure that the P-th element $[P^p] = 0$. In fact, if P is a prime, that's the first 0.
Most importantly, after this 0, everything repeats. Indeed:
$[(P+1)^p] = [1^p] = 1 , [(P+2)^p] = [2^p] , \ldots$
So knowing the beginning, before 0, we know everything.
Of course in this beginning segment some remainders may have repetitions.
So our $\{p : P\}$ list is simply them but listed only once that is as a set.
For simplicity we list them in increasing order but this is just a practical visual choice.
Lets see for example how $\{3 : 7\}$ arises! That is first listing the full remainder set, then the p powers, then the P remainders and finally the actual list.

1 , 2 , 3 , 4 , 5 , 6 , 0

1 , 8 , 27 , 64 , 125 , 216 , 0

1 , 1 , 6 , 1 , 6 , 6 , 0

1 , 6 = $\{3 : 7\}$

The most obvious fact is that 1 and $P - 1$ must always be in $\{p : P\}$.
The 1 is obvious and for $P - 1$ observe : $[(P-1)^p] = [M\,P - 1] = P - 1$
Indeed, the powers of $(P - 1)$ when calculated will have members all containing P except the last $(-1)^p = -1$.
This same argument shows that in general too, if r is in the list, then so is $P - r$.
Indeed, if r came from a B base, that is as $r = [B^p]$ then,
$P - r = [(P - B)^p] = [M\,P - B^p] = P - [B^p]$
Thus, our example above was truly a minimal list.
The multiplication rules of the full remainders will get through to the powers, because:
$[r\,s] = t \rightarrow [[r^p][s^p]] = [t^p]$. In spite of this, many of the full remainders collapse into one common value. But non 0 remains non 0.
So if r , s , t denote remainders in the list, and P is a prime, then still remains true that:
$r \neq 0 , s \neq 0 \rightarrow [r\,s] \neq 0$ and
$r \neq 0 \rightarrow \left[\frac{t}{r}\right]$ exists, that is, for every t there is an s so that $t = [r\,s]$.

Knowing that 1 and P – 1 are always there and non 0, then $\left[\frac{1}{P-1}\right]$ is always there too.

And indeed, in our example above, $\left[\frac{1}{6}\right] = 6$ was because $[6 \bullet 6] = 1$.

The crucial next step is defining Fermat triples in lists as: $[r + s] = t$.
This itself can obviously be written as $[r + s] - t = 0$ or $[r + s - t] = 0$
But the $P - t = t'$ complement is in the list too, and we can add a P to the remainders so:
$[r + s + P - t] = [r + s + t'] = 0$. In reverse too, any combination of sums or differences from three remainders giving a 0 actually mean a Fermat triple.
In these triples, we obviously must allow repeated use of same remainders, because an r could come from different numbers. If we allowed 0 to be in the list too then we could have always trivial triples by simply using $[r + 0] = r$ or $[r + 0 - r] = 0$ for any r in the list.
With our exclusion of 0 from the list to find 0-less triples is quite hard even if they exist.
Both by $[r + s] = t$ or by $[r + s + t] = 0$, we still would have to go by trials.
Luckily, there is a trick to find these triples much easier:

Observe that for an $s \neq 0$, there is its $\left[\frac{1}{s}\right]$ reciprocal pair. That is, a u so that $[s\,u] = 1$.

Also, $[r + s] = t \rightarrow [r\,u + s\,u] = [t\,u]$, that is $[r\,u] + 1 = [t\,u]$.
These $[r\,u]$, $[t\,u]$ can not become 0 either, so we found two consecutive non 0 remainders.
But in reverse too, having such r , r + 1 non 0 consecutive remainders at once implies:
$[(r + 1) + (P - 1)] = r$, that is a zero-less Fermat triple.
So not having Fermat triples is the same as not having consecutive elements in the {p : P} list.
This is the major condition of Sophie Germain's theorem. This was the original vision in reverse.
Then she stumbled upon the extra condition to make the P to p direction stick.
Namely, this condition is that the {p : P} list should not contain p either:

<u>Sophie Germain's First Theorem</u>

If p and P are primes and {p : P} does not contain p nor consecutive members,
then $a^p + b^p = c^p$ implies that p divides one of a , b , c.

The proof boils down to two lemmas:
1.)
If a q prime divides both $a + b$ and $a^p + b^p$ or both $c - a$ and $c^p - a^p$ or both $c - b$ and $c^p - b^p$ then q is p. So thus p divides $a^p + b^p = c^p$ or $c^p - a^p = b^p$ or $c^p - b^p = a^p$.
If there is no such q, then $a + b = u^p$ or $c - a = v^p$ or $c - b = w^p$.

2.)
If $a^p + b^p = c^p$ then:
This second option of no q can not stand in all three cases, that is for $a + b$, $c - a$, $c - b$.

First of all, 1.) and 2.) imply the theorem at once. Indeed, the first options each guarantee that p divides c^p or b^p or a^p and thus, also c or b or a.

Now we prove 1.). Observe the following identities:

$$c^p = a^p + b^p = (a + b)\,(a^{p-1} - a^{p-2}\,b + a^{p-3}\,b^2 - a^{p-4}\,b^3 + \ldots - a\,b^{p-2} + b^{p-1})$$

$$b^p = c^p - a^p = (c - a)\,(c^{p-1} + c^{p-2}\,a + c^{p-3}\,a^2 + c^{p-4}\,a^3 + \ldots + c\,a^{p-2} + a^{p-1})$$

$$a^p = c^p - b^p = (c - b)\,(c^{p-1} + c^{p-2}\,b + c^{p-3}\,b^2 + c^{p-4}\,b^3 + \ldots + c\,b^{p-2} + b^{p-1})$$

If q divides $a + b$ then $a + b = m\,q \;\rightarrow\; b = -(a - m\,q)$. Putting this into the second factor:

$$a^{p-1} + a^{p-2}(a - m\,q) + a^{p-3}(a - m\,q)^2 + a^{p-4}(a - m\,q)^3 + \ldots + a\,(a - m\,q)^{p-2} + (a - m\,q)^{p-1} =$$

$$a^{p-1} + a^{p-1} + m_1 q + a^{p-1} + m_2 q + a^{p-1} + m_3 q + \ldots + a^{p-1} + m_{p-2} q + a^{p-1} + m_{p-1} q =$$

$$p\,a^{p-1} + M\,q$$

If q divides this too, then it must divide p or a^{p-1}. But this second can't happen because q would divide a too and since it divides $a + b$ it would divide b too. But a , b are relative primes.
So q must divide p, that is the same as p.
If there is no such q then the two factors are relative primes, so both have to be p powers:
$a + b = u^p$ and the second $(a^{p-1} - a^{p-2}\,b + \ldots + b^{p-1})$ factor is x^p.

The second case is a bit different.
$c - a = m\,q \;\rightarrow\; a = c - m\,q$. Putting this into the second factor there:

$$c^{p-1} + c^{p-2}(c - m\,q) + c^{p-3}(c - m\,q)^2 + c^{p-4}(c - m\,q)^3 + \ldots + c\,(c - m\,q)^{p-2} + (c - m\,q)^{p-1} =$$

$$c^{p-1} + c^{p-1} + m_1 q + c^{p-1} + m_2 q + c^{p-1} + m_3 q + \ldots + c^{p-1} + m_{p-2} q + c^{p-1} + m_{p-1} q =$$

$$p\,c^{p-1} + M\,q$$

So again, $q = p$ or if there is no q, then:
$c - a = v^p$ and the second $(c^{p-1} - c^{p-2}\,a + \ldots + a^{p-1})$ factor is y^p.
The third case is identical, except a replaced by b. So if there is no q, then:
$c - b = w^p$ and the second $(c^{p-1} - c^{p-2}\,b + \ldots + b^{p-1})$ factor is z^p.

Now we prove 2.) by showing that if $a^p + b^p = c^p$ and all three first options were true in 1.) , then p would have to be in the $\{p : P\}$ list.
$a^p + b^p = c^p \;\rightarrow\; [a^p] + [b^p] = [c^p]$ and so the $\{p : P\}$ list having no triples means that one of these must be 0, that is P must divide one of a , b , c.
If it is c then:
P divides $2\,c = (a + b) + (c - a) + (c - b) = u^p + v^p + w^p \;\rightarrow\; [u^p] + [v^p] + [w^p] = 0$.
If it is a then:
P divides $2\,a = (a + b) - (c - a) + (c - b) = u^p - v^p + w^p \;\rightarrow\; [u^p] - [v^p] + [w^p] = 0$.
If it is b then:
P divides $2\,b = (a + b) + (c - a) - (c - b) = u^p + v^p - w^p \;\rightarrow\; [u^p] + [v^p] - [w^p] = 0$.
In either case, again the $\{p : P\}$ list having no triples means that one of
$[u^p]$, $[v^p]$, $[w^p]$ must be 0.
In the first case, it has to be $[u^p]$, in the second it has to be $[v^p]$ and in the third, $[w^p]$.
Indeed, just showing the first case, if it were $[v^p]$ or $[w^p]$ then P would divide $c - a$ or $c - b$, but since P divides c, this would mean to divide a or b too, contradicting relative primeness.
Continuing again with the first case:
P divides $u^p = a + b$, so $a + b = M\,P \;\rightarrow\; b = -(a - M\,P)$
Putting this into the second factor x^p as we did for the q case, we get x^p as:

$p\,a^{p-1} + M\,P$ and so $[x^p] = [p\,a^{p-1}]$.

But a^{p-1} was also the last member in y^p, the second factor of the second case.

The other members all contain c, which is a P multiple, so $[p\,y^p] = [p\,a^{p-1}]$.
Thus, $[x^p] = [p\,y^p]$. And here $[y^p] \neq 0$ because $[x^p] \neq 0$ either, since x^p and $a + b$ are relative primes and P divides $a + b$. Thus, we can divide $[x^p]$ with $[y^p]$ and so:

$$\left[\frac{[x^p]}{[y^p]}\right] = \left[\frac{[x]^p}{[y]^p}\right] = \left[\left[\frac{[x]}{[y]}\right]^p\right] = p \quad \text{and so} \quad p \quad \text{is in the list.}$$

Sophie Germain's Second Theorem

If p and $P = 2p + 1$ are primes then they satisfy the conditions of the First Theorem, That is: p or consecutive non 0 elements can not be in $\{p : P\}$.

$\{p : P\}$ contains the possible $[B^p]$ values and we can tell these easily by using Fermat's Little Theorem for the $P = 2p + 1$ prime. It says that $[B^{(2p+1)-1}] = [B^{2p}] = 0$ or 1.
The 0 value means that P divides B.
The 1 value means that P divides $B^{2p} - 1 = (B^p)^2 - 1 = (B^p + 1)(B^p - 1)$.
So $[B^p] = 0$ or 1 or $P - 1$.
None of these can be p so it can not be in $\{p : P\}$.
The other condition is equivalent to that there are no zeroless Fermat triples in $\{p : P\}$.
And indeed $r + s + t = 0$ is impossible with using the 1, $P - 1$ values.

Form Restriction Theorem

If P is prime and $p < P - 1$ are relative primes then all $1, 2, \ldots, P - 1, 0$ remainders are in $\{p : P\}$. Thus p is there too, so the condition of p not being there fails.
So, to satisfy this condition, $p < P - 1$ must have some common factor.
Since p is prime and $P - 1$ is even, this can be only an even $2kp$ multiple of p.
So, $P - 1 = 2kp$ or $P = 2kp + 1$ must be.

Enough to show that $1, [2^p], [3^p], \ldots, [(P-1)^p], 0$ are all different because then these being P many, all values will appear. Of course enough to show that the non 0 or 1 ones are different because these can only appear once anyway.

$[r^p] = [s^p]$ implies $\left[\left[\frac{[r]}{[s]}\right]^p\right] = 1$.

So enough to show that $[r^p] = 1$ with $r \neq 1$ can only be if p and $P - 1$ have common factor.
Lets fix an r and look at the different possible exponents that make such 1 remainders.
Obviously if $[r^k] = [r^n] = 1$ then $[r^{k+n}] = 1$ and with $k < n$, $[r^{n-k}] = 1$ too.
Thus all possible exponents are merely the multiples of the m minimal, including $p = i\,m$.
But by Fermat's Little Theorem $[r^{P-1}] = 1$ so $P - 1 = j\,m$ too.
Thus indeed p and $P - 1$ have the m common factor.