Godelian Encryption and Goldbach's Conjecture

Copyright © Paris Rose (s.) Miles Brenden
Albuquerque, NM, United States of America
p.roses.mb@gmail.com

February 18, 2020

Abstract

This paper outlines an idea for an unbreakable encryption-decryption technology within it's entitled difference of *quotient* of (a) methodology suited to and situated on modular relationships. Based on a Godelian concept of emptiness, the dependency on the Goldbach Conjecture is a stated to which a proof is preliminarily afforded or dis-afforded within the mathematical structure of emptiness of *retractile* or *reductive* proof's; to the advantage of the pre-text of leverage of the stochasticity of a variety of homological err and congruence. The co-terminal relation of two modular relations for in that of power to exponentially founded Fundamental Theorem of Algebraic Exponent's advantages the shrinking of an informational capacity requirement to the leverage of the pre-text of diminishment of algebraic and geometric (ray) computational exponents (of-a-certain) logarithmic compressibility on a conventional binary machine. What seems to be 'stripped' or forgotten is the combinatorial re-assortment of a 'dictionary' on that of the prime-modulo enumeration in Godelian pre-scriptive prowess. What is not lost or 'spent' is the afforded gesture that a 'hidden' and 'uncontainable' lamentation at number-series-reductive lemma structure cannot-be-taught; but, must be-learned. The essential idea conjectured at is that if there does not exist a general solution to Goldbach's Conjecture there would exist a solution to Fermat's Last Theorem, and by a-contractual contradiction since it is known that Fermat's Last Theorem has no solution via preliminary works of other's [Et. Al.], Goldbach's Conjecture must be certain in it's derviational certainty & true (within a certain understated context) herein to an existence proof via Godelian emptiness. The demonstrative ideal is to that of the geometric quotient that of a radical free nomenative declaration; that -statedly- that of **one ray** by contractual reduction is reducible from a two (**2**) dimensional enfolding to a radical free (**1**) and (**0**) dimensional ever diminishing exponent by any third (**3**) bi-inclinic ray. From here, an algorithm is deduced that is generative of an unbreakable encryption methodology (todo's); providing the root clause of data supremacy and data encryption; standardization of compactual relations of *an-infinitive nature* and of it's understated recombinatorial addressibility & assembly. Compactual binary space partition(s) are therefore reducible to at most (**5**) elements; (to be depicted as earth, air, fire, water, and wood) to which is the free data right of a simplicially connected/disconnected and (**re**)-establish(-**able**)ed flow of/and regularization concept layer analogous to free radical prime bases of geometrically induced quasilinear relations of **5**th order.

Necessary Preliminaries

Goldbach's Conjecture states that **every** even (e) can be expressed as a sum of two primes with $e \geq 6$ (to be understood as the number six); a number once-off the quotient of 20; for in light of two and three half-in intimating no connective to their subsidiary power and modular relation (an alternative number-theoretic proof).

Fermat's Last Theorem states that (as a hypothesis) there are no solutions in integers to the following equation:

$$x^n + y^n = z^n \tag{1}$$

Infamously printed and re-printed on shirts and diplomas; textbooks; and menus... For $n \geq 3$ and n a prime (as a subsidiary clause) it is sufficient and plausible ($\&$ therefore) general enough to illustrate that there are no free quotient bases to what may be considered as two (or or as three) numbers to which a number generative to a power may satisfy this relation in the range of the surrounding context of algebraic numbers for that of the integers. Due to the Fundamental Theorem of Algebra; a consequence holds true: no two numbers separated by two which are of a counting (or therefore of a carry) are one-(**un**-)separated. Therefore; to a reductive lemma; there can be no numbers in the integer sequence Z of which satisfy the 'Master Theorem' of this paper; and for which a modular and power equivalence inhibits a property of their disinclusion or prohibition of inclusion of three compactual definite clauses; that of additivity and subtraction to which a solution is known.

This is a consequence of the one to which a counting by one must raise the distance between the metricity of the alternative addition (in the co-adjoint measure) less than a quotient; hence by the triangle inequality; there are no two numbers larger than three which will satisfy that of a diminishing proportion to the complete difference in the right hand side and one of the prefactors to the left. No solution can therefore be afforded to Fermat's Last Theorem. Alternatively; that of a quotient geometric base in modular arithmetic for all primes is separated by *at-least* two or more for that of all primes greater than three; to which no x or y (non-exclusively) can be found to agree with a difference in that of a modular reduction. In power and modular relation it is therefore uncontentious to a theoretic 'mitosis' of numbers reasoned herein in relation to the Fundamental Theorem of Algebra $\&$ that there be an equivalence of number 'details' in that of the similitude of the right hand side under loss of one of the factors of the right hand side from the left to ***a subtraction*** in reciprocity to addition vis-a-via the right hand side. Hence; initially, our formation is that: **no radical free basis exists** to that which would impute or implicate that of a modular equivalence of these two sides of (Fermat's Last Theorem) in that of primes. Hence natural numbers do not afford any solution to Fermat's Last Theorem; $\&$ this theorem is true. There are no two (***mutual***) solutions in n greater or equal to three (**3**); for the same reason that no (**2**) primes are unseparated by *less* than two (**2**); afforded by the fact that for any x y or z greater than or equal to three (**3**) ***a modular equivalence is prohibited.***

The equation:

$$p^m + q^n = l^n \tag{2}$$

Pell's equation, however possesses modular in-equivalence in power and base in odd $\&$ even; therefore an infinity of potential solutions in the natural numbers. We will find this fact striking in retrospect when we consider $m \pm 1$ with the other numbers ***hypothetically*** fixed.

Goldbach's Conjecture

Given that an even is expressible as $e = 2k$ ***with*** k even or odd, the number e is decomposable into two (***new***) numbers: $k - r$ and $k + r$, where $2k$ is as a given equivalent to e, and $a = k - r$ and $b = k + r$ are numbers given; equally positive and negative with respect to the residual of $\pm r$ modulo k.

We now arrive at the major consequence which must be shown to prove Goldbach's Conjecture:

Conjecture: ***What must be essentially shown is that two numbers*** $a = k + r$ ***and*** $b = k - r$ ***modularly implicate the existence of two primes*** c ***and*** d ***to which sum to*** e. ***It is reasoned that the 'hint' is that by contradiction, if they did not exist, there would be a solution to Fermat's Last Theorem.*** This is the connection to Fermat's Last Theorem.

Reasoning

Let $a = k+r$ and $b = k-r$ be the numbers under summation to an even, for clearly $k+r+k-r = 2k = e$. Now, given there is no solution, let $c = a^n$ and $d = b^n$ be two new numbers taken to the same power, a prime n. Note that $c + d = (k + r)^n + (k - r)^n \equiv 2k = e \bmod n$ for all primes n and numbers (k, r), by $(k \pm r)^n - k \mp r = 0 \bmod n$ for all primes n and all numbers (k, r, e) since the contractual ***alternation*** of un-individuated combinations sum to a residual algebraically of remainder 0 comparative to $2k \pm 2r$. Now it is understood from before that c and d added are equivalent to an even e mod n, a prime. Furthermore the quantity $c + d = (k + r)^n + (k - r)^n \equiv 0 \bmod e$ for all (r, n, e) by the this alternating equal and opposite modulo residual of $\pm r$ on both terms (to which the number fits a congruence in it's 'end term's - Gaussian distributed via the binomial theorem to $e^- = 2k \pm 2r$). Now it is understood that c and d added equal 0 mod k. One could critique that e and e^- are un-necessitated; but indeed we have **two** strict in-equalities demanding of an answer; therefore we require the ambiguity of $2k \pm 2r$ to be stated declaratively. As a result we have two conditions, for which a statement suffices to prove Goldbach's Conjecture.

If there were no two primes for the numbers a **and** b then for some sets of $(a, b) \bmod n$ these numbers would have an equivalent composite base ***expression*** and under summation would be equivalent to 0 under mod n; the result of which is a prime equivalence by letting $z^n = m$ with m a prime and admitting a solution to Fermat's Last Theorem. Only with these as prime numbers (a, b) is it true that for all n they will be universally equivalent to the even e modulo n when reasoned that e^- holds (**2**) inequalities - since there are two given independent restrictions on their constraints and the ***system*** is exactly-determined. Otherwise; Fermat's Last Theorem fails to hold true as possessive of no solution. Therefore as far as qualitates that of structural composite numbers of even and odd ***with an overlapping integer***; there must be an even to a **and** b. This is provable as otherwise we can choose a number z to a power n, and a solution to Fermat's Last Theorem appears with equation 1. Additionally for the second modular equivalence to 0 to hold true, there must be a prime representation for a and b. **For if there were no prime representation**, there would be a composite structure to c and d (herein taken independently established) as not primes wherein with mod k, ***an odd***, and certain representations would be composite but have no equivalency to 0; therefore we could take $a = k + r + t$ and $b = k - r \pm t$ and produce a solution to Fermat's Last Theorem; as up-to modular and power equivalence the Fundamental Theorem of Algebra would be satisfied.

Finally, by the Fundamental Theorem of Algebra, the modular equivalency for all n implies that this extends to all composite numbers (forin here we have included the composite's with an overlapping set of power and modular integers and those non-overlapping), and Fermat's Last Theorem applies to all numbers. Hence the prime prime decomposition of an even e is guaranteed *when it is considered it is the only case that remains.* This may remain as evidence to the contradiction however only suffices to impute that there is another direction in which to take an *actual* existence proof - however it is plausible from what we know of other additional areas of mathematics.

Declaration

Master Theorem: *The relationship of evens e to primes n is bi-directional in that the summation of any two primes to any two powers is modularly equivalent to an even f modulo prime m as powers, and moduarly equivalent to zero* (**0**) *modulo this even e.*

To that of what otherwise is a compositely shared prime prime enumerability or in return under composition of an algebraic factoring of composite odd's; that of either of the two above conditions impose by that of Fermat's Little Theorm that of a relation of either inclusion to prime residual modulo 0 to which the odd is displaced by one 1 when equation 2 is taken into consideration. For inclusively the relation of but their structure proves to that of a 0 or $2k$ an even relation with pure composites of either given restriction on composites; to which k in that of the relation is but displaced by that of 1. Hence; the delimitation of that of the residual r under either relation to an odd remainder of a or b is the clue that when $m \pm 1$ is taken to exist; *there exist exactly two* (**2**) *prime numbers to which add to the even e for the reason that Pell's equation holds an infinity of solutions when m is displaced by 1 but **not** when $m = n$ for there are no solutions to Fermat's Last Theorem.* Therefore the return of that of one even and one odd in (m, n); a remainder in mod n is *the* signature of displacement by one; and by that of reduction of alternation of $\pm r$ on that of odd $\&$ even; the relation of that of the above reciprocity is that an enumeration of delimitation as expression of the disinclusion of a displacement upon equation (2) *is the given that there is a solution to Goldbach's Conjecture*:

$$a + b = e \qquad \forall \qquad e \qquad (a, b) \in P \tag{3}$$

In alternative terms; that of the inclusion of a prime base n admits even and odd m to which p, q, and l exist; and to which in either relation under modular equivalence by one; the original 0 and $2k = e$ hold capacity for that of two prime's under reduction to the statement (2). Pell's equation therefore yields a displacement to that of the *non-exclusive* relation of inclusion of one differential algebraic 'step' on that of successive generations of modular base and power enumeration to which in either that of k or r there is a prime in *both* (vis-a-via the earlier reasoning of: *'if there were no prime representation'*) illustrated. For then in odd; we locably find that under relation of a base even a displacement of k with $k \pm r$; the 'odd' relation remains that of a modular equivalence under which substitution in Fermat's Little Theorem produces from Pell's equation (**2**) solutions in primes given that the prime enumerability of evens unto their relation remains closed to even or odd and an odd minus an odd is even; to which *as there is no general solution to Pell's equation in $m \pm 1$ there-must-be exactly one solution in prime's in addition to an even $e \geq 6$ with m fixed. Therefore Goldbach's Conjecture is true, as statement* (**3**) *and* (**2**) contain at least two solutions *in relation to every prime non-excepting* (**2**).

Therefore all communsurate odd relations include and cover all evens for all subsidiary composite even's, composite odd's, and prime number enumerations when it is assumed that **two** prime relations prime adjacency sum to any given even. Goldbach's conjecture is therefore proven with the positivist's existence necessitated; and demonstrably; the necessity of that of there being two primes is identified as the contrapositive of Fermat's Last Theorem; it's conjecture the extension to a graph of the nature of De'Abraham De'moivre; that by inclusion of the strong analytical proofs of the Fermat's Little Theorm and the Fundamental Theorem of Algebra ***this is a Godelian Proof***; to which is outside the given Peano Axiom's of number theortic truth valuation. We can see that essentially there is no solution to Fermat's Last Theorem precisely because there is always a solution to Goldbach's Conjecture and vice versa, for the reason that if the above statement does not hold true, either composite structures or non prime even numbers are present which misconstrue the exact equivalence $\&$ inequivalence relation of these as theorems. Therefore, if a solution to Fermat's Last Theorem exists, a solution to Goldbach's Conjecture does not exist *for a certain integer* q *and may remain hidden*, and by contradiction, since no solution to Fermat's Last Theorem exists, there is always a solution to Goldbach's Conjecture and as the above bound is set by the n on k as ≥ 3 by ruling out mutual evens and in summation to an even. The solution is that: for all evens, $e \geq 3 + 3 = 6$ there exists a unique prime-prime reduction under summation. Hence this statement produces the consequence that primes so existing ensure a solution to Goldbach's Conjecture, and which is true as there is an exact fit to 'no lesser than two and no greater than three', because as turned around the existence of a prime ensure's the existence of an even. All other representations are modularly equivalent to another set of numbers as primes under Pell's equation when $m^{-} \neq m \pm 1$; therefore any even e is expressible as a pair of primes. For if there were no prime prime representation a modulo condition would admit a solution to (**1**).

Godelian Encryption

A Godelian number sequence is a number for instance such as:

$$N = 2^p 3^q 5^r \tag{4}$$

The essential idea this encryption amounts to is:

Essential Idea: *Given the numbers* (p, q, r) *is it possible to design an encryption method such that no modular decomposition will render any document or system of communications undecryptable given the lack of factorability of the three numbers* (p, q, r)*?*

Since Godel's Theorem means that certain arthimetic truths are neither provable as True nor False, and are hence undecidable, and that this is true in context because every axiomatic system contains these.

To devise this encryption program, consider as a given the primes (p, q, r) as generative of the additional primes:

$$P = p + q - r \qquad Q = q + r - p \qquad R = r + p - q \tag{5}$$

If these are in turn prime, it must be noted first of all that per Fermat's Little Theorem:

$$a^p - a \equiv 0 \qquad modulo \qquad p \tag{6}$$

Where p is a prime.

From this consider the mapping:

$$C_n^{(p,q,r)} \qquad mod \qquad (P,Q,R) \to C_n^* \tag{7}$$

This mapping is invertable because via properties of Goldbach's Conjecture the primes P are identified with a ***group***. Because the relationship between the keys and the sequence of (C_n) is not decipherable by exterior means via a consequent ***non-commutativity***, it is as a given a relationship that the deciphering by primitive means is as unpredictable as the sequence of primes themselves. To that of what is aforementionedly a limitation of the regress we impose from otherwise that of non-exclusive exceptional inclusion; the mean of 1 otherwise inclusive number theoretic subset of relations; determines that of a graph notion to 'coloring' $\&$ combinatoric rules remains hidden by imposition of limitation of co-extensibility of the free relation of exceptionable enumeration under separation of the operations of algebra. This was the exceptional inclusion of the capability of re-arrangement of Godelian emptiness.

For instance consider that:

$$a^p a^q = a^{p+q} \tag{8}$$

As these are separately not factorable and the sequence of modular relationships is unpredictable as the primes are, neither is their product as a^p and a^q, therefore p and q added or apart are unpredictable in their modular inverse *under group theoretic contrasts*. Then, since the inverse requires the third of any set of primes for two, it is **impossible to decipher the key or engram** by the uniqueness of the prime mappings and the lack of divisibility in discovering a pair from one prime or a prime from two. The modular relationship is unique so it a document is decipherable by the proper encryption key's, but is hidden *in the structure of evaluation and combinatorics of a singular machine state*, therefore, in the lack of divisibility of the three primes as a mutual set for any one in comparison to any other two *un-locabilities*. As a result there is no algebraic way to discover the primes from a set of documents in relation to each other with any computational analysis or mathematical theory **in existence**. Note that Goldbach's conjecture can produce a prime prime relation for the auxiliary primes and evens. However, Goldbach's conjecture cannot be automated to discover a solution to this encryption *for no computer operationally situates through unpredictability alone two steps ahead*, and as a result this encryption is in general unbreakable. In addition, the order of the polynomial is at least with '*one-guess*' still a quintic, and in general has no common zero or solution for which an exact solution may be found in *Galois Theory*.

To note is that this process can be automated as an encryption and decryption based technology when there is co-extensibility of the bit-wide margin of the memory space to a channel or power; for that of what is incorporative of a stated residual quotient generated with each byte of **9** word legth is diminished to **7** and in that of **3** bit-wise width for then in an unseparated interstitial 2 modulo to the 7th power; therefore that of 128 refounded on a divisor of 3 plus 1 to which is 32 bit wide depth in 0 $\&$ 1 and 3 *as* (**5**) unseparated from 9 minus 7 $\&$ 3 to which is two heirarchical self-similar power and modulo statements of the Master Theorem. Any encryption based on this heirarchical re-assortment and dis-assortment pattern is thereforeas unbreakable as: **That as the fact that primes are not divisible by each other**. So, any ideal simplicial unitary gate system holds an identity to which is that a quotient of a radical normative valuation is it's congruence to two statements; one a connotative reflexive summative base rational and the other an indicated free decomposition into subsidiary orientably free exponent sources in base valuation. A number therefore suits a free radical idempotent reflexive inverse addition law over a manifold algebraic isolinear relation of unseparated quotient $\&$ super-valued numberless identity with it's base and power expression.

Conclusion

The Goldbach Conjecture can therefore be summarized as the modular arithmetic fitting inside the modular arithmetic; to which is 2 within 2. This is reducible from the lemma that equivalence of modular bases is assurred given there is a prime notational system of decomposition. The reduction is that two bases reduce alone from that of what is a prime within one. The system is therefore two radical to what is freely unheld of divisional quotient; to which there exists by it's element a factoring from what is a number by two; an even. Therefore even's reduce to exactly two primes; since either solution in '**m**' is identical (and even) to a homogeneous sum in integer's; to which there are only (1) and the number itself within an expression; the true identity of which is noticed for in reason that Pell's equation remains to contain exactly one solution only when either is a multiple of 2.

Therefore as $2 = 2$ under either reproducible iteration of summation; a solution is proven as valid; and sufficient for the additional reason (of necessity) that therefore as two exponent's agree; a radical Pell's solution exists (as this is known); & vis-a-via that:

1.) *There is an identity that there is no solution for what is* $m = n$.

2.) *There is exactly one solution when either is a multiple of* 2 *since the equation is identical with itself.*

3.) *That of* $m \pm 1$ *for all* **m** *prime, is even.*

For in light of consideration of the following; it is directly provable that any two prime's suffice for what is an equivalent even number. As to consider; by the mere impression of that of Fermat's Last Theorem; that unseparatedly taking *either* one of the x^n or y^n to a bearing of subtraction from z^n it is by the abject *missing* quotient (2) on that of what is a held separation of ≥ 1 that none; is the answer to that of prohibition of license to solution. For then in light of what is considered of the separation *under modulo proficiency*; that of at least the denomination is **1** comparative to an aliasing of their given contrast; then for what is a remainder; that of the indication of a suspect exceptionable clause to (2) two solutions; that remarkably there is at least 1 and 1 comparatively illustrated prime in the series of numbers within addition to an even e.

So; it is that with as for instance a stack of dominoes; however they are tilted and replaced in a *row* that the first assembly in *either* order will knock down all; but that of partial way through will only violate half. But for that of one prior that of occassion to a difference with numbers; that of a *secondary* dominoe will knock down within-addition a *first* (number-dominoes) that of **all** in dissimilarity to that of physically innate reality. This juxtapositioning is remarkable; for it is merely akin to an *illusion* broken.

Extension to Riemann Zeta Hypothesis

For then in what is reciprocal; that of two strips; one of which is the $1/2$ projection; and one of which is an annulus; the former a Moebius strip; when connected or disconnected to what are two imputations; that of exchange under a question:

Hypothesis: *It is the second professor to depart the room and exit if this is also the first to enter; otherwise it is the former alternative person.*

Problem: *Two professor's enter a room; and are beyond observation; to which then via introductions; one writes an equation or the other does; then one of the two erase the problem and leave the room after a sincere discussion. Who was the professor to erase the chalk?*

For in that of numbers; to what is imputed as to that of the above dominoes they come in two kinds with numbers; 'Transcripted,' and 'Detailed;' as to a regular dominoe of physical reality; and that of unordinary *number-dominoes* of which correlate with a ***Moebius strip.*** The difference is the same as the equation unwritten or written; but obviously there is a difference in the professor's; for they are individuals; to which human being's are. It is therefore the final word of mathematics that when thought of:

$$(\sigma_1 - 1)(\sigma_1 - 2)(\sigma_1 - 3)(\sigma_1 - 5)...\infty = F[z] \tag{9}$$

Contains even and odd relations of which are a sequence of dominoes; of ordinary and unordinary; to which are therefore freely the unheld room and it's chalkboard. The insistance therefore hold's that **their average** is $1/2$ to what is even divided by odd; to which is the imputation of the final consolidation of Goldbach's Conjecture; notably:

$$2 \quad \epsilon \quad G.C. \quad \forall \quad \frac{1}{2} \quad \epsilon \quad R.Z. \tag{10}$$

For the quotient free radical space of rational to irrational numbers is of a cardinality $\aleph_0$ comparative to $\aleph_1$. This connective is that were one to combine or separate the two hands of a dial on that of the *numbers*; a Moebius Strip and an Annulus would be combined or separated; to what is a top-or-bottom up teir folded relation of collapseability. Therefore all roots of the exceptionable point's of the Riemann Zeta function have a real part of $\frac{1}{2}$.

For in dear; what is a necessity of dearness to a scolding can be reprimanded to it's counterable fellow; for in a forewarned difference of apredictive entrapment by enquement of two deficit relations; theft; to what is then heretical under reversability of sense for in one half-space to another; therefore of (non')sense; the indication at $(@)$ two; is to notice of up-peer what is intimated by ontological befitment of barrierless opening to ardour.

That of befallment of non-preventability of theft but therefore by two from a top-teir; and one from it's then bottom relation; the accounting of which under prolate dissonance accords with via to topological execution of order the line-like apogetic minimal path of least resistance; therefore dissimilitudes in development to priority in executable limitation to re-stochasticity of reversable sense by difference of retromorphic intimation of their criminatory intention; and pure accounting by cross dissimilitudes of all known evidentiary items of offense to what is preparatory investigative tool of progression to standard law teir case and subsidiary structural detail.

Therefore it is that a sorting of item's to which are commutative or non-commutative among 2 the space is a quotient space of the line $\frac{1}{2}$; the median of what is included of a relation of their corresponding zero's; when reduced from ∞. That of a clear difference between the professors is outlined; they cannot hide theft of an idea or notion; and it is to exact correspondence that this case is answerable that the Riemann Zeta Hypothesis is true to an abject point; the **true** infinity!