Proof of a conjecture: Sum of two square integers can produce infinitely many primes.

Author: Debajit Das

ABSTRACT

According to Euclid's theorem there exist infinitely many primes in our numbering system. But the distribution of these prime numbers is so irregular that nobody knows the relation among all the primes. That is why; it has borne the brunt of so many conjectures. One of the vital conjectures is regarding the fact that sum of two square integers, obviously in combination with odd and even, can produce prime and composite both as physically observed. Now the question is whether the produced primes are extended up to infinity or not? I believe that I have been able to give a proof in support of this conjecture with the help of N-equation published in Aug-edition, Vol-4 of IJSER.

Keywords

N-equation, Natural constant (k), Inside factor & Outside factor, Partial & Non-repeating factor, Zygote elements, Zygote ratio (Z_r)

1. Introduction

Please refer my paper published in Aug-edition 2013, Vol-4 of IJSER.
N-equation has been defined as $(\alpha^2 - \beta^2)^2 + (2\alpha\beta)^2 = (\alpha^2 + \beta^2)^2$, where α, β are positive integers named as zygote elements. $(\alpha^2 \pm \beta^2)$ are known as zygote expressions which are conjugate to each other.
For α > β, the zygote ratio ($Z_r = \alpha/\beta$) divides the N-equation into two kinds of equations.
For $Z_r < (\sqrt{2} + 1)$ it is 1st kind & for $Z_r > (\sqrt{2} + 1)$ it is of 2nd kind. For a < b < c when c – b is in the form of $(2n - 1)^2$ it is 1st kind & when c – b is in the form of $2n^2$ it is of 2nd kind where n is a positive integer. This $(2n - 1)^2$ or $2n^2$ is called natural constant (k).
For a N-equation $a^2 + b^2 = c^2$ where a & c are odd integers, the prime numbers excepting two can be divided into two types. Those who belong to 'c' as a prime number can be said as type-2 and the rest can be said as type-1.
Any composite number that satisfies c contains all prime factors of 2nd type only.
The easiest way to recognize these 2nd type prime numbers is that when unit digit is 1 or 9 the 10th digit must be even and when unit digit is 3 or 7 the 10th digit must be odd. By digital analysis or otherwise it can be easily proved.
Another thing is to be noted that all though N-equation $a^2 + b^2 = c^2$ produces composite set intermittently but our concern is for prime set only i.e. gcd(a, b, c) = 1.
Any relation $N = a_1^2 + b_1^2 = a_2^2 + b_2^2 = \ldots\ldots.$ is obtained by virtue of N_s operation in between two elements that satisfy c of a N-eq.
With this refreshment we can proceed further.

2. If c_1 & c_2 satisfy c of a 1st kind N-equation $a^2 + b^2 = c^2$ under a particular value of natural constant (k) then c_1c_2 can also satisfy c of the same equation.

Consider any two elements c_1 & c_2 that satisfy c of the 1st kind N-equation as
$c_1 = \alpha^2 + \beta^2$ & $c_2 = (\alpha + p)^2 + (\beta + p)^2$ where α > β & $k = (\alpha - \beta)^2$.
Now, by Ns operation $c_1c_2 = \{(\alpha^2 + p\alpha) \pm (\beta^2 + p\beta)\}^2 + \{(\alpha\beta + p\alpha) -/+ (\alpha\beta + p\beta)\}^2$
$\Rightarrow c_1c_2 = (\alpha^2 + \beta^2 + p\alpha + p\beta)^2 + (p\alpha - p\beta)^2$ or $= (\alpha^2 - \beta^2 + p\alpha - p\beta)^2 + (2\alpha\beta + p\alpha + p\beta)^2$
For the first case $k = \{(\alpha^2 + \beta^2 + p\alpha + p\beta) - (p\alpha - p\beta)\}^2 = (\alpha^2 + \beta^2 + 2p\beta)^2$.
If it falls under same $k = (\alpha - \beta)^2$ then $\alpha^2 + \beta^2 + 2p\beta = \alpha - \beta$ or, $\alpha^2 + \beta^2 + 2p\beta + \beta = \alpha$ which is absurd.
For the 2nd case which term is greater not clear? Let us take both the cases.
$K = \pm \{(\alpha^2 - \beta^2 + p\alpha - p\beta) -/+ (2\alpha\beta + p\alpha + p\beta)\}^2$ & equating this with $k = (\alpha - \beta)^2$, we get
$2p = \alpha(\alpha \pm 1)/\beta - (\beta + 2\alpha \pm 1)$
Now $\alpha(\alpha \pm 1)/\beta$ will be integer when β is a factor of (α ± 1) as gcd(α, β) = 1 Moreover, $\alpha/\beta < \sqrt{2} + 1$ i.e. $\beta > (\sqrt{2} - 1)\alpha$ & p ≥ 0.
Then only c_1c_2 exists.
If β = 1 only accepted value of α is 2 & all other values of α will invite 2nd kind N-equation as because $\alpha/\beta > (\sqrt{2} + 1)$ for α > 2.
For α = 2 & β = 1, p = 0. It indicates $(2^2 + 1^2)$ & $(2^2 + 1^2)^2$ i.e. 5 & 5^2 both satisfy N-equation of $k = (2 - 1)^2$ i.e. k = 1
So, if c_1 & c_2 both satisfy c of a N-equation of 1st kind, c_1c_2 can also satisfy c again of the same equation subject to condition that the lower zygote element β must be a factor of (α ± 1) such that $\beta > (\sqrt{2} - 1)\alpha$ & corresponding p must be integer ≥ 0.

3. If c_1 & c_2 satisfy c of a 2nd kind N-equation $a^2 + b^2 = c^2$ under a particular value of natural constant (k) then c_1c_2 cannot satisfy c of the same equation.

Here, we can consider any two elements $c_1 = \beta^2 + \alpha^2$ & $c_2 = \delta^2 + \alpha^2$ under $k = 2\alpha^2$. Obviously, β, δ > α & say δ > β
Then by N_s operation $c_1c_2 = (\beta\delta \pm \alpha^2)^2 + (\alpha\delta -/+ \alpha\beta)^2$ having $k = 2(\alpha\delta -/+ \alpha\beta)^2$ or $k = 2(\beta\delta \pm \alpha^2)^2$.
Equating both with $k = 2\alpha^2$ we get either $(\alpha\delta - /+ \alpha\beta) = \alpha$ or $(\beta\delta \pm \alpha^2) = \alpha$
First one implies δ – /+ β = 1 which is absurd.
Second one i.e. $(\beta\delta \pm \alpha^2) = \alpha$ modifies the expression c_1c_2 as $\alpha^2.[1 + (\delta \pm \beta)^2]$ which are the composite sets of (a, b. c) with c.f. α^2 under the leading set of k = 1 or all the sets of $k = 2.1^2$

Hence, c_1c_2 cannot satisfy c for a particular value of k if the equation is already satisfied by c_1 & c_2.
It also implies that if c_1 satisfies c, c_1^2 cannot satisfy c. In general c_1^n cannot satisfy c again.

4. Every composite number that satisfies c of 2nd kind N-equation must contain at least one factor or one prime factor which does not satisfy c.

Let us consider a composite number $N = p_1^{n1}.p_2.^{n2}.p_3^{n3}$…… where p denotes prime, obviously of 2nd type, of a 2nd kind N-equation.
Now divide it into two parts P & Q such that N = P.Q
So, P, Q both cannot satisfy c. There exists at least one which does not belong to c which can be named as Outside factor (O_f)
Hence, proves the theorem.

5. Nature of outside factor (O_f) of a 2nd kind N-equation.

Say, c_1 satisfies c & $c_1 = \alpha^2 + \beta^2$ where $\alpha > \beta$ & $k = 2\beta^2$ and c_2 does not satisfy c & $c_2 = a^2 + b^2$ where $a > b$ & $k \neq 2\beta^2$.
Now, by N_s operation in between c_1 & c_2 we have $c_1c_2 = (a\alpha \pm b\beta)^2 + (b\alpha -/+ a\beta)^2$
If c_1c_2 satisfy c then either $|b\alpha -/+ a\beta| = \beta$ or $a\alpha \pm b\beta = \beta$
From first one with (+) sign, $b\alpha = \beta(1 - a)$ is not valid as LHS is positive integer & RHS is negative integer.
Hence, $b\alpha = \beta(a \pm 1)$ or, $(\alpha/\beta) = (a \pm 1)/b$.
From 2nd one, one is rejected on same ground & from other we get $(\alpha/\beta) = (1 + b)/a$ which is not acceptable as LHS > 1 & RHS < 1.
Hence, $(\alpha/\beta) = (a \pm 1)/b$. As $\gcd(\alpha, \beta) = 1$ we can assume $(a \pm 1) = p\alpha$ & $b = p\beta$.
Hence, $c_2 = a^2 + b^2$ modifies as $c_2 = (p\alpha \pm 1)^2 + (p\beta)^2$ & c_1c_2 satisfies c where p is even otherwise even-odd combination of zygote expression will be disturbed.
So, any zygote expression of c i.e. $c_1 = \alpha^2 + \beta^2$ for $k = 2\beta^2$ can produce infinite nos. of outside factors.
Any composite number of c is constituted either by O_f only or by the product of Inside factors (I_f) & O_f.
So, whatever prime numbers will be produced from c, they cannot constitute any composite number that will satisfy c.
For outside factor $Z_r = (p\alpha \pm 1)/p\beta = (\alpha/\beta) \pm 1/(p\beta)$ where $(\alpha/\beta) > \sqrt{2} + 1$ implies that Z_r may be $> \sqrt{2} + 1$ or may be $< \sqrt{2} + 1$.
Hence, Z_r may belong to 1st kind or may belong to 2nd kind.
While considering O_f, α should be considered right from β + 1 & then β + 3, β + 5. B + 7, ……. i.e. entire sequence of c where initial some portion is of 1st kind and then 2nd kind. 1st kind portion will behave as per property discussed in Heading-2 and 2nd kind portion will behave as per Heading-3.
Obviously, $\{(\beta + 1) + (n - 1)2\}/\beta < \sqrt{2} + 1$ or, $n < (\sqrt{2}\beta + 1)/2$ i.e. $n = [(\sqrt{2}\beta + 1)/2]$ where [x] denotes greatest integer of x & n is nos. of terms under 1st kind.
So, if we consider a sequence of c as $\alpha^2 + \beta^2$ where α = β + 1, β + 3, β + 5, …… , the sequence will remain under 1st kind up to $n = [(\sqrt{2}\beta + 1)/2]$ and then it will switch over to 2nd kind.

6. The outside factor for a 2nd kind N-equation cannot be repeated.

Let's consider two elements $c_1 = \alpha_1^2 + \beta^2$ & $c_3 = \alpha_3^2 + \beta^2$ satisfying c for a 2nd kind N-equation where $k = 2\beta^2$ & $\alpha_1, \alpha_3 > \beta$, also $\alpha_3 > \alpha_1$.
Suppose, $c_2 = a^2 + b^2$ is an outside factor having $k \neq 2\beta^2$ and a > b.
$\Rightarrow c_1c_2 = (a\alpha_1 \pm b\beta)^2 + (b\alpha_1 -/+ a\beta)^2$ & $c_2c_3 = (a\alpha_3 \pm b\beta)^2 + (b\alpha_3 -/+ a\beta)^2$
Now, if c_1c_2 & c_2c_3 both satisfy c then equating k we get:
Against c_1c_2, $(b\alpha_1 \pm a\beta) = \beta$ & $(a\alpha_1 \pm b\beta) = \beta$ & ignoring (+) sign we have $b\alpha_1 = \beta(a + 1)$ …….. (A) or $a\alpha_1 = \beta(b + 1)$ ……..(B)
Similarly, against c_2c_3 we have $b\alpha_3 = \beta(a + 1)$ ……… (C) or $a\alpha_3 = \beta(b + 1)$ ……… (D)
If (A) & (C) or (B) & (D) are true that implies $\alpha_1 = \alpha_3$ which is not accepted.
If (A) & (D) are true then $\alpha_1/\alpha_3 = \{a(a + 1)\}/\{b(b + 1)\}$ which is not accepted as LHS < 1 & RHS > 1.
If (B) & (C) are true then $\alpha_1/\alpha_3 = \{b(b + 1)\}/\{a(a + 1)\}$ which is accepted.
Say, $b(b + 1) = p\alpha_1 \Rightarrow b = \{ - 1 + \sqrt{(4p\alpha_1 + 1)}\}$ & similarly $a = \{ - 1 + \sqrt{(4p\alpha_3 + 1)}\}$
$\Rightarrow (4p\alpha_1 + 1)$ & $(4p\alpha_3 + 1)$ both must be square integer which is absurd.
Because, if $(4p\alpha_1 + 1)$ is a square integer say, I_1^2 then $(I_1^2 - 1)/4$ i.e. $p\alpha_1$ must be product of two consecutive numbers.
Similarly, $p\alpha_3$ must be product of two consecutive numbers. Both cannot be true unless α_1, p, α_3 are consecutive three numbers.
If α_1, p, α_3 are consecutive three numbers then α_1 & α_3 are to be two consecutive zygote elements i.e. either two consecutive odd or two consecutive even numbers and both of them cannot be expressed as product of two consecutive numbers simultaneously.

7. Total outside factor cannot be repeated but its partial factor can be repeated.

Let us consider an $O_f = (p\alpha_1 \pm 1)^2 + (p\beta)^2 = (a^2 + b^2)(g^2 + h^2)$ of the sequence $c = \alpha^2 + \beta^2$ having $k = 2\beta^2$ where a > b.
Now if the partial factor of O_f say $a^2 + b^2$ is present as a factor of an element that satisfies c, then $c_2 = (a^2 + b^2)(\alpha_2^2 + \beta^2)$ where $\alpha_2 > \beta$
Or, $c_2 = (a\alpha_2 \pm b\beta)^2 + (a\beta -/+ b\alpha_2)^2 \Rightarrow$ any one of $| a\alpha_2 \pm b\beta|$ or $| a\beta -/+ b\alpha_2|$ is β i.e. $| a\beta - b\alpha_2| = \beta$ & other cases are absurd.
$\Rightarrow \alpha_2/\beta = (a \pm 1)/b \Rightarrow a = q\alpha_2 \pm 1$ & $b = q\beta$. Hence $c_2 = \{(q\alpha_2 \pm 1)^2 + (q\beta)^2\}(\alpha_2^2 + \beta^2) = \{(q\alpha_2^2 \pm \alpha_2) \pm q\beta^2\}^2 + \{(q\alpha_2\beta \pm \beta) -/+ q\beta\alpha_2\}^2$.
$\Rightarrow c_2 = \{\alpha_2(q\alpha_2 + 1) + q\beta^2\}^2 + \beta^2$ ……… (A) & $|\alpha_2(q\alpha_2 - 1) - q\beta^2|^2 + (2q\alpha_2\beta - \beta)^2$ ……… (B)
From B we find $2q\alpha_2\beta - \beta \neq \beta$ & if $|\alpha_2(q\alpha_2 - 1) - q\beta^2| = \beta$ then $\beta = [-/+ 1 \pm \sqrt{\{1 + 4q\alpha_2(q\alpha_2 - 1)\}}] / (2q) = \alpha_2$.which is absurd.
(A) reveals the condition for repetation of a partial factor of an outside factor. The outside factor as a whole cannot be repeated.
$\Rightarrow$ every composite number of c must contain one factor (at least one prime from outside factor) which cannot be repeated. This can be said as non-repeating factor.

8. GCD of any two non-repeating factors is unity.

Let us consider two non-repeating factors with a common factor $(a^2 + b^2)(c^2 + d^2)$ & $(a^2 + b^2)(f^2 + g^2)$ where a > b, c > d & f > g.
$\Rightarrow (ac \pm bd)^2 + (ad -/+ bc)^2 \equiv (p\alpha_1^2 + \alpha_1 + p\beta^2)^2 + \beta^2$ and $(af \pm bg)^2 + (ag -/+ bf)^2 \equiv (q\alpha_2^2 + \alpha_2 + q\beta^2)^2 + \beta^2$
$\Rightarrow$ there exists following six cases.
$ac - bd = \beta$ ……. (A1), $ad - bc = \beta$ …….. (A2), $ad + bc = \beta$ ……. (A3)

af – bg = β …….. (B1), ag – bf = β ……… (B2), ag + bf = β ……..(B3)
Any one of (A) can be equated with any one of (B) and let us consider one by one.
A1 & B1: ac – bd = af – bg $\Rightarrow$ a/b = (d – g)/(c – f) $\Rightarrow$ a/b = d/c = g/f which is absurd as a/b > 1 but d/c, g/f < 1.
A1 & B2: ac – bd = ag – bf $\Rightarrow$ a/b = (c – g)/(d – f) $\Rightarrow$ a/b = c/d = g/f which is absurd due to same reason.
A1 & B3: ac – bd = ag + bf $\Rightarrow$ a/b = (d + f)/(c – g) $\Rightarrow$ a/b = d/c = f/(–g) which is absurd.
Similarly all the cases are found to be absurd. Even the ratio a/b = c/d = f/g is also not accepted.

Hence, the non-repeating factor is unique not only by magnitude but also with respect to its prime factors and all the prime factors are of 2nd type i.e. can be expressed as $x^2 + y^2$. With respect to a composite number of c, partial factor may be present at front or at back in the sequence of c.
It happens in all sequences of c i.e. $(\beta + i)^2 + \beta^2$ where i = 1, 3, 5, 7, …… & β = 1, 2, 3, 4, ……., when 2nd kind N-equation starts.

Hence, $x^2 + y^2$ can produce infinitely many primes.

9. If c_1 & c_2 that satisfy c of a N-equation have a common factor $q = a^2 + b^2$ then after N_s operation we have $c_1 = q(\alpha_1^2 + \beta_1^2) = f_1^2 + g_1^2 = f_2^2 + g_2^2$ & $c_2 = q(\alpha_2^2 + \beta_2^2) = f_3^2 + g_3^2 = f_4^2 + g_4^2$ where all zygote elements f_i, g_i are bound to be different subject to condition that gcd{(a, b) or (α_i, β_i)} = 1

From previous analysis under heading -8 we can easily conclude this theorem.

10. There exist infinitely many primes of type-1.

We have already classified two types of prime numbers. The first type of prime number P cannot satisfy the element ‘c’ of N-equation but 2nd type Q can satisfy the same.

Any composite odd number which can be defined as
$N = (p_1^{n1}.p_2^{n2}.p_3^{n3}…..).(q_1^{m1}.q_2^{m2}.q_3^{m3}…..)$, where p_1, p_2, p_3,……Є P and
q_1, q_2, q_3,……Є Q & all p_i , $q_i \leq (N/3)$ will be always in the form of $(\text{odd})^2 – (\text{even})^2$ when Σn_i = an even integer or $n_1 = n_2 = n_3 = …. = 0$ and in the form of $(\text{even})^2 – (\text{odd})^2$ when Σn_i = an odd integer. Obviously, 1st type is of the form 4x + 1 and 2nd type is of 4x – 1 where x = 1, 2, 3, ……
Let the first case is denoted by N_2 & second case is denoted by N_1.
$\Rightarrow$ N_1 & P are the symbol of composite odd & prime numbers that are capable of producing a relation $(\text{even})^2 – (\text{odd})^2$ and N_2 & Q are capable of producing a relation $(\text{odd})^2 – (\text{even})^2$.

This two type of odd composite elements N_1 & N_2 alternately come in our numbering system and when there is a break of continuity, the gap is filled up by a newborn prime number of respective category. It implies that twin primes are bound to be of opposite nature.
Type-1 category composite number (N_1) cannot be constituted by type-2 prime numbers (Q) only.
It implies that in between two consecutive composite numbers at least one must contain a prime factor of type-1 category.

Consider a number $N_2 = (Q_1Q_2Q_3…….Q_n).P_1^2$ where P_1 is the 1st prime of type-1 i.e. 3 and where Q_n is the nth prime & $0 < n < \infty$
Now, consider the number C = N_2 + 2.
If C is prime then it must be of type-1 > P_1
If C is composite then it must contain a prime factor of type-1 > P_1
Now, consider a number $C_1 = (Q_1Q_2Q_3…….Q_n).P_1^2\ P_2^2$ where P_2 is next to prime P_1.
Same logic can be established here also.
Hence, type-1 primes also exist infinitely.

Conclusion:

With the proof of this conjecture and also from the property of N-equation published in Aug-edition 2013 & the theory of Ramanujan relations of higher exponents published in April & May edition 2014 of IJSER we can conclude the following facts as a corollary.

a) for $N = a^n + b^n = c^n + d^n$, if n = 2, N must contain all prime factors of type-2 category only but if n is prime > 2 for which N exists, N must contain at least one prime factor of type-1 category which fails to be expressed as $x^2 + y^2$.

b) for n ≥ 3, (a, b), (c, d), …….. are the roots of an algebraic polynomial equation of single variable of degree (n – 1) where one root cannot be equal to zero. Hence, $a^n + b^n = c^n$, n ≥ 3 which is known as Fermat’s Last Theorem (FLT), has no existence. As I believe, this is the easiest and simplest way to prove FLT.

c) 4x ± 1 where x = 1, 2, 3, …… will produce infinitely many primes.

d) for a particular value of b the sequence N = 4x + b where x = 1, 2, 3, …… cannot produce odd composite or prime of mixed nature.

e) general term (T_{n+1}) of the sequence 4x + 1 or 4x – 1 after a particular term ‘b’ can be written as 4n + b which is more generalized & can produce infinitely many primes for n = 1,2,3, …….. Obviously ‘b’ is any odd number & the cases where gcd(n, b) ≠ 1 can be ignored. But 4n + b is still a particular case of Dirichlet’s general theorem (1837)

f) From the property of N-equation & the theory of Ramanujan relations, I believe that so many things are still left out to be explored

References

Books

[1] Academic text books of Algebra.

[2] In April, May edition, Vol-5 2014 of IJSER, Author: self

[3] In August edition, Vol-4 2013 of IJSER, Author: self

Author: Debajit Das (dasdebjit@indianoil.in)

(Company: Indian Oil Corporation Ltd, Country: INDIA)

I have already introduced myself in my earlier publications.