International Journal of Scientific & Engineering Research, Volume 6, issue 6, June-2015
ISSN 2229-5518

Mystery of Fermat Number

Author: Debajit Das

ABSTRACT

If any number in the form of $2^m + 1$ produces a prime number then obviously m is in the form of 2^n where n = 0, 1, 2, 3, 4,……… In honor of great mathematician Pierre de Fermat, this number has been named as Fermat number i.e. $F_n = 2^{2^{\wedge}n} +1$. So Fermat number may produce prime number or composite number. By physical verification it is observed that F_n is prime for n = 0, 1, 2, 3 & 4 But for n > 4 it is found to be composite or a single factor with unknown character. There is no proof in favor of prime number for n > 4. With the help of N_s operation as defined in my paper published in IJSER, Vol-4, Issue-8, Aug-edition 2013 regarding 'Mystery of Beal Equation' it has been possible to prove that there is no existence of any prime for n > 4.

Keywords

Degree of intensity for even number (DOI), Equidistant Gap (EG), Fermat odd factor (F_{of}), Fermat even factor(F_{ef}), wing.

1. Introduction

We know from N_s operation
$\pi\,(e_i^2 + o_i^2) = (e_1^2 + o_1^2)\,(e_2^2 + o_2^2)(e_3^2 + o_3^2)\ldots\ldots\,(e_n^2 + o_n^2) = E(v_j^2 + d_j^2) = (v_1^2 + d_1^2) = (v_2^2 + d_2^2) = (v_3^2 + d_3^2) = \ldots\ldots\, 2^{n-1}$ wings where the symbol π & E stand for continued product & equalities, e, v for even integers & o, d for odd integers. All $(e_i^2 + o_i^2)$ are prime numbers & $\gcd(e_i, o_i) = \gcd(v_j, d_j) = 1$. If any prime is repeated then in all cases $\gcd(v_j, d_j) \neq 1$. For any two equalities. ($v_{max} + d_{max}$) is always a composite number.
For any even number 2^p(odd no.), p can be said as its degree of intensity (DOI). If DOI of two even numbers e_1 & e_2 be p_1 & p_2 respectively ($p_1 \neq p_2$) then DOI of $(e_1 \pm e_2)$ is $\mathrm{Min}(p_1, p_2)$. For $p_1 = p_2$, DOI of $(e_1 \pm e_2) > p_1$ or p_2.
The product & division rules of N_s operation are as follows.
$(e_1^2 + o_1^2).(e_2^2 + o_2^2) = (\,|e_1e_2 \pm o_1o_2|\,)^2 + (\,|e_1o_2 -/+ o_1e_2|\,)^2$ &
$(e_1^2 + o_1^2)/(e_2^2 + o_2^2) = \{|e_1e_2 \pm o_1o_2|/(e_2^2 + o_2^2)\}^2 + \{|e_1o_2 -/+ o_1e_2|/(e_2^2 + o_2^2)\}^2$ consider only one wing which has integer elements.

Based on the above theoretical background we can prove that the Fermat number ($F_n = 2^{2^{\wedge}n} + 1$) will always represent a composite number for n > 4

2. If an odd integer in the form of $e^2 + o^2$ where gcd(e, 0) = 1 is composite then there must exist at least one pair of integer $I_{1,2}$ (one is odd & other is even) so that $[\{\mathrm{Min}(e, o)\}^2 + I_{1,2}]$ & $[\{\mathrm{Max}(e, o)\}^2 - I_{1,2}]$ both are square integers while the existence of any one of $I_{1,2}$ confirms the number to be composite.

Let us consider a composite number $N = (e^2 + o^2) = (e_1^2 + o_1^2)\,(e_2^2 + o_2^2) = (e_1o_2 \pm e_2o_1)^2 + (e_1e_2 -/+ o_1o_2)^2$
Here one wing is $(e_1o_2 + e_2o_1)^2 + (e_1e_2 - o_1o_2)^2$
$\Rightarrow$ even element of other wing $= (e_1o_2 - e_2o_1) = \sqrt{\{(e_1o_2 + e_2o_1)^2 - 4e_1e_2o_1o_2\}} = \sqrt{(e^2 - 4e_1e_2o_1o_2)} \Rightarrow (e^2 - 4e_1e_2o_1o_2)$ must be square integer. Similarly for odd element of other wing $(o^2 + 4e_1e_2o_1o_2)$ must be a square integer.
In this case o < e
For e < o, consider one wing is $(e_1o_2 - e_2o_1)^2 + (e_1e_2 + o_1o_2)^2$
$\Rightarrow$ even element of other wing $= \sqrt{(e^2 + 4e_1e_2o_1o_2)}$ & odd element of other wing is $\sqrt{(o^2 - 4e_1e_2o_1o_2)}$
$\Rightarrow$ both $(e^2 + 4e_1e_2o_1o_2)$ & $(o^2 - 4e_1e_2o_1o_2)$ must be square integer.
Hence, $\{\mathrm{Min}(e, o)\}^2 + 4e_1e_2o_1o_2 = P^2$ & $\{\mathrm{Max}(e, o)\}^2 - 4e_1e_2o_1o_2 = Q^2$ say, $\{\mathrm{Min}(e, o)\}^2 + V = P^2$ & $\{\mathrm{Max}(e, o)\}^2 - V = Q^2$
$\Rightarrow \{\mathrm{Min}(e, o)\}^2 + (Q^2 - P^2 + V) = Q^2$ & $\{\mathrm{Max}(e, o)\}^2 - (Q^2 - P^2 + V) = P^2$ say, $\{\mathrm{Min}(e, o)\}^2 + D = Q^2$ & $\{\mathrm{Max}(e, o)\}^2 - D = P^2$
$\Rightarrow$ If V exists D must exist or vice-versa.
$\Rightarrow$ Existence of D or V confirms the composite nature of the number N.
$\Rightarrow$ For a composite number, internal equidistant elements from both the extremities must be two square integers of even & odd at least for once and this 'Equidistance Gap' (E.G) is multiple of 16 otherwise it is prime.
$\Rightarrow$ $[\{\mathrm{Min}(e, o)\}^2 + 16k] + [\{\mathrm{Max}(e, o)\}^2 - 16k] = P^2 + Q^2$ for a composite number where k = 1, 2, 3, ………

3. For a composite number $N = e_1^2 + o_1^2 = e_2^2 + o_2^2$, $\mathrm{Min}(e_2, o_2) < (e_1 + o_1)/2 < \mathrm{Max}(e_2, o_2)$ & $\mathrm{Min}(e_1, o_1) < (e_2 + o_2)/2 < \mathrm{Max}(e_1, o_1)$

Let $N = (v_1^2 + d_1^2)(v_2^2 + d_2^2) = (v_1d_2 \pm v_2d_1)^2 + (v_1v_2 -/+ d_1d_2)^2$ where v is even & d is odd like e & o respectively.
Say the wing $(v_1d_2 + v_2d_1)^2 + (v_1v_2 - d_1d_2)^2 = e_1^2 + o_1^2$ & other wing $= e_2^2 + o_2^2$
It is obvious, $(v_1d_2 + v_2d_1)^2 < [\{(v_1d_2 + v_2d_1) + (v_1v_2 - d_1d_2)\}/2]^2 < (v_1v_2 - d_1d_2)^2$
$\Rightarrow (e_2^2 + 4v_1v_2d_1d_2\,) < \{(e_1 + o_1)/2\}^2 < \,(o_2^2 - 4v_1v_2d_1d_2\,) \Rightarrow\; e_2^2 < \{(e_1 + o_1)/2\}^2 < o_2^2 \Rightarrow e_2 < \{(e_1 + o_1)/2\} < o_2$
$\Rightarrow \mathrm{Min}(e_2, o_2) < (e_1 + o_1)/2 < \mathrm{Max}(e_2, o_2)$. Similarly, $\mathrm{Min}(e_1, o_1) < (e_2 + o_2)/2 < \mathrm{Max}(e_1, o_1)$
Obviously, all $v_1, v_2, d_1, d_2 < \mathrm{Min}[(e_1 + o_1)/2, (e_2 + o_2)/2]$

For a composite number $1 + e^2$ where lower element is one E.G cannot be more than e^2 hence its all other wings $P_i^2 + Q_i^2$ has the property $1 < P_i, Q_i < e$ i.e. $1 < \mathrm{Min}(P_i, Q_i) < (e + 1)/2$ & $(e + 1)/2 < \mathrm{Max}(P_i, Q_i) < e$ or physically it is quite understood.

4. Fermat Number ($F_n = 2^{2^{\wedge}n} + 1$) always represents a composite number for n > 4.

International Journal of Scientific & Engineering Research, Volume 6, issue 6, June-2015
ISSN 2229-5518

It is quite obvious from the product rule of N_s operation that $F_n = 2^{2^n} + 1$ will represent a composite number when it is possible to divide $2^{2^{n-1}}$ i.e. $(F_{n-1} - 1)$ into two even numbers say e_1o_1 & e_2o_2 where $|e_1e_2 - o_1o_2| = 1$. If not possible it is a prime. The term $|e_1e_2 - o_1o_2|$ can be said as Fermat odd factor (F_{of}) & the term $(e_1o_1 + e_2o_2)$ can be said as Fermat even factor (F_{ef}) of Fermat no. F_n Here, obviously both the even nos. e_1 & e_2 have same degree of intensity i.e. both contain the factors 2^p. DOI of F_{ef} means DOI of e_1 or e_2 i.e. p but actual DOI of $F_{ef} > p$.
Say, $e_1 = (2^pd_1)$ & $e_2 = (2^pd_2)$ $\Rightarrow (F_{n-1} - 1) = (2^pd_1)o_1 + (2^pd_2)o_2 = 2^p(o_1d_1 + o_2d_2)$ and obviously $(o_1d_1 + o_2d_2)$ is in the form of 2^m where $m + p = 2^{n-1}$ $\Rightarrow$ there cannot exist any common factor between any two among d_1, d_2, o_1 & o_2 Hence we cannot have any factor of F_n in the form of $(ke)^2 + (ko)^2 \Rightarrow F_n$ is the product of prime numbers without any exponent to any prime.

Example:

$F_0 = 2^{2^0} + 1 = 3$. As there does not exist any number before F_0 it is prime.
$F_1 = 2^{2^1} + 1 = 5$. Here $F_0 - 1 = 2$ & 2 cannot be divided into two even numbers. Hence, $F_1 = 5$ is a prime.
$F_2 = 2^{2^2} + 1 = 17$. Here $F_1 - 1 = 4$ & $4 = 2.1 + 2.1$ where $F_f = 2.2 - 1.1 \neq 1$. Hence $F_2 = 17$ is a prime.
$F_3 = 2^{2^3} + 1 = 257$. Here $F_2 - 1 = 16$ and 16 can be written as,
$16 = 2.1 + 2.7$ for which $F_f = 1.7 - 2.2 \neq 1$
$16 = 2^2.1 + 2^2.3$ & $F_f \neq 1$ and lastly $16 = 2.3 + 2.5$ for which $F_f \neq 1$
For equal division obviously $F_f \neq 1$ Hence, $F_3 = 257$ is a prime.
$F_4 = 2^{2^4} + 1 = 65537$. Here $F_3 - 1 = 256$ and 256 can be written as,
$2 + 2.127$, $4 + 4.63$, $2.3 + 2.125$, ……. where in all cases $F_{of} \neq 1$ Hence, $F_4 = 65537$ is a prime.

But for $F_5 = 2^{2^5} + 1$ where $F_4 - 1 = 65536$ it is found that $65536 = 4.409 + 25.2556$ where $F_{of} = (409.25 - 4.2556) = 1$
Hence, F_5 is composite & $F_5 = (25^2 + 4^2)(409^2 + 2556^2) = 4294967297$

Let us consider a Fermat composite number
$F_n = \{(2^pd_1)^2 + (o_1)^2\}.\{(2^pd_2)^2 + (o_2)^2\} = \{2^p(d_1o_2 + d_2o_1)\}^2 + (2^{2p}d_1d_2 - o_1o_2)^2$ where $F_{of} = 2^{2p}d_1d_2 - o_1o_2 = 1$& $F_{n-1} - 1 = 2^p(d_1o_2 + d_2o_1)$ where $(d_1o_2 + d_2o_1)$ is in the form of 2^m & obviously, $m + p = 2^{n-1}$ It clearly indicates that for any composite Fermat number F_n, all the factors are expressible in the form of $(\text{even})^2 + (\text{odd})^2$ having different values of DOI of all even elements but if we express all the factors as product of two factors then only in one case both will show same DOI of even elements where F_{of} will exist as 1 for F_{n+1} to be composite. If a Fermat number has only two prime factors then DOI for both as well as F_{ef} for the next is constant.
Now, for F_{n+1}, $F_n - 1 = \{2^p(d_1o_2 + d_2o_1)\}^2 = 2^{2p}(d_1^2o_2^2 + d_2^2o_1^2 + 2d_1d_2o_1o_2) = 2^{2p}d_1^2o_2^2 + 2^{2p}(2d_1d_2o_1o_2 + d_2^2o_1^2)$
Or, $= 2^{2p}d_2^2o_1^2 + 2^{2p}(2d_1d_2o_1o_2 + d_1^2o_2^2)$ for equal degree of intensities (2p).
This degree of intensity can be reduced or increased simply introducing $\pm 2^rd$ or $\pm 2^{2p}$ with both the even parts of F_{ef}.
Say, $F_n - 1 = (2^{2p}d_1^2o_2^2 \pm 2^rd) + \{2^{2p}(2d_1d_2o_1o_2 + d_2^2o_1^2) -/+ 2^rd\} = 2^r(2^{2p-r}d_1^2o_2^2 \pm d) + 2^r\{2^{2p-r}(2d_1d_2o_1o_2 + d_2^2o_1^2) -/+ d\}$. There is no need to consider $\pm 2^rd$ or $\pm 2^{2p}$ because it will produce all other wings of F_n where $F_{of} \neq 1$.
Without considering them we have,
$F_n - 1 = 2^{2p}(d_1^2o_2^2) + 2^{2p}(2d_1d_2o_1o_2 + d_2^2o_1^2) = 2^{2p}\lambda + 2^{2p}(2^{n-2p} - \lambda) = 2^{2p}\lambda_1\lambda_2 + 2^{2p}\lambda_3\lambda_4$ (say) so that $2^{4p}\lambda_1\lambda_3 - \lambda_2\lambda_4 = 1$ i.e. F_{of} of $F_{n+1} = 1$. Whatever may be the mode of divisions it does not matter. If the above mentioned two cases fail to produce F_{ef} & its corresponding $F_{of} = 1$ we can follow the most general case of divisions i.e. $(\lambda_1\lambda_2 + \lambda_3\lambda_4) = (d_1^2o_2^2 + d_2^2o_1^2 + 2d_1d_2o_1o_2)$
Now the question is whether F_{of} of F_{n+1} exists or not? If exists it is composite otherwise it is prime.

In favor of its existence we can say that once F_n has been found to be formed as composite for n = 5 & 6 by the same chain procedure suddenly we cannot receive a prime. If received, say F_m is prime then by backward view F_{m-1} cannot be composite which is contradictory. Hence all F_n for $n > 4$, are composite

For more authentic proof we can follow a simple conjecture which can be easily proved by N-Equation theory.
If $u^2 + 1$ is composite then $u^4 + 1$ is also composite.
As $u^2 + 1$ is composite it must have another wing say, $u^2 + 1 = a^2 + b^2$
Now $u^4 + 1 = (a^2 + b^2)^2 - 2u^2 = (a^2 - b^2)^2 + (2ab)^2 - 2u^2$.
It clearly indicates $u^4 + 1$ must satisfy the left hand odd element of a 2nd kind N-equation where $k = 2u^2$.
Hence $u^4 + 1$ cannot be prime. Because all the elements of a 2nd kind N-equation under $k = 2u^2$ are composite.
In general, if $u^2 + 1$ & $v^2 + 1$ both are composite then $(uv)^2 + 1$ is also composite. (*uv theory)

Now, F_{ef} of $F_{n+1} = 2^{2p}(\lambda_1\lambda_2 + \lambda_3\lambda_4) = 2^{2p}.2^{2m}$ where p is in the form of 2^r & m is in the form of $2^r(\text{odd})$.
$\Rightarrow 2^{2p}.2^{2m} + 1$ is composite & 2^p2^m is expressible in the form of F_{ef} with $F_{of} = 1$.
From general uv theory also it can be analyzed.
$\Rightarrow 2^{2m} + 1$ is a composite number. $2^{2p} + 1$ is also composite after certain operation. Hence, $2^{2p}.2^{2m} + 1$ is also composite.
$\Rightarrow 2^p2^m$ is expressible in the form of F_{ef} with $F_{of} = 1$.
Hence, if F_n is composite F_{n+1} is also composite.
Similarly, F_{ef} of $F_{n+2} = 2^{4p}(\lambda_1\lambda_2 + \lambda_3\lambda_4)^2 = 2^{4p}.2^{4m}$
$\Rightarrow 2^{4m}\ 2^{4m} + 1$ being a composite number $2^{2m}2^{2m}$ is always expressible in the form of F_{ef} with $F_{of} = 1$.
Hence, if F_n is composite F_{n+2} is also composite. By physical verification we have seen that F_5 & F_6 are composite.
Hence, all Fermat numbers are composite for $n > 4$.

Conclusion:

International Journal of Scientific & Engineering Research, Volume 6, issue 6, June-2015
ISSN 2229-5518

I believe that the proof of this composite nature of all Fermat numbers for n > 4 is correct. In general it will not be wrong to conclude that any number in the form of $F_n = (odd)^2 + (even)^{2^n}$ or $(odd)^{2^n} + (even)^2$ where gcd(odd, even) = 1 produces constantly composite numbers after certain operations of n for prime numbers. So at initial stage if $(odd)^2 + (even)^2$ is found to be composite it will never produce prime numbers. Possibility of constant production of prime numbers cannot be ruled out also. For $F_{of} > 1$ we have to follow the same analysis & logic but separately for both the expressions under '±' corresponding to F_{ef} under '-/+'
I also believe that with the help of this N_s operation and N_d operation as defined in my earlier papers published in 'IJSER, Houston, USA' so many problems in Number Theory are possible to be solved.

References

Books

[1] Academic text books of Algebra.

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

Author: Debajit Das
(Company: Indian Oil Corporation Ltd, Country: INDIA)

I have already introduced myself in my earlier publications.