Nature of Composite Numbers that obey Fermat's property & some properties of a Prime

Author: Debajit Das

ABSTRACT: Any prime number 'm' obeys the Fermat property with respect to any number 'a' which is prime to m. But if m is composite it may be or may not be true. The composite numbers that obey Fermat property can be said as Fermat's composite number or simply FC Numbers. This paper contains some natures of so called FC numbers. The existence of such numbers was first detected by the American mathematician Carmichael in 1809. So far divisibility is concerned a prime number possesses several properties out of which we can recall the famous property of Wilson's theorem i.e. p divides (p – 1)! + 1. The proof of this theorem given by the great mathematician Lagrange also indicates some other divisibility properties of a prime which have been lying hidden to the proof itself and never day-lighted. My paper contains the proof of those hidden properties along with the fact that Wilson theorem is a particular case of a general property. My paper also contains an important theorem regarding divisibility of twin primes.

INTRODUCTION: Before we investigate the nature of a FC-number and to extract some properties of a prime it is felt necessary to indicate the meanings of some usual notations and to highlight one useful common theorem.

$\prod(p_i)$ denotes the product sequence of odd primes i.e. $p_1p_2p_3$……

$[x_i,]$ denotes the LCM of x_1, x_2, x_3, …..

$(x_i,)$ denotes the GCF of x_1, x_2, x_3, …..

If x + y = z where (x, y) = 1 then obviously (x, z) = (y, z) = 1

For a number $N = 2^n.p^{n1}p^{n2}p^{n3}$…… Degree of Intensity (DOI) with respect to any base prime is defined as $DOI(N)_2 = n$ or symbolically $\uparrow(N)_2 = n$, $\uparrow(N)_{p1} = n_1, \uparrow(N)_{p2} = n_2$ and so on.

Obviously, for an odd integer $\uparrow(N)_2 = 0$

If N is an odd integer of 1st kind i.e. in the form of 4x – 1, $\uparrow(N - 1)_2 = 1$ & for 2nd kind i.e. 4x + 1 form $\uparrow(N - 1)_2 > 1$.

a|b is the symbol for a divides b.

KEY WORDS: FC-number, Degree of intensity (DOI)

1. Any FC-number is a product sequence of odd primes only i.e. $\prod(p_i)$

According to Fermat Theorem $a^{m-1} \equiv 1 \pmod m$ where m is prime & (a, m) = 1. When m is composite it may be or may not be true. For a composite number $m = p_1^{\alpha1}p_2^{\alpha2}p_3^{\alpha3}$…….. it will obey the Fermat's property if and only if $m - \lambda[\varphi(p_1^{\alpha1}), \varphi(p_2^{\alpha2}), \varphi(p_3^{\alpha3}), \ldots\ldots] = 1$ where λ is any positive integer & $\varphi(x^b) = x^b - x^{b-1}$. The proof can be easily understood by an example given below.

1105 = 5.13.17 Let a be any integer relatively prime to 1105.

Then by Fermat's theorem $a^4 \equiv 1 \pmod 5$, $a^{12} \equiv 1 \pmod{13}$, $a^{16} \equiv 1 \pmod{17}$

This implies $a^{[4, 12, 16]} \equiv 1 \pmod{[5, 13, 17]}$ i.e. $a^{48} \equiv 1 \pmod{1105}$ & raising both sides to the power 23 we have $a^{1104} \equiv 1 \pmod{1105}$ i.e. $a^{m-1} \equiv 1 \pmod m$ where m is composite.

$\Rightarrow (p_1^{\alpha1}p_2^{\alpha2}p_3^{\alpha3}\ldots\ldots) - \lambda[\varphi(p_1^{\alpha1}), \varphi(p_2^{\alpha2}), \varphi(p_3^{\alpha3}), \ldots\ldots] = 1$

$\Rightarrow (p_1^{\alpha1}p_2^{\alpha2}p_3^{\alpha3}\ldots\ldots) - \lambda(p_1^{\alpha1-1}.p_2^{\alpha2-1}.p_3^{\alpha3-1}\ \ldots\ldots)[(p_1 - 1), (p_2 - 1), (p_3 - 1), \ldots\ldots] = 1$

$\Rightarrow (p_1^{\alpha1-1}.p_2^{\alpha2-1}.p_3^{\alpha3-1}\ \ldots\ldots)\{(p_1p_2p_3\ldots\ldots) - \lambda[(p_1 - 1), (p_2 - 1), (p_3 - 1), \ldots\ldots]\} = 1$ which is quite impossible unless all $\alpha_i = 1$. Hence, proved that all FC-numbers are the product of primes only

2. The composite numbers which are the product of twin primes cannot be FC-numbers i.e. $a^{p(p+2)-1} \not\equiv 1$ (mod $p(p+2)$ where p & $(p+2)$ both are primes & $(a, p) = 1 = (a, p+2)$

Here, $m = p(p+2)$ & $a^{[p-1,\, p+1]} \equiv 1 \pmod m$
This implies $p(p+2) - \lambda.(p-1)/2.(p+1)/2 = 1$ this implies $(2-\lambda)p^2 + 4p + (\lambda - 1) = 0$
Obviously, $\lambda < 2$ & m has no existence.

3. For a FC-number $N = \prod(P_i)$ where $i \geq 3$, $\uparrow(p_i - 1)_x$ cannot be all different.

If all $\uparrow(p_i - 1)_x$ are different with respect to any base x, say $\min\{\uparrow(p_i - 1)_x\} = n$ and $\max\{\uparrow(p_i - 1)_x\} = m$
$\Rightarrow \lambda$ is in the form of $x^n\{d_1 + x^r d_2)/x^m d_3$ where all d are some integers free from x.
$\Rightarrow \lambda$ cannot be integer as $n < m$.

4. For a FC-number $N = \prod(P_i)$ where $i \geq 3$, if $\min\{\uparrow(p_i - 1)_2\} = n$ & $\max\{\uparrow(p_i - 1)_2\} = m$ then n must be repeated even number of times irrespective of the fact that other DOI of 2 is repeated or not. For odd numbers of repetitions of n, FC-number cannot exist.

This is simply because of the following fact.
Say, $v_1 + v_2 = v_3$ where v denotes even integers.
If $\uparrow(v_1)_2 = \uparrow(v_2)_2 = x$ then $\uparrow(v_3)_2 > x$ and if $\uparrow(v_1)_2 < \uparrow(v_2)_2$ then $\uparrow(v_3)_2 = \uparrow(v_1)_2$
If $\uparrow(v_i)_2 = x$ for $i = 1, 2, 3, \ldots$ then $\uparrow(\sum v_i) = x$ where $i = 1, 2, 3, \ldots\ldots (2r-1)$ & $> x$ where $i = 1, 2, 3, \ldots., 2r$.
Now, if n is repeated odd nos. of times then numerator of λ contains single term as minimum DOI of 2 i.e. n.
As a result , λ is in the form of $2^n d_1/2^m d_2$ for some integers of d_1 & d_2 where $n < m$.
$\Rightarrow \lambda$ cannot be an integer.
But if n is repeated even nos. of times n may go on increasing by chain rule with other DOI and as a result we may get λ in the form of $2^r d_1 / 2^m d_2$ where $r \geq m \Rightarrow \lambda$ is an integer & FC-number is a product of at least 3 primes.

5. If p is an odd prime then
5.1 $p \mid \sum x^m$ where $x = 1, 2, 3, \ldots\ldots, p-1$ & $m \neq k(p-1)$
5.2 $p \mid \sum x^m$ where x = product of integers among $1, 2, \ldots\ldots, p-1$ taken two at a time for $2m \neq k(p-1)$
5.3 $p \mid \sum x^p$ where x = product of integers among $1, 2, 3, \ldots\ldots, p-1$ taken r at a time & $r < p-1$
5.4 $p \mid \sum x^m$ where x = product of integers among $1, 2, \ldots\ldots, p-1$ taken $(P-2)$ at a time & $m \neq k(p-1)$
5.5 $p \mid \sum x^m$ where x = product of integers among $1, 2, \ldots\ldots, p-1$ taken $(P-3)$ at a time & $2m \neq k(p-1)$

Say, $f(x) = (x-1)(x-2)(x-3)\ldots\ldots..(x-p+1) = x^{p-1} - a_1 x^{p-2} + a_2 x^{p-3} - \ldots\ldots\ldots - a_{p-2}x + (p-1)!$
Where a_r denotes the sum of the product among $1, 2, 3, \ldots.., p-1$ taken r at a time for $r < p-1$ & according to Lagrange theorem $p \mid$ all (a_i)
Now, by logarithmic differentiation,
$f'(x) / f(x) = (x-1)^{-1} + (x-2)^{-1} + (x-3)^{-1} + \ldots\ldots.. + (x-p+1)^{-1}$
$= \{(p-1)x^{p-2} - a_1(p-2)x^{p-3} + \ldots\ldots\ldots - a_{p-2}\}/f(x)$
$\Rightarrow (\sum\alpha^0)x^{-1} + (\sum\alpha^1)x^{-2} + (\sum\alpha^2)x^{-3} + \ldots\ldots. + (\sum\alpha^m)x^{-(m+1)} + \ldots\ldots..$ where α varies from 1 to $(p-1) =$
$(p-1)x^{-1} + b_1x^{-2} + b_2x^{-3} + \ldots\ldots\ldots. + b_m x^{-(m+1)} + \ldots\ldots.$ By algebraic division of $f'(x) / f(x)$
Here, all the coefficients of b are the expression of 'a' not containing any free constant excepting the cases where m is multiple of $(p-1)$ i.e. $m \neq k(p-1)$. By algebraic division it can be easily observed.
Hence, in all other cases $p \mid b_i \Rightarrow p \mid b_m$ & equating the coefficients on both sides we can say,
$P \mid 1^m + 2^m + 3^m + \ldots\ldots + (p-1)^m$ i.e. $p \mid \sum x^m$ where $x = 1, 2, 3, \ldots\ldots, p-1$ for $m \neq k(p-1)$
Now, squaring both sides $p \mid (\sum x^{2m} + 2\sum y^m)$ where y is the product among $1, 2, 3, \ldots.., (p-1)$ taken two at a time. $\Rightarrow p \mid \sum y^m$ as $(\sum x^{2m}$ is divisible by p for $2m \neq k(p-1)$ and hence proved 6.2
Now, $p \mid a_r$ i.e. $p \mid \sum x_r$ say, $p \mid (c_1 + c_2 + c_3 + \ldots..)$ where c is the product of r different integers.
$\Rightarrow p \mid (c_1 + c_2 + c_3 + \ldots..)^p \Rightarrow p \mid (c_1^p + c_2^p + c_3^p + \ldots\ldots) +$ K multiple of p.

$\Rightarrow p \mid (c_1^p + c_2^p + c_3^p + \ldots\ldots) \Rightarrow p \mid \sum x^p$ where x is the product of r different integers & $r < (p-1)$

Hence, proved 5.3

Replacing x by 1/x we have, $f(x) = (p-1)!x^{p-1} - a_{p-2}x^{p-2} + a_{p-3}x^{p-3} - \ldots\ldots\ldots + a_2x^2 - a_1x + 1$ where roots of the equation $f(x) = 0$ are 1, 1/2, 1/3,……., 1/(p – 1)

Now, considering the same logics on $f^{/}(x) / f(x)$ we can say,

P | Numerator of $\{1/1^m + 1/2^m + 1/3^m + \ldots\ldots. + 1/(p-1)^m\}$ for $m \neq k(p-1)$

$\Rightarrow p \mid \sum x^m$ where x is the product of (p – 2) integers at a time.

Again, P | Numerator of $\{1/1^m + 1/2^m + 1/3^m + \ldots\ldots. + 1/(p-1)^m\}^2$

$\Rightarrow$ P | N^r of $\{ \sum x^{2m} + 2\sum y^m\}$ where x = 1, ½, 1/3, ……, 1/(p – 1) & y is the product of two fractions at a time.

$\Rightarrow p \mid \sum y^m$ for $2m \neq k(p-1) \Rightarrow p \mid N^r$ of $\sum y^m \Rightarrow p \mid \sum x^m$ where x is the product taken (p – 3) integers at a time for $2m \neq k(p-1)$ and hence proved.

Note for shifting phenomenon: above mentioned all the theorems are also true if the original set 1, 2, 3, ….., p – 1 is replaced by $1.\mu + p\lambda$, $2.\mu + p\lambda$, $3.\mu + p\lambda$, …….., $(p-1).\mu + p\lambda$ where λ, μ are positive integers. It happens due to same logics applied in $f^{/}(x/\mu - p\lambda)/ f(x/\mu - p\lambda)$ where roots of the equation $f(x) = 0$ have been increased by μ times & then added by $p\lambda$ in the equation $f(x/\mu - p\lambda) = 0$.

e.g. for $m \neq 10k$, $11 \mid 1^m + 2^m + 3^m + \ldots\ldots\ldots + 10^m$ considering $\mu = 1$ & $\lambda = 0$, $12^m + 13^m + 14^m + \ldots\ldots\ldots + 21^m$ considering $\mu = 1$ & $\lambda = 1$, $25^m + 28^m + 31^m + \ldots\ldots\ldots + 52^m$ for $\mu = 3$, $\lambda = 2$ & so on.

Against any two fixed integers λ & μ and with respect to any odd prime p the set of integers $p\lambda \pm x\mu$ where x varies from 1 to (p – 1) will satisfy all the said theorems and also the Lagrange coefficients. All the sets under this particular class are the complete reduced system of (mod p) while (1, 2, 3, ……, p – 1) is the least residue of (mod p).

Hence, in general, $p \mid \prod_{x=1}^{x=p-1}(p\lambda + x\mu) + \mu^{p-1}$ & for a particular case where $\mu = 1$ & $\lambda = 0$, $p \mid (p-1)! + 1$ which is known as Wilson's theorem. It is obtained simply by putting $x = \mu$ in the identity of f(x) after replacement of all the roots by $p\lambda + x\mu$. It is observed LH side is divisible by p & RH side is partially divisible by p. non-divisible part on RH side is $\prod(p\lambda + x\mu) + \mu^{p-1}$ where x varies from 1 to p – 1. Hence, non-divisible part must be divisible by p.

If $(\mu, p) = 1$ then obviously $p \mid \prod (p\lambda \pm x\mu) + 1$ according to Fermat property and after multiplication all the factors $p \mid \mu^{p-1}(p-1)! + 1$

$\Rightarrow p \mid (\mu_1^{p-1} + \mu_2^{p-1} + \mu_3^{p-1} + \ldots\ldots$ p terms$).(p-1)!$ where $(\mu_i, p) = 1$

$\Rightarrow p \mid (\sum_{i=1}^{p}\mu_i^{p-1})(p-1)! \Rightarrow p \mid \sum_{i=1}^{p}(\mu_i^{p-1})$

In view of the above we can establish one important theorem given below.

6. If p & p + 2 are twin primes then $p(p+2) \mid \sum_{x=1}^{p+1} x^{p-1}$

It is quite obvious that if p + 2 is a prime then $(p+2) \mid \sum x^{p-1}$ where x varies from 1 to p + 1 as per Th-5.1

Here, in $\sum x^{p-1}$ sum of all the terms excluding p^{p-1} is also divisible by p. Hence, $\sum x^{p-1}$ is also divisible by p

6.1 Converse of the theorem is also true.

As there exists infinitely many primes we can assume (p + 2) is a prime and accordingly p will be either prime or a FC-number.

Say, p is a FC-number & $p \mid X$ where $X = 1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots\ldots + (p-1)^{p-1} + p^{p-1} + (p+1)^{p-1}$, where obviously $(p+1, p) = 1$

As per Theorem-1 & 4, p must be product of at least 3-primes, say $p = \alpha\beta\gamma$

Now, $\alpha \mid \{1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots\ldots.. + (\alpha-1)^{p-1} + \alpha^{p-1} \} + \{(\alpha+1)^{p-1} + (\alpha+2)^{p-1} + (\alpha+3)^{p-1} + \ldots\ldots\ldots..+$

$(2\alpha - 1)^{p-1} + (2\alpha)^{p-1}\} + \ldots\ldots.. \beta\gamma$ brackets.
$\Rightarrow \alpha | \{1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots\ldots + (p-1)^{p-1} + p^{p-1}\}$
Now, if p|X means $\alpha | X \Rightarrow \alpha | (p+1)^{p-1}$ which is impossible as (p + 1, p) = 1 i.e. (p + 1, α) = 1.
Hence, p cannot be a composite number obeying Fermat property.

So, if it is found that $\sum_{x=1}^{p+1} x^{p-1}$ is divisible by p & p + 2 both then p, p + 2 must be twin primes.

*Apart from the twin prime factors X also contains all the prime factors of (p + 1) say α_i, i = 1, 2, 3, …. Provided $p - 1 \neq k(\alpha_i - 1)$ as per the next theorem.
It is to be noted that in between twin primes there cannot exist an even number in the form of 2^n

7. For a prime number p if all the prime factors of (p – 1) are α_i, i = 1, 2, 3, …… then $X = \sum_{x=1}^{p-1} x^m$ must be divisible by p and all α_i provided $m \neq k(p-1)$ or $k(\alpha_i - 1)$.

Say $p - 1 = \alpha y$ where α is a prime.
$\Rightarrow \alpha | \{1^m + 2^m + 3^m + \ldots\ldots. + (\alpha-1)^m + \alpha^m\} + \{(\alpha+1)^m + (\alpha+2)^m + (\alpha+3)^m + \ldots\ldots. + (2\alpha)^m\} + \ldots\ldots..$ y brackets
$\Rightarrow \alpha | \{1^m + 2^m + 3^m + \ldots\ldots. + (p-1)^m\}$ where $m \neq k(\alpha - 1)$
$\Rightarrow \alpha | X$ and similarly, for other prime factors of (p – 1)

The following two theorems which are easy to establish are also felt necessary to mention.

8.1 $(x\ p) | x^p + (x \pm \alpha)^p + (x \pm 2\alpha)^p + \ldots\ldots\ldots..$ p terms
8.2 $(x\ p) | x^p + (x \pm \alpha)^p + (x \pm 2\alpha)^p + \ldots\ldots\ldots..$up to any odd terms when p is a prime factor of x.

Few examples in favor of theorem 6 & 7

Once again we can redefine clubbing the theorems 6 & 7 as: If p & p + 2 are twin primes where obviously p + 1 is in the form of $2^m 3^n p_1^{n1} p_2^{n2} \ldots\ldots.$ then $p(p+2).\prod(p_i) | \sum x^{p-1}$, x varies from 1 to p + 1& where there exists at least one prime factor y so that $\uparrow(p-1)_y < \uparrow(p_i - 1)_y$ for the existence of p_i.
Let us consider the twin prime (101, 103) where p + 1 = 102 = 2.3.17 & p – 1 = 100 = $2^2 5^2$
$\Rightarrow \{\uparrow(100)_2 = 2\} < \{\uparrow(17-1)_2 = 4\}$. Hence (101.103.17)|X where $X = \sum x^{100}$, x varies from 1 to 102.
For all the twin primes of the form (u_9, u_1) where u_9 is in the form of 2(odd) + 1, X is always divisible by 5.
[u_x denotes a prime having unit digit x]. Say the twin prime (59, 61) where $\uparrow(59-1)_2 = 1$ & as 5 is always a factor of mid-integer of twin obviously $\uparrow(59-1)_2 < \uparrow(5)_2$ Hence, $(59.61.5) | \sum x^{58}$, x varies from 1 to 60.
Say the twin prime (137, 139) where 138 = 2.3.23 & $\{\uparrow(137-1)_{11} = 0\} < \{\uparrow(23-1)_{11} = 1\}$.
Hence, $(137.139.23) | \sum x^{136}$, x varies from 1 to 138.
It is quite evident that if m is odd, then {prime p & all odd prime factors p_i of (p – 1)}$| \sum_{x=1}^{p-1} x^m$ as $\uparrow(p_i - 1)_2 > 0$ but $\uparrow(m)_2 = 0$

9 For a prime number p if (m, p) = 1 then
9.1 p|X where $X = 1 + m^d + (m^d)^2 + (m^d)^3 + \ldots\ldots.$ (p – 1)/d terms, d is any factor of (p – 1) including one but excluding (p – 1) itself, provided $(p, m^d - 1) = 1$
9.2 If d is odd p|Y where $Y = 1 - m^d + (m^d)^2 - (m^d)^3 + \ldots\ldots.$ (p – 1)/d terms, provided $(p, m^d + 1) = 1$
9.3 p|XY without any condition i.e. only for (m, p) = 1 where m or p ≠ 2
9.4 If $(p, m^d \pm 1) = 1$ for d is odd, $p | 1 + (m^d)^2 + (m^d)^4 + (m^d)^8 \ldots\ldots.$ (p – 1)/2d terms

We have $X = \{(m^d)^{(p-1)/d} - 1\}/(m^d - 1) = (m^{p-1} - 1)/(m^d - 1)$ Hence, p|X for $(p, m^d - 1) = 1$
If d is odd then replacing m by –m we have , $Y = -(m^{p-1} - 1)/(m^d + 1) \Rightarrow p | Y$ for $(p, m^d + 1) = 1$
Now, there cannot exist any common odd factor in between two consecutive even or odd numbers.
So, p cannot divide $m^d \pm 1$ both and hence, p|XY without any condition except (m, p) = 1
e.g. for any prime p, $p | 1 + m^{2^{(n-k)}} + \{m^{2^{(n-k)}}\}^2 + \{m^{2^{(n-k)}}\}^3 + \ldots..\ 2^k\beta$ terms where $p - 1 = 2^n\beta$ & (p, m) = 1,

$(p, m^{2^{(n-k)}} - 1) = 1$, $0 \le k \le n \Rightarrow$ for $m = 2$ & $k = 0$, $(p, \prod(F_{n-1})) = 1$, F denotes the Fermat number.
Say the prime number 13 where $p - 1 = 3.4$
$\Rightarrow 13|(1 + 3^3 + 3^6 + 3^{12})(1 - 3^3 + 3^6 - 3^{12})$ where $m^d = 3^3$ or $13|(1 + 7^3 + 7^6 + 7^{12})(1 - 7^3 + 7^6 - 7^{12})$ where $m^d = 7^3$ & so on
Now, multiplying XY we get $p|(r^2 - 1)\{1 + r^2 + r^4 + r^8 + \ldots\ldots (p-1)/2d \text{ terms}\}^2$
$\Rightarrow p|\{1 + r^2 + r^4 + r^8 + \ldots\ldots (p-1)/2d \text{ terms}\}$ where $r = m^d$ for $(p, m^d \pm 1) = 1$

References: any text book in the field of Number Theory.

Conclusion: I believe that with the help of these newly invented theorems it will be possible to extract many more properties of prime numbers. Presently one important question excites our mind regarding existence of other prime factors of X in theorem 7 apart from p & all p_i. If it exists, say p_j-group what is the logic behind its existence? It seems p_i is a FC-number as a whole i.e. $\prod(p_j)$ or product of several FC-numbers i.e. $\prod(p_j)$. $\prod(p_k)$….. where some FC-numbers may contain few primes from p_i-group e.g. say p_i consists a single prime q_1 & p_j also consists a single prime q_2 then pq_1q_2 must be a FC-number as FC-nos. is a product of minimum three primes. If p_j consists two primes q_2 & q_3 then either pq_2q_3 or $q_1q_2q_3$ or $pq_1q_2q_3$ is a FC-number. Of course, it needs further investigation to prove.

About Author: I have already introduced myself in my earlier publications.

DEBAJIT DAS: email address: dasdebjit@indianoil.in, Mob. No. 9006558917