Research Journal of Mathematics and Statistics 1(2): 30-34, 2009
ISSN: 2040-7505
© Maxwell Scientific Organization, 2009
Submitted Date: June 30, 2009 Accepted Date: September 02, 2009 Published Date: November 16, 2009

Number of Solutions of the Equation $\phi(x) = 2^{a-1}$ in the Absence of Sixth Fermat Prime

Manjit Singh
Department of Mathematics, Daulat Ram College, University of Delhi. Delhi -110007. India

Abstract: For any natural number k, $J(k)$ is the set of solutions of the equation $\phi(x)=k$. We find that the set of natural numbers is a disjoint union of $J(k)$ and $O\left(J\left(2^{a-1}\right)\right)=\begin{cases} a+1 \text{ if } 1\le a\le 32 \\ 32 \text{ if } a\ge 33\end{cases}$ in absence of sixth Fermat prime. Explicit expressions of $J(2^{31})$ and $J(2^{32})$ are also obtained.

Key words: Euler's ϕ -function, carmichael's conjecture and fermat primes

INTRODUCTION

In emerging world use of numbers is so common in our part of life in every point like; communication, electronically banking, identification, encryption, cryptography, security, statistics and engineering etc. Therefore the use of number rather than even counting is much more and the study of these numbers becomes imperative to understand the theory of numbers. Today, we need of big numbers with unique properties. Mathematicians are busy in developing numbers with unique properties as far as this study becomes viable. In the note, we are interested in the most interesting topic of number theory among the mathematicians hitherto, that is, Euler's ϕ -function. In particular in the number of solutions of $\phi(x)=k$, also called the multiplicity of k

For any positive integer n, it is well known that Euler's ϕ -function (sometimes called the totient function) is an arithmetic function and is defined as the number of integers less than n and relatively prime to n. Notice that $\phi(1)=1$, $\phi(p)=p-1$ for every prime p and if $n = P_1^{\alpha_1} P_2^{\alpha_2} \ldots P_r^{\alpha_r}$ is the factorization of n as a product of r distinct primes, we find an even number $\phi(n)=n\left(1-\frac{1}{P_1}\right)\left(1-\frac{1}{P_1}\right)\ldots\left(1-\frac{1}{P_r}\right)$ due to its multiplicative property. The study of the properties of Euler's ϕ -function concerns with the fundamental importance in the theory of numbers. Carmichael's Conjecture, one famous unsolved problem concern the possible values of the function $V_\phi(k)$, the number of solutions of $\phi(x)=k$, also called the multiplicity of k and $J(k)=\{n \in N: \phi(n)=k\}$. $J(k)$ is an empty set for every odd number k. Carmichael's Conjecture (Carmichael, 1907; Carmichael, 1922) states that for every m, the equation has either no solutions or at least two solutions. Symbolically for all $m\in$N, there exists $n\in$N, with $m\neq n$, for which $\phi(m) = \phi(n)$.

The work done in last three decades to find the multiplicity of Euler's ϕ -function for a given number k and has not been able to prove or disprove Carmichael's Conjecture stated before one centaury. Guy (1983), presented some results on the conjecture; Carmichael himself proved that, if n_0 does not verify his conjecture, then $n_0>10^{37}$. Self ridge (Selfridge, 1963) gave a solution of Ore's problem that for every $k\ge 1$, there is an odd integer $\bar{k}$ such that $2^k\bar{k}$ is not a value of Euler's ϕ -function i.e. $J(k)$ is again an empty set beside k is not an odd integers. Mendelssohn (Mendelsohn, 1976) showed that there exist infinitely many primes p such that for $k\ge 1$, $V_\phi\left(2^k p\right)=0$. Gupta (Gupta, 1950) proved that $J(k!)$ is non empty set or in other words $\phi(x)=k!$ always have at least one solution. The author claiming a different approach in the direction said above. In the sequel, an equivalence relation and the corresponding equivalence classes are defined and studied a special equivalence class $J(2^{a-1})$ contains elements more than one that insure that the Carmichael's Conjecture is true for all number in the class. Our result is the following

Main result:

(i) $$N = \bigcup_{\substack{k\in N \\ k=\phi(m)}} J(k)$$

(ii) $$O\left(J\left(2^{a-1}\right)\right)=\begin{cases} a+1 \text{ if } 1\le a\le 32 \\ 32 \quad \text{if } a\ge 33\end{cases}$$

in absence of sixth Fermat prime.

MATERIALS AND METHODS

Euler-Carmichael's Classes: In this paper, in the response of above account, we study the equation $\phi(x)=k$ and find a complete set of solution in the form of equivalence classes. In the succession we first define an equivalence relation and the corresponding equivalence classes that originally evaluated by the author.

For any $m,n \in N$, define a relation '$\approx$'on the set of all natural numbers N by setting $m \approx n$ if $\phi(m)=\phi(n)$. We originated here the relation as an equivalence relation (proof is very obvious) and for every positive integer m, the equivalence classes $C_m = \{n \in N: n \approx m\}$ or $C_m = \{n \in N: \phi(n)=\phi(m)\}$, known as Euler-Carmichael's classes [EC], given by the above said equivalence relation on N which is found analogous to $J(k)=\{n \in N: \phi(n)=k\}$ for every $k=\phi(m)$.

Evaluation of Euler-Carmichael's classes [EC] $J(k)=C_m$: The following observations can be made out for any positive integer on the basis the results

(1) $J(k)=\{n \in N: \phi(n)=k\} \neq \varphi$

(2) for any $k_1, k_2 \in N$, either $J(k_1)\cap J(k_2)=\varphi$ or $J(k_1)=J(k_2)$ and

(3) $N = \underset{\substack{k\in N\\ k=\phi(m)}}{U} J(k)$

Theorem (Equipotent) 1: If $k=\phi(m)$, then $J(k)=C_m$ and conversely. Equivalently $J(\phi(m))=C_m$ for all $m \geq 1$.

Theorem 2: Prove that above defined relation '$\approx$' is an equivalence relation.

We see that the relation is an equivalence relation and equivalence class [EC] is given by the rule $C_m = \{n \in N: \phi(n)=\phi(m)\}$ for every number m. Let us institute some well known properties of equivalence classes.

Theorem 3: Prove the followings:

(1) $C_m=\varphi$.
(2) $C_m=C_n$ if and only if $m \approx n$.
(3) $C_m \cap C_n=\varphi$ or $C_m=C_n$.
(4) $N = \underset{m\in N}{U} J(\phi(m)) = \underset{m\in N}{U} C_m = \underset{\substack{m\in N\\ k=\phi(m)}}{U} J(k)$

Proof:
(1) As $\phi(m)=\phi(m)$ for all $m \in N$, we get $m \in C_m$ and therefore $C_m \neq \varphi$.
(2) First suppoe that $C_m=C_n$ for any $m, n \in N$
If, $C_m=J(k)$ then $k=\phi(m)$.

$$\Rightarrow C_n = J(k)$$
$$\Rightarrow k = \phi(n)$$
$$\Rightarrow \phi(m) = \phi(n).$$

Therefore by definition we get $m \approx n$.
On the other hand: if $m \approx n$ the by definition $\phi(m)=\phi(n)$.

$$\begin{aligned} x \in C_m &\Leftrightarrow \phi(m) = \phi(n) \\ &\Leftrightarrow \phi(m) = \phi(x) = \phi(n) \\ &\Leftrightarrow \phi(x) = \phi(n) \\ &\Leftrightarrow x \in C_n \\ &\therefore C_m = C_n \end{aligned}$$

(3) Let $C_m \cap C_n \neq \varphi$ and $x \in C_m \cap C_n$.

$$\begin{aligned} &\therefore \phi(m) = \phi(x) = \phi(n). \\ x \in C_m &\Leftrightarrow \phi(m) = \phi(x) \\ &\Leftrightarrow \phi(m) = \phi(x) = \phi(n) \\ &\Leftrightarrow \phi(x) = \phi(n) \\ &\Leftrightarrow x \in C_n. N = \underset{m\in N}{U} J(\phi(m)) \\ &= \underset{m\in N}{U} C_m = \underset{\substack{m\in N\\ k=\phi(m)}}{U} J(k) \\ &\therefore C_m = C_n \end{aligned}$$

(4) Since for any integer m, $J(k) \subseteq N$ with $k=\phi(\text{m})$,

$$\therefore \underset{\substack{k=\phi(m)\\ m\in N}}{U} J(k) \subseteq N \ldots \quad \text{(i)}$$

One the other hand, let be any number.
Then there exists a unique k such that $k = \phi(n)$.
$\Rightarrow n \in J(k)$ with $k = \phi(n)$ for all n.
Taking union over n, we have

$$N \subseteq \underset{\substack{k=\phi(m)\\ m\in N}}{U} J(k) \ldots \quad \text{(ii)}$$

Using (i) and (ii), we have

$$N = \underset{\substack{k=\phi(m)\\ m\in N}}{U} J(k).$$

Using theorem (Equipotent), we get

$$N = \underset{m\in N}{U} J(\phi(m)).$$

Theorem 4: If $n = n_1 n_2$ and $n_1 \in J(k_1)$, $n_2 \in J(k_2)$ such that $\gcd(n_1, n_2)=1$, then $n \in J(k_1 k_2)$.

Proof: Since $\gcd(n_1, n_2)=1$, we have immediately the result using the multiplicative property of Euler's ϕ -function i.e. $\phi(n_1.n_2) = \phi(n_1).\phi(n_2)$.

Corollary 1: Prove that $mJ(1) \subseteq J(\phi(m))$ for all odd integer m.

Fermat Primes and [EC] $J(2^{a-1})$: Here we present a decisive relation between Fermat prime and [EC] $J(2^{a-1})$.

Fermat primes: In 1650, Pierre Fermat defined the sequence of numbers $F_n = 2^{2^n} + 1$ for $n \geq 0$, known as Fermat numbers. If F_n happens to be prime, F_n is called a Fermat prime. Fermat showed that F_n is a prime for each $n \leq 4$, and he conjectured that F_n is prime for all n. First five Fermat prime $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$ & $F_4=65537$, all primes. In 1732, Euler not only factorized $F_5=641.6700417$, but proved that all the factors of the composite Fermat numbers are of the form $k2^n+1$. It is known that F_n $(5 \leq n \leq 32)$ is composite and so far no special reason why a Fermat number should be considering prime is detected. As of the date of the paper was written, no new Fermat primes had been discovered and there is dilemma that there is only finite number of Fermat primes. Each [EC] of the type contain at least one Fermat prime or a square free factors of these primes as far as it's depends upon the availability of these primes. Unfortunately there are only five Fermat prime so far known and therefore we have only $32=2^5+1-1$ [EC] contains $a+1$ elements and other [EC] of contains 32 elements of the multiplicity 2^{a-1}.

[ECF] $J(2^{a-1})$: For $1 \leq a \leq 32$, we explore the special branch [EC] that has multiplicity $a+1$ and we call it [ECF] $J(2^{a-1})$. Two obvious member of [ECF] are $2^{a-1}+1$ and 2^a where $2^{a-1}+1$ is an odd prime number with $a = 2^n + 1$ for some $n \geq 0$ i.e. $P = 2^{a-1} + 1 = 2^{2^n+1-1} + 1 = 2^{2^n} + 1$ is a Fermat prime. Frequently Fermat prime in $J(2^{a-1})$ and plays an important roll to find other members of the [ECF] of multiplicity $a+1$. Let's define a function that connect [ECF] to various branch of mathematics and plays important roll in order to evaluate multiplicity of 2^{a-1} for $1 \leq a \leq 32$.

Definition: [ECF]Filter function: For $1 \leq a \leq 32$, define a function $f_a : J(2^{a-1}) \to Z_{a+1}$ by setting $f_a(x) = s_x$ where $s_x = \max\{t : 2^t \mid x, 0 \leq t \leq a\}$ and $x \in J(2^{a-1})$, we call this function as filter function .This function provides plenty of information about [ECF] $J(2^{a-1})$ like the number of elements in each class, nature of number within the class and the correspondence with Z_{a+1} (the set of residues system modulo $a+1$) provides a dais for the applications of the Euler-Carmichael's class [ECF] $C_m = J(2^{a-1})$ in Algebra as well. The following results evidently configure [ECF].

Divisibility by different prime factor plays an important role to study [ECF]. This is very useful to describe [ECF].

Lemma (a): If $m \geq 3$ then $\phi(m)$ is even and more precisely if m has k odd prime factors, then $2^k \mid \phi(m)$.

Proof: In view of the fact that

$$\phi(m) = m\prod_{p|m}\left(1 - \frac{1}{p}\right) = \frac{m}{\prod_{p|m} p}\left(\prod_{p|m}(p-1)\right)$$

The denominator of the fraction the most right hands is the product of primes dividing, so the fraction is actually an integer. The second term in bracket has at least one even factor for each odd prime dividing m, because if p is an odd prime then p-1 is even and there are such k odd prime divisor of m and therefore $\phi(m)$ is divisible by 2^k.

Lemma (b): If m has k odd prime factors and $m \in J(2^{a-1})$, then there exists an integer λ such that $\lambda \in J(2^{a-k})$. If m has k odd prime factors such that $V_\phi(m) = a+1$, then there exists an integer λ such that $V_\phi(\lambda) = a-k+2$.

Proof: By lemma (a), $2^k \mid \phi(m)$. Also $m \in J(2^{a-1})$ so that $\phi(m) = 2^{a-1}$. So there exists an integer $\lambda \in J(2^{a-k})$ and $V_\phi(\lambda) = a-k+2$.

Theorem 5: There is one-one correspondence between classes [ECF] $J(2^{a-1})$ and $f_a : J(2^{a-1}) \to Z_{a+1}$ for any integer $1 \leq a \leq 32$.

Proof: First of all we shall show that the above defined function $f_a : J(2^{a-1}) \to Z_{a+1}$ By setting $f_a(x) = s_x$ where $s_x = \max\{t : 2^t \mid x, 0 \leq t \leq a\}$ and $x \in J(2^{a-1})$. f_a is well defined. Let $x = y$ for any $x, y \in J(2^{a-1})$. By definition there exists non negative integers t_x any t_y such that $x = \lambda 2^{t_x}, y = \mu 2^{t_y}$ where λ and μ are odd numbers. If $t_x > t_y$, then μ is even, a contradiction. So that $t_x = t_y$. f_a is one to one function. Now we shall show that f_a is one to one function. Let $s_x = s_y$, then there exists λ and μ are odd numbers such that $x = \lambda 2^{s_x}$ and $y = \mu 2^{s_y}$. Since $s_x = s_y$, we get $\frac{x}{y} = \frac{\lambda}{\mu} = 2^s$, where s is non negative integer. If $s>0$, then we get λ is an even number, a contradiction. So that $s = 0$. Hence f_a is one to one function. Being correspondence plays between finite set, therefore f_a is in desired form.

Corollary 2: $J(2^{a-1})$ contains exactly $a+1$ natural number, i.e. $V_\phi(2^{a-1}) = a+1 > 1$ for every $1 \leq a \leq 32$.

Theorem 6: The number of elements in $J(2^{a-1})$ that are divisible by 3 is same as the number of elements that is co-prime with 3 in $J(2^{a-2})$.

Proof: Let $x \in J(2^{a-1})$ and $3 \mid x$.

$$\Rightarrow x = 3\lambda$$

where λ is an integer and not divisible by 3. Note that 9 do not divide any number in $J(2^{a-1})$ as elements are square free.

$$\Rightarrow \phi(x) = 2\phi(\lambda)$$

Then for each $x \in J(2^{a-1})$ and $3 \mid x$, there exists an integer λ co-prime to 3 such that $\lambda \in J(2^{a-2})$. So that the number of elements in $J(2^{a-1})$ that are divisible by 3 is same as the number of elements that are co-prime with 3 in $J(2^{a-2})$.

Lemma (c):

(1) If m has first k square free Fermat prime factors, then

$$\phi(m) = 2^{2^k - 1}$$

(2) If $m = \left(F_i = 2^{2^i} + 1\right)\left(F_j = 2^{2^j} + 1\right)$ with integers $I > j \geq 0$, then $\phi(m) = 2^{2^j\left(2^{i-j}+1\right)}$.

Proof:

(1) Since m has first k square free Fermat prime factors, we have

$$\phi(m) = m \prod_{p \mid m}\left(1 - \frac{1}{p}\right) = \left(\prod_{p \mid m}(p-1)\right)$$
$$= \prod_{0 \leq i \leq k-1} 2^{2^i} = 2^{2^k - 1}$$

where $p = F_i = 2^{2^i} + 1$ and $0 \leq i \leq k-1$.

(2) Being F_i and F_j are relatively prime, we have

$$\phi(m) = \phi(F_i . F_j) = 2^{2^i} . 2^{2^j} = 2^{2^j\left(2^{i-j}+1\right)}$$

Theorem 7: For any $n \geq m$ and $a \geq b$, F_n and F_m are Fermat prime such that $F_n \in J(2^{a-1})$ and $F_m \in J(2^{b-1})$, then $F_n . 2^{a-b+1} \in J(2^{a-1})$.

Proof: Compute $\phi(F_n . 2^{a-b+1}) = 2^{b-1}.2^{a-b} = 2^{a-1}$.

Corollary 3: For any $n \geq m$, F_n and F_m are two Fermat prime, C_{F_n} is a [ECF], then $F_m.2^{2^n - 2^m + 1} \in C_{F_n}$. This designate that if F_n is the largest Fermat prime in some [ECF], then there exists at least two in [ECF] such that $F_m \mid x$ for all $n \geq m$.

Theorem 8: For $1 \leq a \leq 32$, the number of elements in $J(2^{a-1})$ that divisible by 3 are $\frac{a-1}{2}$ if a is odd or $\frac{a}{2}+1$ if even respectively. Moreover, for $a \geq 33$, the number of elements in $J(2^{a-1})$ that divisible by 3 are 16.

Proof: Here the first five Fermat's primes are $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$ & $F_4=65537$ and their Euler's ϕ -function are $2^1,2^2,2^4,2^8,2^{16}$. For $1 \leq a \leq 32$, choose $m = F_i . m_0 . 2_t$ in $J(2^{a-1})$, where F_i is a Fermat prime, m_0 is the product of Fermat primes different from F_i , $i \geq 0$ and $0 \leq t \leq a$. Clearly and are relatively prime. We have

$$\phi(m) = \phi\left(F_i . m_0 . 2^t\right)$$
$$= 2^{2^i} . 2^{s-1} . 2^{t-1} = 2^{2^i + s + t - 2}$$

In particular take i=0, we have

$$\phi(m) = \phi\left(F_0 . m_0 . 2^t\right) = \phi\left(3 . m_0 . 2^t\right)$$
$$= 2^{2^0 + s + t - 2} = 2^{s+t-1}$$

Clearly $a = s+t$ and being s is an odd number, t is an even or odd number accordingly, a is an odd or even. Since $J(2^{a-1})$ is equivalent to Z_{a+1}. Therefore number of elements in $\{0,1,2,...a\}$ divisible by 3 are $\frac{a-1}{2}$ if a is odd or $\frac{a}{2}+1$ if a even respectively. For all $m = m_0 . 2^t$ in $J(2^{a-1})$, where

$$m_0 = \prod_{\substack{i=0 \\ 0 \leq j \leq 4}}^{j} F_i$$

is the product of Fermat primes such that $\phi(m) = 2^{a-t}$ and in particular take $a = 32$, then we have $J(2^{31}) = \{m_0.2^t : 0 \leq t \leq 32\}$. Now for $a \geq 33$, m_0 can be find

$$^5C_1 + {^5C_2} + {^5C_3} + {^5C_4} + {^5C_5}$$

ways as no new Fermat prime after that and $m_0 . 2^0$, $m_0 . 2^1$ are not in $J(2^{32})$ as they are member of $J(2^{31})$. Therefore $J(2^{32}) = \{m_0.2^t : 2 \leq t \leq 33\}$ and hence this [ECF] contains 32 solutions. Also for all $b \geq 1$, $J(2^{32+b}) = \{m_0.2^{t+b} : 2 \leq t \leq 33\} = 2^b . J(2^{32})$. Therefore we have $O(J(2^{32+b})) = O(J(2^{32})) = 32$.

RESULTS

Our main result motivated by corollary 2 and theorem 8. which assure to prove the Carmichael's Conjecture in this particular situation.

Example:

$$J(1)=\{1,2\};\ J(2)=\{3,4,6\};\ J(4)=\{5,8,10,12\};\ J(8)=\{15,16,20,24,30\}$$
$$J(16)=\{17,32,34,40,48,60\};\ J(32)=\{51,64,68,80,96,102,120\};$$
$$J(64)=\{5,17,5.17.2,3.17.2^2,17.2^3,3.5.2^4,5.2^5,3.2^6,2^7\};\ldots..$$

$$J(2^{31})=\left\{\begin{array}{l} 3.5.17.257.655373,3.5.17.257.655373.2,5.17.257.655373.2^2, \\ 3.17.257.655373.2^3,17.257.655373.2^4,3.5.257.655373.2^5, \\ 5.257.655373.2^6,3.257.655373.2^7,257.655373.2^8,3.5.257.655373.2^9, \\ 5.17.655373.2^{10},3.17.655373.2^{11},17.655373.2^{12},3.5.655373.2^{13}, \\ 5.655373.2^{14},3.655373.2^{15},3.5.17.257.655373.2^{16},3.5.17.257.2^{17},3.5.17.257.2^{18} \\ 3.17.257.2^{19},5.17.257.2^{20},3.5.17.257.2^{21},5.257.2^{22},3.257.2^{23},.257.2^{24}, \\ 3.5.17.2^{25},5.17.2^{26},3.17.2^{27},17.2^{28},3.5.2^{29},5.2^{30},3.2^{31},2^{32} \end{array}\right\}$$

$$J(2^{31})=\left\{\begin{array}{l} 3.5.17.257.655373.2^2,5.17.257.655373.2^3,3.17.257.655373.2^4, \\ 17.257.655373.2^5,3.5.257.655373.2^6,5.257.655373.2^7, \\ 3.257.655373.2^8,257.655373.2^9,3.5.17.655373.2^{10},5.17.655373.2^{11}, \\ 3.17.655373.2^{12},17.65537.2^{13},3.5.65537.2^{14},5.65537.2^{15},3.65537.2^{16}, \\ 3.5.17.257.2^{17},3.5.17.257.2^{18},5.17.257.2^{19},3.17.257.2^{20}, \\ 5.17.257.2^{21},3.5.257.2^{22},5.257.2^{23},3.257.2^{24},257.2^{25}, \\ 3.5.17.2^{26},5.17.2^{27},3.17.2^{28},17.2^{29},3.5.2^{30},5.2^{31},3.2^{32},2^{33} \end{array}\right\}$$

REFERENCES

Carmichael, R.D., 1907. On Euler's ϕ -function, Bull.A.M.S., 13: 241-243.

Carmichael, R.D., 1922. Note on Euler's ϕ -function, Bull.A.M.S. 28: 109-110.

Gupta, H., 1950. On a problem of Erdos. Am. Math. Monthly, 57: 326-329.

Guy, R.K., 1983. Monthly unsolved problems – 1969-1983. Am. Math. Monthly, 90(10): 684.

Mendelsohn, N.S., 1976. The equation $\phi(x) = m$. Math.Mag, 49: 37-39.

Selfridge, J.L., 1963. Solution of a problem by Ore. Am. Math. Monthly, 70: 101.