Theory of n-composite naturals and determination of the generating set for primes of the form 24m+1

Chandan Chattopadhyay
Department of Mathematics
Narasinha Dutt College, Howrah
Email: chandanmath2011@gmail.com

In this paper, concept of 'n-composite natural' has been introduced for naturals of the form 6k+1. A theory has been developed which helps in identifying naturals of the form 6k +1 for different nature of the values of k. It reveals that a natural of the form 24m+1 can be 4n-composite only which finally helps to specify the set of naturals m for which 24m+1 is prime.

Keywords: *Natural numbers, Composite, Prime.*

1. Introduction

To establish an effective algorithm for determining primes is of great interest in the study of number theory. There are many characterizations [1], [3], [4] and algorithms [2], [5],[6] already appeared in literature for determining primes, but the theory developed in this article will supply information on the composites of the form 6k+1, and thereafter answer the following question:

'Can we determine the particular subset of N consisting of naturals m for which $24m + 1$ is prime ?'

Since primes (>3) are of the form $6k-1$ or $6k+1$, in this article we shall consider naturals of the form $6k+1$ only and develop a theory on composite naturals of this form. This theory observes special features of composite naturals of the form $6k+1$ depending upon nature of k.

Since every composite of the form $6k+1$ has proper factors of the form $6t+1$ or $6t-1$ only, it clearly follows that for a composite $6k+1$, $6k+1 = AB$ where A and B are proper factors of $6k+1$ where $B-A = 6n$ for some natural n (ignoring the case that $6k+1$ is a perfect square).

Thus we define

Definition 1.1 *Let the composite* $6k + 1$ *be not a perfect square. Then* $6k + 1$ *is said to be n-composite for some natural n if* $6k+1 = AB$ *for some proper factors A, B of* $6k+1$ *where* $B - A = 6n$.

For example, $55 = 6.9 + 1$ and $55 = 5.11$, where $11 - 5 = 6 = 6.1$. Hence 55 is 1-composite.

Also an n-composite $6k+1$ may be m-composite for some $m(\neq n)$. For example, $385 = 5.7.11$. Hence it is 4-composite, 8-composite and 12-composite.

2 Properties of n-composite naturals and determination of the generating set for primes of the form 24m+1

Theorem 2.1. If $6k+1$ is n-composite then $n \leq \frac{k-4}{5}$.

Proof. Clearly $A \geq 5$, $B \geq 5$. Hence $6k + 1 \geq 5(6n + 5)$. This completes the proof.

Theorem 2.2. If $6k+1$ is $2n$-composite then $n \leq \frac{k-4}{10}$.
Proof is easy.

Theorem 2.3. If $6k+1$ is $4n$-composite then $n \leq \frac{k-4}{20}$.

Proof is easy.

Theorem 2.4. If $6k + 1$ is n-composite then $9n^2 + 6k + 1$ is a perfect square.

Proof. Let $6k + 1 = AB$, $B - A = 6n$. Then $A(A + 6n) - (6k + 1) = 0$ and hence $A = -3n + \sqrt{9n^2 + 6k + 1}$. If A exists then the result follows.

The following lemma will help in proving Theorem 2.6 and Theorem 2.7.

Lemma 2.5. *If t is an odd natural then the equation* $x^2 - y^2 = 6t$ *has no positive integer solutions for x and y.*

Proof. If possible, let $x^2 - y^2 = 6t$ for some naturals x and y where t is an odd natural.

Then $(x + y)(x - y) = 6t$ implies that x and y cannot be even or odd simultaneously, because in that case 4 is a factor of $(x + y)(x - y)$ but 4 is not a factor of $6t$. Hence if x is even then y is odd or if x is odd then y is even. But, in any case $(x + y)(x - y)$ is odd whereas $6t$ is always even. Hence a contradiction arises. This proves the lemma.

Theorem 2.6. *If* $6k + 1$ *is n-composite then* $(6k + 1) + 6t$ *is not n-composite for every odd natural t.*

Proof. Let $6k + 1$ be n-composite and if possible, let $(6k + 1) + 6t$ be n-composite for some odd t. Let $6k + 1 + 6 = AB$ where $B - A = 6n$. Then $A = -3n + \sqrt{9n^2 + 6k + 1 + 6t}$ and since A exists, $9n^2 + 6k + 1 + 6t = y^2$ for some $y \in N$.

Then $9n^2 + 6k + 1 = y^2 - 6t$ (1)

Also by theorem 4, for some $x \in N$ we have

$9n^2 + 6k + 1 = x^2$ (2)

Then by (1) and (2), $y^2 - x^2 = 6t$. But, by Lemma 1, this is not possible. Hence the theorem is proved.

Theorem 2.7.

(*i*) *If k is even then 6k + 1 is not n-composite for every odd n.*

(ii) If k is odd then 6k + 1 is not n-composite for every even n.

Proof. (i): Let k be even. Note that for any n, $(6k + 1)(6k + 1 + 6n)$ is n-composite. Now

$(6k + 1)(6k + 1 + 6n) = (6k + 1) + 6(6k + 1)(k + n) = (6k + 1) + 6t$ say, where $t = (6k + 1)(k + n)$. Hence if n is odd then t is odd, where $(6k + 1) + 6t$ is n-composite. So by theorem 5 it follows that $6k + 1$ is not n-composite. Thus if k is even then $6k + 1$ is not n-composite for every odd n.

(ii) : Let k be odd. Following lines of proof given in (i) we can conclude the result.

Theorem 2.9 and Theorem 2.10 are consequences of the following lemma.

Lemma 2.8. *If t is any odd natural then the equation* $x^2 - y^2 = 12t$ *does not possess any positive odd integer solutions for x and y.*

Proof. If possible, let $x^2 - y^2 = 12t$ for some odd naturals x and y where t is an odd natural.

Let $x = 2t_1 - 1$ and $y = 2t_2 - 1$. Then $(x + y)(x - y) = 12t$ implies $(t_1 + t_2 - 1)(t_1 - t_2) = 3t$.

Since t is odd, both $t_1 + t_2 - 1$ and $t_1 - t_2$ are odd. Let $t_1 + t_2 - 1 = 2A - 1$ and $t_1 - t_2 = 2B - 1$. Adding we get

$2t_1 = 2(A + B) - 1$, which is absurd, since L.H.S. is even whereas R.H.S. is odd. This proves the lemma.

Theorem 2.9. *If* $6k + 1$ *is* $2n$*-composite then* $(6k + 1) + 12t$ *is not* $2n$*-composite for every odd natural* t.

Proof. Let $6k + 1$ be $2n$-composite and if possible, let $(6k + 1) + 12t$ be $2n$-composite for some odd t. Let $6k + 1 + 12t = AB$ where $B - A = 6.2n = 12n$. Then $A = -6n + \sqrt{36n^2 + 6k + 1 + 12t}$ and since A exists, $36n^2 + 6k + 1 + 12t = y^2$ for some $y \in N$.

Then $36n^2 + 6k + 1 = y^2 - 12t$ (3)

Also by theorem 4, for some $x \in N$ we have

$9.(2n)^2 + 6k + 1 = x^2$ (4)

Then by (3) and (4), $y^2 - x^2 = 12t$. Note that x and y are both odd. But, by lemma 2, this is not possible. Hence the theorem is proved.

Theorem 2.10. *If* $k = 4m$ *for any natural* m *then* $6k + 1$ *is not composite for every odd* n.

Proof. Note that for any n, $(6k + 1)(6k + 1 + 12n)$ is $2n$-composite. Now

$(6k + 1)(6k + 1 + 12n) = (6k + 1) + 6(6k + 1)(k + 2n) = (6k + 1) + 12t$ say, where $t = (6k+1)\frac{k+2n}{2}$. Now $k = 4m$. So $t = (6k + 1)(2m + n)$. Hence if n is odd then t is odd, where $(6k + 1) + 12t$ is $2n$-composite. So by theorem 7 it follows that $6k + 1$ is not 2n-composite. Thus if $k = 4m$ then $6k + 1$ is not $2n$-composite for every odd n.

Now we have the following result.

Corollary 2.11. *If* $k = 4m$ *then*

(i) $6k + 1$ *is not n-composite for every odd n and*

(ii) $6k + 1$ *is not* $2n$*-composite for every odd n.*

Proof follows from theorem 2.7 and theorem 2.11.

As a consequence we get

Theorem 2.12. *Let* $k = 4m$ *and* $6k + 1$ *be not a perfect square. Then the following statements are equivalent :*

(i) $24m + 1$ *is prime.*

(ii) $24m + 1 \neq t(24n + t)$ *for all* $n \leq \frac{m-1}{5}$ *and any* t *of the form* $6v - 1$ *or* $6v + 1$.

Proof. (ii) → (*i*). Let $24m + 1$ be composite. Then by corollary 2.11, it can only be $4n$-composite. Hence by theorem 2.3, $n \leq \frac{m-1}{5}$. Now by theorem 2.4, we have $9(4n)^2 + 24m + 1 = y^2$ for some natural y. Then

$9(4n)^2 + 24m + 1 = y^2 = (12n + t)^2$ (5)

for some natural t. So $24m + 1 = t(24n + t)$. Now L.H.S. of (5) is of the form $6w + 1$. Hence t must be of the form $6v - 1$ or $6v + 1$. This completes the proof.

(i) → (ii). This is obvious.

Corollary 2.13. *Let* $k = 4m$ *and* $6k + 1$ *be not a perfect square. Then the following statements are equivalent :*

(i) $24m + 1$ is prime.

(ii) $m \neq nt + \frac{t^2 - 1}{24}$ *for all* $n \leq \frac{m-1}{5}$ *and any* t *of the form* $6v - 1$ *or* $6v + 1$.

(iii) $24m + 1$ is not congruent to $t^2 (\text{mod } 24t)$, for any $t\left(< \sqrt{24m+1}\right)$ of the form $6v - 1$ or $6v + 1$.

Proof is evident.

Now we consider the following important question:

Can we completely determine the particular subset P(24) (say) of N such that for each $m \in P(24)$, $24m + 1$ is prime and conversely if $24m + 1$ is prime then $m \in P(24)$?

The answer to this question is as follows :

Consider the following subsets of N.

$TF(1) = \{nt + \frac{t^2 - 1}{24} : n \in N, t \in N, t = 6v - 1$ or $t = 6v + 1, v \in N\}$.

$TF(2) = \{m : m \in N, 24m + 1 = y^2$, for some $y \in N\}$.

Members of $TF(1)$ are of the forms, $5n + 1, 7n + 2, 11n + 5, 13n + 7, 17n + 12$,............ and so on.

Let $S = TF(1) \cup TF(2)$.

Then it follows by corollary 2.13 that the subset $P(24) = N - S$ of N will be the Prime determining subset for the naturals of the form $24m + 1$. This means, for every $m \in P(24)$, $24m + 1$ is prime and conversely, if $24m + 1$ is prime then $m \in P(24)$.

Writing members of S in ascending order we can enumerate members of $P(24)$ in ascending order.

One can verify the main result obtained in this article for any finite subset of N by using the following algorithm.

Algorithm :

1. Set limit.

2. Generate set $TF(2)$:

2.1. Set $TF(2) \leftarrow \{\}$.

2.2. Set $m \leftarrow 1$.

2.3. While $m \leq$ limit

2.3.1. Set $y^2 + 24m + 1$

2.3.2. If y^2 is a perfect square, add m to TF(2).

2.3.3. Set m $\leftarrow$ m +1 and iterate loop.

3. Generate set $TF(1)$:

3.1. Set $S_1 \leftarrow \{\}$, $S_2 \leftarrow \{\}$, flag $\leftarrow 0$.

3.2. Set $V \leftarrow 1$.

3.3. While $V \leq$ limit

3.3.1. If flag =1, break loop.

3.3.2. Set $n \leftarrow 1$.

3.3.3. While n $\leq$ limit

3.3.3.1. Set $t \leftarrow 6V - 1$, $t_2 \leftarrow 6V + 1$.

3.3.3.2. Set $a \leftarrow n.t_1 + \frac{1}{24}(t_1^2 - 1)$.

3.3.3.3. If $a \leq$ limit, add a to S_1,
else if n = 1, set flag $\leftarrow$ 1 and break current loop, else break current loop.

3.3.3.4. Set $b \leftarrow n.t_2 + \frac{1}{24}(t_2^2 - 1)$.

3.3.3.5. If b $\leq$ *limit*, add b to S_2.

3.3.3.6. Set $n \leftarrow n + 1$ and iterate loop.

3.3.4. Set $V \leftarrow$ V + 1 and iterate loop.

3.4. Set $TF(1) + S_1 \cup S_2$.

4. Set $S \leftarrow TF(1) \cup TF(2)$.

5. Set $N \leftarrow \{1,2,3,\ldots\ldots,$ (largest element of S)$\}$.

6. Set $P(24) \leftarrow N - S$.

7. Set P $\leftarrow \{24p + 1 : p \in P(24)\}$.

8. If all elements of P are prime, declare success, else declare failure.

Conclusion :

It is worthwhile to mention that primes are important in Computer Science and Cryptography because the security of many encryption algorithms is based on the fact that the multiplication of two large prime numbers is very fast, but takes a lot of processing to do the reverse.

This article develops a method which gives us the particular values of m for which $24m + 1$ are prime numbers. An algorithm has been constructed which helps in finding larger values of m and the corresponding values of the primes $24m + 1$. In this way, this algorithm will certainly be helpful in obtaining larger prime numbers which will be useful in developing certain encryption techniques.

Acknowledgement :

I am thankful to my son Archan Chattopadhyay, student of Indian Institute of Science, Bengaluru, India, for his full cooperation in constructing the algorithm in this article. I am grateful to the reviewer for useful comments and suggestions.

References

Adleman, L.A., C. Pomerance, Rumely, R.S., On distinguishing prime numbers from composite numbers, Ann. Math., 117(1983), 173-206.

Agarwal, M., Kayal, N., Saxena, N.,Primes is in P, *Ann. Math*. 160(2004), 781-793.

Bruce,J.W., A Really Trivial Proof of the Lucas Lehmer Test. *The American Mathematical Monthly*. 100(4)(1993), 370 – 371.

Burton, D., Elementary Number Theory, *Allyn and Bacon*, 1976, ISBN 0–205–06965 – 7.

Rabin, M.O., Probabilistic algorithm for testing primality, *J. Number Theory*, 12(1980), 128-138.

Solovay, R., Strassen, V., A fast Monte-Carlo test for primality, *Siam Journal on Computing*, 6 (1977), 84-86.