IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 12, Issue 5 Ver. VIII (Sep. - Oct.2016), PP 01-07
www.iosrjournals.org

Seed and Sieve of Odd Composite Numbers with Applications in Factorization of Integers

Xingbo WANG
[1]*(Department of Mechatronics, Foshan University, Foshan City, Guangdong Province, PRC, 528000)*

Abstract: *The article aims at knowing the type of factors by which a multiplication of integers is produced. By putting forward the concept of composite seed of an odd composite number, the article constructs a sieve to select and produce odd composite numbers of the form 6n±1 and then demonstrates several theorems related with factorization of an odd composite number in terms of its seed. It shows that factorization of a big odd number can be converted into that of small numbers incorporated with the big number's seed. The article also makes an investigation on new characteristics of odd numbers as well as their factorization and reveals several innate laws that are helpful for finding factors of odd numbers. The revealed laws indicate that an odd number might find its factors near the factors of its neighboring odd composite numbers. Subtle mathematical deductions are given for all the conclusions and necessary examples are presented with detail interprets.*

Keywords: *Sieve, Odd numbers, Integer Factorization, Information security*

I. Introduction

Positive odd numbers that are of the form with integer are generally classified into two kinds, odd prime numbers and odd composite numbers. The study of these numbers has been topics in number theory for several hundred years, as introduced in [1]. People have spent much time on study of the prime numbers and factorization of the composite numbers, and the problem of factorizing a large odd number has still been a well-known difficult problem in the world, as stated in articles [2] and [3]. However, when analyzing the present literatures, one will see that, few literatures concern the innate constituents of a multiplication that comes from prime factors' multiplying.

A recent study on multiplication of two nodes of the valuated binary tree, which is introduced in articles [4], implicates the problem of knowing the multiplication's sources, that is, by what kind of nodes the multiplication is produced. This problem is alternatively the problem of knowing what kind of prime factors a composite number is produced by. For example, 45=5×9 with 5 and 9 being of the form 4*k*+1, 21=3×7 with 3 and 7 being of the form 4*k*-1 and 15=3×5 with 3 and 5 being 4*k*-1 and 4*k*+1 respectively. It is sure that, knowing the factors' sources of a composite number is helpful to reduce a large amount of computations when searching a factor of the composite number.

This article aims at solving the problem. The article first puts forward the concept of composite seed of an odd composite number, then constructs a sieve to select and produce odd composite numbers, and then proves several theorems related with factorization of an odd composite in terms of the seeds. Also the article makes an investigation on characteristics of odd numbers of the form 6*n*±1 together with their factorization and obtains several new properties that are helpful for factorization of an odd composite number.

II. Preliminaries

2.1 Definitions and Notations

In this whole article, symbol $\boldsymbol{Z}$ denotes all integers, symbol $\boldsymbol{Z}^{+}$ denotes all the positive integers and symbol $\boldsymbol{Z}^{+0}$ denotes the positive integers together with 0. Symbol $A \Rightarrow B$ means that result B is derived from condition A; symbol $\exists x \in \boldsymbol{Z}^{+}$ means there exists an x in set $\boldsymbol{Z}^{+}$. Symbol $a|b$ means b can be divided by a; symbol a Œb means b cannot be divided by a. Symbol (a, b) and $[a, b]$ are to express respectively the greatest common divisor (GCD) and the least common multiple (LCM) of integers a and b. In this whole article, odd number refers to that is bigger than 3 unless special remark is made. Integer of 3's multiple is simply denoted by 3_m.

Definition 1: An integer k is called a composite seed, or simply a seed, of number 6*k*+1(or 6*k*-1) if the number 6*k*+1(or 6*k*-1) is an odd composite number; meanwhile, the composite 6*k*+1(or 6*k*-1) number is a sprout of the seed k. For example, 8 is the seed of 49 and 11 is the seed of 65; 49 and 65 are sprouts of 8 and 11 respectively.

2.2 Lemmas

Lemma 1: An arbitrary non-negative integers $N \ge 0$ can be expressed by $N = 6n + r, 0 \le r \le 5$, and an odd number bigger than 3 must be of the form either $N = 6n - 1$ or $N = 6n + 1$, where $n \in \boldsymbol{Z}^{+}$.

DOI: 10.9790/5728-1205080107

Lemma 2[5]: An odd number of the form of $3k+1$ must be also of the form of $6n+1$; an odd number of the form of $3k+2$ must be also of the form of $6n-1$. A composite number $6n+1$ must be product of either two factors of the form $6k+1$ or two factors of the form $6k-1$; a composite number $6n-1$ must be product of one factor of the form $6k+1$ with the other of the form $6k-1$.

Lemma 3[6]: Let *p* be a positive odd integer; then among *p* consecutive positive odd integers there exists one and only one that can be divisible by *p*.

Lemma 4[4]: Let *q* be a positive odd number, $S=\{a_i \ | i\in \boldsymbol{Z}^+\}$ be a set that is composed of consecutive odd numbers; if $a_\alpha \in S$ is a multiple of *q*, then so it is with $a_{\alpha+q}$.

III. Main Results and Proofs

Main results in this section include 3 parts. The first part shows the critical pole of the seed in factorization of odd composite number 6*n*±1, the second constructs a sieve to produce composite numbers of 6*n*±1 and shows the way to apply the sieve to factorize composite numbers of 6*n*±1, the third is to show some new properties of the numbers 6*n*±1 and their aids to integers' factorization.

3.1 Seeds and Factorization of Odd Numbers

Theorem 1: The seed of an odd composite number is highly related to the factorization of the composite number by the following rules.

(*i*) The necessary and sufficient condition for a composite number $6n+1$ has a factor $6x+1$ or $6y-1$ is that $(6x+1)|(n-x)$ or $(6y-1)|(n+y)$ respectively.

(*ii*) The necessary and sufficient condition for a composite number $6n-1$ has a factor $6x+1$ or $6y-1$ is that $(6x-1)|(n-x)$ or $(6y+1)|(n+y)$ respectively.

Proof: Here the proof is only for (*i*) since (*ii*) can be proved by the same means.

Sufficiency

$$6x+1|(n-x)\Rightarrow n=(6x+1)m+x\Rightarrow 6n+1=36xm+6x+6m+1=(6x+1)(6m+1)$$
$$6y-1|(n+y)\Rightarrow n=(6y-1)m-y\Rightarrow 6n+1=36ym-6y-6m+1=(6y-1)(6m-1)$$

Necessity

$$6n+1=\begin{cases}(6x+1)(6m+1)\\(6y-1)(6m-1)\end{cases}\Rightarrow 6n+1=\begin{cases}36mx+6x+6m+1\\36my-6y-6m+1\end{cases}=\begin{cases}6(m(6x+1)+x)+1\\6(m(6y-1)-y)+1\end{cases}$$
$$\Rightarrow\begin{cases}n=m(6x+1)+x\\n=m(6y-1)-y\end{cases}\Rightarrow\begin{cases}(6x+1)|(n-x)\\(6y-1)|(n+y)\end{cases}$$

□

The following Theorem 1 can alternatively state theorem 1*.

Theorem 1*: All the odd numbers have the following properties.

(*i*) The necessary and sufficient condition for a composite number $6n+1$ can be factorized by $6n+1=(6l_1+1)(6k_1+1)$ or $6n+1=(6l_2-1)(6k_2-1)$ is that $n=l_1(6k_1+1)+k_1=k_1(6l_1+1)+l_1$ or $n=l_2(6k_2-1)-k_2 \quad =k_2(6l_2-1)-l_2$, where l_1,l_2,k_1 and k_2 are integers less than *n*;

(*ii*) The necessary and sufficient condition for a composite number $6n-1$ can be factorized by $6n-1=(6l+1)(6k-1)$ is that $n=l(6k-1)+k \quad =k(6l+1)-l$, where l,k are positive integers less than *n*;

3.2 Sieves of Odd Composite Numbers

Construct four sequences, $\boldsymbol{S}_1^+,\boldsymbol{S}_2^+$, $\boldsymbol{S}_1^-$ and $\boldsymbol{S}_2^-$, such that

$\boldsymbol{S}_1^+=\{n|N=6n+1=(6k+1)(6l+1);\exists k,l\in\boldsymbol{Z}^+\}$

$\boldsymbol{S}_2^+=\{n|N=6n+1=(6k-1)(6l-1);\exists k,l\in\boldsymbol{Z}^+\}$

$\boldsymbol{S}_1^-=\{n|N=6n-1=(6k+1)(6l-1);\exists k,l\in\boldsymbol{Z}^+\}$

$\boldsymbol{S}_2^-=\{n|N=6n-1=(6k-1)(6l+1);\exists k,l\in\boldsymbol{Z}^+\}$

Obviously, each item in $\boldsymbol{S}_1^+,\boldsymbol{S}_2^+$, $\boldsymbol{S}_1^-$ and $\boldsymbol{S}_2^-$ is a seed of an odd composite number. By Theorem 1*, $\boldsymbol{S}_1^+$, $\boldsymbol{S}_2^+$, $\boldsymbol{S}_1^-$ and $\boldsymbol{S}_2^-$ can be redefined by

$\boldsymbol{S}_1^+=\{n|n=l(6k+1)+k=k(6l+1)+l;k,l\in\boldsymbol{Z}^+\}$ (1)

$\boldsymbol{S}_2^+=\{n|n=l(6k-1)-k=k(6l-1)-l;k,l\in\boldsymbol{Z}^+\}$ (2)

$\boldsymbol{S}_1^-=\{n|n=l(6k-1)+k=k(6l+1)-l;k,l\in\boldsymbol{Z}^+\}$ (3)

$\boldsymbol{S}_2^-=\{n|n=l(6k+1)-k=k(6l-1)+l;k,l\in\boldsymbol{Z}^+\}$ (4)

Note that, for a fixed *k*, $\boldsymbol{S}_1^+$ is an arithmetic progression with $6l^2+2l$ being the initial term and $6l+1$ being the common difference in terms of counting *k* from *l*; hence $\boldsymbol{S}_1^+$ can be equivalently expressed by

$$\boldsymbol{S}_1^+ = \{s_{1,k}^+ \mid s_{1,l}^+ = s_0 + (k-1)d, s_0 = 6l^2 + 2l, d = 6l+1; k,l \in \boldsymbol{Z}^+\} \qquad (5)$$

Actually, let $K = l + k - 1$ then

$$s_{1,k}^+ = 6l^2 + 2l + (k-1)(6l+1) = 6l^2 + 2l + 6kl + k - 6l - 1 = l(6(l+k-1)+1) + l + k - 1 = l(6K+1) + K = K(6l+1) + l$$

which asserts (4) is equivalent to (1).

Similarly, $\boldsymbol{S}_2^+$ and $\boldsymbol{S}^-$ can be equivalently expressed by

$$\boldsymbol{S}_2^+ = \{s_{2,l}^+ \mid s_{2,l}^+ = s_0 + (k-1)d, s_0 = 6l^2 - 2l, d = 6l-1; k,l \in \boldsymbol{Z}^+\} \qquad (6)$$

$$\boldsymbol{S}_1^- = \{s_{1,l}^- \mid s_{1,l}^- = s_0 + (k-1)d, s_0 = 6l^2, d = 6l+1; k,l \in \boldsymbol{Z}^+\} \qquad (7)$$

$$\boldsymbol{S}_2^- = \{s_{2,l}^- \mid s_{2,l}^- = s_0 + (k-1)d, s_0 = 6l^2, d = 6l-1; k,l \in \boldsymbol{Z}^+\} \qquad (8)$$

Sequences (1), (2), (3) and (4) or their equivalent expressions (5), (6), (7) and (8) can of course form a sieve to select every odd composite number of 6*n* ± 1 with $n \in \boldsymbol{Z}^+$. In addition, the following Theorem 2 and 3 provide computational foundations.

Theorem 2: Suppose *N* is an odd composite number; then the following statements are true.

(*i*) If $N = 6n+1$ and there exists a $k < \frac{\sqrt{n}+1}{2}$ such that $(6k+1) \mid (n-k)$, then $(6k+1) \mid N$.

(*ii*) If $N = 6n+1$ and there exists a $k < \frac{\sqrt{n}+1}{2}$ such that $(6k-1) \mid (n+k)$, then $(6k-1) \mid N$.

(*iii*) If $N = 6n-1$ and there exists a $k < \frac{\sqrt{n}+1}{2}$ such that $(6k-1) \mid (n-k)$, then $(6k-1) \mid N$.

(*iv*) If $N = 6n-1$ and there exists a $k < \frac{\sqrt{n}+1}{2}$ such that $(6k+1) \mid (n+k)$, then $(6k+1) \mid N$.

Proof: Take the cases (*i*) and (*ii*) as examples. It can see that

$$(6k+1) \mid (n-k) \Rightarrow n = a(6k+1) + k, a \in \boldsymbol{Z}^+ \Rightarrow 6n+1 = 6(a(6k+1)+k)+1 = (6k+1)(6a+1)$$

which validates $(6k+1) \mid N$.

Now since $6k+1$ is a factor of $N = 6n+1$, it leads to

$$(6k+1) \le \sqrt{6n+1} \Rightarrow l \le \frac{\sqrt{6n+1}-1}{6} \Rightarrow l < \frac{\sqrt{6(n+1)}}{6} = \frac{\sqrt{6}}{6}\sqrt{n+1} < \frac{\sqrt{n+1}}{2} < \frac{\sqrt{n}+1}{2}$$

which finishes proof of the case (*i*).

For case (*ii*), it yields

$$(6k-1) \mid (n+k) \Rightarrow n = a(6k+1) - k, a \in \boldsymbol{Z}^+ \Rightarrow 6n+1 = 6(a(6k-1)-k)+1 = (6k-1)(6a-1)$$

and

$$(6k-1) \le \sqrt{6n-1} \Rightarrow l \le \frac{\sqrt{6n-1}+1}{6} \Rightarrow l < \frac{\sqrt{6n}+\sqrt{6}}{6} < \frac{\sqrt{n}+1}{2}$$

□

Theorem 3: Suppose *N* is an odd composite number; then the following statements are true.

(*i*) If $N = 6n+1$ and there exists an $l < 1 + \frac{\sqrt{n}}{6}$ such that $s_0 = 6l^2 + 2l$, $d = 6l+1$ and $d \mid (n - s_0)$; then $d \mid N$.

(*ii*) If $N = 6n+1$ and there exists an $l < 1 + \frac{\sqrt{n}}{6}$ such that $s_0 = 6l^2 - 2l$, $d = 6l-1$ and $d \mid (n - s_0)$; then $d \mid N$

(*iii*) If $N = 6n-1$ and there exists an $l < 1 + \frac{\sqrt{n}}{6}$ such that $s_0 = 6l^2$, $d = 6l+1$ and $d \mid (n - s_0)$; then $d \mid N$.

(*iv*) If $N = 6n-1$ and there exists an $l \le 1 + \frac{\sqrt{n}}{6}$ such that $s_0 = 6l^2$, $d = 6l-1$ and $d \mid (n - s_0)$, then $d \mid N$.

Proof: Take only case (*i*) as an example to show $d \mid (n - s_0) \Rightarrow d \mid (N = 6n+1)$. It can see that

$$(6l+1) \mid (n - (6l^2 + 2l)) \Rightarrow n = a(6l+1) + (6l^2 + 2l) \Rightarrow 6n+1 = 6(a(6l+1) + (6l^2 + 2l)) + 1$$
$$= 36al + 6a + 36l^2 + 12l + 1 = (6l+1)(6a + 6l + 1)$$
$$(6l-1) \mid (n - (6l^2 - 2l)) \Rightarrow n = a(6l-1) + (6l^2 - 2l) \Rightarrow 6n+1 = 6(a(6l-1) + (6l^2 - 2l)) + 1$$
$$= 36al - 6a + 36l^2 - 12l + 1 = (6l-1)(6a + 6l - 1)$$

Now estimate the bounds of *l* for each case.

(*i*) :

$$(6l+1)\,|\,(n-(6l^2+2l)) \Rightarrow (6l+1)^2 \le (n-(6l^2+2l)) \Rightarrow 42l^2+14l-(n-1)\le 0$$

$$\Rightarrow l \le \frac{-14+\sqrt{(2\times 7)^2+12\times 14(n-1)}}{6\times 14} < \frac{\sqrt{n+1}-1}{6} < 1+\frac{\sqrt{n}}{6}$$

(*ii*)

$$(6l-1)\,|\,(n-(6l^2-2l)) \Rightarrow (6l-1)^2 \le (n-(6l^2-2l)) \Rightarrow 42l^2-14l-(n-1)\le 0$$

$$\Rightarrow l \le \frac{14+\sqrt{14^2+12\times 14(n-1)}}{6\times 14} < \frac{\sqrt{n}+1}{6} < 1+\frac{\sqrt{n}}{6}$$

(*iii*)

$$(6l+1)\,|\,(n-6l^2) \Rightarrow 36l^2+12l+1 \le n-6l^2 \Rightarrow 42l^2+12l-(n-1)\le 0$$

$$\Rightarrow l \le \frac{-12+\sqrt{12^2+168(n-1)}}{84} < \frac{-12+13\sqrt{n}}{7\times 12} = -\frac{1}{7}+\frac{13\sqrt{n}}{6\times 14} < 1+\frac{\sqrt{n}}{6}$$

(*iv*)

$$(6l-1)\,|\,(n-6l^2) \Rightarrow 36l^2-12l+1 \le n-6l^2 \Rightarrow 42l^2-12l-(n-1)\le 0$$

$$l \le \frac{12+\sqrt{12^2+168(n-1)}}{84} < \frac{12+13\sqrt{n}}{6\times 14} = \frac{1}{7}+\frac{13\sqrt{n}}{6\times 14} < 1+\frac{\sqrt{n}}{6}$$

□

3.3 Characteristics of Odd Composite Numbers 6*n*±1

Putting consecutive odd numbers one after another to form a sequence ***O*** by

O={1,3, 5, 7, 9, 11,13,15, 17, … , }

One can see that, by taking 1 to be of the form 6*n*+1, the number before 3_m is of the form 6*n*+1 and the number after 3_m is of the form 6*n*-1. It also sees that, such a law is valid for arbitrary sub-sequence ***O***$_s$ of ***O***, say ***O***$_s$={7,9,11,…}. For this reason, ***O*** can be partitioned by a series of group-units by

$$\boldsymbol{O}=\{\underbrace{1,3,5}_{g_1},\underbrace{7,9,11}_{g_2},\underbrace{13,15,17}_{g_3},\underbrace{19,21,23}_{g_4},\underbrace{25,27,29}_{g_5},\underbrace{31,33,35}_{g_6},\underbrace{37,39,41}_{g_7},\underbrace{43,45,47}_{g_8},\underbrace{49,51,53}_{g_9},$$

$$\underbrace{55,57,59}_{g_{10}},\underbrace{61,63,65}_{g_{11}},\underbrace{67,69,71}_{g_{12}},\underbrace{73,75,77}_{g_{13}},\underbrace{79,81,83}_{g_{14}},\underbrace{85,87,89}_{g_{15}},\underbrace{91,93,95}_{g_{16}},\underbrace{97,99,101}_{g_{17}},$$

$$\underbrace{103,105,107}_{g_{18}},\underbrace{109,111,113}_{g_{19}},\underbrace{115,117,119}_{g_{20}},\underbrace{121,123,125}_{g_{21}},\underbrace{127,129,131}_{g_{22}},\underbrace{133,135,137}_{g_{23}},$$

$$\underbrace{139,141,143}_{g_{24}},\underbrace{145,147,149}_{g_{25}},\underbrace{151,153,155}_{g_{26}},\underbrace{157,159,161}_{g_{27}},\underbrace{163,165,167}_{g_{28}},\underbrace{169,171,173}_{g_{29}},...\}$$

Denote $g_{(i,1)}, g_{(i,2)}$ and $g_{(i,3)}$ to express the first, the second and the third number of group g_i; then it is true for $i=1,2,...$

$$\begin{cases} g_{(i,1)}=6(i-1)+1=g_{(i,2)}-2=g_{(i-1,3)}+2 \\ g_{(i,2)}=6(i-1)+3=g_{(i,1)}+2=g_{(i,3)}-2 \\ g_{(i,3)}=6(i-1)+5=g_{(i,2)}+2=g_{(i+1,1)}-2 \\ g_{(i,j)}=6(i-1)+2j-1,\ j=1,2,3 \\ i=(g_{(i,3)}+1)/6=(g_{(i,1)}+5)/6 \\ j=3-(1+g_{(i,j)})(\bmod 3) \end{cases} \qquad (9)$$

Then the following Theorem 4 holds.

Theorem 4: For the sequence ***O***, the following statements are true.

(*i*) For arbitrary $m\in \boldsymbol{Z}^+$, $m\equiv 0(\bmod 5)$ leads to $5\,|\,g_{(m,1)}$ and $5\,|\,g_{(m+1,3)}$.

(*ii*) Arbitrary $m,k\in \boldsymbol{Z}^+$ yield

$$g_{(m,j)}+6k=g_{(m+k,j)},\ j=1,2,3$$

and arbitrary integer *m*>1 yields

$$g^2_{(m,1)}=g_{(6m^2-10m+5,1)},\ g^2_{(m,2)}=g_{(6m^2-6m+2,2)},$$

$$g^2_{(m,3)}=g_{(6m^2-2m+1,1)} \text{ and } g^3_{(m,3)}=g_{(36m^3-18m^2+3m,3)}$$

(*iii*) Arbitrary $m>n\ge 1$ yields $g_{(m,j)}-g_{(n,j)}=6(m-n)$, where $j=1,2,3$.

(*iv*) For arbitrary $\alpha,\beta\in Z^{+0}$, it holds

$g_{(m,1)} \cdot g_{(n,1)} = g_{(\omega,1)} \Rightarrow (g_{(m,1)} \pm 6\alpha)(g_{(n,1)} \pm 6\beta) = g_{(*,1)}$

$g_{(m,3)} \cdot g_{(n,3)} = g_{(\omega,1)} \Rightarrow (g_{(m,3)} \pm 6\alpha)(g_{(n,3)} \pm 6\beta) = g_{(*,1)}$

where $g_{(*,1)}$ means the first number of certain group.

(*v*) Every $m = 6n^2 + 8n + 2$ yields

$g_{(m,1)} = (6n+1)(6n+7)$, $n \in \boldsymbol{Z}^+$

and generally , every $m = a(6n+1) + (6n^2 + 2n) + 1$ yields

$g_{(m,1)} = (6n+1)(6n+6a+1)$, $a, n \in \boldsymbol{Z}^+$

(*vi*) Every $m = 6n^2 - 4n - 1$ yields

$g_{(m,1)} = (6n-1)(6n+5)$, $n \in \boldsymbol{Z}^+$

and generally, every $a(6n-1) + (6n^2 - 2n)$ yields

$g_{(m,1)} = (6n-1)(6n+6a-1)$, $a, n \in \boldsymbol{Z}^+$

(*vii*) Every $m = 6n^2 + 6n + 1$ yields

$g_{(m,3)} = (6n+1)(6n+5)$, $n \in \boldsymbol{Z}^+$

and generally, every $a(6n+1) + 6n^2$ yields

$g_{(m,3)} = (6n+1)(6n+6a-1)$, $a, n \in \boldsymbol{Z}^+$

(*viii*) For arbitrary integers $m, n, \omega \in \boldsymbol{Z}^+$ and $n > m \geq 1$, $g_{(m,j)} \mid (n-m)$ or $(n-m) \mid g_{(m,j)}$ leads to $g_{(m,j)} \mid g_{(n,j)}$ or $(n-m) \mid g_{(n,j)}$ respectively, where $j = 1, 2, 3$; particularly, if $n \equiv m (\bmod\, \omega)$ and $\omega \mid g_{(m,j)}$, then $\omega \mid g_{(n,j)}$ and thus $(n-m, g_{(m,j)}) \mid g_{(n,j)}$; consequently, $g_{(m,1)}$ and $g_{(n,1)}$ are of the same form of either (6*k*+1)(6*l*+1) or (6*k*-1)(6*l*-1).

(*ix*) For arbitrary integers $m, n, \alpha \in \boldsymbol{Z}^+$ and $n > m \geq 1$, if $g_{(m,j)} \mid g_{(n,j)}$, then $g_{(m,j)} \mid g_{(n+\alpha g_{(m,j)}, j)}$; if $g_{(m,j_n)} \mid g_{(n,j_n)}$, then $g_{(m,j_m)} \mid g_{(n+\alpha g_{(m,j_m)}, j_n)}$

(*x*) For arbitrary integers $m, n \in \boldsymbol{Z}^+$ and $m > n > 1$, it holds $g_{(n,j_n)} \mid g_{(m,j_m)}$, where m and j_m are given by

$$\begin{cases} r = kg_{(n,j_n)} (\bmod 3) \\ m = n + \left\lfloor \dfrac{kg_{(n,j_n)}}{3} \right\rfloor + \left\lfloor \dfrac{j_n}{3} \right\rfloor \\ j_m = (r + j_n) (\bmod 3) \end{cases} \qquad (10)$$

in which $k \in \boldsymbol{Z}^+$.

Proof: (*i*), (*ii*) and (*iii*) are from basic formulas (9), Lemma 3 and direct calculations. (*iv*) is from Lemma 3; (*v*) ,(*vi*) and (*vii*) are from Theorem 3; (*viii*) is from (*iii*); (*ix*) is from (*ii*) and (*viii*). (*x*) is from Lemma 4.

□

Theorem 5: For arbitrary integers $m, n, \alpha \in \boldsymbol{Z}^+$ and $n > \alpha > m \geq 1$, suppose $g_{(m,j_n)} \mid g_{(n,j_m)}$ and $g_{(\alpha,j_\alpha)} - g_{(m,j_m)} = 2k$; then $g_{(\alpha,j_\alpha)} \mid g_{(\beta,j_\beta)}$ if $g_{(\beta,j_\beta)} - g_{(n,j_n)} = 6k$.

Proof: The condition that $g_{(\alpha,j_\alpha)} - g_{(m,j_m)} = 2k$ means there are k numbers between $g_{(\alpha,j_\alpha)}$ and $g_{(m,j_m)}$, thus consider two neighboring numbers first, say $g_{(i,1)}$ and $g_{(i,2)}$. By lemma 4, the ($g_{(i,1)}$)th number that is counted from $g_{(i,2)}$ is a multiple *p* of $g_{(i,1)}$, and the ($g_{(i,2)}$)th number that is counted from $g_{(i,2)} + 2$, namely the one next to $g_{(i,2)}$, is a multiple *q* of $g_{(i,2)}$. That is to say, *q* is the 3rd number following *p*. Figure 1 can intuitively depicts the case. And so forth, the first multiple *s* of $g_{(\alpha,j_\alpha)}$ is the (3*k*)th number following the first multiple *t* of $g_{(m,j_m)}$. Consequently, if $g_{(m,j_n)} \mid g_{(n,j_m)}$ and $g_{(\beta,j_\beta)} - g_{(n,j_n)} = 6k$ then $g_{(\alpha,j_\alpha)} \mid g_{(\beta,j_\beta)}$, as depicted by figure 2.

□

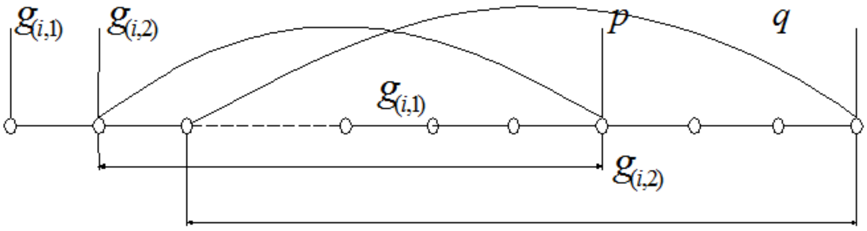

Fig 1. Neighboring numbers and their first multiples

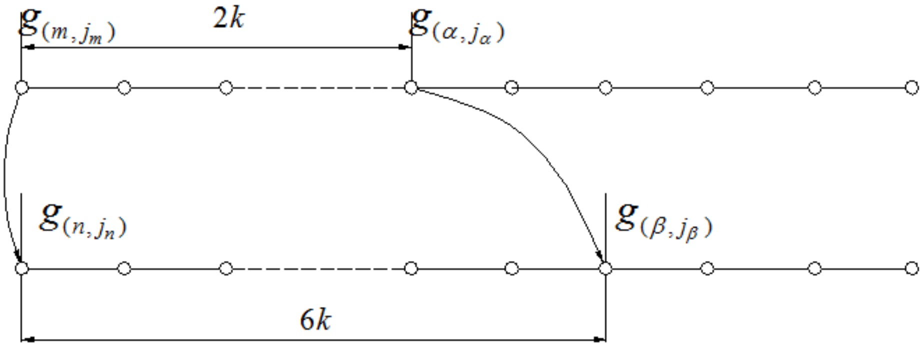

Fig 2. Mapping of two odd numbers to their first multiples

IV. Experiments and Examples

Using the theorems proved previously, approaches to factorize a big composite number can be derived out. First, Theorem 1, 2 and 3 provide a kind of direct search approach such that finding an x to satisfy $(6x+1)|(n-x)$ or $(6x-1)|(n+x)$ for big odd number $N=6n+1$, or finding an x to satisfy $(6x-1)|(n-x)$ or $(6x+1)\ \ |(n+x)$ for big odd number $N=6n-1$. Either Theorem 2 or 3 shows that the searching processes is limited although they might be of very long time. Secondly, Theorem 4 provides another new searching approach that find an m such that $g_{(m,1)}|(n-\ (6m^2-\ 10m+5))$ or $g_{(m,3)}\ \ |(n-(36m^3-18m^2+3m))$. In the end, it can see that Theorem 5 provides a possible inquiry approach to find a divisor of the number 6n±1 by inquiring its neighboring composite number. This approach is indeed a fresh one and is of very high efficiency, which will be specially introduced in my following article.

The following examples are respectively about to show approaches mentioned before. The examples 1 to 5 are based on Theorem 2 and 3; the example 5 and 6 are based on Theorem 4 and the last one is based on Theorem5.

Example 1: Let N=2993; then 2993=6×499-1;so n=499 and $l<\dfrac{\sqrt{499}+1}{2}<12$. It can see that $l=7$ $\Rightarrow(6l-1=41)\ \ |((499-7)=492)=12$. Hence 41 must be a factor of 2993 as the fact shows 2993=41×73.

Example 2: Let N=4573;then 4573=6×762+1;so n=762 and $l<\dfrac{\sqrt{762}+1}{2}<15$. It can see that $l=3$ $\Rightarrow(6l-1=17)|((762+3)=765)=45$. Hence 17 must be a factor of 4573 as the fact shows 4573=17×269.

Example 3: Let $N=2^{11}-1$; then N=6×341+1;so n=341 and $l<\dfrac{\sqrt{341}+1}{2}<10$. It can see that $k=4\Rightarrow(6l-1=23)$ $|((341+4)=345)=15$. Hence 23 must be a factor of $2^{11}-1$ as the fact shows $2^{11}-1=23\times89$.

Example 4: Let $N=7891$; then $7891=6\times1315+1\Rightarrow n=\ 1315\Rightarrow l<1+\dfrac{\sqrt{1315}}{6}<7$;It can see that $l=2\Rightarrow((6l+1)=13)$ $|((1315-6\times2\times2-2\times2)=1827)=99$ which says $13|7891$ as the fact shows 7891=13×607

Example 5: Let $N=23461$; then $23461=6\times3910+1\Rightarrow n=\ 3910\Rightarrow l<1+\dfrac{\sqrt{3910}}{6}<12$;It can see that $l=5\Rightarrow((6l-1)=29)$ $|((3910-6\times5\times5+2\times5)=3770)=130$ which says $29|23461$ as the fact shows 23461=29×809.

Example 6: Let $N=789435281$; then N=6×131572547-1and it has factor of the form $6x-1$. Note that N= 6×131572547-1⇒n=131572547. So need to find an m in $g_{(*,3)}$ such that $g_{(m,3)}|(n-(36m^3-18m^2+3m))$. Computation shows that $(g_{(10,3)}=59)|(131572547\quad-(36\times10^3-18\times10^2+3\times10)=131538317)=2229463$; hence, $59|\,789435281$. $\Rightarrow789435281=59\times2833\times4273$.

Example 7: Let $N=2^{29}-1=536870911$**;** then N=6× 89478485+1⇒n=89478486 and N has factors of the form either 6x+1 or 6x-1. Need to find an m in $g_{(*,1)}$ such that $g_{(m,1)}|(n-(6m^2-10m+5))$. Computation shows that $(g_{(349,1)}=2089)|(89478486-(6\times349^2-10\times349+5)\quad=88751165)\quad=42485$; hence, $2089|536870911$ ⇒ $536870911=2089\times256999$.

Example 8: Let $N=2^{23}-1=33554431$; since $(2^{23}$-1)-$(2^{11}$-1)=2^{11}×$(2^{12}$-1)=5×7×9×13×2^{11}=6×1365×2^{10} and 2^{11}-1=23×89, test 23+2k and then find 31|33554431⇒ 31×1082401.

V. Conclusions

Factorization of big integers has been a research topic in fields of information security. Up to now, human beings have developed many valuated approaches. Nevertheless, new approaches are still necessary for both scientific research and technical demands. By defining seeds of composite number and constructing sieve of odd composite numbers, this article turns factorization of a big odd composite number to that of its seed, and to finding its neighboring composite number. Experiments show that the new approaches are valid and practical. The author thinks that, by aids with other methods, the new approaches are sure to be effective ones.

Acknowledgements

The research work is supported by the national Ministry of science and technology under project 2013GA780052, Department of Guangdong Science and Technology under projects 2015A030401105 and 2015A010104011, Foshan Bureau of Science and Technology under projects 2016AG100311, Special Innovative Projects 2014KTSCX156, 2014SFKC30 and 2014QTLXXM42 from Guangdong Education Department. The authors sincerely present thanks to them all.

References

[1] L E Dickson. History of the Theory of Numbers, Chelesea publishing Company, New York.1971

[2] S Sarnaik，D Gadekar，U Gaikwad. An Overview to Integer Factorization and RSA in Cryptography, International Journal for Advance Research in Engineering and Technology (IJARET),2014,2(IX):21-27

[3] XX Liu ， XX Zou and JL Tan. Survey of large integer factorization algorithms, Application Research of Computers,2014,13(11):3201-3207

[4] WANG Xingbo. Valuated Binary Tree: A New Approach in Study of Integers, International Journal of Scientific and Innovative Mathematical Research (IJSIMR), Volume 4, Issue 3, March 2016, PP 63-67

[5] CD Pan and CB Pan, Elementary Number Theory(3rd Edition), Press of Peking University, 2013,pp-22

[6] WANG Xingbo. New Constructive Approach to Solve Problems of Integers' Divisibility, Asian Journal of Fuzzy and Applied Mathematics, 2014, 2(3):74-82