International Journal of Pure and Applied Mathematics
Volume 85 No. 5 2013, 833-847
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v85i5.2

GENERATION OF PRIME NUMBERS FROM ADVANCED SEQUENCE AND DECOMPOSITION METHODS

Brahim Belhaouari Samir[1], Munwar Ali Zardari[2 §], Youssef A. Y. Rezk[3]

[1]Mathematics Department Science College
Alfaisal University
RIYADH 11533

[2,3]Department of Computer and Information Sciences
Universirti Teknologi PETRONAS
Bandar Seri Iskandar, 31750, Tronoh, Perak, MALAYSIA

Abstract: The generation of prime numbers cause the use of data encryption techniques, as major primal is needed for the generation of pairs of keys. This paper proposes two prime number generation methods which are based on sequence of prime numbers and decomposition of a prime number". In these proposed methods, co-prime and decomposition properties of prime number are used. By considering the co-prime property, any sequence of consecutive primes are coupled together to generate their co-prime numbers. Let n be a number which is co-prime with a sequence of m prime numbers, which can be expressed as:

$$n = \left(\prod_{i=1}^{m} p_i\right).k + V_{mod\left(\prod_{i=1}^{m} p_i\right)},$$

where m is a sequence of prime numbers and p_i be the i^{th} prime number, with $p_1 = 1$. In the second approach i.e decomposition of prime number, the objective is to generate new prime numbers using decomposition of primes. For all integer numbers represented by X less than p_{m+1}^2 are prime numbers, it is shown in the following formula.

Received: August 11, 2012

§Correspondence author

$$X\left(i,w,r\right)=\sum_{j=1}^{i}\left(\prod_{l\varepsilon I_i^j}p_l^{w_i^d(l)}\left(-1\right)^{r_i^d(l)}\right).$$

AMS Subject Classification: 11XX, 11YXX, 11Y11
Key Words: prime numbers, twin primes, co-prime number, prime number decomposition.

1. Introduction

The study of prime numbers and their properties has attracted mathematicians for several centuries because of the use of prime numbers in different fields [1]. The importance of prime numbers has increased especially in the field of information technology, i.e., in data security algorithms. It is easy to generate the product of two prime numbers but extremely difficult and a laborious to decompose prime factors combined together [2] [3]. In [4], Goldstein and co-authors generated the list of first twenty-five prime numbers.

The sequence of primes has an importance in prime number field [5]. Many prime number theorems with their proofs have been proposed to generate prime numbers and sequence of prime numbers (e.g. prime idea in ideal classed and theorem of prime for arithmetic progression) [6] [7]. The proof of GoldBachs conjecture theorem is based on gap diagonal property of prime numbers, in which, the small prime numbers are generated from large prime numbers [8]. In addition, another prime number algorithm is proposed by Riesel and Hans in [9], in which p is considered as a perfect prime number.

The large even or odd integers are decomposable into the number of small integers. All large odd integers can be decomposed as: $n = P_1 + P_2 + P_3$ and all even integers are decomposable by $n = P_1 + P_2$ [10]. LU's contribution in the generation of prime numbers is that the positive integers can be generated by the sums of the prime numbers power [11], and each adequate large integer is the sum of a prime and four squares of primes [12]. Whereas M. Wolf in [13] proposed another algorithm to generate a prime number from the squared sum of prime numbers, this work is an improvement on the work of Liu, L and Zhan (2006) [14], in which $\theta > 9/10$. In another studies of prime number, the twin pair and new factors of prime number are developed by considering the number of distinctiveness of prime numbers [15] [16]. The large prime numbers are generated by the addition of a number and the cube of four prime numbers [17]. The calculation of prime number is simplest to the most tedious calculations as

defined in [18][19]. The simplest up to the most tedious of calculation of prime numbers is defined in [18] and [19].

The proposed methods are developed on the basis of co-prime and decomposition properties of prime numbers. The two numbers a and b are co-prime if their highest common factor is 1. The number 1 is not a prime number; because a prime number must have two divisors, 1 and itself. Although an infinite list of prime numbers exists, as defined by Euclid around 300 BC. $\pi(x)$ is a function to generate prime numbers less than or equal to the given number x, where $\pi(x) \sim \frac{x}{ln(x)}$ and can also be defined as $\lim_{x\to\infty} \frac{\pi(x)}{ln(x)} = 1$. The density of prime numbers within natural numbers is defined by the formula $\frac{ln(ln(n))}{n}$, where n is the length of the partition. The density of all natural numbers is given by: $\lim_{n\to\infty} \frac{ln(ln(n))}{n} = 0$.

In a set of natural numbers, the co-primes are numbers whose highest common factor is 1. According to the definition of co-prime, 8 and 9 are co-primes, because 8 and 9 have no other common factor except 1. Here, we define the set of consecutive numbers from n_0 to m_0.

$$[n_0 : m_0] = \{n_0, n_0 + 1, ..., m_0 - 1, m_0\}.$$

Suppose we have two sets, U and V; their sum and difference can be defined as:

$$U \pm V = \{x \pm y : x \in U, y \in V\}$$

Here, theorem 1 is defined to explain co-prime and theorem 2 is defined to explain decomposition properties of prime number respectively.

Theorem 1. *A prime number is always a co-prime with all other prime numbers. Let n be a co-prime number with a sequence of prime numbers P_i, where $i \leq m$ and can be expressed as:*

$$n = (\prod_{i=1}^{m} P_i).k + V_{mod(\prod_{i=1}^{m} P_i)},$$

where, $k\varepsilon Z$ and V is the set of co-prime numbers with the sequence of prime numbers P_i; where $i \leq m$ and $\forall m \geq 1$.

The set of co-prime numbers V can also be represented as:

$$V_{mod\left(\prod_{i=1}^{m} P_i\right)} = P_{m+1} V_{mod\left(\prod_{i=1}^{m} P_i\right)} + \left(\prod_{i=1}^{m} P_i\right)[1 : P_{m+1} - 1].$$

For any number $x \in V_{mod(\prod_{i=1}^{m} P_i)}$ *and* $x < P_{m+1}^2$ *, this shows that* x *is a prime number. In order to prove theorem 1, we use the following lemma.*

Lemma. *Let* l *be a set which can be defined as:*

$$l = [1 : P_{m+1} - 1]_{mod(P_{m+1})} - V_{mod\left(\prod_{i=1}^{m} P_i\right)}.$$

By considering the above equation of l*, we have three situations:*

i. For all co-primes x *and* y*, we have:*

$$y = x\,[1 : y - 1]_{mod(y)} = [1 : y - 1]_{mod(y)}$$

ii. For all, y *is a co-prime with* P_i *and* $i \leq m$*:*

$$V_{mod\left(\prod_{i=1}^{m} P_i\right)} = yV_{mod\left(\prod_{i=1}^{m} P_i\right)}$$

iii. The set l *also represented as:*

$$l = [P_{m+1} - 1]_{mod(P_{m+1})} - V_{mod\left(\prod_{i=1}^{m} P_i\right)}$$

If we multiply set l *by* $((\prod_{i=1}^{m} P_i) - (P_{m+1}))$*, then* l *is co-prime with* $((\prod_{i=1}^{m} P_i) - (P_{m+1}))$*, and finally* $l = l_{mod(\prod_{i=1}^{m} P_i)}$.

In theorem 1, we explained the co-prime property of prime numbers, and developed the a formula to generate sequence of prime numbers. Now, we discuss theorem 2 to explain the decomposition property of the prime numbers.

Theorem 2. *Let* P_i *be the* i^{th} *prime number, where* $P_1 = 1$ *and all integers are represented by* X *less than* P_{m+1}^2 *are prime numbers, and defined as:*

$$X\,(i, w, r) = \sum_{j=1}^{i} \left(\prod_{l \in I_i^j} P_l^{w_i^d(l)} \,(-1)^{r_i^d(l)} \right),$$

where $2 \leq i \leq m$*,* $w_i^d\,(l) \in N$ *,* $r_i^d\,(l) \in \{-1, +1\}$*, and* $\forall\ 2 \leq i \leq m$ *so,* $\cup I_{j=i}^d = \{0, 1, ..., m\}$*,* $\forall\ 2 \leq i \leq m$*, and* $\forall\ i \leq U \leq m$*; this implies that* $\exists! 1 \leq V \leq i$ *such that* $U \notin I_i^v$.

The rest of paper is arranged as: Section 2 gives the proof of the theorems, Section 3 shows the results of the theorems and Section 4 describes the conclusion and future work.

2. Proof of the Theorems

Proof of Theorem 1. Let n and b be two positive integers. If n is not divisible by a, then a needs to be a multiple of k added to another positive integer b, where b is smaller than a ; under the condition that a and b are co-primes, the positive integer n is co-prime with a and b. This idea leads to the generation of a large prime number from a sequence of previous prime numbers. This idea can be written in mathematical form as follows:

$$n = ak + b, \text{where } b < a$$

$$\nexists p : b = a.p, \text{where } a, b, n, k \text{ and } p \in N.$$

Generalization of the Process. Let n be a number which is co-prime with a sequence of m prime numbers, which can be expressed as:

$$n = \left(\prod_{i=1}^{m} p_i\right).k + V_{mod\left(\prod_{i=1}^{m} p_i\right)},$$

where

- $V_{mod(\prod_{i=1}^{m} p_i)}$ is a set.

- m is the sequence of the prime numbers.

- And $V_{mod\left(\prod_{i=1}^{m} p_i\right)}$ is the set of the numbers less than $\left(\prod_{i=1}^{m} p_i\right)$ and co-prime with p_i, $\forall\ i \leq m$.

If $x \in V_{mod\left(\prod_{i=1}^{m} p_i\right)}$ and $x < (p_{n+1})^2$ then x is a prime number. Suppose (m+1) is the sub-script of a prime number where n is co-prime with (p_{m+1}) and $\left(\prod_{i=1}^{m} p_i\right)$. Here x_i is co-prime with p_i, where, $i \leq m$ and x_2 is co-prime with p_{m+1}, this can be expressed in the following equation:

$$\begin{cases} n = (\prod_{i=1}^{m} p_i).k + V_{mod(\prod_{i=1}^{m} p_i)}.x_1 \\ n = (p_{m+1}).k^{'} + [1 : (p_{m+1} - 1)].x_2, \end{cases} \tag{1}$$

where $[1:(p_{m+1}-1)]$ *is the set of numbers less than* p_{m+1} *and co-prime with it.*

The set of co-primes can be expressed as given below:

$$\left(\prod_{i=1}^{m} p_i\right).k + V_{mod\left(\prod_{i=1}^{m} p_i\right)} = (p_{m+1}).k^{'} + [1:(p_{m+1}-1)].$$

As we know that,

$$l = \left(\prod_{i=1}^{m} p_i\right).k - (p_{m+1}).k^{'} = [1:(p_{m+1}-1)].x_2 - V_{mod\left(\prod_{i=1}^{m} p_i\right)}.x_1.$$

Suppose that k=1 and is defined by equation as:

$$\left(\left(\prod_{i=1}^{m} p_i\right).k - (p_{m+1}).k^{'}\right) \in l,$$

where $k = k^{'} - 1$. *From lemma i, we have the equation for a particular solution.*

$$\left(\left(\prod_{i=1}^{m} p_i\right) - (p_{m+1})\right).l = l.$$

We know that l can be written as $l_{mod(\prod_{i=1}^{m+1} p_i)}$, *now, the above equation can also be rewritten as:*

$$\left(\left(\prod_{i=1}^{m} p_i\right) - (p_{m+1})\right).l_{mod\left(\prod_{i=1}^{m+1} p_i\right)} = l_{mod\left(\prod_{i=1}^{m+1} p_i\right)}.$$

After finding the particular solution, it is already easy to find the general solution:

$$\left(\prod_{i=1}^{m} p_i\right).(k+l-l) - (p_{m+1}).\left(K^{'}+l-l\right) = l,$$

by expanding the above equation we have:

$$\left[\left(\prod_{i=1}^{m} p_i\right).(k-l) - (p_{m+1}).\left(k^{'}-l\right)\right] + \left[\left(\prod_{i=1}^{m} p_i\right).l - (p_{m+1}).l\right] = l,$$

using the property of lemma i, we have:

$$\prod_{i=1}^{m} p_i.(k-l) = (p_{m+1}).\left(k^{'}-l\right),$$

where $(k-l)$ *and* $(k^{'}-l)$ *can be calculated as:*

$$\begin{cases}(k-l)=\vartheta.p_{m+1}\\ \left(k^{'}-l\right)=\vartheta.\left(\prod_{i=1}^{m}p_i\right),\end{cases}$$

where $\vartheta \in Z$, *only specific for* k *and for* $k^{'}$, *we have:*

$$\begin{cases}\{k=\vartheta.p_{m+1}+l\\ k^{'}=\vartheta.\left(\prod_{i=1}^{m}p_i\right)+l,\end{cases}$$

substituting the value of k *in equation (1), we have:*

$$\begin{cases}n=\vartheta\left(\prod_{i=1}^{m+1}p_i\right)+l.\left(\prod_{i=1}^{m}p_i\right)+V_{mod\left(\prod_{i=1}^{m}p_i\right)}\\ n=\vartheta\left(\prod_{i=1}^{m+1}p_i\right)+l.\left(p_{m+1}\right)+\left[1:(p_{m+1}-1)\right],\end{cases}$$

substitute the value of l *in the above equation:*

$$\begin{cases}n=\vartheta\left(\prod_{i=1}^{m+1}p_i\right)+\left(\left[1:(p_{m+1}-1)\right]-V_{mod\left(\prod_{i=1}^{m}p_i\right)}\right).\\ \left(\prod_{i=1}^{m}p_i\right)+V_{mod\left(\prod_{i=1}^{m}p_i\right)}\\ n=\vartheta\left(\prod_{i=1}^{m+1}p_i\right)+\left(\left[1:(p_{m+1}-1)\right]-V_{mod\left(\prod_{i=1}^{m}p_i\right)}\right).\\ \left(p_{m+1}\right)+\left[1:(p_{m+1}-1)\right],\end{cases}$$

we can also rewrite the above equation as:

$$\begin{cases}n=\vartheta.\left(\prod_{i=1}^{m+1}p_i\right)+\left(\left[1:(p_{m+1}-1)\right].\left(\prod_{i=1}^{m}p_i\right)\right)+\\ \left(1-\left(\prod_{i=1}^{m}p_i\right)\right).V_{mod\left(\prod_{i=1}^{m}p_i\right)}\\ n=\vartheta.\left(\prod_{i=1}^{m+1}p_i\right)+\left(\left[1:(p_{m+1}-1)\right].\left(p_{m+1}+1\right)\right)-\\ \left(p_{m+1}\right).V_{mod\left(\prod_{i=1}^{m}p_i\right)}.\end{cases}$$

By modality properties (see Lemma), we have:

$$\begin{cases} (p_{m+1}) \, . V_{mod\left(\prod_{i=1}^{m} p_i\right)} = V_{mod\left(\prod_{i=1}^{m} p_i\right)} \\ and \\ \left(\prod_{i=1}^{m} p_i\right) . [1 : (p_{m+1} - 1)] = [1 : (p_{m+1} - 1)] \, , \end{cases}$$

now, we have two equations, which give the general form of the integer n.

$$\begin{cases} n = \vartheta . \left(\prod_{i=1}^{m+1} p_i\right) \left([1 : (p_{m+1} - 1)] \, . \left(\prod_{i=1}^{m} p_i\right)\right) + (p_{m+1}) \, . V_{mod\left(\prod_{i=1}^{m} p_i\right)} \\ n = \vartheta . \left(\prod_{i=1}^{m+1} p_i\right) \left([1 : (p_{m+1} - 1)] \, . \left(\prod_{i=1}^{m} p_i\right)\right) + (p_{m+1}) \, . V_{mod\left(\prod_{i=1}^{m} p_i\right)}, \end{cases}$$

where both are equivalent due to the similarity of property of the modulo of the last term.

From the above equation, select the first equation of n.

$$n = \vartheta . \left(\prod_{i=1}^{m+1} p_i\right) + \left([1 : (p_{m+1} - 1)] \, . \left(\prod_{i=1}^{m} p_i\right)\right) + (p_{m+1}) \, . V_{mod\left(\prod_{i=1}^{m} p_i\right)},$$

after performing the calculation we have following equation:

$$n = \vartheta . \left(\prod_{i=1}^{m+1} p_i\right) + V_{mod\left(\prod_{i=1}^{m+1} p_i\right)},$$

where

$$V_{mod\left(\prod_{i=1}^{m+1} p_i\right)} = \left([1 : (p_{m+1} - 1)] \, . \left(\prod_{i=1}^{m} p_i\right)\right) + (p_{m+1}) \, . V_{mod\left(\prod_{i=1}^{m} p_i\right)}.$$

Proof of Lemma i. Here we will prove lemma i with following equality:

$$\left(\prod_{i=1}^{m} p_i\right) . [1 : (p_{m+1} - 1)]_{mod(p_{m+1})} = [1 : (p_{m+1} - 1)]_{mod(p_{m+1})} \, .$$

As $(\prod_{i=1}^{m} p_i)$ is co-prime with p_{m+1}, the exist $k \in N$, $(\prod_{i=1}^{m} p_i)$ can be written as:

$(\prod_{i=1}^{m} p_i) = k.p_{m+1} + r$, where $1 \leq r < p_{m+1}$ and the sequence of multiple of integers can be generated as follows:

$$[r, 2r, 3r, ... (p_{m+1} - 1) .r]_{p_{m+1}},$$

where

$$[ir]_{mod(p_{m+1})} \neq 0 \qquad (2)$$

If $[ir]_{mod(p_{m+1})} = 0$, then exists $\mu \in Z$ and $ir = \mu p_{m+1}$ where $i = kp_{m+1}$ and $r = k^{'} p_{m+1}$ (contradiction). Such that p_{m+1} is a prime number where $ir < p_{m+1}$, and can be written as:

$$[ir]_{mod(p_{m+1})} = [jr]_{mod(p_{m+1})} \qquad (3)$$

for $1 < i \neq j < p_{m+1}$, by the contradiction, we have:

$$\begin{cases} ir = k^{'}.p_{m+1} + r_0 \\ jr = k^{''}.p_{m+1} + r_0. \end{cases}$$

Here, the range of values for r_0 is $1 \leq r_0 \leq p_{m+1} - 1$, and $(i - j)r = (k^{'} - k^{''}).p_{m+1}$, which contradicts equation (2). The following equation expresses in detail the sequence of r.

$$[r\ 2r\ 3r... (p_{m+1} - 1)\, r]_{mod(p_{m+1})} = [1 : (p_{m+1} - 1)]_{mod(p_{m+1})}.$$

Generalizing this equation: If $\forall k_1 \neq k_2$, where k_1 and k_2 are co-primes, then k_1 and k_2 are written as:

$$k_1 [1 : (k_2 - 1)]_{mod(k_2)} = [1 : (k_2 - 1)]_{mod(k_2)}.$$

Proof of Lemma ii. Here we will prove lemma ii.

$$p_{m+1}.V_{mod\left(\prod_{i=1}^{m} p_i\right)} = V_{mod\left(\prod_{i=1}^{m} p_i\right)},$$

where $V_{mod(\prod_{i=1}^{m} p_i)}$ is a set of the numbers less than $\prod_{i=1}^{m} p_i$ and co-prime with P_i, $\forall i \leq m$; where $V_{mod\left(\prod_{i=1}^{m} p_i\right)}$ is a set of $r_1, ..., r_M$ can be written as:

$$V_{mod\left(\prod_{i=1}^{m} p_i\right)} = \{r_1, r_2, r_3, ..., r_M\}.$$

Now, we will test the condition:

$$r_i : (r_i).p_{m+1} = k(\prod_{i=1}^{m} p_i),$$

if the condition is true, then: $\frac{r_i}{p_j} \in N$ for all $j \leq m$, where $r_i = k^{'}(\prod_{i=1}^{m} p_i)$ (contadiction) and $[(r_i)p_{m+1}]_{mod(\prod_{i=1}^{m} p_i)} \neq 0$. We have another condition to test:

$$\exists\ i \neq j$$

such that:

$$[(r_i)\, p_{m+1}]_{mod\left(\prod_{i=1}^{m} p_i\right)} = [(r_j)\, p_{m+1}]_{mod\left(\prod_{i=1}^{m} p_i\right)},$$

where r_i and r_j have the following values:

$$\begin{cases} r_i p_{m+1} = k^{'}\left(\prod_{i=1}^{m} p_i\right) + r_0 \\ r_j p_{m+1} = k^{''}\left(\prod_{i=1}^{m} p_i\right) + r_0, \end{cases}$$

and we conclude that

$$(r_i - r_j)\, p_{m+1} = \left(\prod_{i=1}^{m} p_i\right)\left(k^{'} - k^{''}\right),$$

which it means $(r_i - r_j)$ has $p_1, p_2, ...p_m$ as divisors and $(r_i - r_i) \geq (\prod_{i=1}^{m} p_i)$ (Contradiction).

Proof of Lemma iii. If $l = [1 : (p_{m+1} - 1)]_{mod(p_{m+1})}.x_2 - V_{mod(\prod_{i=1}^{m} p_i)}.x_1$ then,

$$((\prod_{i=1}^{m} p_i) - (p_{m+1})).l = l.$$

From the proof of lemma i and ii, we have:

$$k(V_{mod(\prod_{i=1}^{m} p_i)}) = V_{mod(\prod_{i=1}^{m} p_i)},$$

if $k = \prod_{j \in I} (p_j)^q$, $\forall x \in i$ is bigger than $j \in i$, where $j \neq i$ and $q \in Z^+$, and:

$$\begin{cases} \left(p_{m+1} - \prod_{i=1}^{m} p_i\right) . [1 : (p_{m+1} - 1)]_{mod(p_{m+1})} = \\ [1 : (p_{m+1} - 1)]_{mod(p_{m+1})} \\ \left(p_{m+1} - \prod_{i=1}^{m} p_i\right) . V_{mod\left(\prod_{i=1}^{m} p_i\right)} = V_{mod\left(\prod_{i=1}^{m} p_i\right)} \end{cases} .$$

Proof of Theorem 2. To prove that X is a prime number and all prime numbers less than p_{m+1}^2 are not factor of X.

Let p_s be the s^{th} prime number less than p_{m+1}^2,

$$\frac{X\,(i,w,r)}{p_s} = \sum_j \prod_{l \in I_i^j} \frac{p_l^{w_i^j(l)}\,(-1)^{r_j^d(p)}}{p_s},$$

where $l \in l_i^d$ and $\forall\ i \leq m$, $\exists\ !\vartheta$ and $p_s \in I_i^V$, which implies that

$$\frac{X\,(i,w,r)}{p_s} = \sum_{j \neq V} \prod_{l \in I_i^d} \frac{p_l^{w_i^j(l)}\,(-1)^{r_j^d(l)}}{p_s} + \prod_{l \in I_i^V} \frac{p_l^{w_i^V(l) r_i^V(l)}}{p_s} =$$

$$\prod_{l \in I_i^d} \left(\frac{p_l^{w_i^j(l)}\,(-1)^{r_i^d(l)}}{p_s} \right) \in N,$$

if $d \neq V$ and

$$\prod_{l \in I_i^V} \left(\frac{p_l^{w_i^V}\,(-1)^{r_i^V}}{p_s} \right) \notin N.$$

So, it can be concluded that $X(i,w,r)$ is a co-prime number with all p_i, where $i \leq m$. But, still it needs to be prove that $X(i,w,r)$ is a co-prime number with p_i, $i \geq m+1$.

If $X(i,w,r)$ is a factor with p_i; where $i \geq m+1$, which means that: $X(i,w,r) = P_i \times b$, $b \in N$, then $X(i,w,r)$ is co-prime with p_i, where $i \leq m$; therefore $X(i,w,r) \geq p_i^2$, where $i \geq m+1$ and this is a contradiction with our condition $X\,(i,w,r) < p_{m+1}^2$.

3. Results of Proposed Methods

Results of Theorem 1. Let k represent any integer number and all the co-prime numbers with 2 can be written as:

$$n = 2k + r,\ r \in V_{mod(2)},$$

where $V_{mod(2)} = \{1\}$. And all numbers co-prime with 2 and 3 can be written as:

$$n = 2.3k + r,\ r \in V_{mod(2,3)},$$

where $V_{mod(2,3)} = \{1 \quad 5\}$. In the same way, all the numbers co-prime with 2, 3 and 5 can be written as:

$$n = 2.3k + r, r \in V_{mod(2,3,5)}r,$$

where $V_{mod(2,3,5)} = \{1 \quad 7 \quad 11 \quad 13 \quad 17 \quad 19 \quad 23 \quad 29\}$.

Let p_i be the i^{th} prime number starting from $p_1 = 2$ and so on, where $i \leq 4$ and is represented as:

$$n = \left(\prod_{i=1}^{4} p_i\right) k + r, r \in V_{mod\left(\prod_{i=1}^{4} p_i\right)},$$

where the values of set $V_{\left(\prod_{i=1}^{4} p_i\right)}$ are given below:

$$V_{mod\left(\prod_{i=1}^{5} p_i\right)} = \{1 \quad 11 \quad 13 \quad 17 \quad 19 \quad 23 \quad 29 \quad 31 \quad 37 \quad 41 \quad 43 \quad 47 \quad 53 \quad 59$$
$$61 \quad 67 \quad 71 \quad 73 \quad 79 \quad 83 \quad 89 \quad 97 \quad 101 \quad 103 \quad 107 \quad 109 \quad 113 \quad 121 \quad 127 \quad 131$$
$$137 \quad 139 \quad 143 \quad 149 \quad 151 \quad 163 \quad 167 \quad 169 \quad 173 \quad 179 \quad 181 \quad 187 \quad 191 \quad 193 \quad 197$$
$$199 \quad 209\}.$$

Suppose n is a set of numbers and are co-prime with all the numbers of set p_i, where $i \leq 5$; this can be calculated by the following formula:

$$n = \left(\prod_{i=1}^{4} p_i\right) k + r,\ r \in V_{mod\left(\prod_{i=1}^{5} p_i\right)},$$

where the values of set $v_{(\prod_{i=1}^{4}(p_i))}$ are given below:

$$V_{mod\left(\prod_{i=1}^{5} p_i\right)} = \{1 \;\; 11 \;\; 13 \;\; 17 \;\; 19 \;\; 23 \;\; 29 \;\; 31 \;\; 37 \;\; 41 \;\; 43 \;\; 47 \;\; 53 \;\; 59$$
$$61 \;\; 67 \;\; 71 \;\; 73 \;\; 79 \;\; 83 \;\; 89 \;\; 97 \;\; 101 \;\; 103 \;\; 107 \;\; 109 \;\; 113 \;\; 121 \;\; 127 \;\; 131$$
$$...2263 \;\; 2267 \;\; 2269 \;\; 2273 \;\; 2279 \;\; 2281 \;\; 2287 \;\; 2291 \;\; 2293 \;\; 2297 \;\; 2309\}.$$

Results of Theorem 2: In this section we present some results of prime number by decomposition, for that, let $p_0 = 1$ and p_k is the k^{th} prime number.

$i = 2 : 1 + 2 \times 3 \times 5 = 31$; 31 is a prime number because it is less than $(p_4)^2 = 49$.

For $i = 3 : 1 + 2 \times 3 + 2 \times 3 \times 5$; 37 is a prime number because it is less than $(p_4)^2 = 49$.

For $i = 3 : \; 5^2 \times 1 + 2 \times 3 + 2 \times 5 = 41$; 41 is a prime number because it is less than $(p_4)^2 = 49$.

For $i = 3 : \; 2 \times 3 \times 5 \times 7 - 2 \times 3 \times 5 \times 7 \times 11 = 167$; 167 is a prime number because it is less than $(p_6)^2 = 169$.

For $i = 4 : \; 5^2 \times 1 + 2 \times 3 + 2 \times 5 = 41$; 41 is a prime number because it is less than $(p_3)^2 = 72$.

For $i = 6 : -2 \times 3 \times 5 \times 7 \times 11 - 2 \times 3 \times 7 \times 11 + 2 \times 3 \times 5 \times 7 \times 11 + 2 \times 3 \times 5 \times 11 - 2 \times 5 \times 7 \times 11 - 3 \times 5 \times 7 = 127$; 127 is a prime number because it is less than $(p_6)^2 = 169$.

For $i = 2 : 2 \times 3 \times 11 \times 13 \times 17 - 5 \times 7 \times 19 \times 23 = 709$; 709 is a prime number because it is less than $(p_{10})^2 = 841$.

4. Conclusion and Future Work

Two methods i.e. sequence and decomposition of primes are proposed in this paper. These methods are based on co-prime and decomposition" properties of a prime number. The objective of these methods is to generate new prime numbers through co-prime and decomposition properties. It has been proven that the prime numbers can be generated from co-primes and the decomposition of prime numbers as shown in theorem 1 and 2.

We believe that our proposed methods are more efficient and work oriented in finding prime numbers. In the future, it can be proven the inverse method i.e., all prime numbers could be written as $X(i, w, r)$. We can also consider others properties i.e. the infinite existing of twin numbers and deference between prime numbers is the even integer set, i.e., 2. The results of the proposed methods are obtained in MATLAB 7.12.0.

References

[1] E. Mabrouk, J.C. H-Castro, M. Fukushima, Prime number generation using memetic programming, *Life Robotics*, **16** (2011), 53-56.

[2] Z. Qing, H. Zhihua, The large prime numbers generation of RSA algorithm based on genetic algorithm, *International Conference on Intelligence Science and Information Engineering*, (2011) 434-437.

[3] D. H. Lehmer, R. E. Powers, On the factoring of large numbers. *Bull, AMS*. **37** (1931) 134-137.

[4] Goldstein, Catherine, Schappacher, Norbert, Schwermer, Joachim, *The shaping of arithmetic after C.F. Gauss's disquisitions arithmetical*, Springer, Berlin Heidelberg NewYork(2007).

[5] Iovane,Gerado, The set of primes: Towards an optimized algorithm, prime generation and validation, and asymptotic consequences, *Chaos, Silitons & Fractals*, **41** (2008), 1344-1352.

[6] W. Forman, H. N. Shapiro, Abstract prime number theorem, *Communications on Pure and Applied Mathematics*, **7** (2006), 587-619.

[7] H.N Shapiro, Tauberian theorem and elementary prime number theory, *Communications on Pure and Applied Mathematics*, **12** (1959) 579-610.

[8] R. L. Liboff, Prime GAP diagonals and GoldBachs conjecture, *International Journal of Pure and Applied Mathematics*, **70** (2011), 889-900.

[9] Riesel, Hans, Mersenne numbers, *MTAC*, **12** (1958), 207-213.

[10] X Meng, On linear equations with prime variables of special type, *Journal of Number Theory*, **129** (2009), 2504-2518.

[11] G. Lu, On sumx of a prime and four prime squares in short intervals, *Journal of Number Theory*, **128** (2008), 805-8019.

[12] L.K Hua, Some results in the additive prime number theory, *Quarterly Journal of Mathematics*, **9** (1938) 68-80.

[13] M. Wolf, Random walk on the prime numbers. *PhyA*, **250** (1998), 335-344.

[14] J.Y. Liu, G. L, T. Zhan, Exponential sums over primes in short intervals, *Sci. China Ser. A*, **49** (2006) 611619.

[15] R. D. Diaz, J.M. Masque, Optimal strong primes, *Information Processing Letter*, **93** (2005), 47-52.

[16] R. Baillie, New primes of the form, *MathComp*, **33** (1979), 1333-1336.

[17] Derrick, N. Lehmer, *List of prime numbers from 1 to 10 006 721*, first ed., Hefner, Washington (1914).

[18] Z. Liu, Cubes of primes and almost prime, *Journal of Number Theory*, **132** (2012), 12841294.

[19] A. Kumchev, T. Li, Sums of almost equal squares of primes, *Journal of Number Theory*, **132** (2012), 608636.

[20] A. Khaksari, H. Sharif, M. Ershad, On prime submodules of multiplication modules, *International Journal of Pure and Applied Mathematics*, **17** (2004), 4149.