ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

Introducing Sieve of Eratosthenes as a Theorem

M.E. Hassan

Assistant Professor, Department of Mathematics, College of Science and Arts, Taif University, Rania, Saudi Arabia

ABSTRACT: In this paper we establish a theorem, using same technique in sieve of Eratosthenes, to find unknown prime numbers in a given range, also in the given range we prove there exist prime numbers different from known prime numbers .

KEYWORDS: Sieve of Eratosthenes, prime numbers, bounded multiples,

I. INTRODUCTION

Sieve of Eratosthenes is a very simple ancient algorithm for finding all prime numbers in the range from 2 to a given number n. Initially, we have the set of all the numbers $S=\{2,3,4,...,n\}$. At each step we choose the smallest number in the set and remove all its multiples. It is sufficient to remove only multiples of prime numbers not exceeding $\sqrt{n}$. We start first with the smallest element in the set 2, we remove multiples of 2 from the set S, which are $4,6,8,....$ At second step we choose 3 smallest number of the remaining elements of the set S. We remove multiples of 3 from remaining elements of the set S which are $6,9,12,....$ At third step we choose 5 smallest number of the remaining elements of the set S. We remove multiples of 5 from remaining elements of the set S which are $10,15,20,....$ Continue in this process, at each step we choose the smallest number, and remove all its multiples. It is sufficient to remove, in each step, only multiples of primes numbers not exceeding $\sqrt{n}$. In this way, all composite numbers will be removed from the set S, and remain all prime numbers in this set.

Sieve of Eratosthenes is a well known algorithm for finding prime numbers between 2 and n , several authors presented different algorithmic forms see e.g. [1,2,3,4,5,6,7,8,9].

In this paper we define the concept of bounded multiples of an integer in a set and prove some propositions related to bounded multiples, we use these propositions to prove the main result in this paper. The main result can be used to find prime numbers between known two integers. Suppose all prime numbers known to us are n and p_n is the largest prime number known to us. How to find prime numbers between p_n and T_n where $p_1p_2p_3...p_{n-1}p_n=T_n$, is an application of the main result, also we prove there exists at least one prime number between p_n and T_n. In the main result we use the same technique in sieve of Eratosthenes algorithm, here we remove known prime numbers and their multiples, the remaining numbers between p_n and T_n are unknown prime numbers and their products to any powers, which can be written as $\{p_{n+1}^{\alpha_{n+1}}p_{n+2}^{\alpha_{n+2}}p_{n+3}^{\alpha_{n+3}}...p_{n+k}^{\alpha_{n+k}} : k,\alpha_i \text{ integers}, 1\le i\le k, 0\le\alpha_i\}$.

II. RELATED WORK

Here we introduce the concept of finite multiple with some examples and propositions.

Definition 2.1 Let $M=\{1,2,3,...,m\}$ (subset of natural numbers with m elements and greatest element m) and a positive integer we called the set $aM=\{ax : ax\in M, x\in M\}$ boin a set unded multiples of integer a in the set M.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

Example2.2. Let $M=\{1,2,3,4,5,6,7,8,9,10\}$, $2M=\{2,4,6,8,10\}$, $3M=\{3,6,9\}$ and $7M=\{7\}$. From Difnition1.1 for all set M we have $1M=M$.

Remark 2.3. Let $M=\{1,2,3,...,m\}$ and a positive integer, the set $aM=\{a,2a,3a,...,am_1\}$ from Definition 2.1 $aM\subseteq M$ and $m_1\le m$.

Remark2.4. By the set of prime numbers $\{p_1,p_2,p_3,...\}$ we mean $p_1=2$, $p_2=3$, $p_3=5$, ... and so on.

Example2.5. Let $M=\{1,2,3,...,20\}$, $p_1=2$, $p_2=3$, $p_3=5$, $p_3=7$, , ,

$p_1M=\{2,4,6,...,20\}=\{p_1p_i^{\alpha_i}p_j^{\alpha_j}:i,j,\alpha_i,\alpha_j \text{ integers},\ 1\le i\le 3,1\le j\le 3,0\le\alpha_i\le 3,0\le\alpha_j\le 3\}$

$p_1M=\{2,4,6,...,20\}=\{p_1p_i^{\alpha}p_i^{\beta}:i,\alpha,\beta \text{ integers},\ 1\le i\le 4,0\le\alpha\le 3,0\le\beta\le 1\}$

$p_2M=\{3,6,9,...,18\}=\{p_2p_i^{\alpha}p_i^{\beta}:i,\alpha,\beta \text{ integers},\ 1\le i\le 3,0\le\alpha\le 2,0\le\beta\le 1\}$

$M-p_1M=\{x:x \text{ integer not multiple of } 2\}$

$M-p_2M=\{y:y \text{ integer not multiple of } 3\}$

$M-(p_1M\cup p_2)=\{z:z \text{ not multiple of } 2 \text{ and not multiple of } 3\}$

$M-(p_1M\cup p_2)=\{1,5,7,11,13,17,19\}$

$M-(p_1M\cup p_2)=\{p_3^{\alpha_3}p_4^{\alpha_4}p_5^{\alpha_5}p_6^{\alpha_6}p_7^{\alpha_7}p_8^{\alpha_8}:p_i \text{ prime number},0\le\alpha_i,\alpha_i \text{ integer},3\le i\le 8\}$

$aM=\{ax:ax\in M,x\in M\}$

Proposition 2.6. Let aM multiples of integer a in the set M, b is positive integer, $(b)aM$ is multiples of integer b by in the set aM, $(ba)M$ is multiples of integer ba in the set M, then $(b)aM=(ba)M$ and $(ab)M=(ba)M$.

Proof: From Definition 2.1 we have $(b)aM=\{bax:bax\in aM,ax\in aM\}=\{bax:bax\in aM\subseteq M,ax\in aM\subseteq M\}=\{bax:bax\in M,x\in M\}=(ba)M$, and $(ab)M=\{abx:abx\in M,x\in M\}=\{bax:bax\in M,x\in M\}=(ba)M$.

Proposition 2.7. Let aM is bounded finite multiples of integer a by elements of the set M and bT is bounded finite multiples of integer b by elements of the set T, if b is multiple of a then $bM\subseteq aM$ and if $aT\subseteq aM$ then $T\subseteq M$.

Proof: Suppose b is multiple of a then there exists positive integer $c\ge 1$ such that $b=ac$ From Difnition1.1 there exists m,m_1,m_2 such that $M=\{1,2,3,...,m\}$, $aM=\{a.2a,3a,...,m_1a\}$, $bM=\{b,2b,3b,...,m_2b\}$, and $\{a,2a,3a,...,m_1a\}\subseteq M$, $\{b,2b,3b,...,m_2b\}\subseteq M$, where $m_1\le m,m_2\le m$.

Since $\{ca,2ca,3ca,...,m_2ca\}=\{b,2b,3b,...,m_2b\}\subseteq M$, $\{a,2a,3a,...,m_1a\}\subseteq M$ and $c\ge 1,ca\ge a$ we have $m_1\ge m_2$ then $\{ca,2ca,3ca,...,m_2ca\}\subseteq\{a,2a,3a,...,m_1a\}$, therefore $bM\subseteq aM$.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

Suppose $aT \subseteq aM$, from Definition 1.1 $aM = \{a.2a,3a,...,m_1a\}$ such that $M = \{1.2,3,...,m\}$ and $aT = \{a.2a,3a,...,t_1a\}$ such that $T = \{1.2,3,...,t\}$ where m, m_1, t, t_1 are positive integer such that $t_1 \le m_1, m_1 \le m, m_1 \le \frac{m}{a}, t_1 \le t, t_1 \le \frac{t}{a}$, then we have $\frac{t}{a} - 1 \le t_1 \le \frac{t}{a}, \frac{m}{a} - 1 \le m_1 \le \frac{m}{a}$ and $\frac{t-a}{a} \le t_1 \le \frac{t}{a}, \frac{m-a}{a} \le m_1 \le \frac{m}{a}$ therefore $t \le m$ and $T \subseteq M$.

Proposition 2.8. Let aM is bounded finite multiples of integer a by elements of the set M and abT and is bounded finite multiples of integer ab by elements of the set T, where b is any positive integer .If $abT \subset aM$ then we have $bT \subset M$.

Proof: Using Proposition 2.7. and let $aT = abT$ therefore if $abT \subset aM$ then we have $bT \subset M$.

Proposition 2.9. If aM is bounded finite multiples of integer a by elements of the set M and for any positive integer b which satisfies bM is bounded finite multiples, then we have $(ab)M \subseteq aM$.

Proof: From Proposition2.6. we have $(b)aM = (ba)M$. Using Difnition1.1we have $(ba)M = (b)aM = \{bax : bax \in aM, ax \in aM\} \subseteq aM$

III. MAIN RESULT

In next theorem we will prove there exists at least one prime number between p_n and T_n.

Theorem3.1. For prime numbers $p_1, p_2, p_3,..., p_n$, let $p_1p_2p_3...p_n = T_n$ then there exists at least one prime number q such that $p_n < q < T_n$.

Proof: Given $p_1p_2p_3...p_n = T_n$ then $T_n - 1$ can not be divided by any element of the set $\{p_1, p_2, p_3,...p_n\}$, because residue of division $T_n - 1$ by p_i equal $p_i - 1$ and $p_i - 1 \neq 0$ for all $1 \le i \le n$. Since any integer greater than one either prime or composite of finite number of primes and there are infinitely many primes, for $T_n - 1$ is prime number then we have $p_n < T_n - 1 < T_n$, therefore the theorem holds, if $T_n - 1$ is composite then $T_n - 1 = p_{n+1}^{\alpha_1} p_{n+2}^{\alpha_2} p_{n+3}^{\alpha_3} ... p_{n+k}^{\alpha_k}$, where $p_{n+1}, p_{n+2}, p_{n+3},..., p_{n+k}$ are prime numbers such that $p_{n+1} < p_{n+2} < p_{n+3} < ... < p_{n+k}$ and $\alpha_1, \alpha_2, \alpha_3,..., \alpha_k$ are integers not all equal zero, (if all of $\alpha_1, \alpha_2, \alpha_3,..., \alpha_k$ are equal zero, then $T_n - 1 = 1$). If $\alpha_1 \neq 0$ then there exists prime number p_{n+1} such that $p_n < p_{n+1} < T_n$. If $\alpha_2 \neq 0$ then there exists prime number p_{n+2} such that $p_n < p_{n+2} < T_n$. Generally if $\alpha_j \neq 0$ then there exists prime number p_{n+j} such that $p_n < p_{n+j} < T_n$ for all $1 \le j \le k$ therefore the theorem holds for $T_n - 1$ composite. Therefore exists at least one prime number q such that $p_n < q < T_n$.

Example3.2. Let $n = 3, p_1 = 2, p_2 = 3, p_3 = 5$ and $T_3 = 30$, then there exist $p_4 = 7, p_5 = 11, p_6 = 13, ...$ such that $5 < 7 < 30$, $5 < 11 < 30$, $5 < 13 < 30$

Example3.3. Let $n = 4, p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ and $T_4 = 210$, then there exist $p_5 = 11, p_6 = 13, p_7 = 17, ...$ such that $7 < 11 < 210$, $7 < 13 < 210$, $7 < 17 < 210$

Now we are ready to prove our main result.

Theorem 3.5. Let $p_1, p_2, p_3,..., p_n$, be prime numbers, $p_1p_2p_3...p_n = T_n$, and $M = \{1,2,3,..., T_n\}$, and for prime number p, let $pM = \{pt : t \in M, 1 < pt \le T_n\}$ (bounded multiples of the integer p by elements of the set M) then for

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

prime numbers, $p_{n+1}, p_{n+2}, p_{n+3},..., p_{n+k}$ such that $p_n < p_{n+1} < p_{n+2} < p_{n+3} < ... < p_{n+k} < T_n$ then we have

$$M - \bigcup_{i=1}^{n} p_i M = \{p_{n+1}^{\alpha_{n+1}} p_{n+2}^{\alpha_{n+2}} p_{n+3}^{\alpha_{n+3}} ... p_{n+k}^{\alpha_{n+k}} : k, \alpha_i \text{ integers}, 1 \le i \le k, 0 \le \alpha_i\}.$$

Proof: Since $p_1 p_2 p_3 ... p_n = T_n$, and $M = \{1,2,3,...,T_n\}$, by using Theorem 3.1. there exists at least one prime number q such that $p_n < q < T_n$, suppose that all prime numbers between p_n and T_n are $p_{n+1}, p_{n+2}, p_{n+3},..., p_{n+k}$ such that $p_n < p_{n+1} < p_{n+2} < p_{n+3} < ... < p_{n+k} < T_n$. For all $x \in M$ we can write

$x = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} ... p_n^{\alpha_n} p_{n+1}^{\alpha_{n+1}} p_{n+2}^{\alpha_{n+2}} p_{n+3}^{\alpha_{n+3}} ... p_{n+k}^{\alpha_{n+k}} : k, \alpha_i \text{ integers}, 1 \le i \le n+k, 0 \le \alpha_i$

For all $y_1 \in M - p_1 M$ we can say $y_1 \in M$ and y_1 not multiple of p_1, we can write

$y_1 = p_2^{\alpha_2} p_3^{\alpha_3} ... p_n^{\alpha_n} p_{n+1}^{\alpha_{n+1}} p_{n+2}^{\alpha_{n+2}} p_{n+3}^{\alpha_{n+3}} ... p_{n+k}^{\alpha_{n+k}} : k, \alpha_i \text{ integers}, 2 \le i \le n+k, 0 \le \alpha_i$

For all $y_2 \in M - (p_1 M \cup p_2 M)$, we can say $y_2 \in M$ and y_2 not multiple of p_1 or multiple of p_2, we can write

$y_2 = p_3^{\alpha_3} p_4^{\alpha_4} ... p_n^{\alpha_n} p_{n+1}^{\alpha_{n+1}} p_{n+2}^{\alpha_{n+2}} p_{n+3}^{\alpha_{n+3}} ... p_{n+k}^{\alpha_{n+k}} : k, \alpha_i \text{ integers}, 3 \le i \le n+k, 0 \le \alpha_i$

Continue in this process, $y_n \in M - \bigcup_{i=1}^{n} p_i M$, we can say $y_n \in M$ and y_n not multiple of any element of the set $\{p_1, p_2, p_3,..., p_n\}$, we can write

$y_n = p_{n+1}^{\alpha_{n+1}} p_{n+2}^{\alpha_{n+2}} p_{n+3}^{\alpha_{n+3}} ... p_{n+k}^{\alpha_{n+k}} : k, \alpha_i \text{ integers}, n+1 \le i \le n+k, 0 \le \alpha_i$

Therefore, $M - \bigcup_{i=1}^{n} p_i M = \{p_{n+1}^{\alpha_{n+1}} p_{n+2}^{\alpha_{n+2}} p_{n+3}^{\alpha_{n+3}} ... p_{n+k}^{\alpha_{n+k}} : k, \alpha_i \text{ integers}, 1 \le i \le k, 0 \le \alpha_i\}$.

Example 3.6. Let $n = 3, p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, p_6 = 13, p_7 = 17, p_8 = 19, p_9 = 23, p_{10} = 29$ and $T_3 = 2(3)(5) = 30$, $M = \{1,2,3,...,T_3\}$, $2M = \{2,4,6,...,30\}$, and $3M = \{3,6,9,...,30\}$. We have $M - 2M = \{1,3,5,...,29\}$, $M - 3M = \{1,2,4,5,7,8,...,29\}$, $M - (2M \cup 3M) = \{1,5,7,11,...,29\}$, and

$$M - (2M \cup 3M \cup 5M) = M - \bigcup_{i=1}^{3} p_i = \{1,7,11,13,17,...,29\}.$$

Example3.7. Let $n = 4, p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11,..., p_{44} = 193, p_{45} = 197, p_{46} = 199$ and $T_4 = 210$, $M = \{1,2,3,..., T_4\}$, $2M = \{2,4,6,...,210\}$, and $3M = \{3,6,9,...,210\}$. We have $M - 2M = \{1,3,5,...,209\}$, $M - 3M = \{1,2,4,5,7,8,...,209\}$, $M - (2M \cup 3M) = \{1,5,7,11,...,209\}$,

$M - (2M \cup 3M \cup 5M) = \{1,7,11,13,17,...,209\}$,

$$M - (2M \cup 3M \cup 5M \cup 7M) = M - \bigcup_{k=1}^{4} p_k M = \{1,11,13,17,19,...,197,199,209\}$$

$$M - \bigcup_{k=1}^{4} p_k M = \{1,11,13,17,19,...,197,199,209\} = \{1, p_5, p_6, p_7, ... p_{45}, p_{46}, p_5^2, p_5 p_6, p_5 p_7, p_5 p_8, p_6^2\}$$

$$M - \bigcup_{k=1}^{4} p_k M = \{1,11,13,17,19,...,197,199,209\} = \{p_5^{\alpha_5} p_6^{\alpha_6} p_7^{\alpha_7} ... p_{46}^{\alpha_{46}} : \alpha_i \text{ integer}, 5 \le i \le 46, 0 \le \alpha_i\}$$

IV. CONCLUSION

Suppose all prime numbers known to us are n and p_n is the largest prime number known to us. Let $p_1 p_2 p_3 ... p_{n-1} p_n = T_n$ and $M = \{1,2,3,...,T_n\}$, if we apply Theorem 3.5. we can discover a set of prime numbers, since $M - \bigcup_{i=1}^{n} p_i M = \{p_{n+1}^{\alpha_{n+1}} p_{n+2}^{\alpha_{n+2}} p_{n+3}^{\alpha_{n+3}} ... p_{n+k}^{\alpha_{n+k}} : k, \alpha_{n+j} \text{ integers}, 1 \le j \le k, 0 \le \alpha_{n+j}\}$, the two smallest elements in the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

set $M-\bigcup_{i=1}^{n} p_i M$ are $\{1, p_{n+1}\}$. Therefore p_{n+1} is smallest element of discovered set of prime numbers. For the set $M-\bigcup_{i=1}^{n+1} p_i M = \{p_{n+2}^{\alpha_{n+2}} p_{n+3}^{\alpha_{n+3}} p_{n+4}^{\alpha_{n+4}} \ldots p_{n+k}^{\alpha_{n+k}} : k, \alpha_{n+j} \text{ integers}, 2 \le j \le k, 0 \le \alpha_{n+j}\}$, the two smallest elements in the set $M-\bigcup_{i=1}^{n+1} p_i M$ are $\{1, p_{n+2}\}$. Therefore the two smallest elements of discovered set of prime numbers are p_{n+1} and p_{n+2} such that $p_{n+1} < p_{n+2}$. Also $M-\bigcup_{i=1}^{n+2} p_i M = \{p_{n+3}^{\alpha_{n+3}} p_{n+4}^{\alpha_{n+4}} p_{n+5}^{\alpha_{n+5}} \ldots p_{n+k}^{\alpha_{n+k}} : k, \alpha_{n+j} \text{ integers}, 3 \le j \le k, 0 \le \alpha_{n+j}\}$, the two smallest elements in the set $M-\bigcup_{i=1}^{n+2} p_i M$ are $\{1, p_{n+3}\}$. Therefore the smallest three elements of discovered set of prime numbers are $p_{n+1}, p_{n+2}, p_{n+3}$ such that $p_{n+1} < p_{n+2} < p_{n+3}$. Continue in this process the discovered set of primes numbers will be $\{p_{n+1}, p_{n+2}, p_{n+3}, \ldots, p_{n+k}\}$, such that $p_{n+1} < p_{n+2} < p_{n+3} < \ldots < p_{n+k} < T_n$.

REFERENCES

[1] Shank, D. "Class number, a theory of factorization and genera. Proc. Symp. In Pure Mathematics 20, 1969, Amer. Math. Soc. Providence, R.I., (1971), 415-440.
[2] Mairson, H.G. "Some new upper bounds on the generation of prime numbers". Comm. ACM. 20, 9, 664-669(1975).
[3] Carter Bay and Richard Hudson. "The segmented sieve of Eratosthenes and primes in arithmetic progressions to 10^{12}". BIT. 121-127 (1977).
[4] Gries, D. and Misra, J. "A linear sieve algorithm for finding prime numbers". Communications of the ACM, 21(12), 999-1003, (1978).
[5] Bokhari, S. H., "Multi processing the sieve of Eratosthenes", IEEE Comput. 20(4) 50-58, (1978).
[6] Pritchard, P. "Explaining the wheel sieve". Acta. Informatica (17) 477-485 (1982).
[7] Pritchard, P. "Fast compact prime numberssieves". J, Algorithms, (4) 332-344, (1983).
[8] Pritchard, P. "Linear prime number sieves, A family tree". Science of computer programming. (9) 17-35 (1987).
[9] Sorenson, J. and Parberry, I."Two fast parallel prime number sieves." Information and Computation114, 115-130,(11994).
[10] Le Veque, W.J. Topics in Number Theorey, Volume I. Addision-Wesley, Reading, Mass., 1956.
[11] Hunter, J. Number Theory. (Oliver and Boyd, 1964).
[12] Ireland, K. and Rosen, M.A Classical Introduction to Modern Number Theory, Second ed., Springer Verlag, New York, 1990.