Egyptian Informatics Journal 22 (2021) 101–104

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full length article

A new explicit algorithmic method for generating the prime numbers in order

Abd Elhakeem Abd Elnaby [a], A.H. El-Baz [b]

[a] Department of Mathematics, Faculty of Science, Damietta University, New Damietta, Egypt
[b] Department of Computer Science, Faculty of Computers and Information, Damietta University, New Damietta, Egypt

ARTICLE INFO

Article history:
Received 9 October 2019
Revised 2 March 2020
Accepted 11 May 2020
Available online 11 June 2020

Keywords:
Prime numbers
Cryptography
Algorithms

ABSTRACT

This paper presents a new method for generating all prime numbers up to a particular number $m \in N$, $m \geqslant 9$, by using the set theory. The proposed method is explicit and works oriented in finding the prime numbers in order. Also, we give an efficiently computable explicit formula which exactly determines the number of primes up to a particular number $m \in N$, $m \geqslant 9$. For the best of our knowledge, this is the first exact formula given in literature. For the sake of comparison, a unified framework is done not only for obtaining explicit formulas for the well-known sieves of Eratosthenes and Sundaram but also for obtaining exact closed form expression for the number of generated primes using these two sieve methods up to a particular number $m \in N$, $m \geqslant 9$. In addition, the execution times are calculated for the three methods and indicate that our proposed method gives a superior performance in generating the primes.

1. Introduction

Number theory has many increasingly important applications in computer science and cryptography [1]. One of the central topics of number theory is the prime numbers. The prime numbers are natural numbers greater than 1, which have no positive divisors other than 1 and itself but the natural numbers greater than 1 that are not prime are called composite numbers.

Generating prime numbers by using sieving methods has played a vital role in applied number theory. There are two well-known approaches for draining the composite numbers and leaving the prime numbers by sieving namely, the sieves of Eratosthenes and Sundaram [2] that have been used for obtaining all prime numbers up to a particular number.

In this study, we propose a direct method which depends on the concepts of the sets to generate all the prime numbers in order. Moreover, it is well-known that the prime numbers theorem [2] approximately gives number of primes and which stated that if $\pi(x)$ denotes the number of primes up to a particular number x then $\pi(x) \sim x/\ln(x)$, however, using our proposed method, we give an explicit formula which exactly determines the number of primes up to a particular number $m \in N$, $m \geqslant 9$. Besides, we propose a unified framework for obtaining explicit formulas for both the sieves of Eratosthenes and Sundaram. Also, exact explicit closed form formulas for the generated primes using these two sieves methods are obtained.

The reset of the paper is organized as follows: In Section 2, the proposed method for generating the prime numbers is given along with its algorithm. In Section 3, a unified framework is proposed to obtain the sieves of Eratosthenes and Sundaram using our proposed method. Conclusion is summarized in Section 4.

2. The proposed method

We use set theory [3] to generate the prime numbers up to a particular number $m \in N$, $m \geqslant 9$, the proposed method is given by the following theorem:

Theorem:

Let $P^{(m)}$ be the set of primes up to a particular number $m \in N$, $m \geqslant 9$. If $A_i = \{(2i+1)(2i+1+2n_i) : n_i = 0, 1, 2, 3, \ldots, \left\lfloor \frac{m-(2i+1)^2}{2(2i+1)} \right\rfloor\}$ $i = 1, 2, 3, \ldots k$, $A = \bigcup_{i=1}^{k} A_i$, and $B = \{2j+1 : j = 1, 2, 3, \ldots, \left\lfloor \frac{m-1}{2} \right\rfloor\}$, then $A_{k+1} = \varphi$ whenever $\max(n_{k+1}) = \left\lfloor \frac{m-(2k+3)^2}{2(2k+3)} \right\rfloor < 0$, $P^{(m)} = \{2\} \cup (B - A)$ and $\left|P^{(m)}\right| = |B| - |A| + 1$, where $|\cdot|$ denotes the cardinality.

E-mail address: ali_elbaz@yahoo.com (A.H. El-Baz)
Peer review under responsibility of Faculty of Computers and Information, Cairo University.

https://doi.org/10.1016/j.eij.2020.05.002
1110-8665/

Proof:

Firstly, it must be noted that n_i determines number of generated elements in the set A_i, and i determines number of generated sets from the set A_i.

Since $\max(n_{k+1}) = \left\lfloor \frac{m-(2\,k+3)^2}{2(2\,k+3)} \right\rfloor < 0$, then $\min(n_{k+1}) < 0$ which shows no generated elements in the set A_{k+1} because n_{k+1}does not satisfy the condition on n_i as stated in the set A_i. This gives $A_{k+1} = \varphi$. This proves the first requirement.

Since $\max(n_i)$decreases with increasing i and the set $A_{k+1} = \varphi$, then the set $A_k$contains at least one element and this satisfies only when $\max(n_k) = \min(n_k) = 0$. Consequently, $\left\lfloor \frac{m-(2\,k+1)^2}{2(2\,k+1)} \right\rfloor = 0 \Rightarrow k = \left\lfloor \frac{\sqrt{m}-1}{2} \right\rfloor$ because k is positive integer.

Assume A_i and A are as stated and properties and definition of the floor function, we find that minimum and maximum elements in $A = \bigcup_{i=1}^{k} A_i$, are 9 and $\left(2\left\lfloor \frac{\sqrt{m}-1}{2} \right\rfloor + 1\right)^2$ respectively because minimum elements in A_1 is 9 and maximum elements in A_k is $\left(2\left\lfloor \frac{\sqrt{m}-1}{2} \right\rfloor + 1\right)^2$. Moreover,

$$\left(2\left\lfloor \frac{\sqrt{m}-1}{2} \right\rfloor + 1\right)^2 \leqslant m, \text{ when } \sqrt{m} \text{ is a positive real number.}$$

Then the set of odd composite numbers A can be defined as follows:

$$A = \{9 \leqslant c \leqslant m : c \text{ is an odd composite number}\} \tag{1.1}$$

Assume B as stated and use properties of the floor function, we find that minimum and maximum elements in B are 3 and $2\left\lfloor \frac{m-1}{2} \right\rfloor + 1$ respectively. Moreover, $\left\lfloor \frac{m-1}{2} \right\rfloor = \begin{cases} \frac{m-1}{2}, & m \text{ is odd} \\ \frac{m}{2} - 1, & m \text{ is even} \end{cases}$

Suppose $C \subseteq B$ and $P \subseteq B$ which are defined as follows:

$$C = \{9 \leqslant c \leqslant m : c \text{ is an odd composite number}\}. \tag{1.2}$$

And

$$P = \{3 \leqslant p \leqslant m : p \text{ is a prime number}\}. \tag{1.3}$$

Then B can be written as follows:

$$B = C \cup P, \tag{1.4}$$

Also, $P^{(m)}$ as stated can be defined as follows:

$$P^{(m)} = \{2 \leqslant p \leqslant m : p \text{ is a prime number}\}. \tag{1.5}$$

It is clear from (1.1) and (1.2) that A = C Hence, (1.4) becomes

$$B = A \cup P. \tag{1.6}$$

Moreover, it is clear from (1.2) and (1.3) that $C \cap P = \varphi$. Therefor

$$A \cap P = \varphi. \tag{1.7}$$

From (1.6) and (1.7), we have

$$P = B - A \tag{1.8}$$

Also, it is clear from (1.3) and (1.5) that

$$P^{(m)} = \{2\} \cup P. \tag{1.9}$$

Substitution from (1.8) in (1.9), we obtain

$$P^{(m)} = \{2\} \cup (B - A). \tag{1.10}$$

This proves the second requirement.

Since $(B - A) \cap \{2\} = \varphi$, then (1.10) gives

$$\left|P^{(m)}\right| = |\{2\}| + |B - A| = 1 + |B - A|. \tag{1.11}$$

Since $B = (B - A) \cup A$ and $(B - A) \cap A = \varphi$, then

$$|B| = |B - A| + |A| \Rightarrow |B - A| = |B| - |A|. \tag{1.12}$$

Substitution from (1.12) in (1.11) gives

$$\left|P^{(m)}\right| = 1 + |B| - |A|. \tag{1.13}$$

This proves the third requirement and hence the proof is completed.

- **Pseudocode for the proposed method**

The following algorithm gives our proposed method for generating prime numbers.

Algorithm: The proposed method for generating primes

```
function Prime (m)            ▹ m is the limit up to which
                                primes are generated
  i ← 1
    while i ⩽ ⌊(m−1)/2⌋ do
      B(i) ← 2i + 1
      i ← i + 1
  end while
  k ← 1
  i ← 1
  while k > 0 do
      k ← ⌊(m−(2i+1)^2)/(4i+2)⌋
      i ← i + 1
   end while
   k ← i
   i ← 1
   n ← 0
   while i ⩽ k do
   d ← ⌊(m−(2i+1)^2)/(4i+2)⌋
      while n ⩽ d do
         x(n + 1) ← (2i + 1)(2i + 2n + 1)
      end while
A ← x      ▹ save the generated elements x in vector A
      x ← [ ]
   end while
P = B-A    ▹ P is the primes which represents the set
  difference of B and A
   end function
```

3. A unified framework

For the sake of comparison with our proposed technique for generating primes, we proposed a unified framework to obtain the well-known sieving methods, namely the sieves of Eratosthenes and Sundaram.

3.1. Proposed technique for obtaining the sieve of Eratosthenes

In order to obtain the sieve of Eratosthenes using our proposed method for generating all primes up to a particular number, $m \in N$, $m \geqslant 9$, we perform the following steps:

Step 1: Let B^E be the set of numbers less than or equal a particular number m, i.e.

$$B^E = \{j + 1 : j = 1, 2, 3, \ldots, m - 1\}.$$

Step 2: Let C^E be the set of even numbers greater than two and less than or equal a particular number m, i.e.

$$C^E = \left\{2l : l = 2, 3, \ldots, \left\lfloor \frac{m}{2} \right\rfloor \right\}.$$

Step 3: Generate the set A_i^E where

$$A_i^E = \left\{(2i+1)(2n_i+1) : n_i = 1, 2, \ldots, \left\lfloor \frac{m-(2i+1)}{2(2i+1)} \right\rfloor \right\},$$
$$i = 1, 2, 3, \ldots, k.$$

where $\left|A_i^E\right| = \left\lfloor \frac{m-(2i+1)}{2(2i+1)} \right\rfloor$, $\lfloor . \rfloor$ is the Floor function and $|.|$ is the Cardinality.

If $i = k+1$, we obtain $\left\lfloor \frac{m-(2i+1)}{2(2i+1)} \right\rfloor = 0$ then stop generating the set A_i^E.

Step 4: Let $A^E = \bigcup_{i=1}^{k} A_i^E$

Step 5: Let $P_E^{(m)}$ be the set of primes up to a particular number $m \in N$, $m \geqslant 9$, then

$$P_E^{(m)} = B^E - \left(A^E \cup C^E\right).$$

Also, the cardinality of $P_E^{(m)}$ is given by

$$\left|P_E^{(m)}\right| = \left|B^E\right| - \left|A^E \cup C^E\right|$$

3.2. Proposed technique for obtaining the sieve of Sundaram

In order to obtain the sieve of Sundaram using our proposed method for generating all primes up to a particular number, $m \in N$, $m \geqslant 9$, we perform the following steps:

Step 1: Let B^S be the set of numbers less than or equal m.

$$B^S = \{j : j = 1, 2, 3, \ldots, m\}.$$

Step 2: Generate the set C^S where

$$C^S = \left\{ \left\lfloor \frac{m}{2} \right\rfloor + q : q = 0, 1, 2, \ldots, m - \left\lfloor \frac{m}{2} \right\rfloor \right\}$$

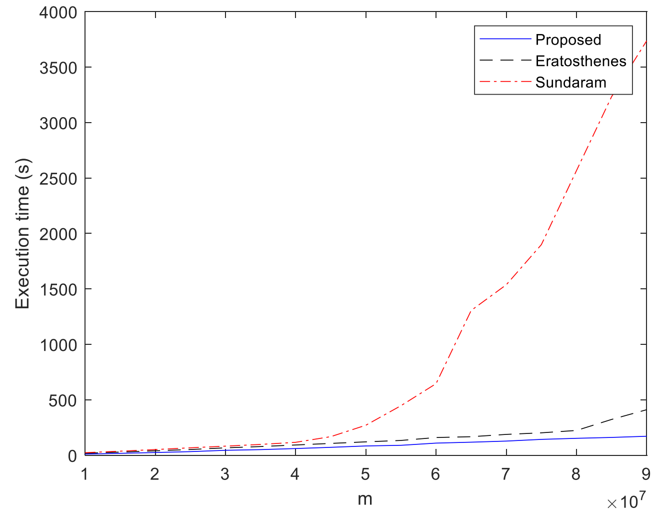

Fig. 1. The execution time versus a particular number $m \in N$, $m \geqslant 9$ for the proposed, Eratosthenes and Sundaram methods.

Step 3: Generate the set A_i^S where

$A_i^S = \{i + n_i(2i+1) : n_i = 1, 2, 3, \ldots \left\lfloor \frac{m-(2i+1)}{2(2i+1)} \right\rfloor\}$, $i = 1, 2, \ldots, k$. And $\left|A_i^S\right| = \left\lfloor \frac{m-(2i+1)}{2(2i+1)} \right\rfloor$, $\lfloor . \rfloor$ is the Floor function and $|.|$ is the Cardinality.

If $i = k+1$, we obtain $\left\lfloor \frac{m-(2i+1)}{2(2i+1)} \right\rfloor = 0$ then stop generating the set A_i^S.

Step 4: Let $A^S = \bigcup_{i=1}^{k} A_i^S$

Step 5: Let $B^S - \left(A^S \cup C^S\right) = \{r : r \in N\}$

Step 6: Let $P_s^{(m)}$ be the set of primes up to a particular number $m \in N$, $m \geqslant 9$, then

Table 1
The execution time versus a particular number $m \in N$, $m \geqslant 9$ for the proposed, Eratosthenes and Sundaram methods.

m	Number of generated sets (k)			Execution time (in second)		
	Proposed method	Eratosthenes	Sundaram	Proposed method	Eratosthenes	Sundaram
1000	15	166	166	0.039534	0.040474	0.040810
10,000	50	1666	1666	0.045739	0.057403	0.072236
100,000	158	16,666	16,666	0.104759	0.174620	0.214130
1,000,000	500	166,666	166,666	1.064138	1.904619	2.361416
10,000,000	1581	1,666,666	1,666,666	9.957602	17.780659	22.484089
15,000,000	1936	2,499,999	2,499,999	16.825560	28.163155	36.187907
20,000,000	2236	3,333,332	3,333,332	24.033616	39.608600	50.809382
25,000,000	2500	4,166,666	4,166,666	32.062576	51.058231	66.644372
30,000,000	2738	4,999,999	4,999,999	44.108035	66.276671	81.603483
35,000,000	2958	5,833,332	5,833,332	50.220697	77.931476	97.107659
40,000,000	3162	6,666,666	6,666,666	59.943121	92.131258	116.128039
45,000,000	3354	7,499,999	7,499,999	70.969666	106.166029	167.198875
50,000,000	3535	8,333,332	8,333,332	83.296963	120.356633	270.250105
55,000,000	3708	9,166,666	9,166,666	89.159296	132.971661	446.401534
60,000,000	3872	9,999,999	9,999,999	108.996244	159.264843	645.043552
65,000,000	4031	10,833,332	10,833,332	117.289075	166.699335	1305.106774
70,000,000	4183	11,666,666	11,666,666	127.232278	187.502824	1536.719741
75,000,000	4330	12,499,999	12,499,999	142.604397	201.772238	1898.559985
80,000,000	4472	13,333,332	13,333,332	152.231903	223.066406	2566.107955
85,000,000	4609	14,166,666	14,166,666	160.146174	322.253137	3232.662483
90,000,000	4743	14,999,999	14,999,999	170.764237	410.198350	3736.636055
95,000,000	4873	15,833,332	15,833,332	187.835150	753.563263	4776.194199
100,000,000	5000	16,666,666	16,666,666	192.269125	1066.539915	6802.735193

$$P_S^{(m)} = \{2\} \cup \{2r+1 : r \in N\}$$

Also, the cardinality of $P_S^{(m)}$ is given by

$$\left|P_S^{(m)}\right| = \left|B^S\right| - \left|A^S \cup C^S\right| + 1$$

Moreover, Table 1 gives the number of generated sets (k) which is used to generate the prime numbers and execution times for the three methods versus a particular number $m \in N,\ m \geqslant 9$. It is clear that the proposed method uses less number of generated sets and less runtimes than the other methods. The results are illustrated in Fig. 1 which indicate the superior performance of our method in obtaining the prime numbers.

The system specifications of the PC that runs the experiments is Intel ® core™ i7-4790 CPU@ 3.60 GHZ, 16 GB Ram and 16-bit Windows operating system, X64-based processor.

4. Conclusion

In this paper, an explicit and direct technique for generating the primes is given. This technique depends on the sets and Floor function. It can be used to generate all primes in order up to a particular number $m \in N,\ m \geqslant 9$. Also; we give an explicit formula which exactly determines the number of primes up to a particular number $m \in N,\ m \geqslant 9$. Moreover, for the sake of comparison, a unified framework is proposed for obtaining the sieves of both Eratosthenes and Sundaram using our proposed method. The execution times are calculated for the three methods and indicate that the proposed method is more efficient in obtaining the primes in order.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Stinson DR. Cryptography: theory and practice. 4th Edition. CRC Press; 2019.
[2] Crandall R, Pomerance C. Prime numbers: a computational perspective. 2nd Edition. New York: Springer; 2005.
[3] Cunningham DW. Set theory: a first course. Cambridge University Press; 2016.