Journal of Modern Technology and Engineering
Vol.4, No.3, 2019, pp.170-177

ON A CALCULATION OF A NUMBER OF COMPOSITE NUMBERS IN A GIVEN INTERVAL

Elnur Nuri[1], Fidan Nuriyeva[2,3*], Urfat Nuriyev[1,3]

[1]Ege University, Department of Mathematics, Izmir, Turkey
[2]Department of Computer Science, Dokuz Eylul University, Izmir, Turkey
[3]Institute of Control Systems of ANAS, Baku, Azerbaijan

Abstract. In this study, computational schema based on dynamic programming technique is proposed to determine the number of composite numbers in a given interval.

Keywords: prime numbers, composite numbers, sieve of eratosthenes, dynamic programming technique, inclusion – exclusion principle, distribution of the prime numbers.
AMS Subject Classification: 11A41, 11B37, 11B75, 11Y11, 11Y16.
Corresponding author: Fidan Nuriyeva, Dokuz Eylul University, Faculty of Science, Department of Computer Science, Izmir, Turkey, Tel.: +90232 301 9504, e-mail: *nuriyevafidan@gmail.com*
Received: 28 May 2019; Accepted: 15 October 2019; Published: 25 December 2019.

1 Introduction

Number theory plays an important role in modern cryptography, which is used to improve the security of electronic communication with the aim of ensuring the security of computers and the internet. In cryptographic protocols, Prime Numbers form the basis of many protocols which are used for sharing keys and sending signed messages (Crandall & Pomerance, 2005).

If the positive factors of a positive integer p ($p > 1$) are only 1 and p, then p is called a *prime number*. An integer that is greater than one and is not a prime is called a *composite number*. As it seen from their definition, the set of prime and composite numbers in any interval of a set of natural numbers greater than 1 form the complementary sets of one another. Therefore, a property of the set that is determined for one of these sets can be arranged appropriately for the other one (Hardy & Wright, 1979).

In 300 BC Euclid proved that prime numbers are infinite. But for many years the question of "how many prime numbers are there less than any integer" has intrigued mathematicians. Beginning at the end of the 18th century, Gauss C., Chebyshev P.L., Hadamard J., de la Vallee Poussin C., Legendre A. has stuides about this topic (Dickson, 2005).

The number of prime numbers less than x is denoted by $\pi(x)$. As a result of the studies of the researchers whose names we have mentioned above, it was determined that the function $\pi(x)$ changes asymptotically as x/lnx, meaning that the ratio of these two expressions converges to 1 as x approaches infinity (Crandall & Pomerance, 2005).

In many problems it is necessary to specify the number of prime numbers in a given interval, for example, the conjecture proposed by Adrien-Marie Legendre in 1808 states that "there is a prime number between n^2 and $(n + 1)^2$ for every positive integer n" (Guy, 2004).

In this case, instead of calculating the number of primes in the given interval, it could be easier to calculate the number of composite numbers in that interval, and then we can use it to find the number of elements of the subset of prime numbers, which is the complement of the set of composite numbers in that interval.

In this paper a method with less computational complexity than the known methods for calculating the number of composite numbers in a given interval is proposed. The proposed method is based on the modelling of the sieve of Eratosthenes (Crandall & Pomerance, 2005). A computational schema based on Dynamic Programming Technique (Bellman & Dreyfus, 1962) has been proposed to determine the number of composite numbers in each interval.

2 Notations

$N = \{1, 2, \ldots, n, \ldots\}$, Set of Natural Numbers.
$\overline{N} = N \backslash \{2, 3, 4, \ldots, n, ...\}$.

$P = \{p_1, p_2, p_3, \ldots\} = \{2, 3, 5, \ldots\}$, Set of Prime Numbers.

$M = \overline{N} \backslash P = CoP$, Set of Composite Numbers.

$M_k = \{m \in \overline{N} | m = k \cdot n, n \in N\}, k \in \overline{N}$, Set of numbers consisting of multiples of k.

$\overline{M_k} = M_k \diagdown \{k\}, k \in \overline{N}$.

The following two propositions follow from the definitions given above:

$M = \cup_{p \in P} \overline{M_p}$.

$P = \overline{N} \backslash M = \overline{N} \backslash (\cup_{p \in P} \overline{M_p})$, (Sieve of Eratosthenes).

Define the sequence A_k as follows:

$A_k = \{a_i^k \in N | a_i^k = k \cdot i, i \in N\}, k \in \overline{N}$.

Denote the set of elements not exceeding n of the sequence A_k by $A_k(n)$.

$1 \leq a_i^k \leq n, i \in N, k \in \overline{N}$.

Now consider the concept of union of several sequences:

$A^{(k)} = \bigcup_{i=1}^{k} A_{p_i}$.

For example, for $k = 1$, $A^{(1)} = A_{p_1} = A_2$,

for $k = 2$, $A^{(2)} = A_{p_1} \cup A_{p_2} = A_2 \cup A_3$,

for $k = 3$, $A^{(3)} = A_{p_1} \cup A_{p_2} \cup A_{p_3} = A_2 \cup A_3 \cup A_5$.

Denote by $A^{(k)}(n)$ the set of all elements of $A^{(k)}$ that are not greater than n.

3 Calculation of the Number of Elements in the Union of Sets by the Principle of Inclusion-Exclusion

Let $s(A)$ be the number of elements of a set A. It is well known that the number of elements in the union of two sets A and B is calculated by the following formula based on the Inclusion-Exclusion Principle (Rosen, 2012):

$$s(A \cup B) = s(A) + s(B) - s(A \cap B) \tag{1}$$

A generalization of this formula for n sets is as follows:

$$
\begin{aligned}
s\left(\bigcup_{i=1}^{n} A_i\right) = &\sum_{i=1}^{n} s(A_i) - \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} s(A_i \cap A_j) \\
&+ \sum_{i=1}^{n-2}\sum_{j=i+1}^{n-1}\sum_{k=j+1}^{n} s(A_i \cap A_j \cap A_k) \\
&- \sum_{i=1}^{n-3}\sum_{j=i+1}^{n-2}\sum_{k=j+1}^{n-1}\sum_{l=k+1}^{n} s(A_i \cap A_j \cap A_k \cap A_l) \\
&+ \sum_{i=1}^{n-4}\sum_{j=i+1}^{n-3}\sum_{k=j+1}^{n-2}\sum_{l=k+1}^{n-1}\sum_{t=l+1}^{n} s(A_i \cap A_j \cap A_k \cap A_l \cap A_t) \\
&+ \cdots + (-1)^{n+1} \cdot s(A_1 \cap A_2 \cap A_3 \cap \ldots A_{n-1} \cap A_n)
\end{aligned} \tag{2}
$$

This principle gives the number of elements in the union of n sets for every positive integer n. For the number of elements in the intersection of each non-empty subset of the collection consisting of a total of n sets there is a term in this formula, therefore there are $2n - 1$ terms in the Formula (2), in other words the computational complexity of the Formula (2) is $O(2^n)$.
Example: Consider the number of elements of the union of four sets:

$$
\begin{aligned}
s(A_1 \cup A_2 \cup A_3 \cup A_4) =&s(A_1) + s(A_2) + s(A_3) + s(A_4) \\
&- s(A_1 \cap A_2) - s(A_1 \cap A_3) - s(A_1 \cap A_4) - s(A_2 \cap A_3) - s(A_2 \cap A_4) \\
&- s(A_3 \cap A_4) + s(A_1 \cap A_2 \cap A_3) + s(A_1 \cap A_2 \cap A_4) + s(A_1 \cap A_3 \cap A_4) \\
&+ s(A_2 \cap A_3 \cap A_4) - s(A_1 \cap A_2 \cap A_3 \cap A_4)
\end{aligned}
$$

It can be seen that there are 15 different terms in this formula, which gives the number of non-empty subsets of these four sets.

4 Calculation of the Nnumber of Prime Numbers in a Given Interval by the Inclusion-Exclusion Principle

As it is known, the Sieve of Eratosthenes method can be used to find all prime numbers that are less than a some positive integer n (Crandall & Pomerance, 2005). Using the principle of inclusion-exclusion, we can find the number of primes not exceeding a specified positive integer with the same reasoning used in the sieve of Eratosthenes. Recall that a composite integer is divisible by a prime number not exceeding its square root. So, to find the number of primes not exceeding 100, first note that composite integers not exceeding 100 must have a prime factor not exceeding 10. Since all prime numbers not exceeding 10 are 2, 3, 5 and 7, prime numbers not exceeding 100 are these four prime numbers and those positive integers greater than 1 and not exceeding 100 that are not divisible by none of 2, 3, 5 and 7. To apply the inclusion-exclusion principle, let P_1 be the property of divisibility by 2, P_2 be the property of divisibility by 3, P_3 be the property of divisibility by 5 and P_4 be the property of divisibility by 7. Thus, the number of primes not exceeding 100 is $4 + N(P_1' P_2' P_3' P_4')$.

Since there are 99 positive integers greater than 1 and not exceeding 100, the inclusion-exclusion principle shows that

$$
\begin{aligned}
N(P_1' P_2' P_3' P_4') =&99 - N(P_1) - N(P_2) - N(P_3) - N(P_4) \\
&+ N(P_1P_2) + N(P_2P_3) + N(P_1P_4) + N(P_2P_3) + N(P_2P_4) + N(P_3P_4) \\
&- N(P_1P_2P_3) - N(P_1P_2P_4) - N(P_1P_3P_4) - N(P_2P_3P_4) \\
&+ N(P_1P_2P_3P_4)
\end{aligned}
$$

Table 1: Number of Composite Numbers up to the Given Number

i	$s(A^{(1)}(i))$	$s(A^{(2)}(i))$	$s(A^{(3)}(i))$	$s(A^{(4)}(i))$	$s(A^{(5)}(i))$	$s(A^{(6)}(i))$	$s(A^{(7)}(i))$	$s(A^{(8)}(i))$	$s(A^{(9)}(i))$
1	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1
3	1	2	2	2	2	2	2	2	2
4	2	3	3	3	3	3	3	3	3
5	2	3	4	4	4	4	4	4	4
6	3	4	5	5	5	5	5	5	5
7	3	4	5	6	6	6	6	6	6
8	4	5	6	7	7	7	7	7	7
9	4	6	7	8	8	8	8	8	8
10	5	7	8	9	9	9	9	9	9
11	5	7	8	9	10	10	10	10	10
12	6	8	9	10	11	11	11	11	11
13	6	8	9	10	11	12	12	12	12
14	7	9	10	11	12	13	13	13	13
15	7	10	11	12	13	14	14	14	14
16	8	11	12	13	14	15	15	15	15
17	8	11	12	13	14	15	16	16	16
18	9	12	13	14	15	16	17	17	17
19	9	12	13	14	15	16	17	18	18
20	10	13	14	15	16	17	18	19	19
21	10	14	15	16	17	18	19	20	20
22	11	15	16	17	18	19	20	21	21
23	11	15	16	17	18	19	20	21	22
24	12	16	17	18	19	20	21	22	23
25	12	16	18	19	20	21	22	23	24
26	13	17	19	20	21	22	23	24	25
27	13	18	20	21	22	23	24	25	26
28	14	19	21	22	23	24	25	26	27
29	14	19	21	22	23	24	25	26	27
30	15	20	22	23	24	25	26	27	28
31	15	20	22	23	24	25	26	27	28
32	16	21	23	24	25	26	27	28	29
33	16	22	24	25	26	27	28	29	30
34	17	23	25	26	27	28	29	30	31
35	17	23	26	27	28	29	30	31	32
36	18	24	27	28	29	30	31	32	33

The number of integers not exceeding 100 (and greater than 1) that are divisible by all the prime numbers in any subset of the set $\{2, 3, 5, 7\}$ is $\lfloor \frac{100}{n} \rfloor$ where n is the product of the prime numbers in this subset since these primes are pairwise relatively prime. Therefore

$$\begin{aligned} N(P_1^{'}P_2^{'}P_3^{'}P_4^{'}) =& 99 - \lfloor\frac{100}{2}\rfloor - \lfloor\frac{100}{3}\rfloor - \lfloor\frac{100}{5}\rfloor - \lfloor\frac{100}{7}\rfloor \\ & + \lfloor\frac{100}{2\cdot 3}\rfloor + \lfloor\frac{100}{2\cdot 5}\rfloor + \lfloor\frac{100}{2\cdot 7}\rfloor + \lfloor\frac{100}{3\cdot 5}\rfloor + \lfloor\frac{100}{3\cdot 7}\rfloor + \lfloor\frac{100}{5\cdot 7}\rfloor \\ & - \lfloor\frac{100}{2\cdot 3\cdot 5}\rfloor - \lfloor\frac{100}{2\cdot 3\cdot 7}\rfloor - \lfloor\frac{100}{2\cdot 5\cdot 7}\rfloor - \lfloor\frac{100}{3\cdot 5\cdot 7}\rfloor + \lfloor\frac{100}{2\cdot 3\cdot 5\cdot 7}\rfloor \\ & = 99 - 50 - 33 - 20 - 14 + 16 + 10 + 7 + 6 + 4 + 2 - 3 - 2 - 1 - 0 + 0 \\ & = 21. \end{aligned}$$

Hence, there are $4 + 21 = 25$ prime numbers not exceeding 100.

5 Dynamically Calculation of the Number of Composite Numbers in a Given Interval

Determination of the number of composite numbers in a given interval by of inclusion-exclusion principle is not very efficient for calculations, so the calculation schema based on Dynamic Programming Technique (Bellman & Dreyfus, 1962) has been proposed below for the determination of the number of composite numbers for each interval.

The calculation schema is based on the model of the Sieve of Eratosthenes method. In proposed NNN Procedure, in order to compute $s(A^{(k)}(i))(i = 1, 2, \ldots, n)$; $(k = 1, 2, \ldots, m)$ Table 1 with a dimension $m \times n$ is prepared by using Dynamic Programming technique as shown below. Numbers n and m are changeable and mainly both of them can be infinite. The values of i, $(i = 1, 2, \ldots, n)$ show the number of rows and the values of the parameters $s(A^{(k)}(i))$ $(k = 1, 2, \ldots, m)$ are given in the kth column.

Table 2: Number of Composite Numbers in a Given Interval

	$s(B^{(k)}(i))$	$s(B^{(1)}(i))$	$s(B^{(2)}(i))$	$s(B^{(3)}(i))$	$s(B^{(4)}(i))$	$s(B^{(5)}(i))$	$s(B^{(6)}(i))$	$s(B^{(7)}(i))$	$s(B^{(8)}(i))$	$s(B^{(9)}(i))$
	Primes	2	2,3	2,3,5	2,3,5,7	2,3,5,7 11	2,3,5,7 11,13	2,3,5,7 11,13, 17	2,3,5,7 11,13,17,19	2,3,5,7 11,13,17,19,23
	Interval									
1	1 - 3	1	2	2	2	2	2	2	2	2
2	4 - 8	3	3	4	5	5	5	5	5	5
3	9 - 15	3	5	5	5	6	7	7	7	7
4	16 - 24	5	6	6	6	6	6	7	8	9
5	25 - 35	5	7	9	9	9	9	9	9	9
6	36 - 48	7	9	9	9	9	9	9	9	9
7	49 - 63	7	10	11	12	12	12	12	12	12
8	64 - 80	9	11	12	13	13	13	13	13	13
9	81 - 99	9	13	15	16	16	16	16	16	16
10	100 -120	11	14	15	16	16	16	16	16	16
11	121 - 143	11	15	16	17	19	19	19	19	19
12	144 - 168	13	17	19	20	20	20	20	20	20
13	169 - 195	13	18	20	20	21	22	22	22	22
14	196 - 224	15	19	21	23	24	25	25	25	25
15	225 - 255	15	21	23	23	24	25	25	25	25
16	256 - 288	17	22	24	26	26	26	26	26	26
17	289 - 323	17	23	25	26	27	28	30	30	30
18	324 - 360	19	25	28	30	31	31	31	31	31
19	361 - 399	19	26	29	30	30	31	32	33	33
20	400 - 440	21	27	29	31	32	33	33	34	34
21	441 - 483	21	29	32	33	35	36	36	36	36
22	484 - 528	23	30	33	35	36	36	36	38	38
23	529 - 575	23	31	35	37	37	39	39	40	41
24	576 - 624	25	33	35	37	38	39	39	40	40
25	625 - 675	25	34	38	39	41	41	42	42	43

6 Algorithm NNN

NNN1: The elements of the first column of Table 1 are calculated by the following formulas:

$$s(A^{(1)}(i)) = \left\lfloor \frac{i}{2} \right\rfloor, (i = 1, 2, \ldots, n) \tag{3}$$

NNN2: The elements of the next colums ($k = 2, \ldots, m$) are calculated by the following formulas: The initial values of z_1^k and $s(A^{(k)}(1))$ are zero for each column ($k = 2, \ldots, m$).

$$z_1^k = 0 \tag{4}$$

$$s(A^{(k)}(1)) = 0 \tag{5}$$

The values of z and s in the next rows ($i = 2, \ldots, n$) are calculated by the following recursive formulas (6) and (7):

$$z_i^k = \begin{cases} z_{i-1}^k + 1 & \text{if } p_k | i \text{ and } s(A^{(k-1)}(i)) = s(A^{(k-1)}(i-1)) \\ z_{i-1}^k & \text{otherwise} \end{cases} \tag{6}$$

$$s(A^{(k)}(i)) = s(A^{(k)}(i-1)) + z_i^k \tag{7}$$

Table 1 of size of (36×9) , $n = (1, 2, \ldots, 36)$, for $m = (2, 3, 5, 7, 11, 13, 17, 19, 23)$ prepared with NNN Procedure is given below.

We give the following theorem for the algorithm NNN.

Theorem 1. *The formulas (3) – (7) are true, so $s(A^k(i))$, $(i = 1, 2, \ldots, n), (k = 1, 2, \ldots, m)$ are calculated correctly: The number in the k.th column and i.th row of the table gives the number of elements of the subset of the set formed by the first k prime numbers in the interval* $[1, i]$.

Proof: As it is seen from Table 1 in column 1 in every row the "integer part of the number i divided by 2 with the Formula (3)" is written, which gives the number of integers divisible by 2 in the interval $[1, i]$.

Clearly the numbers in odd numbered rows in first column are equal to numbers in even numbered rows before them. So, the row numbers that corresponds the first of repeated numbers in column 1 $(2., 4., 6., ...,)$ are divisible by 2, but the row numbers that corresponds to the last(second) of repeated numbers $(3., 5., 7., ...,)$ are not divisible by 2.

For each *i.th* row of the second column a value z_i^2 is added to the number located in a previous 1.st column and *i.th* row: firstly, $z_1^2 = 0$ and then if i is divisible by $p_2 = 3$ and is not divisible by previous $p_1 = 2$, the value of z increases by 1 ($z_i^2 = z_{i-1}^2 + 1$). This guarantees the equality (1).

This is algorithmically done by checking the repeated numbers in the column 1. As it is mentioned above, the row number that corresponds to the first of repeated numbers is divisible by 2, while the row number that corresponds to the second of repeated numbers is not divisible by 2. As it seen from Table 1. the first repeated number in the column 1 is "1"; it is settled in the row 2. and 3: thus "3" becomes the first prime number after "2", and in this column the multiples of "3" are tackled. In 6th row, which is twice the size of "3", "1" will not be added to z_5^2, because in a 6th row of a 1st column the repeated number "3" is not a last number, meaning it is divisible by "2". But in a row 9, which is three times "3", "1" will be added to z_8^2, because in a column 1 and 9.th row the repeated number "4" is the last number, meaning it is not divisible by "2". Consequently, after every 6 rows (i.e. 15., 21., 27., and other.) "1" will added to z.

In each $i.th$ row of $k.th$ of the column, a value z_i^k is added to a number located in a $i.th$ row of a previous $(k-1).th$ column. Firstly, $z_i^k = 0$, and if i is divisible by p_k and is not divisible by previous $p_i(i = 1, 2, \ldots, (k-1))$, value of z is increased by 1 ($z_i^k = z_{i-1}^k + 1$), which guarantees that equality (1) holds true.

As above, this is also algorithmically done by checking the repeated numbers in the column $(k-1)$. As we have said above, the row number that corresponds to the first of repeated numbers is divisible by one, or more than one, of the numbers $p_1, p_2, \ldots, p_{k-1}$, the second is not divisible by any of these numbers.

For example, As it seen from Table 1 for k=3 the first repeated number in the column 2 is "3"; are located in a rows 4. and 5.: thus "5" becomes the prime number after "2" and "3", and in this column the multiples of "5" are tackled. In the 10th row, which is twice the size of "5", "1" will not be added to z_9^3, because in a 7th row of a 2nd column the number "7" is not repeated, similarly, in the 15th row, which is three times of "5", in the 20th row, which is four times of "5", "1" will not be added to z, because the number "10" in a 15th row of a 2.nd column and the number "13" in 20th row of a second column is not repeated.

But in a 25th row of a 2nd column, which is five times of "5", number 16 is repeated and it is the last number and it means that $i = 25$ and is not divisible by prime numbers "2" and "3" which comes before "5". In this row, "1" is added to the number z_{24}^3.

In order to fill the next column, a value of z is added to a value of each row of a previous column. Firstly, the parameter z is equal to 0, in the next steps value z value is incremented by 1 in the rows that corresponds to the second of repeated numbers in previous column.

7 Analysis of Table 1

If we pay attention to the table, we can see the following properties:

A1. For each $k.th$ column in the first $(p_{k+1} - 1)$ rows (in rows $1, 2, \ldots, (p_{k+1} - 1)$) the numbers $0, 1, 2, \ldots, (p_{k+1} - 2)$ are written. In other words, for every $k.th$ column in the first $(p_{k+1} - 1)$ row, in each next row a number of composite numbers increased by 1 beginning from zero. The number of composite numbers in the $(p_{k+1} - 1)$th row is only one less than the row number, that is $((p_{k+1} - 1) - 1) = (p_{k+1} - 2)$. The number of composite numbers in the next $(p_{k+1})th$ row is also $(p_{k+1} - 2)$.

A2. For each k.th column beginning from the $(p_{k+1} + 1)$th row in each row a number of composite numbers increases by one or does not increase at all, it just repeats and the length of the repetition is equal to 2, and it means that only two consecutive rows may have the same values.

A3. The number of operations required to fill the table is $O(m \times n)$.

8 Conclusion

We can fill Table 2 by using Table 1 with the following formula:

$$s(B^{(k)}(i)) = s(A^{(k)}((i+1)^2 - 1)) - s(A^{(k)}((i)^2 - 1)), k = 1, 2, \ldots, m; i = 1, 2, \ldots, n. \quad (8)$$

Here $(A^k(0)) = 0,\ \ k = 1, 2, ..., m.$

Table 2 of size of (25×9) for $(n = 1, 2, \ldots), 25)$, $(m = 2, 3, 5, 7, 11, 13, 17, 19, 23)$ is filled up using Table 1 and by the formula (8). Here the numbers painted with yellow indicate the number of composite numbers in the appropriate interval. If we compare the second method with first one in terms of computational complexity, $O(n \times 2^n)$ operations are needed to fill up the Table 1 with the first method.

In the first method, the space complexity for calculating each element of the table is $O(1)$, whereas in the second method, this complexity is $O(n)$, because the previous column is sufficient to fill up each next column of the table. But in order to fill up Table 1 general space complexity for both methods is $O(m \times n)$.

As it seen from the evaluations above, the computational complexity ($O(m \times n)$) of the second method for filling up Table 1 is better than that of the first method ($O(n \times 2^n)$).

References

Bellman, R., Dreyfus, S. (1962). *Applied Dynamic Programming*, Princeton University Press.

Crandall, R., Pomerance, C. (2005). *Prime Numbers. A Computational Perspective.* Springer.

Dickson, L.E. (2005). History of the Theory of Numbers *Divisibility and Primality, 1.*

Hardy, G.H., Wright, E.M. (1979). *An Introduction to the Theory of Numbers.* 5th ed., Oxford Univ. Press.

Guy, R.K. (2004). *Unsolved Problems in Number Theory.* 3rd ed. New York, Springer-Verlag.

Rosen, K.H. (2012). *Discrete Mathematics and its applications.* 7th ed., New York, McGraw-Hill, 2012.