AN ALGORITHMIC VERSION OF

THE SIEVE OF ERATOSTHENES

PLUS OTHER SOLUTIONS ASSOCIATED

WITH PRIME NUMBERS.

Peter G.Bass.

www.relativitydomains.com

M19 Ver. 1.0.0
June 2015.

SUMMARY.

This paper develops an algorithmic version of the Sieve of Eratosthenes to identify all the prime numbers up to and including any desired natural number. The method also provides for the simple calculation of $\pi(N)$.

In addition, the primary term in the algorithm enables a new and very simple method for the determination of primality or compositeness of any number and, in the case of the latter, the factors involved, which enables these parameters to be easily determined for very large composite numbers.

CONTENTS.

1.0 Introduction.

Some two hundred and fifty years BC, a Greek mathematician, Eratosthenes of Cyrene, devised a method of identifying all the prime numbers by elimination of the composites from the group of natural numbers. Today this method is known as the Sieve of Eratosthenes, and is still the most successful method of producing prime numbers. However, it suffers from the difficulty that, as the method progresses into extremely large numbers, it becomes more and more difficult to identify the composites.

The method presented here eliminates this difficulty by incorporating a simple algorithm for the generation of all the composites, so enabling the fast identification of the primes. This algorithm also provides the means to determine three other important parameters. They are (i) A relatively quick and simple means of determining an exact value for $\pi(N)$. (ii) A very simple method for determining whether any odd number is prime or composite, and (iii) a very simple method for determining the prime factors for extremely large composite numbers.

2.0 An Algorithmic Version of the Sieve of Eratosthenes.

2.1 Development of the Algorithm.

It is well known that the natural numbers are the combination of all the primes and all the composites, thus

$$[N]=[P]\wedge[M] \tag{2.1}$$

where

$[N]$	is the group of natural numbers.
$[P]$	is the group of prime numbers
$[M]$	is the group of composite numbers
$\wedge$	represents a Boolean type operator "AND"

The group of composite numbers can be represented as

$$[M]=[E]\wedge[O] \tag{2.2}$$

where

$[E]$	is the group of even composites = $[2(n + 1)]$.
$[O]$	is the group of odd composites = $[Q(2n + Q - 2)]$.

where Q is the group of odd prime numbers, and where $n = 1 \rightarrow \infty$.

Substitution of (2.2) as defined into (2.1) then yields

$$[N]=[P]\wedge[2(n+1)]\wedge[Q(2n+Q-2)] \tag{2.3}$$

So that

$$[P]=[N]\vee[2(n+1)]\vee[Q(2n+Q-2)] \tag{2.4}$$

and where

$\vee$	represents a Boolean type operator "NOT".

To avoid the presence of [Q] on the right hand side of (2.4), it is replaced with the group of all odd numbers, i.e. [2m + 1] thus

$$[P] = [N] \vee [2(n+1)] \vee [(2m+1)\{2n + (2m+1) - 2\}] \tag{2.5}$$

and this reduces to

$$[P] = [N] \vee [2(n+1)] \vee [4m^2 + 4mn + 2n - 1] \tag{2.6}$$

Where now m and n = 1 $\rightarrow \infty$ independently. Appendix A.3 shows that putting n = 0 in (2.6) is not applicable.

Eq(2.6) can now be used to identify primes as m and n are varied. The second term produces all the even composites, leaving just the number 2 as the only even prime. The third term produces all the odd composites, the remaining odd numbers thereby being prime.
There are two minor anomalies that result. The first is that replacing [Q] by [2m + 1] in (2.4) means that the third term in (2.6) will produce a number of duplicate composites. This however, does not affect the immediate result. The second anomaly is that because the distribution of composites with regard to m and n is irregular, the composites, and therefore primes, will not be identified in the correct order. It also means that in any listing of primes so produced, there may be extraneous composites present.
The second anomaly can be avoided by selecting beforehand a number N up to which all the primes are to be identified. The first anomaly is avoided by composite sorting. The identification of all the primes up to some number N is the subject of the next Section.
Note, in the remainder of this paper, only the odd composites/primes will be considered, so that only the third term in (2.6) is relevant. Consequently, that term is now separately identified thus

$$[O] = [4m^2 + 4mn + 2n - 1] \tag{2.7}$$

2.2 Identification of the Primes up to Some Number *N*.

To effect this exercise it is first necessary to equate (2.7) to N and re-arrange as follows, working with individual terms inside the group.

$$n = \frac{N - 4m^2 + 1}{2(2m+1)} \tag{2.8}$$

Eq.(2.8) determines the maximum value of n for all values of m from unity upwards until n falls below unity. Also, only the integer part of n so determined is taken. This ensures that the list of composites produced by (2.7), up to and including N, with these values of m and n, is complete, so also ensuring that the list of all remaining odd numbers, being prime, is also complete. A brief example for N = 209 follows.
The list of m and maximum n, (integer part), determined from (2.8) for N = 209 is shown in the following table.

m	**Maximum *n***
1	34
2	19
3	12
4	8
5	5
6	2
Total	80

Table 2.1 - List of *m* and Maximum *n* for *N* = 209.

Now, for each value of m in Table 2.1, insert n = 1, 2, 3 etc up to and including its maximum as above, into (2.7). This generates a list of composites, which when sorted produces Table 2.2, thus

EXAMPLE	**Composites for *N* = 209**							
Composites = 80	9	49	77	105	125	**147**	171	**189**
	15	51	81	**105**	129	153	**171**	195
	21	55	**81**	**105**	133	**153**	175	**195**
	25	57	85	111	135	155	**175**	**195**
	27	63	87	115	**135**	159	177	201
	33	**63**	91	117	**135**	161	183	203
	35	65	93	**117**	141	165	185	205
	39	69	95	119	143	**165**	187	207
	45	75	99	121	145	**165**	189	**207**
	45	**75**	**99**	123	147	169	**189**	209

Table 2.2 - Composites for *N* = 209.

Thus 80 composites are produced, 21 of which, (shown in red), are duplicates. Odd numbers NOT in this table, together with the number 2, are therefore the primes from 0 to 209. (It should be noted that unity is considered a prime number).

2.3 Calculation of $\pi(N)$.

Determination of $\pi(N)$ via the parameters developed here is

$$\pi(N) = N - E - O + D \tag{2.9}$$

where

N is the number in question.
E is the number of even composites.
O is the number of odd composites produced by (2.7).
D is the number of duplicate composites produced by (2.7).

and where

$$E = \frac{N-1}{2} - 1 \text{ if } N \text{ is odd.}$$

$$E = \frac{N}{2} - 1 \text{ if } N \text{ is even.} \tag{2.10}$$

$$O = \sum(n).$$

D can be determined from the list of composites, as for instance in Table 2.2, but it is not necessary to produce this table for this purpose as D can be calculated as follows.

If different values of m and n respectively produce the same composite, then the following relationship is valid.

$$4m^2 + 4mn + 2n - 1 = 4m'^2 + 4m'n' + 2n' - 1 \tag{2.11}$$

Solving for n'

$$n' = \frac{2\left(m^2 - m'^2\right) + \left(2m+1\right)n}{2m'+1} \tag{2.12}$$

where n' must be an integer ≤ its applicable maximum. From (2.12) the total number of duplicate composites, unique to m', can be determined for any N by inserting appropriate values of m and m', and trial values of n. As an example, consider the above exercise for N = 209.
Put m' = 1 and m = 2, then from (2.12)

$$n' = \frac{5n}{3} + 2 \tag{2.13}$$

So that the first duplicate appears when n = 3, in which case n' = 7. Thereafter duplicates appear as n increases by 3 in which case n' increases by 5. This continues until n' exceeds the value of n applicable to m in Table 2.1 All the duplicates unique to m' = 1 are therefore, from (2.13)

n	n'	Duplicate
3	7	45
6	12	75
9	17	105
12	22	135
15	27	165
18	32	195

Table 2.3 - Duplicates Created Between *m'* = 1 and *m* = 2 for *N* = 209.

There are thus 6 duplicates created between m' = 1 and m = 2. Repeating these calculations for all other combinations of m' and m produces the following table of unique duplicates applicable to m'. Note, it is not necessary to determine the actual value of each duplicate composite, only the number thereof.

m'	m	Number of Duplicate Composites Unique to m'
1	2→6	15
2	3→6	5
3	4→6	1
4	5→6	0
5	6	0
Total		21

Table 2.4 - Duplicates Unique to m' for N = 209.

$\pi(N)$ is then determined for N from (2.9) with $N = 209$, $E = 103$, $O = 80$ and $D = 21$ as

$$\pi(209) = 47, \text{ (46 excluding unity).}$$

The complete set of duplicates for the above example is calculated in Appendix A.2 where applicability is also detailed.

2.4 A Simple Test for Primality or Compositeness.

This test can be effected by determining the values of n from (2.8) for the required N. Values must be taken to a significant number of decimal places. If all the values are non-integer then N is prime. If N is composite, then at least one value of n will be integer. As examples, consider $N_1 = 861$ and $N_2 = 863$. From (2.8) the following table is produced

m	n for 861	n for 863
1	143	143.33
2	84.60	84.80
3	59	59.14
4	44.33	44.44
5	34.64	34.73
6	27.62	27.69
7	22.20	22.27
8	17.82	17.88
9	14.16	14.21
10	11	11.05
11	8.22	8.26
12	5.72	5.76
13	3.44	3.48
14	1.34	1.38

Table 2.5 - Determination of Primality or Compositeness of N_1 = 861 and N_2 = 863.

Thus for $N_1 = 861$ there are three values of m which produce integer values of n from (2.8), (1→143, 3→59, 10→11). $N_1 = 861$ is therefore composite. For $N_2 = 863$ there are no integer values of n produced so $N_2 = 863$ is prime.

2.5 Determination of the Factors of Very Large Composite Numbers.

If some number N is composite, its factors can be determined as follows. First, via the method in Section 2.4 above, determine the values of n that are integer for all applicable values of m. Now, with N composite, the appropriate term inside (2.7) can itself be factored thus

$$N = (2m + A)(2m + B) \tag{2.14}$$

when multiplied out, comparison of (2.14) with (2.7) shows that

$$\frac{A + B}{2} = n \tag{2.15}$$

and

$$AB = 2n - 1 \tag{2.16}$$

Solving for B in (2.15) and inserting into (2.16) yields

$$A^2 - 2nA + 2n - 1 = 0 \tag{2.17}$$

and solving for A then gives

$$A = 2n - 1 \quad or \quad 1 \tag{2.18}$$

the first term in (2.18) leads to $B = 1$. The factors of N are therefore from (2.14)

$$\begin{aligned} F_1 &= 2m + 2n - 1 \\ F_2 &= 2m + 1 \end{aligned} \tag{2.19}$$

As a simple example, the factors of N = 861 are, from the appropriate integer values of m and n of Table 2.5

F_1	F_2
287	3
123	7
41	21

Table 2.6 - Factors of *N* = 861 from Eq.(2.19) and Table 2.5.

The prime factors of N = 861 are therefore 3, 7 and 41. Note there are valid factors other than (2.14), but these produce non-integer values. A further extensive example is shown in Appendix A.1.

3.0 Conclusions.

It is believed that the most important result produced here is not the algorithmic version of the Sieve of Eratosthenes, but the further results that ensue, namely, (i) the simple calculation of $\pi(N)$, which is always exact, (ii) the simple test for primality or compositeness, and (iii) the ability to easily factor very large numbers.

In order to achieve these tasks, for exceptionally large numbers, it is clear that, although trivial, there are a great many calculations to be completed. However, with the power and speed of computers available in the present day, supplemented by the sophisticated programming of same, such calculations can be completed very quickly.

Also, it is clear from a detailed examination of the example results presented here, and which would be magnified with more extensive examples, they follow very precise patterns, which would make it possible to set up secondary algorithms allowing many results to be determined simply by inspection.

APPENDIX A.

Examples of Application.

A.1 Determination of the Factors of Very Large Composite Numbers.

Consider the composite number

$$N = 98{,}041{,}988{,}499 \tag{A.1}$$

Inserting this number into (2.8) and setting m = 1 immediately produces an integer value of n of 16,340,331,416. Inserting these values of m and n into (2.19) produces the following factors

$$\begin{aligned} F_1 &= 32{,}680{,}662{,}833 \\ F_2 &= 3 \end{aligned} \tag{A.2}$$

Now inserting F_1 into (2.8) and varying m from unity to 3 produces another integer value of n of 2,334,333,057. These values of m and n then produce two more factors

$$\begin{aligned} F_3 &= 4{,}668{,}660{,}119 \\ F_2 &= 7 \end{aligned} \tag{A.3}$$

Continuing in this fashion with F_3 et al produces all the factors of N according to the following table.

m	n	F_a	F_b
1	16,340,331,416	32,680,662,833	3
3	2,334,333,057	4,668,660,119	7
6	179,564,076	359,128,163	13
179	500,000	1,000,357	359

Table A.1 - Factors for *N* = 98,041,988,499

The final number to be tested, 1,000,357, produces no integer values of *n* and is therefore prime. The parameter *m* must be increased to 500 before *n* is reduced to less than unity to achieve this final result. The prime factors of *N* are therefore 3, 7, 13, 359 and 1,000,357.
Note that when testing the intermediate factors, F_a above, it is not necessary to return *m* to unity each time. Each new test can be continued starting with the value of *m* from the previous result.
Also, it is very important not to jump values of *m* in the above process, otherwise a composite/factor may be missed.

A.2 Calculation of All the Duplicate Composites for *N* = 209.

Determination of all duplicate composites can be effected using (2.12), and for *N* = 209 are determined below in tabular form. The parameter *n*' must be integer, and ≤ the value in Table 2.1 for each *m*.

***m*'**	***m***	**Equation for *n*' from (2.12)**	***n***	***n*'**	***D***
1	2	$5n/3 + 2$	3	7	45*
			6	12	75*
			9	17	105*
			12	22	135*
			15	27	165*
			18	32	195*
1	3	$(7n + 16)/3$	2	10	63*
			5	17	105
			8	24	147*
			11	31	189*
1	4	$3n+10$	1	13	81*
			2	16	99*
			3	19	117*
			4	22	135
			5	25	153*
			6	28	171*
			7	31	189
			8	34	207*
1	5	$11n/3 + 16$	3	27	165
1	6	$(13n + 70)/3$	2	32	195
2	3	$7n/5 + 2$	5	9	105*
			10	16	175*
2	4	$(9n + 24)/5$	4	12	135*
2	5	$(11n + 42)/5$	3	15	165*
2	6	$(13n + 64)/5$	2	18	195*
3	4	$9n/7 + 2$	7	11	189*
3	5	$(11n + 32)/7$	For these values, *n*' is in excess of the maximum value in Table 2.1		
3	6	$(13n + 54)/7$			
4	5	$11n/9 + 2$			
4	6	$(13n + 40)/9$			
5	6	$13n/11 + 2$			

Table A.2 - Duplicates for *N* = 209 in Addition to Those in Table 2.3.

The duplicate composites to be used in the determination of $\pi(N)$, are those unique to each m' and are starred in the above table. Those not starred are not unique to each m' and are therefore double duplicates and are not included in the total. The total is therefore 21.

A.3 Proof that $n = 0$ is not Applicable in (2.6) and (2.7).

In $[E] = [2(n + 1)]$, if $n = 0$ then $E = 2$ which is not composite.

In $[O] = [4m^2 + 4mn + 2n - 1]$, if $n = 0$ then $O = 4m^2 - 1$ and if $m = 1$, then $O = 3$ which is not composite. For other values of $m > 1$, composites are produced, but they are all double duplicates and therefore in the determination of the composites/primes for any N, and/or $\pi(N)$, they do not contribute.