PRIMALITY TESTING

A NEW METHOD.

Peter G.Bass.

M7 Version 2.0.0
www.relativitydomains.com
June 2012

ABSTRACT

This paper describes a new method of primality testing of the Natural numbers. This method is based upon an attribute of the Natural numbers designated Multiples, and is effected by comparison of the Multiples of the test number with those of its predecessor.

CONTENTS.

1.0 Introduction.

Since the days of Eratosthene's Sieve, the testing of the Natural numbers for primality has become a favourite pastime of number theorists, professional and amateur alike. With the advent of electronic communications, however, this pastime has become of significant importance in the security aspects of the transmission of sensitive information.
Ignoring probabilistic methods, at the moment, the most efficient method of testing for primality, is to consecutively divide the test number by all the primes less than its square root, (the Primes Division method). For relatively small numbers, this is a simple operation, but for very large numbers, containing many thousands or even millions of digits, the task becomes progressively more difficult, and lengthy, for even the most advanced computing facilities. Coupled with this is the necessity of maintaining a prime number database, of up to the square root of any number to be tested.

To provide some alleviation of these difficulties, a new method of primality testing has been devised. This method is based upon the comparison of the sum of the Multiples of the test number with that of its predecessor. This method, if appropriately implemented, provides a virtually instantaneous result by performing all the calculations simultaneously.
The method has its separate advantages and disadvantages which are fully described below.

2.0 Primality Testing By Multiples Comparison.

The concept of Multiples Comparison is very simple. Consider a Natural number *N*. Its Multiples are defined as

$$M(N)=\sum_{p=2}^{\sqrt{N}} INT\left(\frac{N}{p}\right) \qquad (2.1)$$

where *p* ranges over all the primes from 2 to that prime closest to $\sqrt{N}$. The *INT*( ) notation indicates that only the integer part of the division is taken.
Similarly, for the predecessor to *N*

$$M(N-1)=\sum_{p=2}^{\sqrt{N-1}} INT\left(\frac{N-1}{p}\right) \qquad (2.2)$$

If *N* is prime, then it has no integer divisors and therefore (2.1) and (2.2) will produce the same result. The condition for primality of *N* is therefore

$$M(N)-M(N-1)=0 \qquad (2.3)$$

A proof of this method is presented in Appendix A together with four simple examples.

3.0 Implementation.

The method of Multiples Comparison has been implemented in a demonstration EXCEL spreadsheet. The primary display is shown in Fig. 3.1 below.

Ver. 1.0.0 May 2012. © P.G.Bass.

Number Primality Testing.

N. 31,622,777 ADD SUBTRACT

Output Results. N is Prime.

Instructions.

Input the number to be tested into N, it must be greater than zero.

The ADD/SUBTRACT buttons will add/subtract 2 from N to enable a prime number search.

Important Note :UNITY IS ASSUMED PRIME.

Maximum Input Number. 3,599,880,001

Messages.

N.	Multiples Difference Sum.
31,622,777	
5,623.41329	0

Primes	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
Multiples	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1609	1613	1619	1621	1627	1637	1657	1663	1667	1669	1693	1697	1699	1709	1721	1723	1733	1741	1747	1753
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	3623	3631	3637	3643	3659	3671	3673	3677	3691	3697	3701	3709	3719	3727	3733	3739	3761	3767	3769	3779
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 3.1 - Multiples Comparison EXCEL Demonstration Implementation.

Operation is simply to enter the test number in the input cell indicated and press the RETURN key. The result is "immediately" shown in the Output Cell. The ADD/SUBTRACT Buttons allow addition/subtraction to/from the test number to facilitate a

search as required. The cell denoting "Maximum Input Number" is simply the square of the maximum prime number in the primes database. The database is contained in a range of cells below the computation area. The largest prime in the database is 59,999 which thus sets the largest input number permitted to that shown.
The maximum computational capability of EXCEL is to 15 significant digits, and to test a number of this magnitude would require a prime number database of from 2 to 31,622,777.

In the next paper, the subject of which is the generation of $\pi(N)$, the prime number distribution, a method of generating a suitable prime number database of any size, that could update the one in the spreadsheet, will be presented.
While this spreadsheet provides a good demonstration of this method, EXCEL is, as stated above limited to numbers up to 10^{15}, and to use this method efficiently for much larger numbers would require a mainframe implementation.

4.0 Conclusions.

With regard to the Multiples Comparison method, one question that could be raised is that, because each method requires division by all primes up to the square root of the test number, what advantage does this method have over the Primes Division method, if all computations for the latter were also carried out simultaneously. The answer is that in the Primes Division method, each separate division must be checked for a zero remainder which essentially doubles the number of computations that have to be made. In the Multiples Comparison method, effectively only two extra simple computations are necessary to achieve the same result.
While the "simultaneous" computation of all terms in the Multiples Comparison method allows a virtuously instantaneous result, it does require an extensive database of prime numbers plus a considerable amount of coding to implement this feature. However, given the size and computational capabilities of modern computers, especially mainframe, this should not be a difficult method to implement to any required extent, especially given the shortcuts that are available in spreadsheet coding.

APPENDIX A.

Proof of the Multiples Comparison Method Plus Examples.

This Appendix provides proof of the Multiples Comparison method plus four simple examples.

For any Natural number *N*, the Multiples attribute of (2.1) expands to

$$M(N) = INT\left(\frac{N}{2}\right) + INT\left(\frac{N}{3}\right) + INT\left(\frac{N}{5}\right) + \ldots + INT\left(\frac{N}{p_n}\right) \qquad \text{(A.1)}$$

where p_n is the largest prime number closest to $\sqrt{N}$.
For (*N* - 1) it is

$$M(N-1) = INT\left(\frac{N-1}{2}\right) + INT\left(\frac{N-1}{3}\right) + INT\left(\frac{N-1}{5}\right) + \ldots + INT\left(\frac{N-1}{p_n}\right) \qquad \text{(A.2)}$$

Proof of the concept is as follows, (note that $INT\left(\frac{N-1}{p}\right)$ can never be greater than $INT\left(\frac{N}{p}\right)$).

(i) Assume *N* is prime and > 2. *N* is therefore odd and (*N* - 1) even, then

(a) *N*/2 has remainder 1, and (N-1)/2 has remainder 0. therefore

$$INT\left(\frac{N}{2}\right) = \frac{(N-1)}{2} = INT\left(\frac{N-1}{2}\right) \qquad \text{(A.3)}$$

(b) For $2 < p < p_n$, *N*/*p* has remainders in the range 1 to (p_n - 1) and (*N* - 1)/*p* has remainders in the range 0 to (p_n - 2), so that $INT\left(\frac{N}{p}\right) = INT\left(\frac{N-1}{p}\right)$.

This is sufficient to prove that $M(N) = M(N-1)$ when *N* is prime.

(ii) Assume *N* is composite and odd, then

(a) (i)(a) still applies.

(b) For some *p*, *N*/*p* will have remainder 0, while (*N* - 1)/*p* will have remainders in the range 1 to (p_n - 1), so that $INT\left(\frac{N}{p}\right) > INT\left(\frac{N-1}{p}\right)$.

This is sufficient to prove that $M(N) > M(N-1)$ when *N* is odd and composite.

(iii) Assume *N* is composite, even and > 2, then

(a) N/2 has remainder 0 while (N - 1)/2 has remainder 1, so that $INT\left(\frac{N}{p}\right) > INT\left(\frac{N-1}{p}\right)$.

This is sufficient to prove that $M(N) > M(N-1)$ when *N* is even and > 2.

Examples

(i) N = 101.

$\sqrt{N} = 10.05$ so that $p_n = 7$.

$$M(N) = INT\left(\frac{101}{2}\right) + INT\left(\frac{101}{3}\right) + INT\left(\frac{101}{5}\right) + INT\left(\frac{101}{7}\right) \tag{A.4}$$

$$= 50 + 33 + 20 + 14 = 117$$

$$M(N-1) = INT\left(\frac{100}{2}\right) + INT\left(\frac{100}{3}\right) + INT\left(\frac{100}{5}\right) + INT\left(\frac{100}{7}\right) \tag{A.5}$$

$$= 50 + 33 + 20 + 14 = 117$$

Therefore

$$M(N) - M(N-1) = 0 \tag{A.6}$$

and *N* is therefore prime.

(ii) N = 102.

$\sqrt{N} = 10.1$ so that $p_n = 7$.

$$M(N) = INT\left(\frac{102}{2}\right) + INT\left(\frac{102}{3}\right) + INT\left(\frac{102}{5}\right) + INT\left(\frac{102}{7}\right) \tag{A.7}$$

$$= 51 + 34 + 20 + 14 = 119$$

Therefore, from (A.4) and (A.7)

$$M(N) - M(N-1) = 2 \tag{A.8}$$

and *N* is composite.

(iii) *N* = 103.

$\sqrt{N} = 10.15$ so that $p_n = 7$.

$$M(N) = INT\left(\frac{103}{2}\right) + INT\left(\frac{103}{3}\right) + INT\left(\frac{103}{5}\right) + INT\left(\frac{103}{7}\right) \tag{A.9}$$

$$= 51 + 34 + 20 + 14 = 119$$

Therefore, from (A.7) and (A.9)

$$M(N) - M(N-1) = 0 \tag{A.10}$$

and N is prime.

(iv) $N = 111$.

$\sqrt{N} = 10.54$ so that $p_n = 7$.

$$M(N) = INT\left(\frac{111}{2}\right) + INT\left(\frac{111}{3}\right) + INT\left(\frac{111}{5}\right) + INT\left(\frac{111}{7}\right) \tag{A.11}$$

$$= 55 + 37 + 22 + 15 = 129$$

$$M(N-1) = INT\left(\frac{110}{2}\right) + INT\left(\frac{110}{3}\right) + INT\left(\frac{110}{5}\right) + INT\left(\frac{110}{7}\right) \tag{A.12}$$

$$= 55 + 36 + 22 + 15 = 128$$

Therefore

$$M(N) - M(N-1) = 1 \tag{A.13}$$

so that N is composite.