The Mathematics Enthusiast

Volume 9
Number 3 *Number 3*

Article 11

7-2012

Evaluating Mersenne Primes Using a Single Quadrant Expanding Square

Cory P. Daignault

Douglas Sprague

Joe L. Mott

Follow this and additional works at: https://scholarworks.umt.edu/tme

 Part of the Mathematics Commons

Let us know how access to this document benefits you.

Recommended Citation
Daignault, Cory P.; Sprague, Douglas; and Mott, Joe L. (2012) "Evaluating Mersenne Primes Using a Single Quadrant Expanding Square," *The Mathematics Enthusiast*: Vol. 9 : No. 3 , Article 11.
Available at: https://scholarworks.umt.edu/tme/vol9/iss3/11

This Article is brought to you for free and open access by ScholarWorks at University of Montana. It has been accepted for inclusion in The Mathematics Enthusiast by an authorized editor of ScholarWorks at University of Montana. For more information, please contact scholarworks@mso.umt.edu.

Evaluating Mersenne Primes Using a Single Quadrant Expanding Square

Cory P. Daignault[a], Douglas Sprague, Joe L. Mott
Florida State University, Dept of Mathematics

Abstract

By forming a table of sequential odd numbers using a single quadrant expanding square pattern it was observed that multiple Mersenne primes fall into the first column. We prove that the Mersenne primes which fall into the first column will be of the form $p \equiv 3 \bmod 4$, where p is the Mersenne prime exponent. Focusing the search of primes to those which fall into the first column of this square may be a means to increase the speed at which large primes are discovered.

Keywords: Algorithms; Mersenne Primes; Primes

Introduction

A Mersenne prime is a prime of the form $2^p - 1$. For example, the first Mersenne primes are 2, 3, 7, 31, and 127 which corresponds to *p* values of 1, 2, 3, 5, and 7. Currently only 47 Mersenne primes have been discovered.[1] The first attempt to compile the primes was performed in the 17th century by the French scholar Marin Mersenne. The search for these primes intensified with the advent of digital computing. As with all primes, as the numbers become larger, the primes become increasingly more remote, making an exhaustive search labor intensive. The aim of this paper is to explore a potential means to limit the set of the eligible numbers to those most likely to be a Mersenne Prime. To this end, sequential odd numbers are arranged in the expanding square pattern described below.

Single Quadrant Expanding Square Pattern

This is defined as expansion of a square limited to one quadrant (Figure 1).

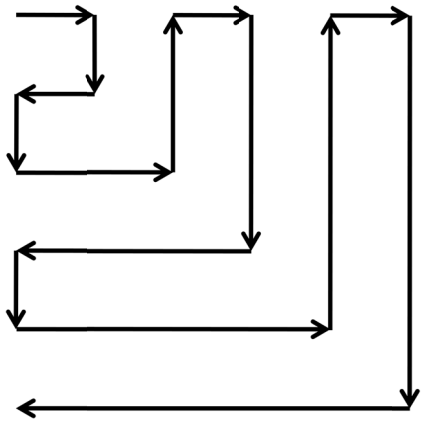

Figure 1 - Single Quadrant Expanding Square

[a] cpdaignault@gmail.com

2012©Authors & Dept of Mathematical Sciences-The University of Montana

With odd numbers placed along the lines of expansion a limitless grid of numbers is formed. This will be referred to as an Odd Number Single Quadrant Expanding Square, ONSQES, and is demonstrated in Figure 2 (Mersenne primes are bold). The numbers in the first column will be referred to as First Column Odd Number Single Quadrant Expanding Square Integers, FCONSQESI.

1	**3**	17	19	49	51	97	99
7	5	15	21	47	53	95	101
9	11	13	23	45	55	93	103
31	29	27	25	43	57	91	105
33	35	37	39	41	59	89	107
71	69	67	65	63	61	87	109
73	75	77	79	81	83	85	111
127	125	123	121	119	117	115	113

Figure 2 – 8 x 8 Odd Number Single Quadrant Expanding Square (ONSQES)

Theorem: *Mersenne primes which occur in the first column of the ONSQES will be of the form* $p \equiv 3 \bmod 4$*, where p is the Mersenne Prime exponent.*

Proof: Given that the numbers of interest in the first column of the ONSQES follow the equation:

$R = 2^{\frac{p-1}{2}}$, where *R* is the row number of the ONSQES and *p* is the Mersenne prime exponent.

By applying the Theorem of Quadratic Residue and using Legendre symbols this equation becomes $\left(\frac{R}{p}\right) = \left(\frac{2^{\frac{p-1}{2}}}{p}\right)$. So when the statement $\frac{2^{\frac{p-1}{2}}}{p} = -1$ is true, the statement $p \equiv 3 \bmod 4$ will also be true. To that end, observe that the expression $\frac{p-1}{2}$ is at all times either even or odd.

If $\frac{p-1}{2}$ is even, then $\frac{2^{\frac{p-1}{2}}}{p} = \left(\frac{2}{p}\right)^{\frac{p-1}{2}} = 1$

If $\frac{p-1}{2}$ is odd, then $\frac{2^{\frac{p-1}{2}}}{p} = -1.$

Therefore, $p \equiv 3 \bmod 4$

Yet for the case $\frac{2^{\frac{p-1}{2}}}{p} = -1$, the Law of Quadratic Reciprocity states:

$$\left(\frac{2}{p}\right)^{\frac{p-1}{2}} = \left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p \equiv \pm 1 \bmod 8 \\ -1 \text{ if } p \equiv \pm 5 \bmod 8 \end{cases}$$

Thus there now exists $p \equiv 3 \bmod 4$ and $p \equiv \pm 5 \bmod 8$.
This creates two possibilities:
Case 1: $p \equiv 3 \bmod 4$ and $p \equiv -5 \bmod 8 \equiv 3 \bmod 8$
$p \equiv 3 \bmod 4 = p \equiv 3,7 \bmod 8$
so $p \equiv 3 \bmod 4$ becomes $p \equiv 3 \bmod 8$
Case 2: $p \equiv 3 \bmod 4$ and $p \equiv 5 \bmod 8 \equiv 5 \bmod 8$
This cannot occur because
$p \equiv 3 \bmod 4 \equiv 3,7 \bmod 8$ and then $p \neq 5 \bmod 8$

Thus to achieve $\frac{2^{\frac{p-1}{2}}}{p} = -1$, p must be of the form $p \equiv 3 \bmod 4$

Remarks

Fundamentally there are two ways to increase the speed of the search for Mersenne primes. One is through increased speed of assessment of the individual candidates, such as with faster processors or with more efficient verification of the individual candidates. The second is by decreasing the number of candidates to be considered. The theorem described above is meant to address the latter.

Figure 2 lists the p values of the Mersenne primes discovered at the time of writing.[1] In this table the primes which conform to $p \equiv 3 \bmod 4$ are placed in bold. Only 19 of the 47 known primes follow this form. While not capable of capturing all of the Mersenne prime numbers, these primes are significant in that they arise from a much smaller set of integers.

2	61	2281	21701	859433	**24036583**
3	89	3217	23209	**1257787**	**25964951**
5	**107**	4253	44497	1398269	30402457
7	**127**	**4423**	**86243**	2976221	32582657
13	521	9689	**110503**	3021377	**37156667**
17	**607**	9941	132049	6972593	42643801
19	**1279**	11213	**216091**	13466917	43112609
31	**2203**	19937	**756839**	**20996011**	

Figure 2 - List of the p values for all known Mersenne Prime

A summary article by Schroeder discusses the distribution of Mersenne primes.[2] When the sequence of Mersenne primes are graphed as $Log_2 p$ the slope is 0.59. The same graphic can be applied to the set of FCONSQESI Mersenne primes which yields a slope of 1.28 (Figure 3). This increased rate of growth is compatible with the smaller number Mersenne primes that fall in the FCONSQESI set.

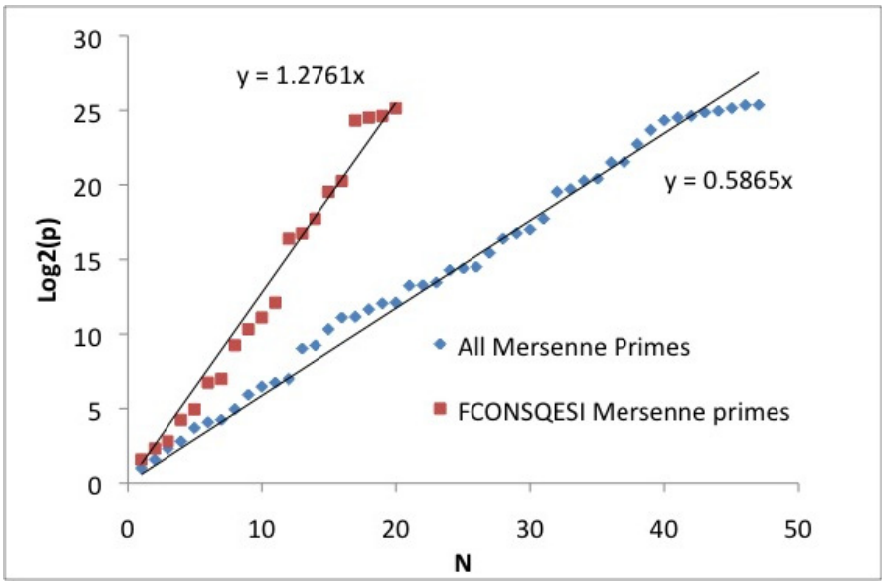

Figure3 – The set of FCONSQESI Mersenne primes compared to that of all Mersenne primes

To consider the discordance of the sizes of the set, consider the number of odd integers less than the FCONSQESI for a given row. From this FCONSQESI set, consider the set conforms to $R = 2^{\frac{p-1}{2}}$ with integer solutions for p. Figure 4 compares the sizes of these sets. In general $\{2^{\frac{p-1}{2}}$ FCONSQESI$\}$ is many orders of magnitude smaller than {Odd}. A PYTHON code for the FCONSQEI is described in the Appendix. Thus limiting the search for Mersenne primes to those which fall into the first column of the ONSQES may be a means to increase the rate at which very large prime numbers are found.

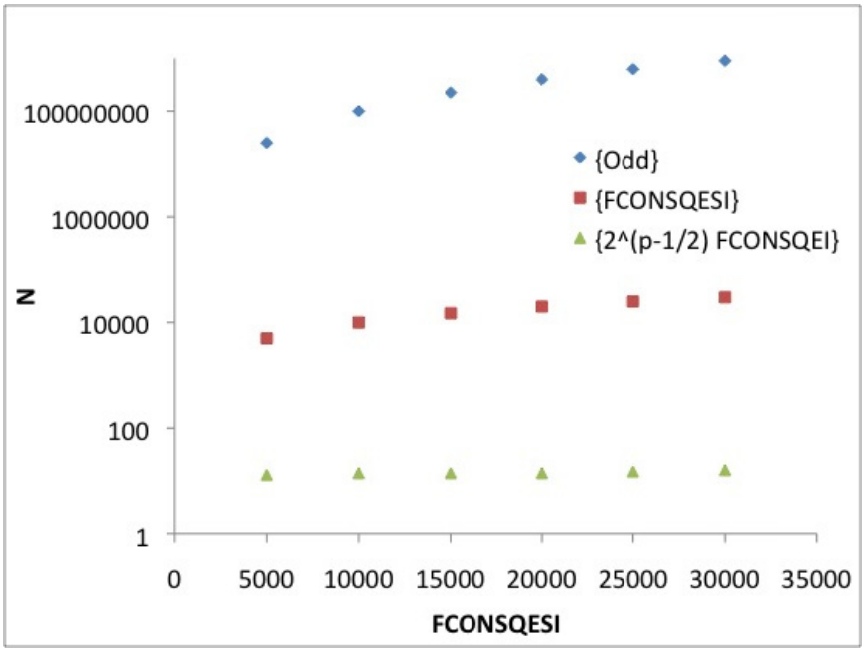

Figure4 – The size of the sets less than the FCONSQESI for a given row.

In conclusion, arranging integers as described by the ONSQES provides a novel method to analyze the distribution of Mersenne primes. Further more the finding that the Mersenne primes which fall in the first column take the form of $p \equiv 3 \bmod 4$ is just one application of this technique to the search for Mersenne primes. While the overall utility of the approach remains to be determined, the future seems promising.

References

1. http://en.wikipedia.org/wiki/Mersenne_prime. Accessed May 22,2012.

2. Manfred R. Schroeder. "Where Is the Next Mersenne Prime Hiding?" The Mathematical Intelligencer. VOL. 5, NO. 3. p31-33.

Appendix

PYTHON code for FCONSQESI

```
#!/usr/bin/python
"""
This PYTHON program provides the numbers necessary to form the
sets describe in the above paper.  A primality test can be
applied to them to verify which are primes. As written below,
this program describes rows 4 to 512.

A sample printout is:
row, Mersenne_prime, p-value
4 31 5.0
6 71 6.16992500144
8 127 7.0
10 199 7.64385618977
...

"""
import math
FCONSQESI_2_rows_up = 7
    #since we will start on row 4, this is for row 2
print "row, Mersenne_prime, p_value"
for row in range(4,513,2):#calc even rows 4 to 512
    FCONSQESI=FCONSQESI_2_rows_up +2+((row // 2)*16)-10
     #use integral division above since row always even
    p_value = 1 + 2 * math.log(row) / math.log(2)
    print row, FCONSQESI, p_value
    FCONSQESI_two_rows_above = FCONSQESI
exit()
```