Five Steps Primality Test

Manuel Meireles
profmeireles@uol.com.br
Department of Exact Sciences
FACCAMP
Brazil

Abstract: *This article is divided into four parts. In the first one, the natural numbers are* N^* *hexagonally stratified. For each stratification, the names* $\alpha,\pi,\varphi,\chi,\beta,\psi$ *are given. This is done in a penta-hexagonal stratification which allows a primality test in just five steps of simple division, independent of the size of the number being tested. The basic structure of the algorithm is supplied here. This way is opened for people interested in Mathematical Sciences and Technology, the opportunity to develop more powerful and fast algorithms to test the primality of the odd numbers. Then it becomes easier, not only to identify a potential prime number but, also, to certify if a number* n *is or is not a prime number. The ability to discover bigger prime numbers depends only on ability and computational potency.*

1. Introduction

When will we have a prime number of one billion digits? The largest known prime has almost always been a Mersenne prime. Why Mersennes? Because the way the largest numbers N are proven prime is based on the factorizations of either N+1 or N-1, and for Mersennes the factorization of N+1 is as trivial as possible (a power of two).

When will we have a one billion digit prime? Let's look more closely at the recent data: using a regression line we might guess when it will be discovered[1]: i) a 10,000,000 digit prime, well, by now!; ii) a 100,000,000 digit prime by early 2015, and ; iii) a 1,000,000,000 digit prime by 2024.

On September 4, 2006, in the same room just a few feet away from their last find, Dr. Curtis Cooper and Dr. Steven Boone's CMSU team broke their own world record, discovering the 44th known Mersenne prime. The new prime at 9,808,358 digits is 650,000 digits larger than their previous record prime found last December. However, the new prime falls short of the 10 million digits required for GIMPS to claim the Electronic Frontier Foundation $100,000 award.

Now it is possible to obtain prime number with more than 10 million digits applying the properties of the hexa-pentagonal Stratification of Numbers that is presented in this paper.

The results presented in this paper, including the algorithm, are original and new.

2. Numbers Hexagonal Stratification

The notion of prime number is reserved only to natural whole numbers [2], and the present work will consider only the set of non-negative whole numbers: $N = N^* \cup \{0\} = \{0,\ 1,\ 2,\ 3,...\}$. The set of natural numbers is considered in the hexagonal spiral, with radiuses, leaving from the center O, as shown in Figure 1.

The hexagonal stratification of whole numbers of which $N\varepsilon \subset N$ subset has the following features:

a) the $N\alpha$ numbers of the α radius are odd, and they are generated by the $N\alpha = 6a+1$ function, where $a \in N, a \geq 0$; along this radius many prime numbers are found. To see [4] that related computations to find prime triples of the form 6m+1, 12m-1, 12m+1.

b) the $N\pi$ numbers of the π radius are even and they are generated by the $N\pi = 6a+2$ function, where $a \in N, a \geq 0$;

c) the $N\varphi$ numbers of the radius φ are multiples odd of 3 and they are generated by the $N\varphi = 6a + 3$ function, where $a \in N, a \geq 0$;
d) the $N\chi$ numbers of the χ radius are even and they are generated by the $N\chi = 6a + 4$ function, where $a \in N, a \geq 0$;
e) the $N\beta$ numbers of the β radius are odd and they are generated by the $N\beta = 6a + 5$ function, where $a \in N, a \geq 0$; along this radius many prime numbers are found; and
f) the $N\psi$ numbers of the ψ radius are even and they are generated by the $N\psi = 6a + 6$ function, where $a \in N, a \geq 0$.

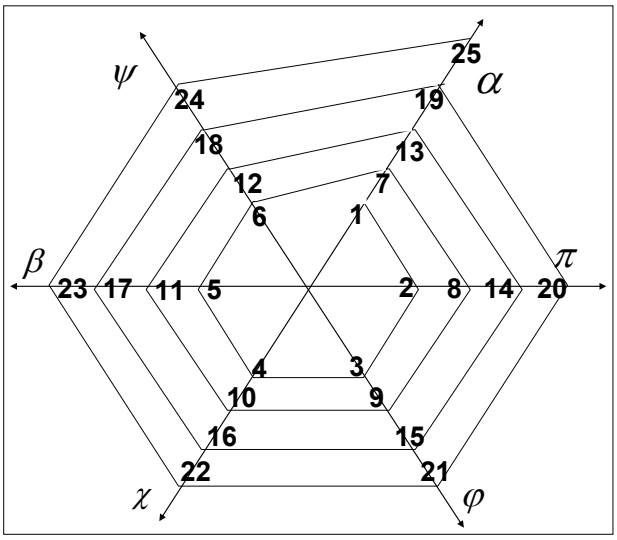

Figure 1 Start numbers hexagonal stratification N^*. Source: Author

Two radiuses are relevant to the present study: the α radius and the β radius, thus on their length are distributed prime numbers. To the primes along the α radius we give the name "prime α" $(P\alpha)$ and to the primes along the β radius we give the name "prime β" $(P\beta)$.

α	π	φ	χ	β	ψ
1	2	3	4	**5**	6
7	8	9	10	**11**	12
13	14	15	16	**17**	18
19	20	21	22	**23**	24
	26	27	28	**29**	30
31	32	33	34		36
37	38	39	40	**41**	42
43	44	45	46	**47**	48
49	50	51	52	**53**	54
	56	57	58	**59**	60
61	62	63	64		66
67	68	69	70	**71**	72

Table 1: Hexagonal stratification of the first 108. N^* numbers. Source: Author

Not even all $N\alpha, N\beta$ numbers are primes, it could be observed that in such radiuses all prime numbers (except the numbers 2 and 3) are concentrated. However it must be observed that the "density" of the prime numbers on the α, β radiuses is three times greater than the normal density, regarding only N, on the dimension which the prime numbers are gathered into two of the six stratifications.

Table 1 shows a hexagonal stratification of the first 72 N^* numbers. The α, β columns are the ones that have the prime numbers $N\alpha$ and $N\beta$ respectively. In these columns, the multiple numbers of 5 were withheld and the non-prime numbers were underlined.

The hexagonal stratification of the N^* numbers doesn't assure the α, β radiuses just with prime $P\alpha, P\beta$ numbers. With the $N\alpha = 6a + 1$ and $N\beta = 6a + 5$ functions it is possible to know if an odd number is, potentially, prime: for this, you have to verify that the division by 6 leaves a remainder 1 or 5.

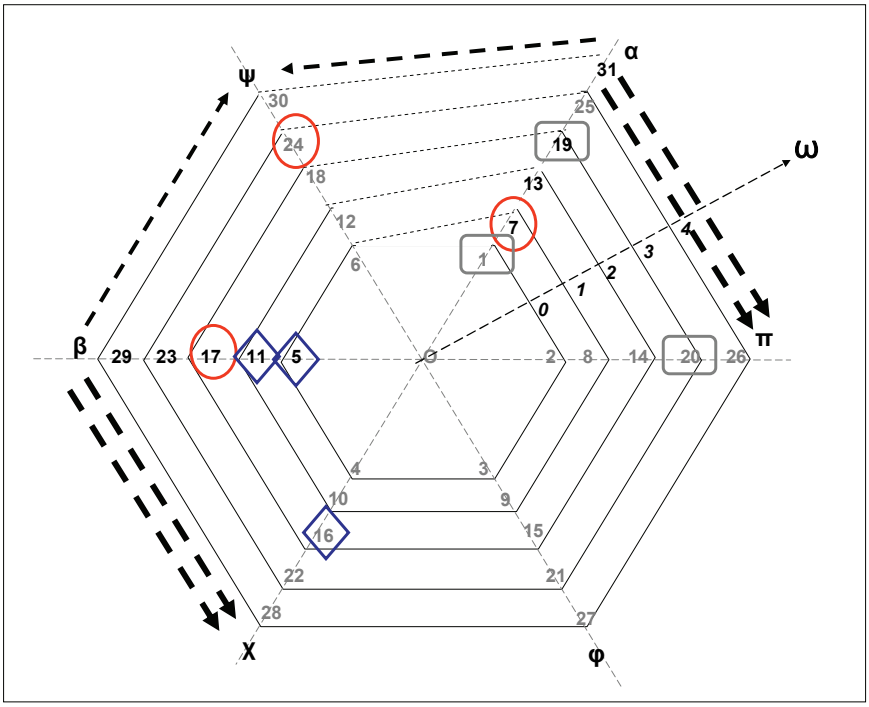

Figure 2: All and any even number is the result of the sum of two odd numbers of specific radiuses
Source: Author

An interesting property of hexagonal stratification of the natural numbers N^* is the confirmation that it is possible to explore the existence of prime numbers of any value, since the N^* numbers have been located on the right radius property. To locate such number on the respective radius, you have to divide by 6 and verify the remainder. The remainder 1 corresponds to the α radius; the remainder 2 to the π radius and so on. The ω layers of the stratification are numbers from 0, 1, 2...n..., as shown in Figure 2; 0 has been the inside stratification layer. Generally speaking, all and any N^* number can be stratified by the $N\varepsilon = 6\omega + r$ function, where $\omega, r \in N, \omega \geq 0; 1 \leq r \leq 6$.

It is easily noticed and demonstrated that all and any even number is the result of the sum of two odd numbers on specific radiuses, as shown in Figure 2:

a) the even numbers of the π radius are the sum of two odd numbers of the α radius: $N\pi = N\alpha + N\alpha'$;

b) the even numbers of the χ radius are the sum of two odd numbers on the β radius: $N\chi = N\beta + N\beta'$;

c) the even numbers of the ψ radius are the sum of two odd numbers: one from the α radius and the other from the β radius: $N\psi = N\alpha + N\beta$

There are the following theorems derived of the hexagonal stratification [3]:

Theorem 1: In N all and any $N\pi$ even numbers in the form of $(6a+2)$ is the result of two odd numbers, one $N\alpha$ on the form $(6b+1)$ and other $N\alpha'$ on the form $(6c+1)$ liable to $a = b + c$.

Theorem 2: In N all and any $N\chi$ even number in the form $(6a+4)$ is the result of the sum of two odd numbers, one $N\beta$ in the form $(6b+5)$ and other $N\beta'$ in the form $(6c+5)$ liable to $a - 1 = b + c$.

Theorem 3: In N all and any $N\psi$ even number in the form $(6a+6)$ is the result of the sum of two odd numbers, one $N\alpha$ in the form $(6b+1)$ and another $N\beta$ in the form $(6c+5)$ liable to $a = b + c$.

3. Hexa-pentagonal Stratification

The first hexagonal stratification obtained two sets of numbers; sets that contain all the prime numbers:

Set $N\alpha = \{1,\ 7,\ 13,\ 19,\ 25,\ ...\}$ and

Set $N\beta = \{5,\ 11,\ 17,\ 23,\ 29,\ ...\}$.

Now each set is stratified as a pentagon, as shown in Figure 3.

In Figure 3 the numbers of the sets $N\alpha, N\beta$, written inside of circles, are arranged sequentially in the rays. Each ray takes the name α, β according to the stratified set, and the number refers to the final digit of the numbers. For example, in the ray $\alpha 3$ there are numbers that end in 3; in the ray $\beta 7$ there are numbers that end in 7.

Once stratified, the numbers were numbered sequentially. The numeration sequence(s) is placed inside of hexagons. For example, the number $N\alpha = 43$, belongs to the set α, it is in the ray $\alpha 3$ and it is the element 7 of the set: $s_{43} = 7$.

s corresponds to the position of the number: $s = \text{int}\left(\frac{n}{6}\right)$: $s = \text{int}\left(\frac{43}{6}\right) = 7$ (1)

With the hexa-pentagonal stratification it is possible to deduce that:

1) any number of the type $6a+1$ (prime or no prime number) can be written in the forms:

$$1+30a$$
$$7+30a$$
$$13+30a \quad (2)$$
$$19+30a$$
$$25+30a$$

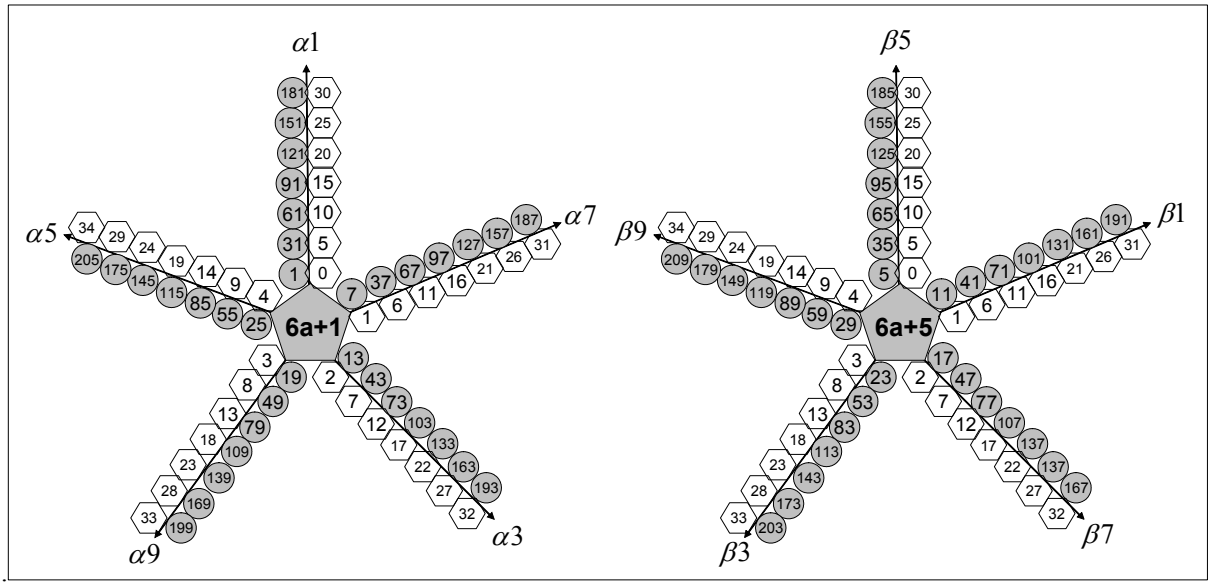

Figure 3: Pentagonal stratification of the sets $N\alpha, N\beta$ In the left sketch , the numbers (in the circles) were disposed successively on the rays. Same procedure was made in the right sketch for the numbers. Source: Author

2) any number of the type $6a+5$ (prime or no prime number) can be written in the forms:

$$\begin{aligned} &5+30a \\ &11+30a \\ &17+30a \\ &23+30a \\ &29+30a \end{aligned} \qquad (3)$$

This way it can be derived that, if the number is a compound number, then the number is the result of the product of two other numbers. To verify if a number is a compound number or not, it is enough to verify if the value c it is a natural whole number:

$$(q+30a)=(r+30b)(s+30c) \qquad (4)$$

Then:

$$c=\frac{n-rs-30s*b}{900*b+30r} \qquad (5)$$

If the value c is a natural whole number, then $n=(q+30a)$ is a compound number that divides for $(s+30c)$. The equation (5) is the basic equation of the algorithm presented in this paper.

3. Properties of the test for primality and algorithms

In 1975, Miler used a small property based on the Fermat Little Theorem to get the polynomial algorithm settling in time to test the primality considering the Generally Riemann's Hypothesis (HRG)[4].

In less than one year, its test was modified by Rabin to produce the unconditional but aleatory algorithm on polynomial time. Miller Rabin's test is an algorithm to test the primality on polynomial time but not deterministic, it means, to determine if a great number P has a probability p of being a prime number. In August 2002, Manindra Agrawal, Neeraj Kayal and Nitin Saxena published their article on the web, with the title *Prime is in P.* [5].

Here a test is proposed that will make it possible to verify the primality of a number more efficient than some nowadays methods in use ([6][7][8][9]).

AKS (Agrawal, Kayal and Saxena) [10] is the first deterministic algorithm to execute this trial in polynomial time. AKS deterministic algorithm shows that the primality is polynomial, it solves the theoric problem that for many years was believed unsolved.

No efficient algorithm is known for determining if a given whole odd is prime or not [6]. However, several probabilistic algorithms have been published, being able to determine with a margin of error so small how it would be if a whole odd is prime [11].

The algorithm presented above (Table 2) is based on the properties of the hexa-pentagonal stratification. The amount of tests k to accomplish, for a number n, in the form (6s+1) or (6s+5) corresponds the: $k = \lfloor \sqrt{s} \rfloor$. The program is written in BASIC language and it can be easily transformed in any programming language, in any platform.

Program

```
Five Steps Primality Test
rem Primality30-v02 program
rem 03-05-2008 This program tests
the primality odd numbers
rem in the interval among the values
QM and M
rem The program was developed for
Manuel Meireles
rem with base in the hexagonal
stratitication of the numbers
rem '    profmeireles@uol.com.br
rem beginning of the program
[begin]
print "enter with odd number to test
"
input "  ";  tab(46);QM
U= QM MOD 2      ' it tests if
number is an even number
if U=0 then [evennumber]
input "to test to the number  ";
tab(46);M
print "Multiple numbers of 3 and of
5 are excluded"
print TIME$()
hora00$= TIME$()
Cont=0
QM=QM-2
[process]
QM=QM+2
if QM>M then goto [final]
U= QM MOD 5      'it tests if the
number divides for 5
if U=0 then goto [process]
U= QM MOD 3      'it tests if the
number divides for 3
if U=0 then goto [process]
'[stage01] ' to define k
n=QM
K=int(SQR(n/30))
rem Define type
T=(n-1)/6
If T=int(T) then goto [alpha]
T=(n-5)/6
If T=int(T) then goto [beta]
goto [process]
[alpha]
rem define ending
E=(n-1)/10
if E=int(E) then [finalA1]
E=(n-3)/10
if E=int(E) then [finalA3]
E=(n-7)/10
if E=int(E) then [finalA7]
goto [finalA9]
[finalA1]
R=1
S=1
RS=1
gosub [totA]
R=13
S=7
RS=91
gosub [totest]
R=11
S=11
RS=121
gosub [totest]
R=19
S=19
RS=361
gosub [totest]
R=23
S=17
RS=391
gosub [totest]
R=29
S=29
RS=841
gosub [totest]
Cont=Cont+1
print  tab(5);Cont; tab(10);n
goto [process]

[finalA3]
R=13
S=1

RS=13
gosub [totest]
R=19
S=7
RS=133
gosub [totest]
R=23
S=11
RS=253
gosub [totest]
R=29
S=17
RS=493
gosub [totest]
Cont=Cont+1
print  tab(5);Cont; tab(10);n
goto [process]
[finalA7]
R=7
S=1
RS=7
gosub [totest]
R=17
S=11
RS=187
gosub [totest]
R=19
S=13
RS=247
gosub [totest]
R=29
S=23
RS=667
gosub [totest]
Cont=Cont+1
print  tab(5);Cont; tab(10);n
goto [process]

[finalA9]
R=19
S=1
RS=19
gosub [totest]
R=7
S=7
```

```
RS=49
gosub [totest]
R=13
S=13
RS=169
gosub [totest]
R=29
S=11
RS=319
gosub [totest]
R=17
S=17
RS=289
gosub [totest]
R=23
S=23
RS=529
gosub [totest]
Cont=Cont+1
print  tab(5);Cont; tab(10);n
goto [process]

[beta]
rem define ending
E=(n-1)/10
if E=int(E) then [finalB1]
E=(n-3)/10
if E=int(E) then [finalB3]
E=(n-7)/10
if E=int(E) then [finalB7]
goto [finalB9]
[finalB1]
R=11
S=1
RS=11
gosub [totest]
R=23
S=7
RS=161
gosub [totest]
R=17
S=13
RS=221
gosub [totest]
R=29
S=19
RS=551
gosub [totest]
Cont=Cont+1
print  tab(5);Cont; tab(10);n
goto [process]
[finalB3]
R=23
S=1
RS=23
gosub [totest]
R=29
S=7
RS=203
gosub [totest]
R=13
S=11
RS=143
gosub [totest]
R=19
S=17
RS=323
gosub [totest]
Cont=Cont+1
print  tab(5);Cont; tab(10);n
goto [process]
[finalB7]
R=17
S=1
RS=17
gosub [totest]
R=11
S=7
RS=77
gosub [totest]
R=29
S=13
RS=377
gosub [totest]
R=23
S=19
RS=437
gosub [totest]
Cont=Cont+1
print  tab(5);Cont; tab(10);n
goto [process]
[finalB9]
R=29
S=1
RS=29
gosub [totest]
R=17
S=7
RS=119
gosub [totest]
R=23
S=13
RS=299
gosub [totest]
R=19
S=11
RS=209
gosub [totest]
Cont=Cont+1
print  tab(5);Cont; tab(10);n
goto [process]

[totest]
A=n-RS
B=30*S
C=30*R
for x=0 to K
m=(A-B*x)/(900*x+C)
if m=int(m) then goto [noprime]
next x
RETURN

[totA]
A=n-RS
B=30*S
C=30*R
for x=1 to K
m=(A-B*x)/(900*x+C)
if m=int(m) then goto [noprime]
next x
RETURN

[noprime]
F2=(30*m+S)
F3=(30*x+R)
print tab(10); n; tab(25);F2; " x ";
tab(30);F3
goto [process]

[final]
print "beginning of the program =
"; tab(35);hora00$
print "end of the program=  ";
Tab(35); TIME$()
print " "
goto [begin]
rem end of the program
```

Table 2: Five Steps Primality Test. Source: Author

The program executes 5 steps or stages:

Stage 1: to determine if the number n is of the type (6a+1) or (6a+5);

Stage 2: being of the type (6a+1), to determine if it is of the type (30s+1) or (30s+7), or (30s+13) or (30s+19; being of the type (6a+5), to determine if it is of the type (30s+11) or (30s+17) or (30s+23) or 30s+29);

Stage 3: to determine $k = \lfloor \sqrt{s} \rfloor$;

Stage 4: to test if exists c (whole number) by algorithm running x of 0 to k;

Stage 5: to print n in the case of prime number, or $n = (r + 30b)(s + 30c)$ in the case of composed number.

Output example:

```
enter with odd number to test
                                        987654321
to test to the number                   987654341
Multiple numbers of 3 and of 5 are excluded
17:04:01
  1   987654323
      987654329     890581 x 1109
      987654331     9588877 x 103
  2   987654337
      987654341     35257 x 28013
beginning of the program =      17:04:01
end of the program=             17:04:02
```

4. About Mersenne prime numbers

A prime number which can be written in the form 2^n-1 is called a Mersenne prime. The Mersenne number M_n is prime for many values of n, for instance n=2, 3, 5, 7, 13. It is necessary for n to be prime, but not every prime number n leads to a Mersenne prime 2^n-1; for instance n=11 does not give a Mersenne prime. The first few are:

$$2^2 - 1 = 3$$

$$2^3 - 1 = 7$$

$$2^5 - 1 = 31 \qquad (6)$$

$$2^7 - 1 = 127$$

$$2^{13} - 1 = 8191$$

Note that if 2^n-1 is prime, then $2^{p-1}(2^p-1)$ is a perfect number.

Theorem 4: The Mersenne prime numbers are numbers of the type $N\alpha$ and they can be written in the form $6a+1$.

Demonstration: Let $Q = 2^n - 1$. If Q is a prime number, then $Q = 6a+1$ or $Q = 6a+5$ (to see theorem 1).

Then

$$6a + 1 = 2^n - 1 \text{ or } 6a + 4 = 2^n - 1 \qquad (7)$$

$$6a = 2^n - 2 \text{ or } 6a = 2^n - 5 \qquad (8)$$

It is possible to observe that the first Mersenne primes are:

$$
\begin{aligned}
&2^2-1=3\\
&6*1+1=2^3-1=7\\
&6*5+1=2^5-1=31\\
&6*1+1=2^7-1=127\\
&6*85+1=2^9-1=511 \quad (*)\\
&6*341+1=2^{11}-1=2047 \quad (*)\\
&6*1365+1=2^{13}-1=8191\\
&6*5461+1=2^{15}-1=32767 \quad (*)
\end{aligned}
\tag{9}
$$

The numbers marked with (*) are not Mersenne prime numbers. The next possible Mersenne prime number will be in the number with $a_n = 4(a)+1$. For example, next Mersenne should be tested in

$$
\begin{aligned}
&6*[4.1365+1)]+1=2^{15}-1\\
&6.5461+1=2^{15}-1\\
&32767=2^{15}-1
\end{aligned}
\tag{10}
$$

It was already said above that Dr. Curtis Cooper and Dr. Steven Boone's CMSU team broke their own world record, discovering the 44th known Mersenne prime, $2^{32582657}-1$. Then exists a number a, such that

$$6a+1=2^{32582657}-1. \tag{11}$$

Then

$$
\begin{aligned}
&6a = 2^{32582657} - 2\\
&6a = 2^{32582656}\\
&a = \frac{2^{32582656}}{6}
\end{aligned}
\tag{12}
$$

This way, the next number to research is a number with $a_n = 4(a)+1$:

$$a_n = 4*(\frac{2^{32582656}}{6})+1 \tag{13}$$

That is: next Mersenne to be researched is

$$6.a_n+1=6*[4*(\frac{2^{32582656}}{6})+1]+1 \tag{14}$$

It is so forth.

It can be useful to know the following:

Let

$$
\begin{aligned}
&6a+1=2^n-1\\
&6a_i+1=2^{n+s}-1
\end{aligned}
\tag{15}
$$

Then

$$a_i=(n+s)\left[4^{\frac{s}{2}}a+\frac{4^{\frac{s}{2}}-1}{3}\right] \tag{16}$$

Acknowledgments

The author wishes to thank M. Cantareira and R. Borgatti of University Paulista; J. Rezende, Paulo dos Santos and M. Biazzi of University of Sorocaba by their helpful comments and suggestions. The author also thanks to FACCAMP, especially to professor Nelson Gentil for their support and the computing time necessary to carry out this work.

References

[1] CALDWELL, C. at http://primes.utm.edu/notes/by_year.html.

[2] SHOKRANIAN, S. Números notáveis. Brasília: UnB, 2002.

[3] MEIRELES, M. Hexagonal Stratification of Numbers and Goldbach Conjecture. at http://www.profmeireles.com.br/site/indice/grupo/teoria.asp

[4] MILLER, G.L. Riemann's hypothesis and tests for primality. J. Comput. Sys. Sci., 13:300-317, 1976.

[5] COUTINHO, S.C. Primalidade em tempo polinomial: uma introdução ao algoritmo AKS. Rio de Janeiro; UFRJ/Sociedade Brasileira de Matemática, 2004.

[6] SILVA FILHO, J.G. Informação, codificação e segurança de dados. Brasília: ENE-UnB, 2007.

[7] RIESEL, H. Prime Numbers and Computer Methods for Factorization, 2.nd Edition, Birkhäuser, (1994). MR 95h:11142.

[8] SOLOVRAY, R; STRASSEN, V. A fast Monte Carlo test for primality. SIAM J. Comput. 6, 84-5, 1977.

[9] STEIN, A.; STEIN, H.C. WILLIAMS. Explicit primality criteria for (p -1) pn – 1. Mathematics of Computation. V. 69, N. 232, p. 1721-1734, S 0025-5718(00)01212-6, Article electronically published on February 23, 2000

[10] JACOBSON, M. An Exposition of the AKS Polynomial Time Primality Test: http://www.cpsc.ucalgary.ca/~jacobs/jacobs/PDF/dmath2002.pdf

[11] CONRADO, L.N.; MORETE,L.F.; BIAZZI,M. Os grandes desafios da aritmética: primos em p. Revista de Estudos Universitários, v.31, n.1, jun. 2005, p.139-164.