AN EFFICIENT PROBABLE PRIME TEST FOR NUMBERS OF THE FORM $\frac{2^n+1}{3}$

By Renaud LIFCHITZ[1] & *Henri LIFCHITZ*[2]

July 2000
second release (last update : May 18, 2002)

ABSTRACT :
The developpement of a new probabilistic test for numbers of the form $\frac{2^p+1}{3}$, which have many common properties with Mersenne numbers. This test gave us probable prime numbers with an exponent $100000 < p < 400000$ and confirms the "new Mersenne conjecture" with new exponents.

1 Introduction :

The numbers N of the form $\frac{2^n+1}{3}$ have an important role in "The new Mersenne conjecture" (Cf. [1]). Effectively, Bateman, Selfridge and Wagstaff have conjectured that if two of the following conditions hold, then so does the third :
1°) $p = 2^k \pm 1$ or $p = 4^k \pm 3$
2°) $2^p - 1$ is prime
3°) $\frac{2^p+1}{3}$ is prime
The first condition can be easily verified, the second quite easily using the well known Lucas-Lehmer test for Mersenne numbers but the last condition is much more difficult to verify because there are no known deterministic test for this sort of numbers. Moreover, the Fermat probable prime test is very slow compared to the Lucas-Lehmer test since these numbers are not a power of 2 plus or minus 1 (so the reduction is very hard to speed up !). The idea is to find such a test to quickly check if these numbers are probable primes.

2 The test :

There is no need to test $N_n = \frac{2^n+1}{3}$ for an even n (3 doesn't divide $2^n + 1$) and for a composite n (if $n = a.b$ for any $a \geq b > 1$, $2^a + 1$ and $2^b + 1$ divide N_n). So, n must be a prime number p.

[1]Student at PARIS VI University (Jussieu) : **RenaudL@orange.fr**
See http ://ourworld.compuserve.com/homepages/hlifchitz/Renaud.html
[2]Engineer at AP-HP, PARIS : **HLifchitz@compuserve.com**
See http ://ourworld.compuserve.com/homepages/hlifchitz/

Let's take a $N_p = \frac{2^p+1}{3}$ that has no small factors. If N_p is prime, the Fermat little theorem tells us that $b^{N_p-1} \equiv 1 \pmod{N_p}$ for a base b such that $gcd(b, N_p) = 1$. So $b^{\frac{2^p-2}{3}} \equiv 1 \pmod{N_p} \Longrightarrow b^{2^p-2} \equiv 1 \pmod{N_p}$ which can be written $b^{2^p-2} - 1 = Q.\frac{2^p+1}{3}$. Since $2^p - 2$ is even, $b^2 - 1$ divides $b^{2^p-2} - 1$ but $gcd(b^2 - 1, N_p) = 1$ so $b^2 - 1$ divides Q. Let $Q' = \frac{Q}{b^2-1}$, then we have $b^{2^p-2} - 1 = Q'.(b^2 - 1).\frac{2^p+1}{3}$. The trick is to throw out the denominator 3 from the right part. This can be done if $b^2 - 1 \equiv 0 \pmod 3$ and if N_p is not trivially pseudoprime to the base b. Thus, we have $b^{2^p-2} \equiv 1 \pmod{2^p + 1} \Longrightarrow b^{2^p} \equiv b^2 \pmod{2^p + 1} \Longrightarrow (b^2)^{2^{p-1}} \equiv b^2 \pmod{2^p + 1}$. The smallest base b with the required conditions is 5 (with $b = 2$ and $b = 4$, N_p is always pseudoprime like the Mersenne and Fermat numbers). Finally, the test is the following :

$$\boxed{\frac{2^p+1}{3} \text{ is prime} \Longrightarrow 25^{2^{p-1}} \equiv 25 \pmod{2^p + 1}}$$

This test is fast since it only requires $p - 1$ successive squarings with a DWT reduction modulo $2^p + 1$. It is a little bit faster than the Lucas-Lehmer test because it doesn't need any subtraction. The converse may be probably true since no counterexamples were found for the moment, but no demonstration is known.

Moreover, if a number passes this test, it implies that $25^{2^{p-1}} \equiv 25 \pmod{\frac{2^p+1}{3}}$ because $\frac{2^p+1}{3}$ divides $2^p + 1$, so $5^{2^p} \equiv 25 \pmod{\frac{2^p+1}{3}} \Longrightarrow 5^{2^p+1} \equiv 125 \pmod{\frac{2^p+1}{3}} \Longrightarrow (5^3)^{\frac{2^p+1}{3}} \equiv 125 \pmod{\frac{2^p+1}{3}} \Longrightarrow 125^{\frac{2^p+1}{3}} \equiv 125 \pmod{\frac{2^p+1}{3}}$, and because $gcd(N_p, 5) = 1$, $125^{\frac{2^p+1}{3}-1} \equiv 1 \pmod{\frac{2^p+1}{3}}$, so N_p is a PRobable Prime in base 125.

Consequently, we have the following scheme :

$$\boxed{N_p \text{ is a 5-PRP} \Longrightarrow 25^{2^{p-1}} \equiv 25 \pmod{2^p + 1} \Longrightarrow N_p \text{ is a 125-PRP}}$$

Interestingly, if we can note S the "safety" of a test, it implies for a N_p test that :

$$\boxed{S(\text{125-PRP}) \leq S(\text{fast test}) \leq S(\text{5-PRP})}$$

Remark : It exists a generalization of the test for numbers of the form : $\frac{16^p+1}{17}$, $\frac{256^p+1}{257}$ and $\frac{65536^p+1}{65537}$. (Cf. [3])

3 Comparisons between N_p and M_p :

	$M_p = 2^p - 1$	$N_p = \frac{2^p+1}{3}$
number mod 8	$M_p \equiv 7$ [8]	$N_p \equiv 3$ [8]
prime factors	$q = 2.k.p + 1$ with $q \equiv \pm 1 \pmod 8$	$q = 2.k.p + 1$ with $q \equiv 1$ or $3 \pmod 8$
p Sophie Germain ($2p + 1$ prime)	If $p \equiv 3 \pmod 4$ then $(2p + 1) \mid M_p$	If $p \equiv 1 \pmod 4$ then $(2p + 1) \mid N_p$
Pseudoprime to base 2	$\surd$	$\surd$
Factorization of $N - 1$	$M_p - 1 = 2.(\mathbf{2^{p-1} - 1})$	$N_p - 1 = \frac{2}{3}.(\mathbf{2^{p-1} - 1})$
Factorization of $N + 1$	$M_p + 1 = 2^p$	$N_p + 1 = \frac{4}{3}.(2^{p-2} + 1)$
$\equiv 1 \pmod p$	$\surd$	$\surd$
DWT reduction	modulo $2^p - 1$	modulo $2^p + 1$
$p \neq q \Longrightarrow$	$gcd(M_p, M_q) = 1$	$gcd(N_p, N_q) = 1$
conjecture	square-free	square-free

Here is a table of the computed prime exponents for the N_p and M_p :

n°	M_p prime : $p =$	N_p prime : $p =$
1	2	3
2	3	5
3	5	7
4	7	11
5	13	13
6	17	17
7	19	19
8	31	23
9	61	31
10	89	43
11	107	61
12	127	79
13	521	101
14	607	127
15	1279	167
16	2203	191
17	2281	199
18	3217	313
19	4253	347
20	4423	701
21	9689	1709
22	9941	2617
23	11213	3539
24	19937	5807
25	21701	10501
26	23209	10691*
27	44497	11279
28	86243	12391
29	110503	14479*
30	132049	42737*
31	216091	83339*
32	756839	95369*
33	859433	117239*
34	1257787	127031*
35	1398269	138937*
36	2976221	141079*
37	3021377	267017*
38	6972593	269987*
39	13466917	374321*

Remark : The N_p with a * aren't proved prime (they are only PRP).

The primality of N_{1709}, N_{2617}, N_{3539}, N_{10501}, N_{12391} was proved by François Morain (Cf. [5]).

The primality of N_{5807}, N_{11279} was proved by Preda Mihaïlescu.

4 Some relations between N_p and M_p :

4.1°) $2^q.N_p.M_p + N_q = N_{2p+q}$

In particular, for $q = 1$, we have $2.N_p.M_p + 1 = N_{2p+1}$

It exists general formulas of the form :

$N_{2.k.p+4} - 1 \equiv 0\ [2.a.p.N_p.M_p]$ when p is prime. Then, a is a function of k.

Practical application : If M_p or N_p is prime and if $2p+1$ is prime (p Sophie-Germain prime), then $N_{2p+1} - 1$ has got $2p$ and M_p or N_p has prime factors, so $N_{2p+1} - 1$ is more than 50% factorized, which implies that it is a primality-provable number ($N-1$ test). Values of $2p+1$ for which M_p or N_p is prime and $2p+1$ is prime are : 5, 7, 11, 23, 47, 179, 383, 7079, 19379, 21383, 43403, 166679 and 1718867. N_5, N_7, N_{11} and N_{23} are provable PRP but the other exponents aren't PRP for $2p+1 \leq 400000$. It remains 1718867, which gives $N_{1718867}$ composite.

4.2°) $N_p.M_p + N_q = 2^q.N_{2p-q}$ (p and q odd)
In particular, for $q = 1$, we have $N_p.M_p + 1 = 2.N_{2p-1}$

4.3°) $3.N_p.M_p = 2^{2p} - 1$ (p and q odd)

4.4°) Cyclotomic numbers : (Cf. [6]) (p odd prime)
$M_p = \Phi_p(2)$ and $N_p = \Phi_p(-2)$

4.5°) M_p and N_p as Lucas sequences :
$U_n(P,Q) = (a^n - b^n)/(a-b)$ and $V_n(P,Q) = a^n + b^n$ with $a+b = P$, $a.b = Q$.
If $a = 2$ and $b = -1 \Longrightarrow P = a+b = 1$, $Q = a.b = -2$ and $D = P^2 - 4Q = 9$

$U_n(1,-2) = \frac{2^n-(-1)^n}{3}$ and $V_n(1,-2) = 2^n + (-1)^n$

If n is an odd prime, $\boxed{U_p(1,-2) = \frac{2^p+1}{3} = N_p \text{ and } V_n(1,-2) = 2^p - 1 = M_p}$

and if $n = 2p$, $U_{2p} = (2^p-1)(2^p+1)/3 = M_p.N_p$

or $3.M_p.N_p = 2^{2p} - 1 = 4^p - 1$

4.6°) $N_p + M_p + 1 = N_{p+2}$ (p odd)

4.7°) $4.N_p - 1 = N_{p+2}$ (p odd)

4.8°) $12.N_p.((M_p^2 + M_p + 1)/3) - 1 = N_{3.p+2}$ (p odd)

4.9°) $N_{p.q+2} + 1 \equiv 0\ [4.N_p.M_p]$ (p, q odd primes)
If $p.q \equiv 1\ [4]$ and if $p.q+2$, N_p and M_p are primes then :

$N_{p.q+2} + 1 \equiv 0\ [4.N_p.M_p.(2.p.q+1)]$

5 The practical test :

First of all, a sieve is done among prime exponents in a range by sieving probable divisors of the form $d = 2.k.p+1$ with $d \equiv 1$ or $3 \pmod 8$ using a quick program written in C and ASM. The fast test described in section 2 is done using the program *mprime* by George Woltman, used in the GIMPS research (Cf. [2]). This program has to be modified by removing the subtraction by 2 at each step of the Lucas-Lehmer test, by switching the DWT mode to 2^n+1 mode, by changing the starting value to 25 instead of 4, and by subtracting 25 at the final result of the test, in order to be compared with 0.

Using this program, we have found the known exponents for $p < 100000$ and the probable primality of all N_p with $100000 < p < 400000$ in the table of the section 3, and now, N_{374321} is probably the largest known PRP (Cf. [4]).

Because *mprime* is very fast, the test for $N_{6972593}$ has been done in only 5 weeks using a Pentium 233 MMX with Linux RedHat 7.0 ! And, unfortunately, this number is... composite ! , which confirms "the new Mersenne conjecture" like the tests we have made which prove the compositeness of N_{86243} (divisible by 1 627 710 365 249) and $N_{1398269}$.

6 Bibliography and references :

[1] P. T. Bateman, J. L. Selfridge and Wagstaff, Jr., S. S., "The new Mersenne conjecture", Amer. Math. Monthly, 96 (1989) 125-128.

[2] The Great Internet Mersenne Prime Search (GIMPS) :
http ://www.mersenne.org/prime.htm

[3] Mersenne and Fermat primes field :
http ://ourworld.compuserve.com/homepages/hlifchitz/Henri/us/MersFermus.htm

[4] The Probable Primes Top 1000 page :
http ://www.primenumbers.net/prptop/prptop.php

[5] The François Morain's primality proving program (ECPP) :
http ://www.lix.polytechnique.fr/~morain/Prgms/ecpp.english.html

[6] Yves Gallot, "Cyclotomic polynomials and prime numbers" (November 12, 2000) :
http ://perso.wanadoo.fr/yves.gallot/papers/cyclotomic.html

[7] Andy Steward, Generalized Repunits :
http ://www.users.globalnet.co.uk/~aads/index.html

[8] Lifchitz Renaud, "Introduction to a new tool : the antiorder" :
http ://ourworld.compuserve.com/homepages/hlifchitz/Renaud.html