A Fermat-Like Sequence and Primes of the Form $2h.3^n + 1$

Yannick Saouter

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

A Fermat-like sequence and primes of the form $2h.3^n + 1$

Yannick Saouter

N° 2728

Novembre 1995

PROGRAMME 1

ISSN 0249-6399

INRIA
RENNES

A Fermat-like sequence and primes of the form $2h.3^n + 1$

Yannick Saouter†

Programme 1 — Architectures parallèles, bases de données, réseaux et systèmes distribués
Projet API

Rapport de recherche n ° 2728 — Novembre 1995 — 15 pages

Abstract: Fermat numbers are a classical topic in elementary number theory. Fermat introduced them and claimed that all these numbers are prime. This claim was disproofed by Euler who gave a property on the eventual divisors of the Fermat numbers. In this article we exhibit another serie whose definition is close to the one of Fermat numbers and which exhibit similar properties. This problem will lead us to the sets of covering congruences for numbers $2h.3^n + 1$ as similarly Fermat numbers lead to Sierpinski's problem.

Key-words: Fermat's numbers; Prime numbres; Sierpinski's problem

(Résumé : tsvp)

† email: **saouter@irisa.fr**

Unité de recherche INRIA Rennes
IRISA, Campus universitaire de Beaulieu, 35042 RENNES Cedex (France)
Téléphone : (33) 99 84 71 00 – Télécopie : (33) 99 84 71 71

Une séquences de nombres et nombres premiers de la forme $2h.3^n + 1$

Résumé : Les nombres de Fermat sont un sujet classique en théorie des nombres. Fermat les introduidit et conjectura que tous ces nombres sont premiers. Cette affirmation fut montré fausse par Euler qui donna une propriété sur les diviseurs éventuels des nombres de Fermat. Dans cet article nous définissons une autre suite dont la définition est proche de celle des nombres de Fermat et qui révèle des propriétés similaires. Ce problème nous conduira aux ensembles de couvertures de congruences pour les nombres $2h.3^n + 1$ comme, de manière similaire les nombres de Fermat nous conduise au problème de Sierpinski.

Mots-clé : Nombres de Fermat; Nombres premiers; Problème de Sierpinski

1 Introduction

Fermat numbers are a classical topic in elementary number theory. Fermat introduced them and claimed that all these numbers are prime. This claim was disproofed by Euler who gave a property on the eventual divisors of the Fermat numbers. In this article we exhibit another serie whose definition is close to the one of Fermat numbers and which exhibit similar properties. This problem will lead us to the sets of covering congruences for number $2h.3^n + 1$ as similarly Fermat numbers lead to Sierpinski's problem.

2 Properties of Fermat numbers

A certain number of properties are known for Fermat numbers. We denote $f_n = 2^n + 1$. Then we have the following theorem:

Theorem 2.1 *If f_n is a prime number, then $n = 2^k$.*

At this point we denote $F_n = 2^{2^n} + 1$. We have then the following property:

Theorem 2.2 (Pepin's test) *The number F_n is prime if and only if there exists $k \geq 2$ such that $J(k, F_n) = -1$ and $k^{(F_n-1)/2} = -1$ [mod. F_n], where J denotes the Jacobi's symbol.*

We refer the reader to [1] for the definition and the computation rules of the Jacobi's symbol. More precisely, the number 3 is always a good choice for k:

Theorem 2.3 *The number F_n is prime if and only if $3^{(F_n-1)/2} = -1$ [mod. F_n].*

This test is rapidly unfeasible because of the exponential growth of the numbers F_n, but it was used in by Lucas to show that F_6 is composite. We have also:

Theorem 2.4 *The numbers F_n are pairwise relatively prime.*

Some information is also known on the divisors of F_n:

Theorem 2.5 *If p is a prime divisor of F_n, then $p = 1$ [mod. 2^{n+2}].*

This theorem enables Keller to claim in 1985 that F_{23471} is not a prime since it is divisible by $5 \times 2^{23473} + 1$. At the present time the only Fermat prime numbers known are F_n, $1 \leq n \leq 4$.

3 Another serie

In this section we define a new serie $a_n = 4^n + 2^n + 1$ which exhibits the same kind of properties than the Fermat numbers. We have at first:

Theorem 3.1 *If a_n is a prime number, then $n = 3^k$.*

Similarly we denote $A_n = 4^{3^n} + 2^{3^n} + 1$. We have then:

Theorem 3.2 *The number A_n is prime if and only if there exists $k \geq 2$ such that $J(k, A_n) = -1$ and $k^{(A_n-1)/2} = -1$ [mod. A_n].*

More precisely, the number 5 is always a good choice for k:

Theorem 3.3 *The number A_n is prime if and only if $5^{(A_n-1)/2} = -1$ [mod. A_n].*

We have also:

Theorem 3.4 *The numbers A_n are pairwise relatively prime.*

and:

Theorem 3.5 *If p is a prime divisor of F_n, then $p = 1$ [mod. 3^{n+1}].*

It is here noteworthy that the exponent is only $n + 1$. The following sections are devoted to prove the previous claims.

4 Proof of theorem 3.1

This proof uses two lemmas:

Lemma 4.1 *For all* $k \geq 1$, $2^{3k} = 1$ $[mod.\ a_k]$.

Proof Verify that $2^{3k} - 1 = (2^k - 1).a_k$. □
and:

Lemma 4.2 *For all* $k \geq 1$, $2^{4k} + 2^{2k} + 1 = 0$ $[mod.\ a_k]$.

Proof Verify that $2^{4k} + 2^{2k} + 1 = (4^k - 2^k + 1).a_k$. □
We have then:

Theorem 4.1 *For all* $k \geq 1$ *and* $n \geq 1$, $a_{(3n+1)k}$ *and* $a_{(3n+2)k}$ *are divisible by* a_k.

Proof We have indeed: $a_{(3n+1)k} = 2^{(6n+2).k} + 2^{(3n+1)k} + 1 = (2^{6k})^n.2^{2k} + (2^{3k})^n.2^k + 1$. Thus according to lemma 4.1, we have $a_{(3n+1)k} = 2^{2k} + 2^k + 1$ $[mod.\ a_k]$ and so $a_{(3n+1)k} = 0$ $[mod.\ a_k]$.

Likewise $a_{(3n+2)k} = 2^{4k} + 2^{2k} + 1$ $[mod.\ a_k]$ and then lemma 4.2 establishes the theorem. □

At this point, it is clear that if a_k is a prime number then any prime divisor of k is congruent to 0 modulo 3, i.e. k is an exact power of 3.

5 Proofs of theorems 3.2 and 3.3

The proof of theorem 3.2 here requires a special theorem (see [2]):

Theorem 5.1 (Pocklington's theorem) *Let* N *be an integer such that* $N - 1 = F_1.R_1$ *with* $(F_1, R_1) = 1$ *and such that complete factorization of* F_1 *is known. If for each prime number* p_i *dividing* F_1 *there exist an integer* a_i *such that* ${a_i}^{N-1} = 1$ $[mod.\ N]$ *and* $(a_i^{(N-1)/p_i} - 1, N) = 1$, *then each prime divisor* p *of* N *is such that* $N = 1$ $[mod.\ F_1]$.

Proof of theorem 3.2
Sufficiency: Suppose that A_n is a prime number. Then $k^{(A_n-1)/2} = J(k, A_n)$ $[mod.\ A_n]$ (see [3] for instance). But here the Jacobi's symbol is indentical to Legendre's symbol and amongst all k such that $1 \leq k \leq A_n - 1$, exactly the half are such that $J(k, A_n) = 1$ while the other ones are such that $J(k, A_n) = -1$. So there exists k such that $k^{(A_n-1)/2} = -1$ $[mod.\ A_n]$ and $J(k, A_n) = -1$.

Necessity: Now suppose that there exists k such that $J(k, A_n) = -1$ and $k^{(A_n-1)/2} = -1$ $[mod.\ A_n]$. Then we have $A_n - 1 = F_1.R_1$ with $F_1 = 2^{3^n}$ and $R_1 = 2^{3^n} + 1$. So $k^{(A_n-1)/2} - 1 = -2$ $[mod.\ A_n]$ and then $(k^{(A_n-1)/2} - 1, N) = (2, N)$. But by definition N is odd so $(k^{(A_n-1)/2} - 1, N) = 1$. Moreover $k^{(A_n-1)} = (-1)^2 = 1$ $[mod.\ A_n]$. So according to Pocklington's theorem every prime divisor p of A_n is such that $p = 1$ $[mod.\ 2^{3^n}]$. Let us suppose that A_n has at least two prime divisors $p_1 = 1 + k_1.2^{3^n}$ and $p_2 = 1 + k_2.2^{3^n}$ with $k_1, k_2 \geq 1$. Then $A_n \geq (1 + k_1.2^{3^n})(1 + k_2.2^{3^n}) \geq (1 + 2^{3^n})^2 = 4^{3^n} + 2.2^{3^n} + 1 > A_n$. So we have a contradiction and thus A_n is a prime number. □

To complete this section it suffices to show that we always have $J(5, A_n) = 1$.

Proof of theorem 3.3 At first we need to compute the remainder of the division of A_n by 5. If $n = 2.k$, $k \geq 1$, then $3^{2k} = (3^2)^k = 1^k = 1$ $[mod.\ 4]$. Then $2^{3^{2k}} = 2$ $[mod.5]$ (indeed $2^4 = 1$ $[mod.5]$). Then $A_n = 2^2 + 2 + 1 = 7 = 2$ $[mod.5]$. If $n = 2.k + 1$, $k \geq 0$, we obtain in a similar way $2^{3^{2k}} = 3$ $[mod.5]$ and then $A_n = 3^2 + 3 + 1 = 3$ $[mod.5]$. Then, in both cases, A_n is relatively prime with 5 and we can apply the quadratic reprocity law and then:

$$\begin{aligned} J(5, A_n) &= (-1)^{\frac{5-1}{2}.\frac{A_n-1}{2}} J(A_n, 5) \\ &= (-1)^{A_n-1} J(A_n, 5) \end{aligned}$$

But $A_n - 1$ is even and then $J(5, A_n) = J(A_n, 5)$. Then if r is such that $A_n = r\ [mod.5]$, then $J(5, A_n) = J(r, 5)$. As we have seen $r = 2$ or 3. But $J(2, 5) = J(3, 5) = -1$, since 5 is a prime number and neither 2 nor 3 is a quadratic residue modulo 5. □

6 Proof of theorem 3.4

In order to prove the theorem 3.4, we prove firstly the next lemma:

Lemma 6.1 *Let n be an integer, then $A_{n+1} = 3\ [mod.A_n]$.*

Proof Verify that $A_{n+1} = 3 + A_n.(2^{4.3^n} - 2^{3.3^n} + 2.2^{3^n} - 2)$. □
Then by an obvious recurrence we obtain:

Lemma 6.2 *Let n and m be integers such that $n > m \geq 0$, then $A_n = 3\ [mod.A_m]$.*

Proof of theorem 3.4 Let n and m be integers such that $n > m \geq 0$. Then according to lemma 6.2, the greatest common divisor of A_n and A_m divides 3. Then it is either 3 and 1. But 3^k is odd and $2^{2h+1} = 2\ [mod.\ 3]$ and thus $A_n = 2^2 + 2 + 1 = 7 = 1\ [mod.\ 3]$. Thus the greatest common divisor of A_n and A_m is equal to 1. □

7 Proof of theorem 3.5

The proof requires the following lemma:

Lemma 7.1 *Let n be an integer then $2^{3^{n+1}} = 1\ [mod.\ A_n]$.*

Proof Verify that $2^{3^{n+1}} - 1 = A_n.(2^{3^n} - 1)$. □

Proof of theorem 3.5 Let p be a prime divisor of A_n. Then according to the previous lemma, we have $2^{3^{n+1}} = 1\ [mod.\ p]$. Let k be the order of 2 in the multiplicative field Z_p. Then k divides 3^{n+1}. Let us suppose that $k < 3^{n+1}$, then we would have $2^{3^n} = 1\ [mod.\ p]$. But this implies $A_n = 1^2 + 1 + 1 = 3\ [mod.\ p]$ and thus $p = 3$. But as we have seen in the proof of 3.4, 3 divides none of the A_n. So we have $k = 3^{n+1}$. But since p is a prime number we have also $3^{p-1} = 1\ [mod.\ p]$ and thus k divides $p - 1$, i.e. 3^{n+1} divides $p - 1$. This establishes the theorem. □

8 Numerical results

The six first numbers of the series were easy to check for primality. Amongst them only $A_0 = 7$, $A_1 = 73$, and $A_2 = 262657$ appears to be prime. A_3 splits easily in three factors on general purposes symbolic computation software. A_4 splits into four factors by Pollard's rho method [4] in less than 10 minutes on a Sparc-Station (assuming Pollard's conjecture[4]). The unfactored part of A_5 counts 130 decimal digits and its factorization is unlikely for the time being: a trial during two weeks reveals unsuccessful. The table 1 summarizes the set of non trivial divisors for the integers A_n with $n < 40$. This table, let apart the cases where $n \leq 4$ was obtained by testing any number A_n for divisibility with all numbers $2h.3^{n+1} + 1$ for $1 \leq h \leq 1.5 \times 10^6$. For numbers for which this search was unsuccessful, the upper bound of search was raised to 1.5×10^7 but no additionnal divisor was found. Only values of h are reported.

n	h
0	prime
1	prime
2	prime
3	16, 439, 602999
4	1, 34472805800, 397061122816, 7639897455249297
5	55, 67, 260
6	9, 1738968
7	16, 99
8	3596
9	4, 343092, 575979
10	None factor found.
11	83
12	1367973
13	None factor found.
14	9
15	None factor found.
16	13, 849332
17	15539
18	None factor found.
19	95, 838543
20	None factor found.
21	4
22	None factor found.
23	63
24-25	None factor found.
26	693
27-28	None factor found.
29	1241739
30	149
31-32	None factor found.
33	144
34-38	None factor found.
39	64, 7576

Table 1: Divisors of the series A_n for $0 \leq n \leq 39$

9 Related Sierpinski's problem

In [5], Sierpinski proved that there exists values k such that $k*2^n+1$ is never a prime number. The least known value k assuming this property is in fact 78557. It is also conjectured that it is indeed the least number with this property. Likewise, we prove in this paragraph that there exists values h such that $2h.3^n+1$ is never a prime number and there is no prime number dividing all the terms of this serie. The proof is in its outlines the same as Sierpinski's one but in this case we have some additionnal technichal problems. We have at first:

Lemma 9.1 *Any integer N verifies at least one of the following congruences:*

$$\begin{aligned}
N &= 0\ [mod\ 3]\\
N &= 0\ [mod\ 4]\\
N &= 1\ [mod\ 6]\\
N &= 2\ [mod\ 8]\\
N &= 5\ [mod\ 12]\\
N &= 3\ [mod\ 16]\\
N &= 6\ [mod\ 16]\\
N &= 23\ [mod\ 24]\\
N &= 11\ [mod\ 48]\\
N &= 14\ [mod\ 48]\\
N &= 46\ [mod\ 48]
\end{aligned}$$

Proof It just suffices to verify this for any integer $0 \leq N \leq 47$. □
Moreover, we have:

Lemma 9.2 *If $d \neq 3$ is such that $3^k = 3^{k+r}\ [mod\ d]$, then d divides $3^r - 1$.*

Proof Substract and factorize. □

That lemma can be used to establish the first part of the theorem:

Theorem 9.1 *There is no integer $d > 1$ such that d divides all the numbers $2h.3^n + 1$.*

Proof It is immediate that neither 2 nor 3 divide anumber of the form $2h.3^n + 1$. Now if $d > 3$ divides any of these terms then d divides $3^1 - 1 = 2$ which is impossible. □

By lemma 9.2, we show also:

Theorem 9.2 *For all integer k, at least one of the following congruences is verified:*

$$\begin{aligned}
3^k &= 1\ [mod\ 13]\\
3^k &= 1\ [mod\ 5]\\
3^k &= 3\ [mod\ 7]\\
3^k &= 9\ [mod\ 41]\\
3^k &= 3^5\ [mod\ 73]\\
3^k &= 3^3\ [mod\ 17]\\
3^k &= 3^6\ [mod\ 193]\\
3^k &= 3^{23}\ [mod\ 6481]\\
3^k &= 3^{11}\ [mod\ 97]\\
3^k &= 3^{14}\ [mod\ 577]\\
3^k &= 3^{46}\ [mod\ 769]
\end{aligned}$$

Proof This theorem expresses in fact exactly the same congruences as lemma 9.1 but in a different fashion. Let us see it on the first congruence. To find a congruence for 3^k respected by all values k such that $k = 0\ [mod.\ 3]$, in virtue of lemma 9.2, we need to find factors of $3^3 - 1$. In fact, we have $3^3 - 1 = 2.13$. The value d is not acceptable since it would lead to the congruence $3^k = 1\ [mod.\ 2]$, trivially respected by all integers k and thus would render all the other congruences useless. Likewise for a reason that will be clear in the next theorem we need distinct moduli in right-hand side and thus this explains the presence of 6481 since all the others smaller factors of $3^{24} - 1$ are already used. □

We have then:

Theorem 9.3 *For any integral value k, $3^k - 2288554933256759222642$ is composite.*

Proof If a is an even number solution of the system of theorem 9.2, replacing 3^k by a then $3^k - a$ is always divisible by at least one of the moduli. By solving the system we find the above value. □

This theorem explains why we needed distinct moduli: in order to have a solution for the congruence system this condition is necessary.

With this theorem we may state:

Theorem 9.4 *For any integral value k, $3^k * 1556149149683450570754 + 1$ is composite. Moreover the set of integers h such that $2h * 3^k + 1$ is always composite, has a positive density.*

Proof If $3^k - a$ is always divisible by at least one moduli, so is also for $b.3^k + 1$ where $b = -a^{-1}$ in the multiplicative group of the product P of all moduli. By solving the equation we find the above value. Moreover this value b can be incremented by any multiple of $2 * P$ (P is odd). It will still give an even number and won't affect the congruences. This point establishes the second part of the theorem. □

Moreover:

Theorem 9.5 *Let c be any integer. If for all integer k with $0 \leq k \leq 47$, $3^k + c$ is dividable by at least one of the moduli of the system of theorem 9.2, then for all k, $3^k + c$ is composite.*

Proof Let d be modulo of the system. By lemma 9.2, d divides $3^r - 1$ where r is a modulo of the system of theorem 9.1. But in this case r is a divisor of 48. For any $a > 1$ and any k, $a^k - 1$ is always divisible by $a - 1$. As a consequence $3^r - 1$ divides $3^{120} - 1$ and thus d divides $3^{48} - 1$. Now if we suppose that $3^k + c$ for a given k and a given c is divisible by d, then any number of the form $3^{k+120.l} + c$ is also divisible by d. Whence the result. □

So we have:

Corollary 9.1 *For any integral value k, $3^k * 1556149149683450570754 + 1$ and $3^k + 1556149149683450570754$ are always composite.*

Proof For all integer k with $0 \leq k \leq 47$, $3^k + b$ is dividable by at least one of the moduli of the system of theorem 9.2 and thus the previous theorem applies. □

At this point several questions arise. Firstly what is the least value h such that $2h*3^k+1$ is always composite ? This question is still unsolved for the case of powers of 2 although the interval of research is much more reduced [6]. So without additionnal theoretical results, it is quite clear that this question will not be answered in the near future.

One another question arises: can we have covering sets of congruence with less than 11 moduli ? This question makes sense since since the original example of Sierpinski for powers of 2 counts 7 moduli and it was proved after that 6 moduli suffice in fact. It is also noteworthy that the case of powers of 3 is the worst in this sense since for higher powers less moduli are needed.

The exact determination of the least number of moduli would require a huge amount of computation time but as we shall see in the nextion section it is possible to prove that this number is at least 5.

10 Least number of moduli

Firstly theorem 9.1 proves that at least two moduli are needed. Likewise we have the following theorem:

Theorem 10.1 *The covering set of congruences of the numbers* $2h.3^n + 1$ *counts at least 5 numbers.*

In the following we will use the notation of Stanton [7] to illustrate the covering set of the numbers $2h.3^n + 1$: the successive numbers are represented by a row of cells and a cell can contain only numbers dividing the corresponding term in the serie. An important fact is to be noted:

Fact 10.1 *The number 2 does not belong to the covering set.*

Indeed it is clear that 2 cannot divide a number of the form $3h.2^n + 1$.

Proof Firstly in virtue of lemma 9.2, a number cannot succeed to itself. Let us suppose that only two numbers form the covering set. Then necessarily the congruences of the terms of the series are as follows:

	A	B	A	B	

But then in virtue of lemma 9.2, A and B divides $3^2 - 1$. But $3^2 - 1 = 8$ is divisible by 2 and 2 does not belong to the set. So there is a contradiction. From this we may also note that the offset between successive places of a same number cannot be equal to 2.

Now let us suppose that we have three numbers A, B, C in the set. Since the position of a same number cannot differ of 1 or of 2, necessarily the four first locations in the row are something as follows:

A	B	C	A	

But now the fifth location cannot contain neither A neither C. So necessarily it contains B and the locations of both A and B differs from 4. Then in virtue of lemma 9.2 both A and B divides $3^4 - 1 = 80$. But 80 has only one odd divisor and thus you have a contradiction.

Suppose now that we have four primes. Then the first four locations of the row can have two configurations either:

A	B	C	A	

or:

A	B	C	D	

Let us treat the first case. The fifth location cannot then be A (offset 1), C (offset 2) nor B. Indeed in the latter case in virtue of lemma 9.2, both A and B should divide $3^3 - 1 = 2.13$ which is impossible. Thus the fifth location contains D:

A	B	C	A	D	

Then the sixth position cannot contain A (offset 2), C (offset 3 in concurrence with A) nor D (offset 1). So we have:

A	B	C	A	D	B	

The seventh position contains then A since this number has an offset equal to 3:

A	B	C	A	D	B	A	

Then the eighth position cannot contain A, B nor D (concurrence with A) and thus contains C.

A	B	C	A	D	B	A	C	

Then the ninth position contains D. But then both B and D have 4 as offset while $3^4 - 1$ has only one odd divisor. This establishes the contradiction for the first case.

The second case splits in two subcase depending on whether we put A or B in the fifth position. As the reader may verify if the letter is A or B, in both cases, we obtain a contradiction for the tenth position.

□

This method although simple is rapidly unfeasible by hand because of the multiplications of subcases which have to be considered.

11 Least period

In this section, we take the problem from the opposite side and wonder whether there is no covering set with a period smaller than 48. Throughout this paragraph we will denote P the least value of the period. We have at first the following theorem:

Theorem 11.1 *The number P is not a prime number.*

Proof If we cover a set $2h.3^n + 1$ by a set of congruences with a period P, it necessarily uses the divisors of $3^P - 1$. But as we have seen only odd divisors can appear in the set of congruence. Let k be the number of odd prime divisors of $3^P - 1$ then necessarily $k < P$. Indeed, a number which is divisible by P odd primes is greater than 3^P. So the covering set counts at most $P - 1$ congruences. Since P has no non trivial divisors, the periodicity of all this congruences must be equal to P. Then by density it is clear that at most 1 number out of P is not covered. □

In fact the argument of density is very powerful and discard most of the candidate periods. Let P' a candidate period. Our algorithm to check it was the following:

- Factor $3^{P'} - 1$ as well as $3^p - 1$ for all p dividing P'.
- For all odd prime factors dividing $3^p - 1$ and not dividing $3^q - 1$ with q dividing p, count $1/p$ as covering density.
- Add all the densities. If the result is smaller than 1, the number P' cannot be a period. If the result is greater than 1 then check for the existence of an effective covering set.

The numbers where factored by using Maple[8]. One remark is that here we accept duplicated basis in the corresponding covering set of the integers on the contrary of Erdös example.

Numerical example Let us take $P' = 20$. Then $P' = 2^2.5$ and P' has 2, 4, 5, 10, 20 as divisors. The respective contributions to density are:

- $3^2 - 1 = 2^3 \rightarrow$ no contribution.
- $3^4 - 1 = 2^4.5 \rightarrow 1/4$.
- $3^5 - 1 = 2.11^2 \rightarrow 1/5$.
- $3^{10} - 1 = 2^3.11^2.61 \rightarrow 1/10$.
- $3^{20} - 1 = 2^4.5^2.11^2.61.1181 \rightarrow 1/20$.
- Total density: $1/4 + 1/5 + 1/10 + 1/20 = 3/5 < 1$.

Then $P' = 20$ cannot be a period for a covering set for numbers $3h.2^n + 1$. The reader may not that we only have a majoration of the density : For instance in the previous example, since 4 and 5 are relatively prime, in a set of 20 following terms at least one would have been divisible by 5 and e.g. 11. As a consequence one can refine the approximation by substracting 1/40 to the final density since one of the congruence makes double use.

The table 2 summarize the results in terms of density.

As we can see few candidates pass this first test with success: 24, 36, and 48. But as we have seen we may refine the majoration. For instance for 24 has 2, 3, 4, 6, 8, 12, 24 as divisors. If we would have a covering set for numbers $2h.3^n + 1$ with 24 as period then it would result into a covering set of congruences of the set of natural numbers containing 3 and 4 as basis of moduli. Since those two numbers are relatively prime, one integer out of 12 would verify the two congruences, so the estimation for the density of 24 can be lowered by 1/24. At this point it becomes smaller than 1 and then 24 can be discarded from the candidates. Likewise the estimation for the density of 36 can be lowered by $1/24 + 1/72$ since 4 is relatively prime with 3 and 9. The obtained value is still greater than 1 and so with this test it is impossible to conclude for this value. An exact search of covering has to be done. The factorization of $3^k - 1$ were k divides 36 gives the number of congruences modulo k that are possible to accept:

- $3^2 - 1 = 2^3 \rightarrow$ No congruence modulo 2.

P'	d(P')	P'	d(P')	P'	d(P')
4	1 / 4	21	11 / 21	35	2 / 5
6	1 / 2	22	3 / 11	36	13 / 12
8	3 / 8	24	1 / 1	38	3 / 19
9	4 / 9	25	7 / 25	39	19 / 39
10	3 / 10	26	3 / 26	40	3 / 4
12	5 / 6	27	5 / 9	42	17 / 21
14	3 / 14	28	15 / 28	44	25 / 44
15	3 / 5	30	14 / 15	45	7 / 9
16	1 / 2	32	17 / 32	46	5 / 46
18	13 / 18	33	6 / 11	48	19 / 16
20	3 / 5	34	7 / 34		

Table 2: Estimations of density

- $3^3 - 1 = 2.13 \rightarrow$ 1 congruence modulo 3.
- $3^4 - 1 = 2^5.5 \rightarrow$ 1 congruence modulo 4.
- $3^6 - 1 = 2^3.7.13 \rightarrow$ 1 congruence modulo 6.
- $3^9 - 1 = 2.13.757 \rightarrow$ 1 congruence modulo 9.
- $3^{12} - 1 = 2^4.5.7.13.73 \rightarrow$ 1 congruence modulo 12.
- $3^{18} - 1 = 2^3.7.13.19.37.757 \rightarrow$ 2 congruences modulo 18.
- $3^{36} - 1 = 2^4.5.7.13.19.37.73.757.530713 \rightarrow$ 1 congruence modulo 36.

In a neglictible amount of time a dedicated program established that no such covering set exists. The program chose at first moduli for the least basis and then in order to cut the searching tree evaluated how many additionnal points might be covered by the other congruences. For instance the congruence modulo 36 can only cover at most one additionnal point while the second congruence modulo 18 together with the congruence modulo 36 can cover at most 3 additionnal points out of 36. By adding this estimation to the number of points effectively covered we obtained an upper bound for the total covering. If this estimation is less than 36 the corresponding part of the searching tree can be discarded. This test enabled to avoid to consider all subcases for larger moduli which would have led to a great combinatorial cost. Thus it is established that the least period for a covering set for numbers of the form $2h.3^n + 1$ is 48.

12 Conclusion

This study can be made for other type of numbers. For instance numbers of the form $32^n+16^n+8^n+4^n+2^n+1$ exhibit also similar properties but then the critical value 3 in what precedes has to be replaced by 5. No doubt that most conjectures about Fermat numbers can still apply to these numbers. However at least one of this conjecture does not apply to all these series. Indeed, while no non-squarefree Fermat numbers are known the number $32 + 16 + 8 + 4 + 2 + 1 = 63$, first term of the previous series admit $9 = 3^2$ as divisor. This property allow to suppose that if this conjecture is true for Fermat numbers, it might be accidental, i.e. true while no strong reason to justify it.

As for Sierpinski's problem it is clear that the least value h for which all numbers $2h.3^n + 1$ are all composite will not be known in the near future. At most this value might be supposed by assuming that the least number h has a finite number of moduli and that this number is 48. An intensive search was done, with the multiprecision package GMP[9], by searching numbers such that $2h.3^n + 1$ and $2h.3^{n+48} + 1$ have a common divisor for all $0 \leq n < 48$. This experimentation took several days on a SparcStation 10 and no value h with such property was found up to 2^{31}. This illustrates once again that Sierpinski's problem for powers of 3 is much harder than for 2.

References

[1] P. Ribenboim. – *The Book of Prime Number Records.* – Springer-Verlag, 1988.

[2] H.C. Pocklington. – The determination of the prime and composite nature of large numbers by Fermat's theorem. – *Proc. Cambridge Philos. Soc.*, 1914.

[3] R. Solovay and V. Strassen. – A fast Monte-Carlo test for primality. – *SIAM J. Comput.*, 1977.

[4] J.M. Pollard. – A Monte-Carlo method for factorization. – *BIT*, 15:331–334, 1975.

[5] W. Sierpinski. – Sur un problème concernant les nombres $k.2^n + 1$. – *Elem. Math.*, pages 27–30, 1961.

[6] G. Jaeschke. – On the smallest k such that all $k.2^n + 1$ are composite. – *Math.Comp.*, 40(161):381–384, 1983.

[7] R.G. Stanton. – Further results on covering integers of the form $1 + k.2^n$ by primes. – In *LNM 884. Combinatorial Mathematics VIII*, pages 107–114, 1980.

[8] B.W. Char, K.O. Geddes, and G.H. Gonnet. – *First leaves: a tutorial introduction to MAPLE V.* – Springer-Verlag, 1992.

[9] T. Grandlung. – The GNU multiple precision arithmetic library. – Technical documentation, 1993.

Unité de recherche INRIA Lorraine, Technopôle de Nancy-Brabois, Campus scientifique,
615 rue du Jardin Botanique, BP 101, 54600 VILLERS LÈS NANCY
Unité de recherche INRIA Rennes, Irisa, Campus universitaire de Beaulieu, 35042 RENNES Cedex
Unité de recherche INRIA Rhône-Alpes, 46 avenue Félix Viallet, 38031 GRENOBLE Cedex 1
Unité de recherche INRIA Rocquencourt, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex
Unité de recherche INRIA Sophia-Antipolis, 2004 route des Lucioles, BP 93, 06902 SOPHIA-ANTIPOLIS Cedex

Éditeur
INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex (France)
ISSN 0249-6399