A SEARCH FOR SOME SMALL BRIER NUMBERS

YVES GALLOT

ABSTRACT. In 1998, Eric Brier proved the existence of some numbers k such that $k \cdot 2^n$ is never adjacent to a prime. At that time, the smallest known "Brier Number" was a 41-digit number. The search was extended to find the smallest Brier number. Today, the smallest known number of this form is the 27-digit number $k = 878503122374924101526292469$.

1. DEFINITIONS

Definition 1.1. A **Sierpiński number** is a positive integer k such that $k \cdot 2^n + 1$ is not prime for any integer n.

Definition 1.2. A **Riesel number** is a positive integer k such that $k \cdot 2^n - 1$ is not prime for any integer n.

Definition 1.3. A **Brier number** is both a Sierpiński number and a Riesel number.

2. A CONSTRUCTIVE APPROACH

Let $S = \{p_1, p_2, ..., p_s\}$ a set of prime numbers and $P = \prod_{1 \le i \le s} p_i$. Let e_i the order of 2 modulo p_i (see [1, Definition 22]) and $e_S = \operatorname{lcm}(e_1, e_2, ..., e_s)$.

Definition 2.1. If one of the primes of the set S divides $k \cdot 2^n + 1$ for any number n, and if for every prime p_i of S there is at least one n_i such that no other prime of S divides $k \cdot 2^{n_i} + 1$, then S is called a **covering set** for the Sierpiński number k (*idem* for Riesel numbers). e_S is called the **order** of S.

Note that it is enough to verify the conditions for any number $0 \le n < e_S$. Note also that a covering set may generate different Sierpiński numbers. To compute them, we should generate all possible sets of solutions $\{a_1, a_2, ..., a_s\}$ such that $k \equiv a_i \pmod{p_i}$ and determine k with Chinese Remainder Theorem.

Theorem 2.2. *If S is a covering set for a Sierpiński number, then it is a covering set for a Riesel number and vice versa.*

Proof. We can choose $k_R = 2P - k_S$. □

Definition 2.3. Let S_1 be a covering set and S_2 another covering set such that $S_1 \bigcap S_2 = \emptyset$ or $\{3\}$. S_2 is called the **complement** of S_1.

Date: February 6, 2000.

2000 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11A41.

Key words and phrases. prime numbers.

Theorem 2.4. *If S_2 is a complement of S_1, then $S_1 \bigcup S_2$ generates some Brier numbers.*

Proof. The prime 3 can be used in both sets, eliminating even values of n in one case and odd values in the other one. $\square$

3. A systematic search for covering sets

We search for all covering sets for a Sierpiński number with a fixed e_S. The order of 2 modulo p_i are some divisors of e_S then the covering sets are some subsets of the list of prime factors of $2^{e_S}-1$. A necessary condition is $\sum_i e_i \geq 1$, but it is not sufficient.

To test completely a subset, we create an array of e_S cells. For each prime p_i and for each $0 \leq o_i < e_i$, we fill the cells of the array at position $o_i + j \cdot e_i$. If the array is totally filled, and if for each p_i there exists a cell which has been filled only once, then the subset of primes is a covering set and we can compute k with the relations $k \equiv a_i \equiv -1/2^{o_i} \pmod{p_i}$.

We can generate all covering sets by applying this method, but the number of operations grows very fast with e_S. So another method was used to find some small Brier numbers initially.

4. A search for the "best" covering set

For a covering set S, the different sets of solutions $\{a_i\}$ can be considered as some random numbers modulo p_i. Thus the values of k are some random numbers modulo P. Then to find some small values of k, we search for some covering sets with P being small.

Definition 4.1. The **best** covering set of order e_S is the covering set for which P is minimal.

To find some small Brier numbers, we can search for the best complements. We start the search with a covering set S_1. If we find its best complement S_2, we have a good chance to find the smallest Brier number that can be generated by S_1 and any of its complements. We iterate the process by searching for S_3, the best complement of S_2, and stop when $S_{i+2} = S_i$.

Table 1. Some covering sets and their "good" complement

Set	e	Prime list	P size (digits)	compl.
S_1	24	3 7 5 17 13 241	7	S_2
S_2	420	3 31 127 11 43 151 41 337 29 113 331 71 122921 5419 61 1321 281 86171 1429 14449 29191 106681 152041	65	-
S_3	64	3 5 17 257 65537 641 6700417	20	S_4
S_4	144	3 7 73 13 19 241 37 109 97 673	17	S_5
S_5	120	3 5 31 17 11 151 41 331 61681 61	18	S_6
S_6	144	3 7 73 13 257 19 241 37 109 97	16	S_5
S_7	160	3 5 31 17 11 257 41 65537 61681 414721	25	S_4

The search for the best complement is often unpractical because its size is too large. Then a program was written to find quickly a "good" complement: for a fixed

e_S, the prime factors of $2^{e_S}-1$ are sorted in ascending order size and in ascending size if the orders have the same size. Rather than searching for each $0 \leq o_i < e_i$, we select the o_i for which the number of filled free cells is the larger one and only search with this value. Surprisingly, this simple algorithm is very efficient: for all e_S for which all covering sets are known, the algorithm finds the best one (*to be verified with recent results*).

Some results, found using this method, are shown in Table 1. If the order of the first set is too small then the second set contains several primes and the resulting Brier number is not small.

No pair of sets better than S_5 and S_6 was discovered. The smallest Brier number generated by these sets is 878503122374924101526292469.

5. A return to the systematic search

The orders of the sets found during the partial search were small enough to attempt the discovery of a smaller Brier number with an exhaustive search. All covering sets of Sierpiński numbers having $e_S < 180$ were generated and many others for some fixed s (see Table 2).

All complementary sets were paired and arranged in ascending P, where P is the product of the prime numbers of both sets. The smallest Brier numbers associated to the first pairs of the list were computed (see Table 3 for the top of them) But none of them was smallest than the previously found 27-digit Brier number. It is unlikely that a smaller Brier number will be found with two complementary sets.

Is it possible to find a smaller Brier number for which no complementary sets exist? A program was written to search for some Brier numbers directly, by filling two arrays of e_S cells. With this program, it was proved that no Brier number exists for $e_S < 180$. The possible candidates for $e_S < 288$ are 180, 240, 252 and 264. Some Brier numbers exist for $e_S = 288$: for example, the covering sets {3, 7, 5, 17, 73, 13, 257, 19, 241, 65537, 37, 109, 97, 673, 433, 38737, 193, 577, 1153, 6337} can be used. But the size of the Brier numbers found in this way is really larger than the numbers found by using two complementary sets.

References

1. D. Shanks, *Solved and Unsolved Problems in Number Theory*, 4th ed., Chelsea, New York, 1993.

E-mail address: galloty@wanadoo.fr

Table 2. Count of covering sets

e_S	n	Set
24	1	3 7 5 17 13 241
36	4	
48	15	
60	23	
64	1	3 5 17 257 65537 641 6700417
72	93	
80	1	3 5 31 17 11 257 41 61681 4278255361
84	8	
96	71	
108	24	
112	1	3 5 127 17 43 257 29 113 15790321 5153 54410972897
120	698	
128	2	
140	1	3 5 31 127 11 43 41 29 113 71 122921 281 86171 7416361 47392381
144	3376	
160	28	
168	1475	
180	?	

Table 3. Brier numbers generated by some covering sets having a small P

$e_1 = 120$	3 5 31 17 11 151 41 331 61681 61
$e_2 = 144$	3 7 73 13 257 19 241 37 109 97
k	878503122374924101526292469 (27/34)
$e_1 = 120$	3 5 31 17 11 151 41 331 61681 61
$e_2 = 144$	3 7 73 13 19 241 37 109 97 673
k	3872639446526560168555701047 (28/34)
$e_1 = 120$	3 5 31 17 11 151 41 61681 61 1321
$e_2 = 144$	3 7 73 13 257 19 241 37 109 97
k	6752111260707276586600527347 (28/34)
$e_1 = 120$	3 5 31 17 11 151 41 331 61681 61
$e_2 = 144$	3 7 73 13 257 19 241 37 109 673
k	2573455513910801216010607729 (28/35)
$e_1 = 120$	3 5 31 17 11 41 331 61681 61 1321
$e_2 = 144$	3 7 73 13 257 19 241 37 109 97
k	11252264900274601966567368371 (29/35)
$e_1 = 120$	3 5 31 17 11 151 41 61681 61 1321
$e_2 = 144$	3 7 73 13 19 241 37 109 97 673
k	2668934159979395835274330907 (28/35)
$e_1 = 120$	3 5 31 17 11 151 41 331 61681 1321
$e_2 = 144$	3 7 73 13 257 19 241 37 109 97
k	27456735936026361614526507061 (29/35)
$e_1 = 120$	3 5 31 17 11 41 331 61681 61 1321
$e_2 = 144$	3 7 73 13 19 241 37 109 97 673
k	16985143930825825363784428577 (29/35)
$e_1 = 120$	3 5 31 17 11 151 41 61681 61 1321
$e_2 = 144$	3 7 73 13 257 19 241 37 109 673
k	1723525455942005335396308929 (28/35)
$e_1 = 120$	3 5 31 17 11 151 41 331 61681 1321
$e_2 = 144$	3 7 73 13 19 241 37 109 97 673
k	71304118104020595224410968529 (29/36)
$e_1 = 120$	3 5 31 17 11 41 331 61681 61 1321
$e_2 = 144$	3 7 73 13 257 19 241 37 109 673
k	19387161879696990635166458771 (29/36)
$e_1 = 64$	3 5 17 257 65537 641 6700417
$e_2 = 144$	3 7 73 13 19 241 37 109 97 673
k	623506356601958507977841221247 (30/36)
$e_1 = 120$	3 5 31 17 11 151 41 331 61681 1321
$e_2 = 144$	3 7 73 13 257 19 241 37 109 673
k	5005425549902954169655052777 (28/36)
$e_1 = 120$	3 5 31 17 11 151 41 331 61681 61
$e_2 = 144$	3 7 73 13 257 19 241 37 97 433 577
k	713331160941223303050450522407 (30/37)