

# Equivalent Representations of the F-FCSR Keystream Generator

Simon Fischer<sup>1</sup>, Willi Meier<sup>1</sup>, and Dirk Stegemann<sup>2</sup>

<sup>1</sup> FHNW, 5210 Windisch (Switzerland)

<sup>2</sup> University of Mannheim, 68131 Mannheim (Germany)

**Abstract.** In this technical report, we investigate the security of the eSTREAM phase 3 stream cipher candidate F-FCSR. Our analysis shows a link to an equivalent representation. We conclude that this other representation is not weaker than the original one and thus does not constitute a practical threat.

**Key words:** Stream ciphers, Cryptanalysis, eSTREAM, F-FCSR

## 1 Introduction

Linear feedback shift registers (LFSRs) provide an efficient method for generating pseudorandom sequences with good statistical properties, they are widely used in stream cipher designs. However, the inherent linear structure must be overcome with additional methods, such as nonlinear filtering functions. As a potential replacement device of LFSRs, feedback shift registers with carry (FCSRs) have been investigated. The eSTREAM phase 3 candidate F-FCSR consists of an FCSR with 8 (resp. 16 in another instance) linear, thus hardware-efficient filters applied to the main register of the FCSR automaton to produce 8 (resp. 16) keystream bits with each iteration. The security of F-FCSR was investigated in different directions, and it was recently noted in [8] that an equivalent description exists. It is an open question if this equivalent description results in a simplified structure to be used in a cryptanalytic attack. In the new description (1) only one variable of the main state is updated in each iteration, (2) the memory is very small, but (3) the filter is transformed. We focus our analysis on this alternative description of F-FCSR.

## 2 Theoretical Background

An FCSR can be represented in Fibonacci or Galois architecture, see [6]. In this section, we review the definition and some basic theory from [1, 2, 6, 7] on FCSRs in both representations.

### 2.1 2-Adic Numbers and Periods

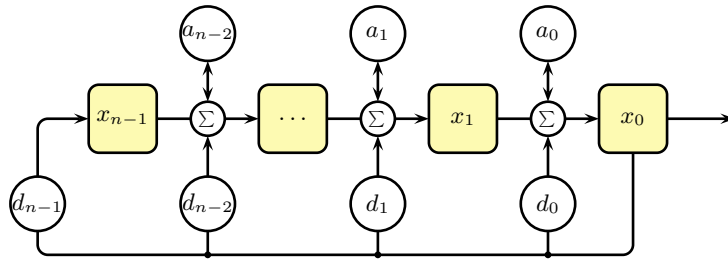
Following the definition in [7], we call a state of a finite state machine (an FCSR, for instance) periodic if, left to run, the machine will return to that same state after a finite number of steps. Similarly, we call a sequence  $u = (u_i)_{i \geq 0}$  (strictly) periodic with period  $T$  if  $u_{i+T} = u_i$  for all  $i \geq 0$ . We call a sequence  $u$  eventually periodic if there exists a  $t \geq 0$  such that  $u' = (u_i)_{i \geq t}$  is periodic. A 2-adic integer is a formal

power series  $\alpha = \sum_{i=0}^{\infty} u_i 2^i$  with  $u_i \in \{0, 1\}$ . The collection of all such formal power series forms the ring of 2-adic numbers. This ring especially contains rational numbers  $p/q$  where  $p$  and  $q$  are integers and  $q$  is odd. Such rational numbers and eventually periodic binary sequences are linked by the following well-known theorem [7].

**Theorem 1.** *There is a one-to-one correspondence between rational numbers  $\alpha = p/q$  (where  $q$  is odd) and eventually periodic binary sequences  $u$  which associates to each such rational number  $\alpha$  the bit sequence  $u = (u_0, u_1, u_2, \dots)$  of its 2-adic expansion. The sequence  $u$  is strictly periodic if and only if  $\alpha \leq 0$  and  $|\alpha| < 1$ .*

## 2.2 Galois FCSRs

*Description.* A Galois FCSR (which is similar to a Galois LFSR) consists of  $n$  binary register cells  $x = (x_0, \dots, x_{n-1})$  with some fixed binary feedback positions  $d = (d_0, \dots, d_{n-1})$ , and  $n-1$  binary memory cells  $a = (a_0, \dots, a_{n-2})$ . We also use the integer representation  $x = \sum_{i=0}^{n-1} 2^i x_i$  (correspondingly for  $d$  and  $a$ ). Starting from an initial configuration  $(x, a)$ ,  $x_0$  is output, and the sums  $\sigma_i = x_{i+1} + a_i d_i + x_0 d_i$  are computed for  $0 \leq i < n$  (with  $x_n = 0, a_{n-1} = 0$ ). Then, the state is updated by  $x_i \leftarrow \sigma_i \pmod 2$  for  $0 \leq i < n$ , and  $a_i \leftarrow \text{div } 2$  for all  $0 \leq i < n-1$ , see Fig. 1.



**Fig. 1.** FCSR with Galois architecture.

*Evolution of the States.* Consider the special case where memory bits of a Galois FCSR are only present on those positions with feedback (which means that the effective number of memory bits is  $l \leq n$ , and  $a$  can only have some restricted values). In this case, the Galois FCSR can be described by the connection integer  $q = 1 - 2d$ . The initial state is denoted  $(x, a)$ , with an associated value  $p = x + 2a$  (assuming that  $x$  is not the all-zero or all-one state). Note that different states  $(x, a)$  may lead to the same  $p$ , *i.e.*, the function to compute  $p$  from  $(x, a)$  is not injective. The sequence generated by the FCSR is the 2-adic expansion of  $p/q$ , *i.e.*, the output sequence depends only on  $p$  and  $q$  [6]. In other words, let  $p^t$  be the state at time  $t$ , with initial state  $p^0 = p$ . Then the Galois FCSR produces  $2p^{t+1} = p^t \pmod q$ , or

$$p^t = 2^{-t} p \pmod q, \quad (1)$$

and the output bit at time  $t$  is  $z^t = p^t \pmod 2$ . It is  $0 \leq p \leq |q|$ , hence the output sequence is periodic (see Th. 1). According to Eq. 1, the period of the output sequence

is the order of 2 modulo  $q$ . The maximum value of the period is  $|q| - 1$  and can only be reached if  $|q|$  is prime [1]. In the case of a maximum-length FCSR, i.e., the period of the output sequence is maximal, the transition graph representing the evolution of the states  $(x, a)$  consists of a main cycle of length  $|q| - 1$  with small paths converging to it. It is known [4] that any state  $(x, a)$  converges to the main cycle (i.e. it synchronizes) after at most  $n + 4$  iterations. Furthermore, a single cycle of the output consists of two half periods (which are binary complements of each other).

### 2.3 Fibonacci FCSRs

*Description.* A Fibonacci FCSR consists of a main register  $y = (y_0, \dots, y_{n-1})$  of  $n$  bits, with some fixed binary feedback taps  $d = (d_0, \dots, d_{n-1})$  and an additional memory register  $b$  of  $l$  bits. Starting from an initial configuration  $(y, b)$ ,  $y_0$  is output, the sum  $\sigma = b + \sum_{i=0}^{n-1} y_i d_{n-i-1}$  is computed, and the registers are updated according to  $y \leftarrow (y_1, \dots, y_{n-1}, \sigma \bmod 2)$  and  $b \leftarrow \sigma \text{ div } 2$ , see Fig. 2. If the Fibonacci FCSR is in a periodic state, then the value of the memory  $b$  is in the range  $0 \leq b < \text{wt}(d)$ , where  $\text{wt}(d)$  denotes the Hamming weight of  $d$ , see [6].

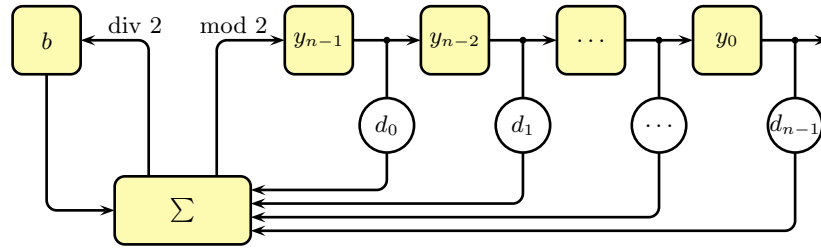


Fig. 2. FCSR with Fibonacci architecture.

*Evolution of the States.* The connection integer is again defined by  $q = 1 - 2d$ , and the state is represented by an integer  $p$ . Then, the output sequence of the Fibonacci FCSR is again the 2-adic expansion of  $p/q$ . However,  $p$  does not correspond to  $y + 2b$  here, but to

$$p = b2^n - \sum_{k=0}^{n-1} \sum_{j=0}^k d_{j-1} y_{k-j} 2^k \quad (2)$$

where  $d_{-1} = -1$ , see [6]. If memory bits of a Galois FCSR are only present on those positions with feedback (i.e., for Galois FCSRs represented by a connection integer  $q$ ), then the Galois FCSR can be mapped to a Fibonacci FCSR (and vice versa) with the same connection integer  $q = 1 - 2d$  such that both produce the same output. Note that a Galois FCSR can be implemented more efficiently than a Fibonacci FCSR since the additions may be carried out in parallel.

### 3 Sequences Produced by a Single Galois Register Cell

In a Galois FCSR, the values  $x_i$  in the main register are modified in each cycle, and not only shifted. Assume an initial state  $(x, a)$  and a connection integer  $q = 1 - 2d$ . Then, according to Th. 4 in [1], there exists some  $p_i$  such that the sequence  $(x_i^t)_{t \geq 0}$  of values produced by a fixed register cell  $i$  in a Galois FCSR corresponds to the 2-adic expansion of  $p_i/q$ . From [3], we know that  $p_i = F_i(x, a) \cdot q + M_i \cdot p$  with  $F_i(x, a) = \sum_{j=i}^{n-1} (x_j + 2a_j)2^{j-i}$  and with constants  $M_i = 2 \sum_{j=i}^{n-1} d_j 2^{j-i}$ . The following proposition is a simple consequence of this for periodic states:

**Proposition 1.** *Consider a maximum-length Galois FCSR with initial state  $(x, a)$  and output sequence  $(p^t \bmod 2)_{t \geq 0}$ , where  $p^0 = x + 2a$ . If  $(x, a)$  is a periodic state, the sequence  $(x_i^t)_{t \geq 0}$  of a fixed register cell  $i$  corresponds to  $(p^{t+s_i} \bmod 2)_{t \geq 0}$  with a phase shift  $s_i = -\log_2(M_i) \bmod q$  and  $M_i = 2 \sum_{j=i}^{n-1} d_j 2^{j-i}$ .*

*Proof.* If  $(x, a)$  is periodic, the 2-adic expansions of  $p_i/q$  have to be strictly periodic for all  $i$ . Th. 1 implies that  $0 \leq p_i < |q|$ , hence  $p_i = p_i \bmod q = M_i \cdot p \bmod q$ . In a maximum-length Galois FCSR, each possible value of  $p_i \bmod q$  is passed after a number of  $s_i$  iterations of  $p$ , hence  $p_i = 2^{-s_i} p \bmod q$ , and we can set  $M_i = 2^{-s_i} \bmod q$ .  $\square$

Note that the phase shifts  $s_i$  are independent of the initial state  $p$  and depend on  $i$  (and  $q$ ) only. Here is an example:

*Example 1.* Consider the toy example of [1] with  $q = -347$ , hence  $n = 8$  and  $d = 174$ . The output of the FCSR is strictly periodic with period  $-q - 1 = 346$ . We find  $M_0 = 1$ ,  $M_1 = 174$ ,  $M_2 = 86$ ,  $M_3 = 42$ ,  $M_4 = 20$ ,  $M_5 = 10$ ,  $M_6 = 4$ ,  $M_7 = 2$ . The phase shifts are  $s_0 = 0$ ,  $s_1 = 1$ ,  $s_2 = 23$ ,  $s_3 = 250$ ,  $s_4 = 67$ ,  $s_5 = 68$ ,  $s_6 = 344$ ,  $s_7 = 345$ .  $\square$

### 4 A Canonical Representative for $[p]$

Note that more than one state  $(x, a)$  may be mapped to  $p \in \mathbb{Z}_{|q|+1}$ . We define an equivalence relation  $\sim$  on the set of FCSR-states in Galois representation by

$$(x, a) \sim (x', a') \Leftrightarrow x + 2a \equiv x' + 2a' \pmod{q}.$$

With the following proposition, we define a canonical representative for the equivalence classes  $[p]$ .

**Proposition 2.** *For a state  $(x, a)$  with  $p = x + 2a$  of a maximum-length Galois FCSR with connection integer  $q$ , the only strictly periodic state in the equivalence class  $[p]$  is the state  $(x', a')$  with  $x'_i = M_i \cdot p \bmod q \bmod 2$  and  $a' = (p - x')/2$ .*

*Proof.* Let  $p = x + 2a$ . We have  $x' + 2a' = x' + 2 \frac{p-x'}{2} = x' + p - x' = p$ , hence  $(x', a') \sim (x, a)$ . In the case  $p = 0$ , we have  $(x, a) = (0, 0) = (x', a')$ , and  $(x^t, a^t) = (0, 0)$  for all  $t$ , so  $(x', a')$  is periodic. Similarly for  $p = |q|$ , the only possible state  $(x, a)$  is  $(2^n - 1, d - 2^{n-1})$ , and this state is periodic [1]. If  $p \neq 0$ , the state transition graph representing the evolution of the states  $(x^t, a^t)$  consists of a main cycle of

length  $|q| - 1$  and paths converging to it. Hence, for each state  $(x, a)$  there exists exactly one equivalent state  $(\tilde{x}, \tilde{a})$  that lies on the main cycle. For this state  $(\tilde{x}, \tilde{a})$ , the sequences  $(\tilde{x}_i^t)_{t \geq 0}$  have to be strictly periodic. Due to Prop. 1, the first bit of the 2-adic expansion of  $\tilde{p}_i/q$  and hence  $x'_i$  is equal to  $\tilde{p}_i \pmod 2$  with  $p_i = M_i \cdot p \pmod q$ . Moreover,  $\tilde{a}$  is uniquely determined by  $\tilde{x}$  and  $p$ , which implies  $(\tilde{x}, \tilde{a}) = (x', a')$ .  $\square$

This suggests to define the state  $(x', a')$  as the canonical representative for the equivalence class  $[x' + 2a']$ . Here is an example:

*Example 2.* Let  $q = -347$ , hence  $n = 8$  and  $d = 174$ . For  $p = 100$ , we find the canonical representative  $(x', a') = (80, 10)$  which is a strictly periodic state.  $\square$

## 5 Analysis of F-FCSR in Fibonacci Representation

We recall the specification of two instances of the F-FCSR family of stream ciphers and present our analysis in Fibonacci representation.

### 5.1 Filtered FCSRs

In [2], the stream cipher F-FCSR-H with security level 80 bits was presented. It consists of a Galois FCSR of size  $n = 160$  and with a memory of size  $l = 82$ . There are  $k = 8$  fixed linear filter functions (applied on the intermediate state bits of the Galois FCSR) to produce 8 keystream bits in each iteration. A similar stream cipher F-FCSR-16 with security level 128 bits was presented, with  $n = 256$ ,  $l = 130$  and  $k = 16$ . According to [1, 3], we can expect the FCSR to be in a periodic state after the key/IV setup has completed. Our observations imply that both versions of F-FCSR can be equivalently described based on a Fibonacci FCSR instead of a Galois FCSR, but with a transformed filter. This transformation can be done in different ways, which gives different scenarios of potential attacks.

### 5.2 Transformation with Nonlinear Filter

If the initialization  $p$  of the Galois FCSR of F-FCSR is known, it can be mapped to an initial state of a Fibonacci FCSR such that both versions produce the same output. The advantage of the Fibonacci representation (from a cryptanalytic point of view) is that only one bit of the main state is modified per iteration, and 8 bits are sent to the keystream. However, this also requires a transformation of the linear filter to obtain the correct keystream: the linear filter of F-FCSR operates on the intermediate states of the Galois FCSR. In order to compute the input of the filter function, we need to compute the values of certain Galois main register cells in each clock cycle:

**Proposition 3.** *The value  $x_i$  of the  $i$ -th cell in the main register of the Galois FCSR can be computed from the (strictly) periodic state  $(y, b)$  of the corresponding Fibonacci FCSR by*

$$x_i = M_i \left( b2^n - \sum_{k=0}^{n-1} \sum_{j=0}^k d_{j-1} y_{k-j} 2^k \right) \pmod q \pmod 2 . \quad (3)$$

*Proof.* We first use Eq. 2 to compute the value of  $p$  that corresponds to the Fibonacci state  $(y, b)$  and then apply Prop. 2 to compute  $p_i$ .  $\square$

Hence, every keystream reveals the sum of several bits given by Eq. 3, but we currently see no way to efficiently exploit these relations.

### 5.3 Transformation with Linear Filter

Given some periodic initialization  $(x, a)$  of a maximum-length Galois FCSR, the sequence of a cell  $i$  corresponds to the FCSR output with a phase shift  $s_i$ , see Prop. 1. Consequently, the F-FCSR keystream can be produced by a linear filter applied on the FCSR output, where the required size of the FCSR output depends on the values of the involved  $s_i$ . The FCSR output can be produced with a Fibonacci FCSR (initialized by the state corresponding to  $p$ ). Alternatively, one could think of an FCSR-combiner with linear filter, where the number of identical FCSRs correspond to the number of filter taps, and where the initial states are not independent, but related according to Prop. 1.

### 5.4 Attack with Linearization

We describe a trivial attack on a Fibonacci FCSR with  $n = 160$ ,  $l = 82$  and with  $k = 8$  linear filters. Initially, there are 160 binary variables (ignoring the memory), and each updated bit is represented by a new variable (ignoring the details of the construction and assuming independence). Each iteration gives another 8 linear equations in these (initial and newly introduced) state variables. The main state can be recovered by solving the system of linear equations, if the number of equations is at least as large as the number of variables. This requires  $r$  iterations, where  $8r \geq 160 + r$ . Consequently,  $r = 23$  iterations are sufficient, or 184 bits of keystream. Gaussian elimination of this system requires a computational effort of about  $184^3$ , which is about  $2^{23}$ . After recovering the main state, one can recover the memory state. If the FCSR is in a periodic state (which can be expected already after the initialization phase), then the effective size of the memory state reduces to 7 bits. Consequently, the memory can be guessed or recovered by FCSR-synthesis, and the whole state can be recovered in about  $2^{30}$  steps and with less than 200 bits of keystream. A similar attack is possible for any other construction of this type with  $k > 1$ .

However, the stream cipher F-FCSR with Fibonacci representation and with linear filters has initially a number of variables which corresponds to the maximum of involved  $s_i$ . In Appendix A, we observe that the phase shifts  $s_i$  for F-FCSR-H are distributed over a significant part of the period of the FCSR output sequence. Depending on the linear filters, the extracted bits to produce one keystream bit may involve the whole cycle of FCSR output. On the other hand, the FCSR-combination generator requires many new variables. Consequently, we expect that the above scenario does not constitute a practical threat to neither of the two F-FCSR instances.

## 6 Conclusion

In this paper we have given a simplified description of the sequences produced by a single cell of a Galois FCSR given the register's initial state is periodic. Additionally

we have shown how to compute for a given state of a maximum length FCSR the unique equivalent periodic state. Based on these observations and the well-known correspondence between Fibonacci and Galois representations of FCSRs, we have proposed several new attack strategies. Currently, our analysis does not lead to an efficient attack, but may be useful as a starting point for further cryptanalytic research.

## Acknowledgments

We would like to thank T. Berger and F. Arnault for their valuable comments.

## References

1. F. Arnault and T. P. Berger, Design and Properties of a New Pseudorandom Generator Based on a Filtered FCSR Automaton. In *IEEE Transactions on Information Theory*, 54(11):1374-1383, 2005.
2. F. Arnault, T. P. Berger, and C. Lauradoux. Update on F-FCSR Stream Cipher. In *eSTREAM, ECRYPT Stream Cipher Project*, Report 2006/025. See also [5].
3. F. Arnault, T. P. Berger, and M. Minier. On the Security of FCSR-based Pseudorandom Generators. In *SASC 2007*.
4. F. Arnault, T. P. Berger, and M. Minier. Some Results on FCSR Automata with Applications to the Security of FCSR-based Pseudorandom Generators. To appear in *IEEE Transactions on Information Theory*, 2008.
5. eSTREAM - The ECRYPT Stream Cipher Project - Phase 3. See [www.ecrypt.eu.org/stream](http://www.ecrypt.eu.org/stream).
6. M. Goresky and A. Klapper. Fibonacci and Galois Representations of Feedback-With-Carry Shift Registers. In *IEEE Transactions on Information Theory*, 48(11):2826-2836, 2002.
7. A. Klapper and M. Goresky. Feedback Shift Registers, 2-Adic Span, and Combiners with Memory. In *Journal of Cryptology*, 10:111-147, 1997.
8. D. Stegemann. Extended BDD-based Cryptanalysis of Keystream Generators. Preproceedings version. In *Selected Areas in Cryptography - SAC 2007*.
9. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. In *J. Symbolic Comput.*, 24(3-4):235-265, 1997.

# A Phase Shifts in F-FCSR-H

$i$	$M_i$	$s_i$
0		1
1	996762295659137507664020805672107518230070043982	1
2	498381147829568753832010402836053759115035021990	1
3	249190573914784376916005201418026879557517510994	1
4	124595286957392188458002600709013439778758755496	1
5	62297643478696094229001300354506719889379377748	1
6	31148821739348047114500650177253359944689688874	1
7	15574410869674023557250325088626679972344844436	1
8	7787205434837011778625162544313339986172422218	1
9	3893602717418505889312581272156669993086211108	1
10	1946801358709252944656290636078334996543105554	1
11	973400679354626472328145318039167498271552776	1
12	486700339677313236164072659019583749135776388	1
13	243350169838656618082036329509791874567888194	1
14	121675084919328309041018164754895937283944096	1
15	60837542459664154520509082377447968641972048	1
16	30418771229832077260254541188723984320986024	1
17	15209385614916038630127270594361992160493012	1
18	7604692807458019315063635297180996080246506	1
19	3802346403729009657531817648590498040123252	1
20	1901173201864504828765908824295249020061626	1
21	950586600932252414382954412147624510030812	1
22	475293300466126207191477206073812255015406	1
23	237646650233063103595738603036906127507702	1
24	118823325116531551797869301518453063753850	1
25	59411662558265775898934650759226531876924	1
26	29705831279132887949467325379613265938462	1
27	14852915639566443974733662689806632969230	1
28	7426457819783221987366831344903316484614	1
29	3713228909891610993683415672451658242306	1
30	1856614454945805496841707836225829121152	1
31	928307227472902748420853918112914560576	1
32	464153613736451374210426959056457280288	1
33	232076806868225687105213479528228640144	1
34	116038403434112843552606739764114320072	1
35	58019201717056421776303369882057160036	1
36	29009600858528210888151684941028580018	1
37	14504800429264105444075842470514290008	1
38	7252400214632052722037921232527145004	1
39	3626200107316026361018960617628572502	1
40	1813100053658013180509480308814286250	1
41	906550026829006590254740154407143124	1
42	453275013414503295127370077203571562	1
43	22663750670725164756385038601785780	1
44	113318753353625823781842519300892890	1
45	56659376676812911890921259650446444	1
46	2832968833840645594546062982523222	1
47	141648441692032279772730314912611610	1
48	7082422084601613986365157456305804	1
49	3541211042300806993182578728152902	1
50	177060521150403496591289364076450	1
51	885302760575201748295644682038224	1
52	442651380287600874147822341019112	1
53	221325690143800437073911170509556	1
54	110662845071900218536955585254778	1
55	55331422535950109268477792627388	1
56	27665711267975054634238896313694	1
57	13832855633987527317119448156846	1
58	6916427816993763658559724078422	1
59	3458213908496881829279862039210	1
60	1729106954248440914639931019604	1
61	864553477124220457319965509802	1
62	432276738562110228659982754900	1
63	216138369281055114329991377450	1
64	108069184640527557164995688724	1
65	54034592320263778582497844362	1
66	27017296160131889291248922180	1
67	13508648080065944645624461090	1
68	6754324040032972322812230544	1
69	3377162020016486164106115272	1
70	1688581010008243080703057636	1
71	844290505004121540351528818	1
72	422145252502060770175764408	1
73	211072626251030385087882204	1
74	105536313125515192543941102	1
75	52768156562757596271970550	1
76	26384078281378798135985274	1
77	13192039140689399067992636	1
78	6596019570344699533996318	1
79	3298009785172349766998158	1
80	1649004892586174883499078	1
973635050333243268578935491582393694135630715055	1	
483426367822718686544121001295277675729147306272	1	
927380559681454790408764863402966045946752057201	1	
927380559681454790408764863402966045946752057202	1	
927380559681454790408764863402966045946752057203	1	
758344865222122650233177326466087773251292785576	1	
758344865222122650233177326466087773251292785577	1	
911127416851730251991600045466358366053055302457	1	
911127416851730251991600045466358366053055302458	1	
1832842846520994303195629737505467073913566838161	1	
1832842846520994303195629737505467073913566838162	1	
1832842846520994303195629737505467073913566838163	1	
394438960334467105809551664918698950982629374595	1	
394438960334467105809551664918698950982629374596	1	
394438960334467105809551664918698950982629374597	1	
394438960334467105809551664918698950982629374598	1	
394438960334467105809551664918698950982629374599	1	
1542579694750750487223162750505798481890705347739	1	
1542579694750750487223162750505798481890705347740	1	
1380086804388631757659189018767114120731432626002	1	
1380086804388631757659189018767114120731432626003	1	
1078802727948333585713216285980983240503278571366	1	
1382207965002592774152651594012759930846379979975	1	
167993048606343931454309223372459315774200884429	1	
167993048606343931454309223372459315774200884430	1	
91952241676936842617352143022652755453337077056	1	
598587450490682512240830827130922261186129784430	1	
881824337976372067087447061586008363041219393986	1	
132415388929517392410873105359844727934804027497	1	
132415388929517392410873105359844727934804027498	1	
132415388929517392410873105359844727934804027499	1	
132415388929517392410873105359844727934804027500	1	
132415388929517392410873105359844727934804027501	1	
132415388929517392410873105359844727934804027502	1	
132415388929517392410873105359844727934804027503	1	
1198640149747527579573484362590310318071396821475	1	
1198640149747527579573484362590310318071396821476	1	
1198640149747527579573484362590310318071396821477	1	
1130256754959843418654086368612920094144856598582	1	
268857509327548734833816579297946611448206934269	1	
268857509327548734833816579297946611448206934270	1	
1195954573006431943268969640901304511809238045084	1	
1195954573006431943268969640901304511809238045085	1	
1028874585295389927840725907041052247520293323025	1	
1028874585295389927840725907041052247520293323026	1	
5810253321407188422766400546212175394594565511	1	
1675694188246351780738859392351735484355722203869	1	
1675694188246351780738859392351735484355722203870	1	
9509255556141166284424667032237721509991621979332	1	
10685793473170484823722195300901484055107946725	1	
10685793473170484823722195300901484055107946726	1	
10685793473170484823722195300901484055107946727	1	
10685793473170484823722195300901484055107946728	1	
1406532195309567246060932291519468415260515898241	1	
1406532195309567246060932291519468415260515898242	1	
1964984368983557569814988833497375264018907336049	1	
1270198753462812720961865489549333653794573339798	1	
1838932638186082761289211962663277341667652316445	1	
982736070215157474363678017305669439690426851503	1	
982736070215157474363678017305669439690426851504	1	
1161460792531421893077724313263857656434425744024	1	
1161460792531421893077724313263857656434425744025	1	
700806390342822442537205805529567734204501691938	1	
700806390342822442537205805529567734204501691939	1	
1631363260511310085335173213145859166090307194118	1	
1631363260511310085335173213145859166090307194119	1	
143345025729670374390994110649096508752064896813	1	
143345025729670374390994110649096508752064896814	1	
143345025729670374390994110649096508752064896815	1	
143345025729670374390994110649096508752064896816	1	
1812593907843623049081724725325521652323105172048	1	
1812593907843623049081724725325521652323105172049	1	
1812593907843623049081724725325521652323105172050	1	
981383091417729418629940931838441194603762007067	1	
189662212182648400724334277386037910129032616322	1	
1348771746331344830369588596167000270475600205149	1	
1348771746331344830369588596167000270475600205150	1	
1659501931738906067175588851301653064787885654615	1	
956096983760354433954700963667576369842916849068	1	

$i$	$M_i$	$s_i$
81	824502446293087441749538	1498426256550790252009012862495220093171963833409
82	412251223146543720874768	1167664495785406969076088708700837365815249345203
83	206125611573271860437384	1167664495785406969076088708700837365815249345204
84	103062805786635930218692	1167664495785406969076088708700837365815249345205
85	51531402893317965109346	1167664495785406969076088708700837365815249345206
86	25765701446658982554672	1646129649588890386644127847613781912620365107705
87	12882850723329491277336	1646129649588890386644127847613781912620365107706
88	6441425361664745638668	1646129649588890386644127847613781912620365107707
89	322071268083272819334	1646129649588890386644127847613781912620365107708
90	1610356340416186409666	1161229933682105586614366460627128560240732929325
91	805178170208093204832	1197759154157032614248093208226604498512578715003
92	402589085104046602416	1197759154157032614248093208226604498512578715004
93	201294542552023301208	1197759154157032614248093208226604498512578715005
94	100647271276011650604	1197759154157032614248093208226604498512578715006
95	50323635638005825302	1197759154157032614248093208226604498512578715007
96	25161817819002912650	1593445083285452713917185473568444248416309333642
97	12580908909501456324	162547888417125655487616274954752250782796062235
98	6290454454750728162	162547888417125655487616274954752250782796062236
99	3145227227375364080	471463272834857769097454917438159446026869143632
100	1572613613687682040	471463272834857769097454917438159446026869143633
101	786306806843841020	471463272834857769097454917438159446026869143634
102	393153403421920510	471463272834857769097454917438159446026869143635
103	196576701710960254	122127515941488347041137458469580126813852051502
104	98288350855480126	551854766844849607680694091431852344960732913429
105	49144175427740062	4665040794063680979996927426269763369304377444
106	24572087713870030	1240643188890939020180474827163507200690576310993
107	12286043856935014	1978011465630120594285659762041548700534648617616
108	6143021928467506	54579292790000112365049062040095915280474292502
109	3071510964233752	844150197214213071024718567655890697486633021540
110	1535755482116876	844150197214213071024718567655890697486633021541
111	76787741058438	844150197214213071024718567655890697486633021542
112	383938870529218	557637422766867795276309931178007150017200602430
113	191969435264608	1565882931673033818899312238175668093796584237228
114	95984717632304	1565882931673033818899312238175668093796584237229
115	47992358816152	1565882931673033818899312238175668093796584237230
116	23996179408076	1565882931673033818899312238175668093796584237231
117	11998089704038	1565882931673033818899312238175668093796584237232
118	5999044852018	501486839282041163609551289161767535545443168053
119	2999522426008	1313503603375490017010962119938407460872811659507
120	1499761213004	1313503603375490017010962119938407460872811659508
121	749880606502	1313503603375490017010962119938407460872811659509
122	374940303250	1684447776752483614963335703581481623217207159611
123	187470151624	1484687500936286075648085269921694888197512769230
124	93735075812	1484687500936286075648085269921694888197512769231
125	46867537906	1484687500936286075648085269921694888197512769232
126	23433768952	1451559215416067296038582387282626695223606761513
127	11716884476	1451559215416067296038582387282626695223606761514
128	5858442238	1451559215416067296038582387282626695223606761515
129	2929221118	182876978082684459121621639149011648319732519529
130	1464610558	99202745599118655970514966864568238257092522396
131	732305278	545823687214166349470755781577766892092712860848
132	366152638	767977333379175621402870184558978911372840706065
133	183076318	165446774782834645146215015040220160602446648916
134	91538158	70950729504311392655242448023355860933570359107
135	45769078	104946404942416962278090928473405215375855920656
136	22884538	1464151269091629247350729516177016072013085324065
137	11442268	661175221396459982950623788526869865803009201192
138	5721134	661175221396459982950623788526869865803009201193
139	2860566	190289626139258205116001182010073438227019457536
140	1430282	1780490613120718555124908224957355127482877169102
141	715140	611172924250787254381655617179120854673077830577
142	357570	611172924250787254381655617179120854673077830578
143	178784	120283631919932099343969398275137791582880267466
144	89392	120283631919932099343969398275137791582880267467
145	44696	120283631919932099343969398275137791582880267468
146	22348	120283631919932099343969398275137791582880267469
147	11174	120283631919932099343969398275137791582880267470
148	5586	602583441997436309910094724102711960285338500511
149	2792	1832544807064618537524150113667471641952149221494
150	1396	1832544807064618537524150113667471641952149221495
151	698	1832544807064618537524150113667471641952149221496
152	348	1862404951884868062993939036882416972524206811785
153	174	1862404951884868062993939036882416972524206811786
154	86	578282337176907917514878905492233552372712125524
155	42	126263351870613901800905401618416641258406191463
156	20	643217672317509420866297326619549776274714793075
157	10	643217672317509420866297326619549776274714793076
158	4	1993524591318275015328041611344215036460140087960
159	2	1993524591318275015328041611344215036460140087961