Equivalent Representations of the F-FCSR Keystream Generator

Simon Fischer[1], Willi Meier[1], and Dirk Stegemann[2]

[1] FHNW, 5210 Windisch (Switzerland)
[2] 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 α the bit sequence $u = (u_0, u_1, u_2, \ldots)$ 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 $x = (x_0, \ldots, x_{n-1})$ with some fixed binary feedback positions $d = (d_0, \ldots, d_{n-1})$, and $n-1$ binary memory cells $a = (a_0, \ldots, a_{n-2})$. 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 $x_i \leftarrow \sigma_i \mod 2$ for $0 \leq i < n$, and $a_i \leftarrow \text{div } 2$ for all $0 \leq i < n-1$, see Fig. 1.

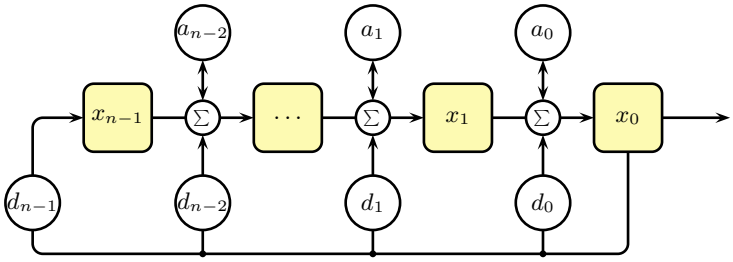

Fig. 1. FCSR with Galois architecture.

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 $2p^{t+1} = p^t \mod q$, or

$$p^t = 2^{-t} p \mod q \,, \tag{1}$$

and the output bit at time t is $z^t = p^t \mod 2$. 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 $y = (y_0, \ldots, y_{n-1})$ of n bits, with some fixed binary feedback taps $d = (d_0, \ldots, d_{n-1})$ 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 $y \leftarrow (y_1, \ldots, y_{n-1}, \sigma \mod 2)$ and $b \leftarrow \sigma \operatorname{div} 2$, see Fig. 2. If the Fibonacci FCSR is in a periodic state, then the value of the memory b is in the range $0 \leq b < \mathrm{wt}(d)$, where $\mathrm{wt}(d)$ denotes the Hamming weight of d, see [6].

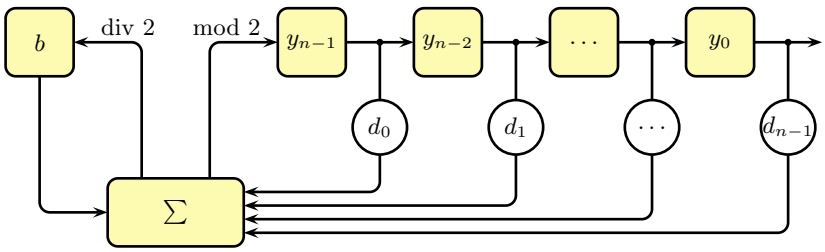

Fig. 2. FCSR with Fibonacci architecture.

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

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

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 $(p^t \mod 2)_{t\geq 0}$, 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 $(p^{t+s_i} \mod 2)_{t\geq 0}$ with a phase shift $s_i = -\log_2(M_i) \mod q$ 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 $p_i = p_i \mod q = M_i \cdot p \mod q$. In a maximum-length Galois FCSR, each possible value of $p_i \mod q$ is passed after a number of s_i iterations of p, hence $p_i = 2^{-s_i}p \mod q$, and we can set $M_i = 2^{-s_i} \mod q$. □

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 $s_0 = 0$, $s_1 = 1$, $s_2 = 23$, $s_3 = 250$, $s_4 = 67$, $s_5 = 68$, $s_6 = 344$, $s_7 = 345$. □

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

$$(x, a) \sim (x', a') \Leftrightarrow x + 2a \equiv x' + 2a' \mod q\ .$$

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 $x'_i = M_i \cdot p \mod q \mod 2$ 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 $\tilde{p}_i \mod 2$ with $p_i = M_i \cdot p \mod q$. Moreover, $\tilde{a}$ is uniquely determined by $\tilde{x}$ and p, which implies $(\tilde{x}, \tilde{a}) = (x', a')$. □

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. □

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*

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

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. □

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.
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	0
1	99676229565913750766402080567210751823007004398 2	1
2	49838114782956875383201040283605375911503502199 0	97363505033324326857893549158239369413563071505 5
3	24919057391478437691600520141802687955751751099 4	48342636782271868654412100129527767572914730627 2
4	12459528695739218845800260070901343977875875549 6	92738055968145479040876486340296604594675205720 1
5	6229764347869609422900130035450671988937977748	92738055968145479040876486340296604594675205720 2
6	3114882173934804711450065017725335994468988874	92738055968145479040876486340296604594675205720 3
7	1557441086967402355725032508862667997234484443 6	75834486522212265023317732646608777325129278557 6
8	7787205434837011778625162544313339986172422218	75834486522212265023317732646608777325129278557 7
9	3893602717418505889312581272156669993086211108	91112741685173025199160004546635836605305545 7
10	1946801358709252944656290636078334996543105554	91112741685173025199160004546635836605305530245 8
11	973400679354626472328145318039167498271552776	18328428465209943031956297375054670739135668381 61
12	486700339677313236164072659019583749135776388	18328428465209943031956297375054670739135668381 62
13	243350169838656618082036329509791874567888194	18328428465209943031956297375054670739135668381 63
14	121675084919328309041018164754895937283944096	39443896033446710580955166491869895098262937459 5
15	60837542459664154520509082377447968641972048	39443896033446710580955166491869895098262937459 6
16	30418771229832077260254541188723984320986024	39443896033446710580955166491869895098262937459 7
17	15209385614916038630127270594361992160493012	39443896033446710580955166491869895098262937459 8
18	7604692807458019315063635297180996080246506	39443896033446710580955166491869895098262937459 9
19	3802346403729009657531817648590498040123252	15425796947507504872231627505057984818907053477 39
20	1901173201864504828765908824295249020061626	15425796947507504872231627505057984818907053477 40
21	950586600932252414382954412147624510030812	13800868043886317576591890187671141207314326260 02
22	475293300466126207191477206073812255015406	13800868043886317576591890187671141207314326260 03
23	237646652330631035957386030369061275077 02	10788027279483335857132162859809832405032785713 66
24	118823325116531551797869301518453063753850	13822079650025927741526515940127599308463799799 75
25	59411662558265775898934650759226531876924	16799304860634393145430922337245931577420088442 9
26	29705831279132887949467325379613265938462	16799304860634393145430922337245931577420088443 0
27	14852915639566443974733662689806632969230	91952241676936842617352143022659275545333707705 6
28	7426457819783221987366831344903316484614	59858745049068251224083082713092226118612978443 0
29	3713228909891610993683415672451658242306	88182433797637206708744706158600836304121939398 6
30	1856614454945805496841707836225829121152	13241538892951739241087310535984472793480402749 7
31	928307227472902748420853918112914560576	13241538892951739241087310535984472793480402749 8
32	464153613736451374210426959056457280288	13241538892951739241087310535984472793480402749 9
33	232076806868225687105213479528228640144	13241538892951739241087310535984472793480402750 0
34	116038403434112843552606739764114320072	13241538892951739241087310535984472793480402750 1
35	58019201717056421776303369882057160036	13241538892951739241087310535984472793480402750 2
36	29009600858528210888151684941028580018	13241538892951739241087310535984472793480402750 3
37	14504800429264105444075842470514290008	11986401497475275795734843625903103180713968214 75
38	7252400214632052722037921235257145004	11986401497475275795734843625903103180713968214 76
39	3626200107316026361018960617628572502	11986401497475275795734843625903103180713968214 77
40	1813100053658013180509480308814286250	11302567549598434186540863686129200941444565985 82
41	906550026829006590254740154407143124	26885750932754873483381657929794661144820693426 9
42	453275013414503295127370077203571562	26885750932754873483381657929794661144820693427 0
43	226637506707251647563685038601785780	11959545730064319432689696409013045118092380450 84
44	113318753353625823781842519300892890	11959545730064319432689696409013045118092380450 85
45	56659376676812911890921259650446444	10288745852953899278407259070410522475202933230 25
46	28329688338406455945460629825223222	10288745852953899278407259070410522475202933230 26
47	14164844169203227972730314912611610	58102533214071884227664005462121753945994456551 1
48	7082422084601613986365157456305804	16756941882463517807388593923517354843557222038 69
49	3541211042300806993182578728152902	16756941882463517807388593923517354843557222038 70
50	1770605521150403496591289364076450	95092555561411662844246670322377215099916197933 2
51	885302760575201748295644682038224	10685793473170484823722195300901484055107946725	
52	442651380287600874147822341019112	10685793473170484823722195300901484055107946726	
53	221325690143800437073911170509556	10685793473170484823722195300901484055107946727	
54	110662845071900218536955585254778	10685793473170484823722195300901484055107946728	
55	553314225359501092684777926273 88	14065321953095672460609322915194684152605158982 41
56	276657112679750546342388963136 94	14065321953095672460609322915194684152605158982 42
57	138328556339875273171194481568 46	19649843689835575698149888334973752640189073360 49
58	691642781699376365855972407842 2	12701987534628127209618654895493336537945733397 98
59	345821390849688182927986203921 0	18389326381860827612892119626632773416676523144 45
60	172910695424844091463993101960 4	98273607021515747436367801730566943969042685150 3
61	864553477124220457319965509802	98273607021515747436367801730566943969042685150 4
62	432276738562110228659982754900	11614607925314218930777243132638576564344254024
63	216138369281055114329991377450	11614607925314218930777243132638576564344254025
64	108069184640527557164995688724	70080639034282244253720580552956773420450169193 8
65	54034592320263778582497844362	70080639034282244253720580552956773420450169193 9
66	27017296160131889291248922180	16313632605113100853351732131458591660903071941 18
67	13508648080065944645624461090	16313632605113100853351732131458591660903071941 19
68	6754324040032972322812230544	14334502572967037439099411064909650875206489681 3
69	3377162020016486161406115272	14334502572967037439099411064909650875206489681 4
70	1688581010008243080703057636	14334502572967037439099411064909650875206489681 5
71	844290505004121540351528818	14334502572967037439099411064909650875206489681 6
72	422145252502060770175764408	18125939078436230490817247253255216523231051720 48
73	211072626251030385087882204	18125939078436230490817247253255216523231051720 49
74	105536313125515192543941102	18125939078436230490817247253255216523231051720 50
75	52768156562757596271970550	98138309141772941862994093183844119460376200706 7
76	26384078281378798135985274	18966221218264840072433427738607291012903261632 2
77	13192039140689399067992636	13487717463313448303695885961670002704756002051 49
78	6596019570344699533996318	13487717463313448303695885961670002704756002051 50
79	3298009785172349766998158	16595019317389606071755888513016530647878856546 15
80	1649004892586174883499078	95606968376035443395470096366757636984291684906 8

i	M_i	s_i
81	824502446293087441749538	14984262565507902520090128624952200931719638334096
82	412251223146543720874768	11676644957854069690760887087008373658152493452032
83	206125611573271860437384	11676644957854069690760887087008373658152493452048
84	103062805786635930218692	11676644957854069690760887087008373658152493452056
85	51531402893317965109346	11676644957854069690760887087008373658152493452064
86	257657014466589825546720	16461296495888903866441278476137819126203651077056
87	128828507233294912773360	16461296495888903866441278476137819126203651077064
88	64414253616647456386680	16461296495888903866441278476137819126203651077072
89	32207126808323728193340	16461296495888903866441278476137819126203651077080
90	16103563404161864096660	11612299336821055866143664606271285602407329293250
91	8051781702080932048320	11977591541570326142480932082266044985125787150032
92	4025890851040466024160	11977591541570326142480932082266044985125787150040
93	2012945425520233012080	11977591541570326142480932082266044985125787150056
94	1006472712760116506040	11977591541570326142480932082266044985125787150064
95	503236356380058253020	11977591541570326142480932082266044985125787150072
96	251618178190029126500	15934450832854527139171854735684442484163093336420
97	125809080950145632400	16254788841712565548761627495475225078276960622350
98	62904544547507281620	16254788841712565548761627495475225078276960622360
99	31452272273753640800	47146327283485776909745491743815944602686914363200
100	15726136136878620400	47146327283485776909745491743815944602686914363300
101	7863068068438410200	47146327283485776909745491743815944602686914363400
102	3931534034219205100	47146327283485776909745491743815944602686914363500
103	1965767017109602540	12212755159414883470411374584695801268138520515020
104	982883508554801260	55185476684484960768069409143185234496073291342900
105	491441754277400620	46650407940636809799969274262697633693043774445000
106	245720877138700300	12406431888909390201804748271635072006905763109930
107	122860438569350140	19780114656301205942856597620415487005346486176160
108	61430219284675060	54579292790000112365049062040095915280474023920200
109	30715109642337520	84415019721421307102471856765589069748663302154000
110	15357554821168760	84415019721421307102471856765589069748663302154100
111	7678777410584380	84415019721421307102471856765589069748663302154200
112	3839388705292180	55763742276686779527630993117800715001720060243000
113	1919694352646080	15658829316730338188993122381756680937965842372280
114	959847176323040	15658829316730338188993122381756680937965842372290
115	479923588161520	15658829316730338188993122381756680937965842372300
116	239961794080760	15658829316730338188993122381756680937965842372310
117	119980897040380	15658829316730338188993122381756680937965842372320
118	59990448520180	50148683928204116360955128916176753554544316805300
119	29995224260080	13135036033754900170109621199384074608728116595070
120	14997612130040	13135036033754900170109621199384074608728116595080
121	7498806065020	13135036033754900170109621199384074608728116595090
122	3749403032500	16844477767524836149633357035814816232172071596110
123	1874701516240	14846875009362860756480852699216948881975127692300
124	937350758120	14846875009362860756480852699216948881975127692310
125	468675379060	14846875009362860756480852699216948881975127692320
126	234337689520	14515592154160672960385823872826266952236067615130
127	117168844760	14515592154160672960385823872826266952236067615140
128	58584422380	14515592154160672960385823872826266952236067615150
129	29292211180	18287697808268445912162163914901164831973251952900
130	14646105580	99202745599118655970514966864568238257092522396000
131	7323052780	54582368721416634947075578157776689209271286084800
132	3661526380	76797733337917562140287018455897891137284070606500
133	1830763180	16544677478283464514621501504022016060244664891600
134	915381580	70950729504311392655242448023355860933570359107000
135	457690780	10494640494241696227809092847340521537585592065600
136	228845380	14641512690916292473507295161770160702130853240650
137	114422680	66117522139645998295062378852686986580300920119200
138	57211340	66117522139645998295062378852686986580300920119300
139	28605660	19028962613925820511600118201007343822701945753600
140	14302820	17804906131207185551249082249573551274828771691020
141	7151400	61117292425078725438165561717912085467307783057700
142	3575700	61117292425078725438165561717912085467307783057800
143	1787840	12028363191993209934396939827513779158288026746600
144	893920	12028363191993209934396939827513779158288026746700
145	446960	12028363191993209934396939827513779158288026746800
146	223480	12028363191993209934396939827513779158288026746900
147	111740	12028363191993209934396939827513779158288026747000
148	55860	60258344199743630991009472410271196028533850051100
149	27920	18325448070646185375241501136674716419521492214940
150	13960	18325448070646185375241501136674716419521492214950
151	6980	18325448070646185375241501136674716419521492214960
152	3480	18624049518848680629939390368824169725242068117850
153	1740	18624049518848680629939390368824169725242068117860
154	870	57828233717690791751487890549223355237271212552400
155	420	12626335187061390180090540161841664125840619146300
156	200	64321767231750942086629732661954977627471479307500
157	100	64321767231750942086629732661954977627471479307600
158	40	19935245913182750153280416113442150364601400879600
159	20	19935245913182750153280416113442150364601400879610