ELSEVIER Applied Mathematics and Computation 143 (2003) 165–172

APPLIED MATHEMATICS AND COMPUTATION

www.elsevier.com/locate/amc

3-Step Fibonacci series modulo *m*

Engin Özkan [a,*], Hüseyin Aydın [a], Ramazan Dikici [b]

[a] *Atatürk Üniversitesi, Fen Edebiyat Fak. Matematik Böl. 25240 Erzurum, Turkey*

[b] *Atatürk Üniversitesi, K.Karabekir Eğitim Fak. Matematik Eğitimi Böl. 25240, Erzurum, Turkey*

Abstract

We have proved two original theorem concerning Wall number of the the 3-step Fibonacci sequences. We give five conjectures concerning 3-step Fibonacci sequence. Furthermore, we also give a computer verification of those conjectures for the primes less than 5×10^5.

© 2002 Elsevier Science Inc. All rights reserved.

Keywords: Fibonacci sequence; Wall number; Fibonacci recurrence

1. Introduction

Let G be finite group. We define a family of recurrences, parameterized by natural numbers n, via equations

$$x_i = x_{i-1}, x_{i-2}, \ldots, x_{i-n} \quad (R_n).$$

We fix $n > 1$. We may 'start' the recurrence with any initial data $g_0, g_1, \ldots, g_{n-1}$ and then the recurrence will define a periodic bi-infinite sequence (g_i) indexed by the integers. We use the loop to describe a bi-infinite sequence satisfying the recurrence. Notice that, if $\alpha \in \mathbb{Z}$, then putting $h_i = g_{i+\alpha}$ for $0 \leqslant i < n$ gives another set of initial data. The recurrence R_n then gives us another loop (h_i) of G. Notice that (h_i) is just (g_i) shifted through α steps. We say that (h_i) is a rotation of (g_i).

The fundamental period of a loop is clearly a significant number, and we call it Wall's number after a Pioneer in this area. Following Wall [1], we shall use

* Corresponding author.
E-mail address: eozkan@atauni.edu.tr (E. Özkan).

0096-3003/02/$ - see front matter © 2002 Elsevier Science Inc. All rights reserved.
doi:10.1016/S0096-3003(02)00360-0

the letter k to describe this period. Wall investigated the recurrence R_2 in finite cyclic groups. This subject immediately reduces to the study of cyclic groups of prime power order. Winson was particularly interested in ranks of apparition in ordinary Fibonacci sequences [2]. In the mid eighties, Wilcox extended the problem to Abelian groups [3]. Prolific co-operation of Campbell et al. expanded the theory to some finite simple groups [4]. Ryba constructed and analyzed a pair of sequences of representations of the symmetric groups [5].

In the recent years, there has been much interest in applications of Fibonacci numbers and sequences. Takahashi gives a fast algorithm which is based on the product of Lucas number to compute large Fibonacci numbers [6]. Fibonacci sequences have been an interesting subject in applied mathematics. West has shown using transfer matrices that the number $|S_n(123, 3214)|$ of permutations avoiding the patterns 123 and 3214 is the Fibonacci number F_{2n} [7].

Aydın and Smith proved in [8] that the lengths of ordinary 2-step Fibonacci sequences are equal to the lengths of the 2-step Fibonacci recurrences in finite nilpotent groups of nilpotency class 4 and exponent a prime number p. Dikici and Işık investigated the similar problem for modular group and proved theorems concerning the periodicity of 2-step Fibonacci sequences constructed by two generating elements of modular group and these sequences are indeed the periodic although the modular group has order infinity [9]. This work has been generalized to cover the general recurrences in modular group [10].

One of the latest works in this area is [11] where it is shown that for the 3-step general Fibonacci recurrence and any finite p-group of exponent p and nilpotency class 2, the length of a fundamental period of any loop satisfying the recurrence must divide the period of the ordinary 3-step general Fibonacci sequence in the field $GF(p)$.

The inquiry is concerned with determining the length of the recurring series obtained by reducing a Fibonacci series by a modulo m. The problem arose in connection with a method for generating random numbers, but it turned out to be unexpectedly intricate, and so quickly became of interest in its own right. The function studied (length of period as a function of starting values and modulus) exhibits quite a few apparent properties which are established here.

Wall distinguishes the special loop $s = (s_i)$ defined by the recurrence $s_0 = 0$ and $s_1 = 1$ in $\mathbb{Z}/p^n\mathbb{Z}$. Let $k(s, p^n)$ denote the fundamental period of s.

Theorem 1 (D.D. Wall [1]). *The number $k(s, p^n)$ divides $k(s, p)p^{n-1}$, and the two quantities are equal provided $k(s, p) \neq k(s, p^2)$.*

Wall goes on to conjecture that for all primes p, we always have $k(s, p) \neq k(s, p^2)$. He announced that he had verified this result for all primes

$p < 10^4$. We know by [12] that this is indeed the case for all primes $p < 10^8$. This work has also been a recent one in this area and proves that short loops must be geometric for the 3-step Fibonacci recurrences in H, the additive group of the finite field $GF(p^n)$.

We summarize some of Wall's results in the following, using a group setting for convenience.

Theorem 2 (D.D. Wall [1]). *In* $\mathbb{Z}_m$, *the following hold*:

(1) *If* p *is a prime and* $p = 10x \pm 1$, *then* $k|(p-1)$.
(2) *If* p *is a prime and* $p = 10x \pm 3$, *then* $k|(2p+2)$.
(3) *If* p *is a prime and* $p = 10x \pm 3$, *then* $h(p^e) = k|(p^e)$.

Corollary (D.D. Wall [1]). *If* $p = 10x \pm 3$, *then* $k \equiv 0 (\text{mod } 4)$.

Now, let $s = (s_1)$ denote the ordinary 3-step Fibonacci sequence in $GF(p)$ defined by the recurrence $s_{i+3} = s_i + s_{i+1} + s_{i+2}$ and the initial data $s_0 = 0$, $s_1 = 0$ and $s_2 = 1$. This is a bi-infinite periodic sequence or loop indexed by the integers. The shortest period of this sequence is called the fundamental period and it will be denoted by k.

Example. The values of $s_n (\text{mod } 7)$ are 0, 0, 1, 1, 2, 4, 0, 6, 3, 2, 4, 2, 1, 0, 3, 4, 0, 0, 4, 4, 1, 2, 0, 3, 5, 1, 2, 1, 4, 0, 5, 2, 0, 0, 2, 2, 4, 1, 0, 5, 6, 4, 1, 4, 2, 0, 6, 1, 0, 0, 1, ... and then repeat; so $k(7) = 48$. We are curious as to the relation between the number 48 and the number 7.

Theorem 3. *Let* f_n *be* 3*-step Fibonacci sequence. Then* $f_n (\text{mod } m)$ *forms a simply periodic series. That is, the series is periodic and repeats by returning to its starting values.*

Proof. The series repeats because there are only a finite number m^3 of trios of terms possible, and the recurrence of a trios results in recurrence of all following terms. From the defining relation we have $f_{n-2} = f_{n+1} - f_n - f_{n-1}$ so if $f_{t+1} \equiv f_{s+1}, f_t \equiv f_s$ and $f_{t-1} \equiv f_{s-1} (\text{mod } m)$, then $f_{t-2} \equiv f_{s-2}, \ldots, f_{t-s+2} \equiv f_2, f_{t-s+1} \equiv f_1$ and $f_{t-s} \equiv f_0$, so that the series is simply periodic. □

Corollary. $s_k \equiv 0$ *and* $s_{k+1} \equiv 0$ (mod m)

A direct consequence of Theorem 3.

Theorem 4. *If m has the prime factorization $m = \prod p_i^{e_i}$ and if h_i denotes the length of the period of $f_n(\mathrm{mod}\ p_i^{e_i})$, then $h = \mathrm{lcm}[h_i]$, the least common multiple of the h_i.*

Proof. The statement, "h_i is the length of the period of $f_n(\mathrm{mod}\ p_i^{e_i})$", implies that the series $f_n(\mathrm{mod}\ p_i^{e_i})$ repeats only after blocks of length dh_i; and the statement, "h is the length of the period of $f_n(\mathrm{mod}\ m)$", implies that $f_n(\mathrm{mod}\ p_i^{e_i})$ repeats after h terms for all values of i. Therefore h is of the form dh_i for all values of i, and since any such number gives a period of $f_n(\mathrm{mod}\ m)$, we conclude that $h = \mathrm{lcm}[h_i]$. □

In view of Theorem 4, we may henceforth assume that m is of the form $m = p^e$.

Let us consider the more general recurrences written multiplicatively as

$$x_i = x_{i-1}^{a_1}, x_{i-2}^{a_2}, \ldots, x_{i-n}^{a_n}$$

or additively as

$$x_i = \sum_{r=1}^{n} a_r x_{i-r}.$$

The exponents/coefficients are deemed to be integers. Such a recurrence may not be so well behaved as (R_n), for it may be singular in a particular group. This means that initial data may not define a unique bi-infinite periodic sequence; the problem arises when attempting to extend the sequence through negative integer subscripts. Certainly all is well if $a_n \in \{1, -1\}$. Equally well, if we are working in a p-group all is well provided $\mathrm{lcm}(p, a_n) = 1$.

We now press on to discuss the recurrences R_3 and R_4. We work in the additive group H of the a finite field $GF(p^n)$.

Let the standard loop s begin (0,0,1), and let its period be $k_3(p)$, written as k in this paper. As before, the period of any loop must divide k for the usual reasons.

Theorem 5. *Short loop must be geometric for the* 3*-step Fibonacci recurrence in H, the additive group of the finite field $GF(p^n)$* [12].

The situation here is more complex than in the 2-step case; it is possible for all three roots of the $x^3 - x^2 - x - 1$ to give rise to genuine short loops. This kind of loops are called golden loops. The first few instances of this phenomenon are given in [12] as follows:

Prime	Golden loop Uzunluğu	Wall number
4481	2240	4480
	640	
	896	
4621	84	4620
	660	
	2310	
6917	364	6916
	532	
	3458	
14,281	595	4760
	680	
	952	

Table 1

p (p is a prime number)	k (Wall's number of 3-step Fibonacci sequence)
83	287
101	680
173	2494
197	3234
211	5565
439	6424
491	10,045
571	40,755
593	3256
613	46,971
653	22,477
677	11,752
739	22,755
821	28,085
857	61,204
977	136,501
1019	43,265
1063	70,623
1151	5520
1289	12,040
1531	58,599
1553	14,356
1579	207,770
1741	32,611
1777	150,368
1871	500,359
1913	304,964

We now give a couple of conjectures similar to Theorem 2 (D.D. Wall [1]).

Conjecture 1. *If p is a prime and $k < p$, then $k|(p-1)$.*

Conjecture 2. *If p is a prime and $k \equiv 0 (\mathrm{mod}\ 2)$, then $(p \pm 1)|k$.*

Conjecture 3. *If p is a prime and $k \equiv 1 (\mathrm{mod}\ 2)$, then $(p \pm 1)|(k-1)$ or $p|(k-1)$.*

Truths of those are determined by a computer code written in MAPLE and FORTRAN. We have lots of data for various of primes less than 5×10^5. But we give all the prime numbers up to 2000 in Table 1 for which those conjectures are not satisfied.

In addition, Table 2 shows some primes for which the conjectures are certainly true.

We can give the following conjecture for n-step Fibonacci sequences where n is an even positive integer.

Table 2

p (p is a prime number)	k (Wall's number of 3-step Fibonacci sequence)	Results
5	31	$p\|(k-1)$
13	168	$(p-1)\|k$
23	553	$p\|(k-1)$
67	1519	$(p-1)\|(k-1)$
107	1272	$(p-1)\|k$
179	32,221	$p\|(k-1)$
241	29,040	$(p-1)\|k$
317	100,807	$p\|(k-1)$
389	151,711	$p\|(k-1)$
557	103,416	$(p-1)\|k$
839	704,761	$p\|(k-1)$
881	777,043	$p\|(k-1)$
971	943,813	$p\|(k-1)$
1033	1,067,088	$p\|(k-1)$
1103	1,217,713	$p\|(k-1)$
1301	1,693,903	$p\|(k-1)$
1447	2,093,808	$(p-1)\|k$
1759	3,094,080	$(p-1)\|k$
2851	8,128,200	$(p-1)\|k$
3347	11,205,760	$p\|(k-1)$
4831	11,669,280	$(p-1)\|k$
13367	7,444,862	$(p-1)\|k$
15791	10,389,820	$(p-1)\|k$
17207	17,206	$(p-1)\|k$
18047	1,696,324	$(p-1)\|k$

Table 3

p (p is a prime number)	k (Wall's number of 4-step Fibonacci sequence)	Results
3	26	$(p-1)\|k$
13	84	$(p-1)\|k$
41	240	$(p-1)\|k$
67	100,254	$(p-1)\|k$
151	533,256	$(p+1)\|k$
211	9,393,930	$(p-1)\|k$
433	92,880	$(p-1)\|k$
907	822,648	$(p-1)\|k$
1277	1,630,728	$(p-1)\|k$
1579	623,310	$(p-1)\|k$
1951	3,798,600	$(p-1)\|k$
2593	1,680,912	$(p+1)\|k$
2749	7,557,000	$(p-1)\|k$
3079	4,740,120	$(p-1)\|k$
3331	396,270	$(p-1)\|k$
3581	3,205,890	$(p+1)\|k$
3733	23,225,448	$(p+1)\|k$
3823	3822	$(p-1)\|k$
4019	8,076,180	$(p-1)\|k$
4253	6,029,336	$(p-1)\|k$

Conjecture 4. *If $p > 2$ and k is the Wall number of n-step Fibonacci sequence such that $n = 2t$ and $t > 1$, then k is an even number.*

Conjecture 5. *Let k be Wall number of n-step Fibonacci sequence such that $n = 2t$ and $t > 1$. Then $(p \pm 1)|k$, except for some primes.*

We have demonstrated that the last two conjectures are satisfied using MAPLE and Fortran for $p < 5 \times 10^5$. Moreover, we have lots of data for various values of p. Computer calculations and its results shows in Table 3 that Wall number of 4-step Fibonacci sequence is even number for all and conjecture 5 is certainly true for some primes.

Acknowledgements

We acknowledge the computer algebra systems MAPLE and FORTRAN using which many of results in this area were originally discovered as experimental truths.

References

[1] D.D. Wall, Fibonacci series modulo m, American Mathematical Monthly 67 (1960) 525–532.
[2] J. Vinson, The relations of the period modulo m to the rank of apparition of m in the Fibonacci sequence, The Fibonacci Quarterly 1 (1963) 37–45.
[3] H.J. Wilcox, Fibonacci sequences of period n in groups, The Fibonacci Quarterly 24 (1986) 356–361.
[4] C.M. Campbell, H. Doostie, E.F. Robertson, in: G.E. Bergum et al. (Eds.), Applications of Fibonacci Numbers, vol. 3, Kluwer Academic Publishers, 1990, pp. 27–35.
[5] A.J.E. Ryba, Fibonacci representations of the symmetric groups, Journal of Algebra 170 (1994) 678–686.
[6] D. Takahashi, A fast algorithm for computing large Fibonacci numbers, Information Processing Letters 75 (2000) 243–246.
[7] J. West, Generating trees and the forbidden subsequences, Discrete Mathematics 157 (1996) 363–374.
[8] H. Aydın, G.C. Smith, Finite p-quotient of some cyclically presented groups, Journal of London Mathematical Society 49 (2) (1994) 83–92.
[9] R. Dikici, A. Işık, Fibonacci sequences in modular groups, Journal of Institute of Mathematics & Computer Science (Math. Ser.) 10 (3) (1997) 187–189.
[10] R. Dikici, E. Özkan, General recurrences in modular groups, Journal of Faculty of Science Ege University 21 (1998) 2.
[11] R. Dikici, E. Özkan, An Application of Fibonacci Sequences in Groups, Applied Mathematics and Computation 136 (2003) 323–331.
[12] H. Aydın, R. Dikici, G.C. Smith, Wall and Vinson Revisited, in: G.E. Bergum et al. (Eds.), Applications Fibonacci Numbers, vol. 5, Kluwer Academic Publishers, 1993, pp. 61–68.