NNTDM 4 (1998) 4, 165-174

FIBONACCI NUMBERS WITHIN MODULAR RINGS

J V Leyendekkers

The University of Sydney, 2006, Australia

A G Shannon

University of Technology, Sydney, 2007, &
KvB Institute of Technology, North Sydney, 2060, Australia

1. Introduction

Various authors, for example, de Carli (1970), Shannon (1979) and Wyler (1965), have considered aspects of the structure of second-order recurrences in the context of ring theory. It is the purpose of this paper to consider Fibonacci numbers within modular rings using an approach modelled on that of Carlitz (1955). We also consider the merits of comparing linear recursive sequences of the same order in terms of their structure at given values of the general term.

We represent integers within the modular ring $\mathbb{Z}_4$ by $4R_i + i$, where $i \in \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ represents the class number (Leyendekkers ***et al***, 1997). (Strictly speaking, $\overline{1} \equiv \overline{1}_4 \equiv 1\ (mod\, 4)$ and so on, but we have opted for brevity where there is no danger of confusion.)

2. The Class of Fibonacci Numbers

The class of Fibonacci numbers, $F_m \in \mathbb{Z}_4$ is easily established from

$$m = q + 6w \tag{2.1}$$

with $w = 0, 1, 2, 3, \ldots$, and q from Table 1.

Class	q
$\overline{0}$	0
$\overline{1}$	1, 2 *or* 5
$\overline{2}$	3
$\overline{3}$	4

Table 1

For example, when $m = 37$, $F_m \in \overline{1}$ with $q = 1$. We might expect from Table 1 that $\overline{1}$ will hold the largest number of Fibonacci numbers, and this is confirmed in Table 2 in

which we observe a period of 6 between successive $F_m \in \overline{0}$. Of these, 3 are in $\overline{1}$ and 1 each in $\overline{0}, \overline{2}$ and $\overline{3}$.

Row	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
0	$\underline{0}$	1	2	$\underline{3}$
1	4	$\underline{5}$	6	7
2	$\underline{8}$	9	10	11
3	12	$\underline{13}$	14	15
4	16	17	18	19
5	20	$\underline{21}$	22	23
6	24	25	26	27
7	28	29	30	31
8	32	33	$\underline{34}$	35

Table 2

This periodicity tells us succinctly in which row a Fibonacci number occurs. The row, $R(F_m)$, is itself curiously a Fibonacci number given by

$$R(F_m) = \sum_{j=1}^{t} F_{m-6j+3}. \tag{2.2}$$

The largest value of m in each block of 6 is given by $m_{max} = 10 + 6s$, $s = 0, 1, 2, 3, \ldots$; the smallest value of m in each block is given by $m_{min} = m_{max} - 5$, and $t = 2s + 1$ for the six values of m in the block. Some examples are contained in Table 3.

m	s	t	*Class* F_m
5	0	1	$\overline{1}$
7	0	1	$\overline{1}$
9	0	1	$\overline{2}$
13	1	3	$\overline{1}$
14	1	3	$\overline{1}$
16	1	3	$\overline{3}$
17	2	5	$\overline{1}$
18	2	5	$\overline{0}$
20	2	5	$\overline{1}$
23	3	7	$\overline{1}$
28	3	7	$\overline{3}$
42	6	13	$\overline{0}$

Table 3

The period of 6 is a particular case of Brent (1994), that if one of the initial values for $\{F_m\} \in \mathbb{Z}_4$ is odd, then the sequence has period 6 and is a maximal sequence. This result

has more recently been extended by Morgan (1998) who has completely determined the distribution of any maximal sequence which satisfies the Fibonacci recurrence relation (mod 2^n). By way of concluding this section we observe that if $[F_m]$ represents the class in which F_m occurs, then

$$[F_{6n+r}] = [F_{6n}] + [F_r],$$

which follows from Table 2 and the Fibonacci recurrence relation.

3. F_m as a Sum of Squares

Numbers in classes $\overline{1}$ and $\overline{2}$ can be sums of squares (Leyendekkers *et al*, 1997), and it is interesting to analyse which F_m equal $(d^2 + e^2)$, $d, e \in \mathbb{Z}$. As can be seen from Table 4, when m is odd for F_m in these two classes, one set of d, e values equals a Fibonacci set. These values of d and e in the set are simply obtained from Hoggatt (1969):

$$F_m = \left(F_{\frac{1}{2}(m+1)}\right)^2 + \left(F_{\frac{1}{2}(m-1)}\right)^2. \tag{3.1}$$

If F_m is a prime, then there will be only one d, e pair. Non-primes will have the same number of d, e pairs as there are factors, or a single d, e pair will have common factors (Leyendekkers *et al*, 1998). However, only one of the d, e pairs will satisfy Equation (3.1).

m	F_m	*Factors*	d	e
1	1		–	–
5	5		1	2
7	13		3	2
11	89		5	8
13	233		13	8
17	1597		21	34
19	4181	37, 113	55	34
			41	50
23	28657		89	144
25	75025	25, 3001	233	144
			73	264
29	514229		377	610
31	1346269		987	610
35	9227465	5, 13, 141961	1597	2584
			3037	64
			1109	2828
37	24157817	73, 149, 2221	4181	2584
			4909	244
			3859	3044

Table 4(a): Odd m $\in \overline{1}$

m	F_m	*Factors*	d	e
2	1		–	–
8	21	3, 7	–	–
14	377	13, 29	19	4
			11	16
20	6765	3, 5, 451	–	–
26	121393		303	172
32	2178309	3, 726103	–	–
38	39088169	37, 113, 9349	4795	4012
			5837	2240
			4613	4220

Table 4(b): Even m $\in \overline{1}$

Table 1 shows that m will be even for $F_m \in \{\overline{0}, \overline{3}\}$ and when $q = 2$ for $F_m \in \overline{1}$. Hence Equation (3.1) will not apply to these cases, as can be seen in Table 4(b).

m	F_m	d	e
3	2	–	–
9	34	5	3
15	610	21	13
21	10946	89	55
27	196418	377	233
33	3524578	1597	987
39	63245986	6765	4181

Table 5: Equation (3.1); Class $\overline{2}$

Furthermore, the numbers in Class $\overline{3}$ can never be sums of squares (Leyendekkers *et al*, 1997), while numbers in Class $\overline{0}$ can be sums of squares (although not necessarily so); for example, $32 \in \overline{0}$ and $32 = 4^2 + 4^2$. Since m is always even for Class $\overline{0}$ the d and e values will not be Fibonacci numbers when the number itself is. For Class $\overline{1}$, $q = 2$, the series $m = 14 + 12k$, $k = 0, 1, 2, 3, \ldots$, has a sum of squares for F_m. However, there are no sums of squares for the series $m = 8 + 12k$. We further observe that Tables 6,7 and 8 in the next section contain examples of a less well-known theorem of Fermat to the effect that a prime $p = a^2 + b^2, a, b, \in \mathbb{Z}$, iff $p = 2$ or $p \equiv 1\ (mod\, 4)$, that is $p \in \overline{1}$ (Dilcher, 1998).

4. Some Other Second Order Recurrences

The best known of other second order sequences are the Lucas $\{L_n\}$ and the Pell $\{P_n\}$ which are defined respecitvely by the following recurrence relations and initial terms:

$$L_n = L_{n-1} + L_{n-2}, \qquad n \geq 2,$$

with $L_0 = 2,\ L_1 = 1$ and

$$P_n = 2P_{n-1} + P_{n-2}, \qquad n \geq 2,$$

with $P_0 = 0,\ P_1 = 1$.

The first few terms and their corresponding classes are set out in Table 6, where we observe that P_n, unlike L_n, also satisfies Equation (3.1).

n	0	1	2	3	4	5	6	7	8	9	10
L_n	2	1	3	4	7	11	18	29	47	76	123
Class	$\overline{2}$	$\overline{1}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
P_n	0	1	2	5	12	29	70	169	408	985	2378
Class	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Table 6

It can be seen that $\{L_n\}$ has a period of 6 like the Fibonacci numbers, whereas $\{P_n\}$ has a period of 4, and that $L_n \in \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ like F_n, but $P_n \notin \{\overline{3}\}$. The discriminant, ∂, of the associated auxiliary equation is 5 in the case of the Fibonacci and Lucas sequences and it is 8 in the case of the Pell sequence.

We now consider some other second order linear recursive sequences with varying discriminants. In the notation of Horadam (1965) we define $\{W_n\} \equiv \{W_n(a, b; p, q)\}$ by the recurrence relation

$$W_n = pW_{n-1} - qW_{n-2}, \qquad n \geq 2,$$

with initial conditions $W_0 = a,\ W_1 = b$. In turn let

$$\{S_n\} \equiv \{W_n(0, 1; 1, -2)\}, \quad \{T_n\} \equiv \{W_n(0, 1; 1, -3)\},$$
$$\{U_n\} \equiv \{W_n(0, 1; 1, -4)\}, \quad \{V_n\} \equiv \{W_n(0, 1; 1, -7)\}.$$

We notice immeditately the basic facts which are set out in Tables 7 and 8.

m	S_m	*Class*	T_m	*Class*	U_m	*Class*	V_m	*Class*
1	1	$\overline{1}$	1	$\overline{1}$	1	$\overline{1}$	1	$\overline{1}$
2	1	$\overline{1}$	1	$\overline{1}$	1	$\overline{1}$	1	$\overline{1}$
3	3	$\overline{3}$	4	$\overline{0}$	5	$\overline{1}$	8	$\overline{0}$
4	5	$\overline{1}$	7	$\overline{3}$	9	$\overline{1}$	15	$\overline{3}$
5	11	$\overline{3}$	19	$\overline{3}$	29	$\overline{1}$	71	$\overline{3}$
6	21	$\overline{1}$	40	$\overline{0}$	65	$\overline{1}$	176	$\overline{0}$
7	43	$\overline{3}$	97	$\overline{1}$	181	$\overline{1}$	673	$\overline{1}$
8	85	$\overline{1}$	217	$\overline{1}$	441	$\overline{1}$	1905	$\overline{1}$
9	171	$\overline{3}$	508	$\overline{0}$	1165	$\overline{1}$	6616	$\overline{0}$

Table 7

W_n	*Classes*	*Period*	∂
S_n	$\overline{1}, \overline{3}$	2	9
T_n	$\overline{0}, \overline{1}, \overline{3}$	3	13
U_n	$\overline{1}$	1	17
V_n	$\overline{0}, \overline{1}, \overline{3}$	6	29

Table 8

Further analysis reveals that the sums of squares for $\{T_n\}$ in Table 9: does the period 6 have a role to play in this?

n	T_n	*Sums of Squares*
6	40	$2^2 + 6^2$
7	97	$4^2 + 9^2$
13	14209	$103^2 + 60^2, 95^2 + 72^2$
14	32689	$17^2 + 180^2, 145^2 + 108^2$

Table 9

The foregoing suggests that we may be able to learn more about the structure of some of the sequences by comparing them at particular points of these ordered sets. For instance,

$$W_5 = a^2 + 3a + 1$$

yields the values in Table 10.

a	1	2	3	4	7
W_5	5	11	19	29	71
$=$	F_5	S_5	T_5	U_5	V_5

Table 10

Similarly, for

$$W_8 = (2a + 1)(2a^2 + 4a + 1)$$

we get the values in Table 11.

a	1	2	3	4	7
W_8	21	85	217	441	1905
$=$	F_8	S_8	T_8	U_8	V_8

Table 11

We are, in effect, considering 'm sequences' at each value of m in W_m. Each m sequence has distinct characteristics. For example, for $m = 6$ and $m = 8$ all the $W_m \equiv W_m(\mathfrak{d})$ values are composite. This can be seen with the expansion of

$$W_8(\mathfrak{d}) = (1 + \mathfrak{d})(\mathfrak{d}^2 + 6\mathfrak{d} + 1)/16 \tag{4.1}$$

$$= (2r_1 + 1)(2r_1^2 + 4r_1 + 1) \tag{4.2}$$

with $\mathfrak{d} \in \overline{1}$, $\mathfrak{d} = 4r_1 + 1$, .

This is to be compared with the equation for a composite N (Leyendekkers *et al*, 1998):

$$N = (2t + 1)(2(t + s) - 1) \tag{4.3}$$

with $t, s = 0, 1, 2, 3$, so that $t = r_1$ and $s = (r_1^2 + r_1 + 1)$. On the other hand, the sequence $\{W_5(\mathfrak{d})\}$ is prime-rich in a sense. It is given by

$$W_5(\mathfrak{d}) = r_1^2 + 3r_1 + 1. \tag{4.4}$$

When the right-most digit of $W_5(\mathfrak{d})$ is 5, $r_1 = 1 + 5v$, $v = 0, 1, 2, 3, \ldots$. When Equations (4.3) and (4.4) are compatible, $W_5(\mathfrak{d})$ will be composite. This occurs in regular doublet sequences for rows following the equation

$$r_1 = A + fv \tag{4.5}$$

where f is a prime factor of $W_5(\mathfrak{d})$ and $v = 0, 1, 2, 3, \ldots$ (Table 12).

f	5	11	19	29	31	41	59	61	71	79
A	1	13	13	22	11	33	24	16	61	28
	–	17	22	33	17	46	32	42	78	48

Table 12

Note that, apart from $f = 5$, the right-most digit of f is always $\pm 1 (mod 10)$. A similar form to Equation (4.5) applies for $m = 7$ when

$$W_7(\mathfrak{d}) = r_1^3 + 6r_1^2 + 5r_1 + 1. \tag{4.6}$$

However, A can have up to three values, and the right-most digit of f is $1, \pm 3\ (mod\ 10)$. For $m = 9$

$$W_9(\mathfrak{d}) = (1 + r_1)(r_1^3 + 9r_1^2 + 6r_1 + 1) \tag{4.7}$$

so that there are no primes in this sequence.

In general, since

$$W_m(\mathfrak{d}) = (x^m - y^m)/\mathfrak{d}^{\frac{1}{2}}$$

where x, y are the zeros of the characteristic polynomial, with $x - y = \mathfrak{d}^{\frac{1}{2}}$, and $x + y = 1$,

$$W_m(\mathfrak{d}) = [(x^{\frac{1}{2}(m-n)} - y^{\frac{1}{2}(m-n)})(x^{\frac{1}{2}(m-n)} + y^{\frac{1}{2}(m-n)})(x^n + y^n) - x^n y^n(x^{m-2n} - y^{m-2n})]/(x - y) \tag{4.8}$$

with $m - 2n > 0$. Thus it can be readily established if there are any primes in the sequence. For example, when $m - 2n = \frac{1}{2}(m - n)$ $(m = 6, n = 2;\ m = 9, n = 3;\ m = 15, n = 5; \ldots)$, or when $\frac{1}{2}(m - 2n) = n$ $(m = 8, n = 2;\ m = 16, n = 4;\ m = 32,\ n = 8; \ldots)$, there will be a common factor. $W_m(\mathfrak{d})$ is a prime only when m is a prime.

Neither of the integers f and g is a Fibonacci number for the sequence $m = 14 + 12k$,

$$W_m = f^2 + g^2$$

with f odd and g even. However, with $k > 0$, $F_{\frac{1}{2}(m-2)} < g < F_{\frac{1}{2}m} < f < F_{\frac{1}{2}(m+2)}$. Moreover, $g = 4r_0 \in \overline{0}$ and $f = 4r_3 + 3 \in \overline{3}$.

5. Conclusion

Similar modular-ring analyses may be applied to generalized Lucas sequences $\{G_n\} \equiv \{G_n(2, 1; 1, -r)\}$ which satisfy the recurrence relation

$$G_n = G_{n-1} + rG_{n-2},\quad n \geq 2. \tag{5.1}$$

Some cases are illustrated in Table 13, which includes the ordinary Lucas sequence $\{L_n\} \equiv \{G_n(2, 1; 1, -1)\}, \mathfrak{d} = 4r + 1$.

$\mathfrak{d}$	r	n	1	2	3	4	5	6	7	8
5	1	L_n	1	3	4	7	11	18	29	47
9	2	A_n	1	5	7	17	31	65	127	257
13	3	B_n	1	7	10	31	61	154	337	799
17	4	C_n	1	9	13	49	101	297	701	1889
21	5	D_n	1	11	16	71	151	506	1261	3791

Table 13

These generalized Lucas sequences are related to the corresponding generalized Fibonacci sequences $\{W_n(0, 1; 1, -r)\}$ by

$$G_n = W_n + 2rW_{n-1},\ n \geq 1, \tag{5.2}$$

which can be readily proved by mathematical induction with the use of Equation (5.1). Equation (5.2) is a generalization of Hoggatt (1969)

$$L_n = F_n + 2F_{n-1}.$$

The modular results then follow since the general term for W_n is given by (Barakat,1964):

$$W_{n+1} = \sum_{j=0}^{\lfloor \frac{1}{2}n \rfloor} \binom{n-j}{j} r^j. \tag{5.3}$$

A similar analysis can be carried out for the modular ring $\mathbb{Z}_6$ within which the integers can be represented by $(6r_i + (i-3))$ where $i \in \{1,2,3,4,5,6\}$ represents the class number (Leyendekkers *et al*, 1997). W_m increases rapidly as d becomes large. Of interest too is the relation of these sequences to one another. For instance, how often do they intersect. There are many unanswered facets of the question for generalized Fibonacci and Lucas sequences as in Stein (1962). For example, from Table 13 we can see that

$$\#(A_n \cap B_n) \geq 3.$$

Another related topic for further research is the study of order relations on square-free rings using D'Antona's counting function (1998). So too is the frequency of a sum of squares for its members. Of course, one can also try to extend the ideas to third order recurrences and then to arbitrary order recurrences along the lines of Shannon (1972,1974).

References

Barakat, Richard. 1964. The matrix operator e^X and the Lucas polynomials. *Journal of Mathematics and Physics*. **43**: 332-335.

Brent, R P. 1994. On the periods of generalized Fibonacci recurrences. *Mathematics of Computation*. **63**: 207.

Carlitz, L. 1955. Some class number relations. *Mathematische Zeitschrift*. **62**: 167-170.

D'Antona Ottavio, M. 1998. The would-be method of targeted rings, in Bruce Sagan & Richard P Stanley (eds). *Mathematical Essays in Honor of Gian-Carlo Rota*. Boston: Birkhauser, pp.157-172.

DeCarli, D J. 1970. A generalized Fibonacci sequence over an arbitrary ring. *The Fibonacci Quarterly*. **8.2**: 182-184.

Dilcher, Karl. 1998. Nested squares and evaluations of integer products. *8th International Conference on Fibonacci Numbers and Their Applications*, Rochester, USA, 22-26 June.

Hoggatt, V E. Jr. 1969. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin.

Horadam, A. F. 1965. Generating functions for powers of a certain generalized sequence of numbers. *Duke Mathematical Journal.* **32.3**: 437-446.

Leyendekkers, J V, Rybak, J M & Shannon, A G. 1997. Analysis of Diophantine properties using modular rings with four and six classes. *Notes on Number Theory & Discrete Mathematics*. **3.2**: 61-74.

Leyendekkers, J V, Rybak, J M & Shannon, A G. 1998. The characteristics of primes and other integers within the modular ring $\mathbb{Z}_4$ and in class $\bar{1}$. *Notes on Number Theory & Discrete Mathematics*. **4.1**: 1-17.

Morgan, Mark D. 1998. The distribution of second order linear recurrence sequences mod 2^m. *Acta Arithmetica*. **83.2**: 181-195.

Shannon, A.G. 1972. Iterative formulas associated with third order recurrence relations. *S.I.A.M. Journal of Applied Mathematics*. **23.3**: 364-368.

Shannon, A.G. 1974. Some properties of a fundamental linear recursive sequence of arbitrary order. *The Fibonacci Quarterly*. **12.4**: 327-335.

Stein, S.K. 1962. The intersection of Fibonacci sequences. *The Michigan Mathematics Journal*. **9**: 399-402.

Wyler, O. 1965. On second order recurrences. *American Mathematical Monthly*. **72.5**: 500-506.

AMS Classification Numbers: 11R29, 11B39.