THE FIBONACCI MATRIX MODULO m[*]

D. W. ROBINSON, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CALIF.[†]

In this paper we investigate some of the arithmetical properties of the famous Fibonacci sequence by use of elementary matrix algebra. We believe the approach to be conceptual and, at least in part, novel. Thus, it is our purpose to explore the pedagogical advantages of matrix methods for problems of this kind as well as to provide a refreshing appreciation of the arithmetical properties themselves. At the conclusion of the paper we also indicate how the methods may be applied to other linear recurrent sequences.

We begin by considering the following example. Suppose that the Fibonacci sequence

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \cdots$$

is reduced modulo 8:

$$0, 1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0, 1, 1, \cdots$$

We observe that the reduced sequence is periodic. Indeed, the 12 terms of the period form two sets of 6 terms each, the terms of the second half being 5 times the corresponding terms of the first half. We say that the Fibonacci sequence reduced modulo 8 is of period 12 and restricted period 6 with multiplier 5. Also, we observe that the multiplier is of exponent 2 modulo 8.

More generally, let $u_0, u_1, \cdots, u_n, \cdots$ be the Fibonacci sequence of integers satisfying $u_{n+2} = u_{n+1} + u_n$ for $n \geq 0$ with $(u_0, u_1) = (0, 1)$. Given any integer $m > 1$ we provide below an elementary proof of the fact that there is a positive integer n such that $(u_n, u_{n+1}) \equiv (0, 1) \pmod{m}$. The least such integer $\delta(m)$ is called the period of the Fibonacci sequence modulo m. The least positive integer n such that $(u_n, u_{n+1}) \equiv s(0, 1) \pmod{m}$, where s is some integer, is called the restricted period $\alpha(m)$ of the sequence modulo m. If $(u_{\alpha(m)}, u_{\alpha(m)+1}) \equiv s(m)(0,1)$ $\pmod{m}$, $0 < s(m) < m$, then $s(m)$ is called the multiplier of the Fibonacci sequence modulo m. Obviously $s(m) \equiv u_{\alpha(m)+1} \pmod{m}$. Finally, we denote the exponent modulo m of the multiplier $s(m)$ by $\beta(m)$.

[*] Presented to the Mathematical Association of America, Southern California Section, March 9, 1963.

[†] Presently on sabbatical leave from Brigham Young University and at California Institute of Technology under an N. S. F. Faculty Fellowship Program.

By direct calculation we obtain the following table:

m	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\alpha(m)$	3	4	6	5	12	8	6	12	15	10	12	7	24	20	12	9	12	18
$\beta(m)$	1	2	1	4	2	2	2	2	4	1	2	4	2	2	2	4	2	1
$\delta(m)$	3	8	6	20	24	16	12	24	60	10	24	28	48	40	24	36	24	18

The results of this table illustrate several interesting arithmetical properties. In fact, if (a,b) and $[a,b]$ denote the greatest common divisor and the least common multiple, respectively, of the integers a and b, then we propose to establish the following:

(i) $m \mid u_n$ if and only if $\alpha(m) \mid n$, and $m \mid u_n$, $m \mid (u_{n+1} - 1)$ if and only if $\delta(m) \mid n$;

(ii) $\delta(m) = \alpha(m)\beta(m) = (2, \beta(m))\,[\gamma(m), \alpha(m)]$, where $\gamma(2) = 1$ and $\gamma(m) = 2$ for $m > 2$;

(iii) $\alpha([m_1, m_2]) = [\alpha(m_1), \alpha(m_2)]$, and $\delta([m_1, m_2]) = [\delta(m_1), \delta(m_2)]$;

(iv) for every odd prime p there is a positive integer e(p) such that $\alpha(p^e) = \alpha(p)p^{\max(0, e-e(p))}$ and $\delta(p^e) = \delta(p)p^{\max(0, e-e(p))}$;

(v) $\alpha(p) \mid (p - (5/p))$, where $(5/p)$ is the usual Legendre symbol; furthermore, if $p \neq 5$, then $\delta(p) \mid (p-1)$ or $\delta(p) \mid 2(p + 1)$.

With the possible exception of the last equation of (ii), which is due to Morgan Ward, these properties are all well known. Indeed, the fact that reduced sequences of this type are periodic was observed by J. L. Lagrange in the eighteenth century. A century later E. Lucas engaged in an extensive study of the arithmetic divisors of such sequences. These early results together with some of the later developments in the subject are reviewed in Chapter 17 of Dickson's *History* [6]. However, it is suggested that this general background be supplemented with at least the papers of Carmichael [3], Lehmer [11], and Ward [19]. (See also [4, 7, 8, 9, 10, 17, 20, 21].)

Furthermore, since the main purpose of this present paper is to indicate the use of matrix algebra for the study of linear recurrence relations, we also remark that such techniques are certainly not new. (See for example [1, 13, 16, 18].) In fact, some of the arithmetical properties of linear recurrent sequences have been studied by means of matrices. (See for example [2, 12, 15].) It is our aim to now indicate some of the further possibilities of this method.

We begin by introducing the main tool of our discussion. Specifically, we view the linear recurrence above as defining a mapping of the ordered pair (u_{n-1}, u_n) onto the ordered pair (u_n, u_{n+1}). Since $u_{n+1} = u_{n-1} + u_n$, it is clear that this mapping is represented by the matrix product $(u_{n-1}, u_n)U = (u_n, u_{n+1})$, where

$$U = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} .$$

Furthermore, by induction on n, we observe that $(u_n, u_{n+1}) = (0, 1)U^n$ and

$$U^n = \begin{bmatrix} u_{n-1} & u_n \\ u_n & u_{n+1} \end{bmatrix} .$$

Because of these results we call U the Fibonacci matrix.

From the foregoing it is evident that $(u_n, u_{n+1}) \equiv (0, 1) \pmod{m}$ if and only if U^n is congruent (elementwise) modulo m to the identity matrix. Thus, the study of the period of the Fibonacci sequence modulo m is equivalent to the study of the period of the sequence I, U, U^2, $\cdots$, U^n, reduced modulo m. In particular, since there are only a finite number of distinct matrices in this reduced sequence, it follows that there are integers k and n such that U^{k+n} is congruent to U^k with $k + n > k \geq 0$. But since the determinant of U is the unit -1, this means that for some positive integer n, $U^n \equiv I \pmod{m}$. Thus, there exists a least such positive integer n, which is in fact $\delta(m)$ as defined above. Also, it is clear that every such n is an integral multiple of $\delta(m)$. That is, $U^n \equiv I \pmod{m}$ if and only if $\delta(m) | n$, which is equivalent to the second statement of (i).

By a similar argument we have $(u_n, u_{n+1}) \equiv s(0, 1) \pmod{m}$ if and only if $U^n \equiv sI \pmod{m}$. Indeed, U^n is congruent to a scalar matrix modulo m if and only if $\alpha(m) | n$, where $\alpha(m)$ is the restricted period defined above. This result is equivalent to the first part of (i).

Furthermore, we have

$$U^{\alpha(m)} \equiv s(m) I \pmod{m} ,$$

where the multiplier s(m) is of exponent $\beta(m)$ modulo m. Since $U^{\alpha(m)\beta(m)} \equiv s(m)^{\beta(m)} I \equiv I \pmod{m}$, $\delta(m) | \alpha(m)\beta(m)$. On the other hand, since it is evident that $\alpha(m) | \delta(m)$, we have by a similar argument that $\beta(m) | \delta(m)/\alpha(m)$. Thus, $\delta(m) = \alpha(m)\beta(m)$, which establishes the first equation of (ii).

Also, since the determinant of U is -1, we have from the matrix congruence above that

$$(-1)^{\alpha(m)} \equiv (s(m))^2 \pmod{m}$$

Hence, these congruent integers have the same exponent modulo m. Specifically,

$$\frac{\gamma(m)}{(\gamma(m),\ \alpha(m))} = \frac{\beta(m)}{(2, \beta(m))} \quad ,$$

where $\gamma(m)$ is the exponent of -1 modulo m. Tnat is,

$$\delta(m) = \alpha(m)\beta(m) = (2, \beta(m)) \frac{\gamma(m)\alpha(m)}{(\gamma(m), \alpha(m))} \ ,$$

which is clearly equivalent to (ii). In particular, we observe that $\delta(m)$ is even for $m > 2$ and that $\beta(m) | 4$.

We now demonstrate the second equation of (iii). We first observe that if $m' | m$, then $U^{\delta(m)} \equiv I \pmod{m'}$ and $\delta(m') | \delta(m)$. Thus, since m_1 and m_2 both divide $[m_1, m_2]$, it follows that $\delta([m_1, m_2])$ is a common multiple of $\delta(m_1)$ and $\delta(m_2)$. On the other hand, suppose $\delta(m_1)$ and $\delta(m_2)$ both divide δ. Since U^{δ} is congruent to the identity matrix modulo both m_1 and m_2, the congruence is also valid modulo $[m_1, m_2]$. That is, $\delta([m_1, m_2])$ divides δ and is therefore the least common multiple of $\delta(m_1)$ and $\delta(m_2)$.

We obtain similarly the first equation of (iii). Thus, we observe that both α and δ are factorable (l. c. m. multiplicative) functions of the argument m, which suggests next the consideration of property (iv).

Therefore, let p be any odd prime and let e be any positive integer. Since $U^{\delta(p^e)} = I + p^eB$ for some matrix B, $U^{p\,\delta(p^e)} = (I + p^eB)^p \equiv I \pmod{p^{e+1}}$. That is, $\delta(p^{e+1}) | p\,\delta(p^e)$. But obviously $\delta(p^e) \mid \delta(p^{e+1})$. We conclude, since p is a prime, that $\delta(p^{e+1})$ is either $\delta(p^e)$ or $p\,\delta(p^e)$. In particular, $\delta(p^e)/\delta(p)$ is some non-negative power of p. Similarly, $\alpha(p^e)/\alpha(p)$ is some non-negative power of p. Recalling that for any given modulus the ratio of the period to the restricted period divides 4 and that p is odd, it is immediate from the identity

$$\frac{\alpha(p^e)}{\alpha(p)} \cdot \frac{\delta(p^e)}{\alpha(p^e)} = \frac{\delta(p^e)}{\delta(p)} \cdot \frac{\delta(p)}{\alpha(p)}$$

that $\alpha(p^e)/\alpha(p) = \delta(p^e)/\delta(p)$ and $\delta(p^e)/\alpha(p^e) = \delta(p)/\alpha(p)$.

Moreover, suppose that $\delta(p^{e+1}) \neq \delta(p^e)$. Then $U^{\delta(p^e)} = I + p^eB$ with $B \neq 0 \pmod p$. Hence,

$$U^{p\,\delta(p^e)} = I + p^{e+1}B \neq I \pmod{p^{e+2}} \quad .$$

That is, if $\delta(p^{e+1}) = p\delta(p^e)$, then $\delta(p^{e+2}) = p\delta(p^{e+1})$. Consequently, if $e(p)$ is the largest positive e such that $\delta(p^e) = \delta(p)$, then $\delta(p^e) = \delta(p)$ for $1 \leq e \leq e(p)$ and $\delta(p^e) = p^{e-e(p)}\delta(p)$ for $e > e(p)$. Finally, the existence of $e(p)$ is assured from a consideration of the alternative: if $U^{\delta(p)} \equiv I \pmod{p^e}$, $e = 1, 2, \cdots$, then $U^{\delta(p)} = I$, which is impossible. This completes the proof of (iv).

It is of interest to remark that a test [17] with a digital computer has shown that $e(p) = 1$ for all primes p less than 10,000. However, the problem of identifying the exceptional primes p with $e(p) > 1$ remains unsolved.

Finally, we prove property (v). For every prime p we define the <u>restricted graph</u> $R(p)$ of U modulo p to consist of the $p + 1$ points $P_0 = (0, 1), P_1 = (1, 1), \cdots, P_{p-1} = (p - 1, 1), P_\infty = (1, 0)$ together with the collection of all directed edges $P_i \rightarrow P_{i'}$, where $P_{i'}$ is the unique point which is linearly dependent upon the matrix product P_iU. (Contrast this with, for example, [5].) By way of illustration, $R(5)$ consists of the 1-cycle $P_2 \rightarrow P_2$ and the 5-cycle $P_0 \rightarrow P_1 \rightarrow P_3 \rightarrow P_4 \rightarrow P_\infty \rightarrow P_0$. In general, since this graph is determined by a one-to-one correspondence, it follows that $R(p)$ consists of a collection of disjoint cycles. (See for example [14] pp. 25-27.) Furthermore, it is clear that P_i belongs to a 1-cycle (or in other words is a fixed point under the correspondence) if and only if P_i is a characteristic vector of U modulo p. Moreover, suppose that P_i belongs to an α-cycle with $\alpha > 1$. Since $\{P_i, P_iU\}$ is a linearly independent set, it follows that $P_iU^\alpha \equiv sP_i \pmod p$ implies $U^\alpha \equiv sI \pmod p$, which means that $\alpha(p)|\alpha$. Thus, since obviously $\alpha|\alpha(p)$, $\alpha = \alpha(p)$. That is, $R(p)$ consists of a collection of 1-cycles and $\alpha(p)$-cycles. Consequently, $\alpha(p)|(p + 1 - t)$, where t is the number of 1-cycles of $R(p)$. But t is also the number of linearly independent characteristic vectors of U modulo p, or equivalently the number of distinct roots modulo p of the minimum polynomial $\lambda^2 - \lambda - 1$ of U. Since the discriminant of this quadratic is 5, it follows that t is 0, 1, or 2 according as the Legendre symbol $(5/p)$ is -1, 0, or 1.

That is, $\alpha(p) \mid (p - (5/p))$, which means that $U^{p-(5/p)} \equiv sI$ and $U^p \equiv sU^{(5/p)} \pmod{p}$, for some integer s depending upon p. Now, considering the trace of each of the matrices in this last congruence, $\mathrm{tr}\, U^5 \equiv 2s \pmod{5}$ and $\mathrm{tr}\, U^p \equiv (5/p)s \pmod{p \neq 5}$. But, since $U^{-1} = U - I$ implies $U^{-p} \equiv U^p - I \pmod{p}$, we have $-\mathrm{tr}\, U^p \equiv \mathrm{tr}\, U^p - 2$ and $\mathrm{tr}\, U^p \equiv 1 \pmod{p}$. Therefore $U^5 \equiv 3I \pmod{5}$ and

$$U^{p-(5/p)} \equiv (5/p)\, I \qquad (\mathrm{mod}\ p \neq 5)\ ,$$

which establishes property (v). As a corollary we obtain the well-known congruence $u_p \equiv (5/p) \pmod{p}$. Also, it is of interest to add that, by the quadratic reciprocity law, we have $(5/p) = 1$ if $p = 5k \pm 1$ and $(5/p) = -1$ if $p = 5k \pm 2$.

Thus, by use of the Fibonacci matrix, we have established some of the principal arithmetical properties of the sequence 0, 1, 1, 2, ··· . Although we may use this matrix to establish many other interesting properties and identities of the Fibonacci numbers, we feel that the foregoing is sufficient to illustrate the application of this tool (at least as far as the arithmetical properties are concerned). However, we indicate in conclusion how the idea may be readily adapted to the study of more general linear recurrent sequences.

Specifically, let $x_0, x_1, \cdots, x_n, \cdots$ be the sequence of integers satisfying the linear recurrence

$$x_{n+r} = a_1 x_{n+r-1} + \cdots + a_r x_n\ ,$$

for $n \geq 0$ where $x_0, \cdots, x_{r-1}$ and $a_1, \cdots, a_r$ are given integers. A study of this linear recurrent sequence may be made by means of the equation $X_n = X_0 A^n$, where $X_n = (x_n, \cdots, x_{n+r-1})$ and

$$A = \begin{bmatrix} 0 & \cdots & 0 & a_r \\ 1 & \cdots & 0 & a_{r-1} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 1 & a_1 \end{bmatrix} .$$

Indeed, the arithmetical properties of this sequence may be investigated by a generalization of the methods suggested by this present paper. In particular, if m is a positive integer such that $\{X_0, \cdots, X_{r-1}\}$ is linearly independent modulo m, then

$X_n \equiv sX_0 \pmod{m}$ if and only if $A^n \equiv sI \pmod{m}$. Furthermore, if $(m, a_r) = 1$, then the determinant of A is the unit $(-1)^{r-1}a_r$ modulo m and the sequence of powers of this matrix reduced modulo m is periodic. That is, under these assumptions, the periodic properties of the sequence of integers reduced modulo m may be identified with those of the sequence $I, A, \cdots, A^n, \cdots$ reduced modulo m. For example, we have that (ii) above is a special case of the equation

$$\delta(m) = \alpha(m)\beta(m) = (r, \beta(m))\,[\,\gamma(m), \alpha(m)\,] ,$$

where r is the order of the recurrence, $\gamma(m)$ is the exponent of the determinant of A modulo m, and $\alpha(m)$, $\beta(m)$, and $\delta(m)$ are obvious extensions of the definitions above.

REFERENCES

1. E. T. Bell, Notes on recurring series of the third order, Tôhoku Math. J. 24 (1924) 168-184.

2. J. L. Brenner, Linear recurrence relations, Amer. Math. Monthly 61 (1954) 171-173.

3. R. D. Carmichael, On sequences of integers defined by recurrence relations, Quart. J. Math. 48 (1920) 343-372.

4. ________________, A simple principal of unification in the elementary theory of numbers, Amer. Math. Monthly 36 (1929) 132-143.

5. R. H. Crowell, Graphs of linear transformations over finite fields, J. Soc. Indust. Appl. Math. 10 (1962) 103-112.

6. L. E. Dickson, History of the theory of numbers, vol. I, Chelsea, New York, 1952.

7. E. B. Dynkin and W. A. Uspenski, Mathematische Unterhaltungen II, Kleine Ergänzungsreihe XIV, Deutscher Verlag der Wissenschaften, Berlin, 1956.

8. H. T. Engstrom, On sequences defined by linear recurrence relations, Trans. Amer. Math. Soc. 33 (1931) 210-218.

9. M. Hall, An isomorphism between linear recurring sequences and algebraic rings, Trans. Amer. Math. Soc. 44 (1938) 196-218.

10. G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, 4th ed., Oxford University Press, London, 1960, pp. 148-150.

11. D. H. Lehmer, An extended theory of Lucas' functions, Ann. of Math. (2) 31 (1930) 419-448.

12. N. S. Mendelsohn, Congruence relationships for integral recurrences, Can. Math. Bull. 5 (1962) 281-284.

13. E. P. Miles, Jr., Generalized Fibonacci numbers and associated matrices, Amer. Math. Monthly 67 (1960) 745-752.

14. O. Ore, Theory of graphs, Amer. Math. Soc. Colloq. Publ., vol. 38, Providence, 1962.

15. D. W. Robinson, A note on linear recurrent sequences modulo m, submitted for publication in the Amer. Math. Monthly.

16. R. A. Rosenbaum, An application of matrices to linear recursion relations, Amer. Math Monthly 66 (1959) 792-793.

17. D. D. Wall, Fibonacci series modulo m, Amer. Math. Monthly 67 (1960) 525-532.

18. M. Ward, The algebra of recurring series, Ann. of Math. (2) 32 (1931) 1-9.

19. ________, The characteristic number of a sequence of integers satisfying a linear recursion relation, Trans. Amer. Math. Soc. 33 (1931) 153-165.

20. ________, The arithmetical theory of linear recurring series, Trans. Amer. Math. Soc. 35 (1933) 600-628.

21. N. Zierler, Linear recurring sequences, J. Soc. Indust. Appl. Math. 7 (1959) 31-48.

Brigham Young University
and
California Institute of Technology

REQUEST

The Fibonacci Bibliographical Research Center desires that any reader finding a Fibonacci reference send a card giving the reference and a brief description of the contents. Please forward all such information to:

Fibonacci Bibliographical Research Center,
Mathematics Department,
San Jose State College,
San Jose, Calif.