ACTA ARITHMETICA
XVI (1969)

On arithmetical functions related to the Fibonacci numbers*

by

JOHN D. FULTON (Clemson, S. Carolina)
and WILLIAM L. MORRIS** (Houston, Texas)

1. Introduction. It was known to Lagrange [3] that the sequence of Fibonacci numbers, i.e., $u_0 = 0$, $u_1 = 1$, $u_{n+2} = u_{n+1} + u_n$ for $n = 0, 1, 2, \ldots$, is periodic modulo m for every integer $m > 1$. Let M be the set of integers greater than one and for $m \in M$, let $\pi(m)$ denote the period of the Fibonacci sequence modulo m. Also, let $\pi(\pi(m)) = \pi^2(m)$ and $\pi(\pi^n(m)) = \pi^{n+1}(m)$ for $n = 2, 3, \ldots$ The two main results of this paper are:

FIXED POINT THEOREM. *For $m \in M$, $\pi(m) = m$ if and only if $m = (24)5^{\lambda-1}$ for some positive integer λ.*

ITERATION THEOREM. *For each $m \in M$, there exists a least integer ω such that $\pi^{\omega+1}(m) = \pi^{\omega}(m)$.*

These theorems imply the existence of two new arithmetical functions, namely λ and ω. The three related functions π, λ, and ω are called the Pisano period, the Leonardo logarithm, and the Fibonacci frequency, respectively, where $\pi^{\omega}(m) = 24(5)^{\lambda-1}$.

2. Known results. Robinson [4] has summarized the known results concerning the periodicity of the Fibonacci numbers modulo m and has employed elementary matrix algebra to give new proofs of most of them. Also, he offers an extensive bibliography. Following his terminology, we need the following:

DEFINITION 2.1. For $m \in M$, the least integer n such that $(u_n, u_{n+1}) \equiv (0, 1) \pmod{m}$ is denoted by $\pi(m)$ and is called the (Pisano) *period of* m.

* Research sponsored in part by the Oak Ridge National Laboratory operated by the Union Carbide Corporation under contract with the U. S. Atomic Energy Commission.

** Presented January 23, 1968, to the American Mathematical Society meeting in San Francisco, California, under the title: *The Pisano period, Fibonacci frequency and Leonardo logarithm of the positive integers.*

DEFINITION 2.2. For $m \in M$, the least integer n such that $(u_n, u_{n+1}) \equiv \sigma(0,1) \pmod m$ for some positive integer σ is denoted by $a(m)$ and is called the *restricted period of* m.

DEFINITION 2.3. If $(u_{a(m)}, u_{a(m)+1}) \equiv \sigma(m)\,(0,1) \pmod m$, then $\sigma(m)$ is called the *multiplier of* m.

DEFINITION 2.4. For $m \in M$, the order of $\sigma(m)$ in Z_m, the ring of integers modulo m, is denoted by $\beta(m)$ and is called the *exponent of* $\sigma(m)$.

For $a, b \in M$, $[a, b]$ denotes the least common multiple, (a, b) the greatest common divisor, and (a/b) the Legendre symbol of a and b. That portion of Robinson's summary which is applicable here are the following fundamental theorems.

THEOREM 2.1. (i) $m \mid u_n$ *if and only if* $a(m) \mid n$.

(ii) $m \mid u_n$ *and* $m \mid (u_{n+1}-1)$ *if and only if* $\pi(m) \mid n$.

THEOREM 2.2. *If* p *is a prime,*

(i) $a(p) \mid (p-(5/p))$,

(ii) *if* $p \equiv \pm 1 \pmod 5$, *then* $\pi(p) \mid (p-1)$,

(iii) *if* $p \equiv \pm 2 \pmod 5$, *then* $\pi(p) \mid 2(p+1)$.

THEOREM 2.3. (i) *If* $m > 2$, *then*

$$\pi(m) = a(m)\beta(m) = (2, \beta(m))[2, a(m)].$$

(ii) *For each* $m, n \in M$,

$$a([m, n]) = [a(m), a(n)].$$

(iii) *For each* $m, n \in M$,

$$\pi([m, n]) = [\pi(m), \pi(n)].$$

THEOREM 2.4. *If* p *is an odd prime, then there exists a positive integer* ε *such that for any* $k > 1$, $a(p^k) = a(p)p^\gamma$ *and* $\pi(p^k) = \pi(p)p^\gamma$, *where* $\gamma = \max(0, k-\varepsilon)$.

An analysis involving the so-called Fibonacci matrix $F = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ is central to Robinson's development. Notice that

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

The matrix F along with some general theorems by Bollman [1] are employed here to provide new proofs of Theorems 2.2 and 2.4.

3. Some new proofs. The following is a new proof of parts (ii) and (iii) of Theorem 2.2.

(ii) The minimal polynomial of the Fibonacci matrix F is $m(x) = x^2-x-1$, and the discriminant of $m(x)$ is 5. It is known that $p \equiv \pm 1 \pmod 5$ implies 5 is a square and thus

$$m(x) = (x-2^{-1}(1+\sqrt{5}))(x-2^{-1}(1-\sqrt{5})),$$

where each of the zeros of $m(x)$ has order a divisor of $p-1$ in the multiplicative group of $GF(p)$. Hence, Bollman's Theorem 4.1 [1] requires F to have order a divisor of $p-1$ in $GF(p)$ if $p \equiv \pm 1 \pmod 5$.

(iii) If $p \equiv \pm 2 \pmod 5$, then 5 is not a square in $GF(p)$. Thus, $m(x)$ is irreducible in the polynomial ring $GF[p; x]$. Then the splitting field of $m(x)$ is $GF(p^2)$, which is isomorphic to $GF[p; x]/(m(x))$, where $(m(x))$ is the cyclic ideal generated by $m(x)$ in $GF[p; x]$. Therefore, t and $1-t$, the isomorphic copies in $GF(p^2)$ of the cosets $x+(m(x))$ and $1-x+(m(x))$, respectively, are roots of $m(x)$ in the splitting field $GF(p^2)$. Now $t^2 = 1+t$ and

$$t^{2(p+1)} = (1+t)^{p+1} = \sum_0^{p+1} \binom{p+1}{k} t^k = 1+t+t^p+t^{p+1},$$

since $GF(p^2)$ has characteristic p. Moreover, it can be shown by induction that $t^n = u_n t + u_{n-1}$. Hence,

$$t^{2(p+1)} = 1+t+u_p t+u_{p-1}+u_{p+1}t+u_p.$$

It is shown in [5] that $u_p \equiv -1$ and $u_{p+1} \equiv 0 \pmod p$ if $p \equiv \pm 2 \pmod 5$. Hence $t^{2(p+1)} = 1$ in $GF(p^2)$. Furthermore, $(1-t)^{2(p+1)} = (-t^{-1})^{2(p+1)} = 1$ in $GF(p^2)$. Hence, Bollman's Theorem 4.1 applies and $\pi(p) \mid 2(p+1)$.

This proof is offered as an algebraic alternative to Robinson's graph theoretic proof of Theorem 2.2.

COROLLARY 3.1. *If* q *is a prime and* $q \mid \pi(p)$, *where* $p > 5$, *then* $q < p$.

Theorem 2.4 is a corollary to Bollman's Theorem 5.2. To prove Theorem 2.4, let $T = F^{\pi(p)}$ in Bollman's Theorem 5.2 and notice that β exists for each prime p as the exponent of p in the factorization of $u_{\pi(p)}$ into positive integral powers of distinct primes.

4. The Leonardo logarithm and the Fibonacci frequency. The results of the previous sections are needed to prove the main results of this paper, the two theorems stated in the introduction. Parts of these proofs rely on a knowledge of values of $\pi(m)$ for specific arguments. These values are to be found in the accompanying table. Also, it is known [5] that $\pi(p^k) = \pi(p)p^{k-1}$ for all $k > 1$ and all primes $p < 10000$, and this fact is implicit in some of the following.

LEMMA 4.1. *If* $m = (24)5^{\lambda-1}$, *where* $\lambda = 1, 2, 3, \ldots$, *then*

$$\pi(m) = m.$$

Proof. If $\lambda > 1$, then

$$\pi\left((24)5^{\lambda-1}\right) = [\pi(2^3), \pi(3), \pi(5^{\lambda-1})]$$

so that

$$\pi\left((24)5^{\lambda-1}\right) = [(3)2^2, 2^3, (2^2)5^{\lambda-1}] = (24)5^{\lambda-1}.$$

Also,

$$\pi(24) = 24.$$

LEMMA 4.2. *If* $\pi(m) = m$, *then* $m = (24)5^{\lambda-1}$ *for some* $\lambda > 0$.

Proof. Let $m = 2^{\beta_1}3^{\beta_2}5^{\beta_3}p_1^{\theta_1}p_2^{\theta_2}\dots p_r^{\theta_r}$ be the factorization of m as a product of integral powers of distinct primes with the $\beta_i \geqslant 0$, $i = 1, 2, 3$, with the $\theta_j > 0, j = 1, 2, \dots, r$, and with $5 < p_1 < \dots < p_r$. As in Theorem 2.4, let $\gamma_i = \max(0, \theta_i - \varepsilon_i)$ and $\pi(p^{\theta_i}) = \pi(p)p^{\gamma_i}$. If each $\beta_i \geqslant 1$ for $i = 1, 2, 3$, then $m = \pi(m) = [(3)2^{\beta_1-1}, (2^3)3^{\beta_2-1}, (2^2)5^{\beta_3-1}, \pi(p_1)p_1^{\gamma_1}, \dots, \pi(p_r)p_r^{\gamma_r}]$. Again by Theorem 2.4, $\theta_r > \gamma_r$ if and only il $\theta_r \neq 0$ and by Corollary 3.1, $p_r \nmid \pi(p_i)$ for any $i = 1, 2, \dots, r$. Thusf $\theta_r = 0$, and it follows (by an inductive argument) that $\theta_i = 0$ for al, $i = 1, 2, \dots, r$. Hence, $m = 2^{\beta_1}3^{\beta_2}5^{\beta_3}$ so that $\beta_1 = 3$ and $\beta_2 = 1$. Therefore, $m = (24)5^{\beta_3}$. Clearly, $\pi(m) \neq m$ if some or all $\beta_i = 0$.

The Fixed Point Theorem follows from Lemmas 4.1 and 4.2.

LEMMA 4.3. *For each* $m \in M$, $24 \mid \pi^N(m)$ *for all* $N \geqslant 5$.

Proof. If $m > 2$, then by Theorem 2.3 (i), $2 \mid \pi(m)$, and since $\pi(2) = 3$, $3 \mid \pi^2(m)$. But $\pi(3) = 2^3$ so that $2^3 \mid \pi^3(m)$. Thus, $\pi(2^3) = (3)2^2 \mid \pi^4(m)$. Finally, $\pi(24) = 24$ so that $24 \mid \pi^5(m)$. By the same argument if $2 \mid m$, then $24 \mid \pi^4(m)$. The assertion follows by a simple inductive argument.

LEMMA 4.4. *If* $m = 2^{\theta_1}3^{\theta_2}5^{\theta_3}$, *where* $\theta_1 \geqslant 3$, $\theta_2 \geqslant 1$, *and* $\theta_3 \geqslant 0$, *then for some* N, $\pi^N(m) = (24)5^{\theta_3}$.

Proof. If $\theta_3 = 0$ then $\pi(m) = [(3)^{2\theta_1-1}, (2^3)3^{\theta_2-1}] = 2^{\beta_1}3^{\beta_2}$, where $3 \leqslant \beta_1 < \theta_1$ and where $1 \leqslant \beta_2 < \theta_2$. Thus, for some N, $\pi^N(m) = 24$. If $\theta_3 > 0$, then $\pi(m) = 2^{\beta_1}3^{\beta_2}5^{\theta_3}$ since $\pi(5^{\theta_3}) = 2^2 5^{\theta_3}$. Thus, for some N, $\pi^N(m) = (24)5^{\theta_3}$.

Proof of the Iteration Theorem. By Lemma 4.3, we can assume, without loss of generality, that $m = 2^{\theta_1}3^{\theta_2}5^{\theta_3}p_1^{\beta_1}p_2^{\beta_2}\dots p_r^{\beta_r}$, where each p_i is a prime, where $5 < p_1 < \dots < p_r$, and where $\theta_1 \geqslant 3$, $\theta_2 \geqslant 1$, $\theta_3 \geqslant 0$, $\beta_r \geqslant 1$. By Theorem 2.4, Theorem 2.3 (iii), and Corollary 3.1, $\pi(m) = 2^{\gamma_1}3^{\gamma_2}5^{\gamma_3}p_1^{\delta_1}p_2^{\delta_2}\dots p_r^{\delta_r}$, where $0 \leqslant \delta_r < \beta_r$. Thus, for each iteration of π the power of the largest prime greater than five which divides m is strictly decreasing. Hence, for some N, $\pi^N(m) = 2^{\gamma_1}3^{\gamma_2}5^{\gamma_3}$, where $\gamma_1 \geqslant 3$, $\gamma_2 \geqslant 1$, $\gamma_3 \geqslant 0$. By Lemma 4.4, the Iteration Theorem follows.

As a final remark, we note that it follows by a very simple argument that ω is unbounded on M. To see that, let n be a positive integer and let $m = 2^{n+4}$. One can show that $\omega(m) = n+1$. It is clear that λ is unbounded on M.

5. A table. The following is a brief table of the functions discussed in this paper. A more extensive table is to be found in [2].

TABLE 5.1. Arithmetical function values for $\pi(m)$, $\beta(m)$, $\alpha(m)$, $\omega(m)$, and $\lambda(m)$, $m = 2, 3, \dots, 40$.

m	$\pi(m)$	$\beta(m)$	$\alpha(m)$	$\omega(m)$	$\lambda(m)$
2	3	1	3	4	1
3	8	2	4	3	1
4	6	1	6	2	1
5	20	4	5	3	2
6	24	2	12	1	1
7	16	2	8	2	1
8	12	2	6	2	1
9	24	2	12	1	1
10	60	4	15	2	2
11	10	1	10	3	2
12	24	2	12	1	1
13	28	4	7	3	1
14	48	2	24	2	1
15	40	2	20	3	2
16	24	2	12	1	1
17	36	4	9	2	1
18	24	2	12	1	1
19	18	1	18	2	1
20	60	2	30	2	2
21	16	2	8	2	1
22	30	1	30	2	2
23	48	2	24	2	1
24	24	2	12	1	1
25	100	4	25	3	3
26	84	4	21	3	1
27	72	2	36	2	1
28	48	2	24	2	1
29	14	1	14	3	1
30	120	2	60	1	2
31	30	1	30	2	2
32	48	2	24	2	1
33	40	2	20	3	2
34	36	4	9	2	1
35	80	2	40	2	2
36	24	2	12	1	1
37	76	4	19	3	1
38	18	1	18	2	1
39	56	2	28	3	1
40	60	2	30	2	2

References

[1] Dorothy A. Bollman, *Some periodicity properties of transformations on vector spaces over residue class rings*, J. Soc. Indust. Appl. Math. 13 (1965), pp. 902–912.

[2] Beth H. Hannon and William L. Morris, *Tables of arithmetical functions related the Fibonacci numbers*, Oak Ridge National Laboratory Report ORNL-4261, 1968.

[3] J. L. Lagrange, *Oeuvres de LaGrange*, Gauthier Villars, Paris 7 (1877), pp. 5–182.

[4] D. W. Robinson, *The Fibonacci matrix modulo m*, Fibonacci Quart. 1 (1963), pp. 29–36.

[5] D. D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly 67 (1960), pp. 525–532.

Reçu par la Rédaction le 15. 7. 1968

ACTA ARITHMETICA
XVI (1969)

Mittlere Darstellungen natürlicher Zahlen als Differenz zweier k-ter Potenzen

von

EKKEHARD KRÄTZEL (Jena)

§ 1. Einleitung. Es bezeichne

$$t_k(\varrho) = 2 \sum_{m^k - n^k = \varrho}{}' 1$$

mit nicht-negativen ganzen Zahlen m, n unter der Bedingung $m > n \geqslant 0$. Die natürliche Zahl k werde stets als größer oder gleich 3 vorausgesetzt. Der Strich am Summenzeichen bedeute, daß das Glied $n = 0$ den Faktor $\frac{1}{2}$ erhält. Untersucht werden soll die Funktion

$$T_k(x) = \sum_{1 \leqslant \varrho \leqslant x} t_k(\varrho)$$

auf ihr Verhalten für große x. Ohne Schwierigkeiten kann man

$$T_k(x) = \frac{1}{2k\cos\frac{\pi}{k}} \cdot \frac{\Gamma^2\left(\frac{1}{k}\right)}{\Gamma\left(\frac{2}{k}\right)} x^{\frac{2}{k}} + 2\zeta\left(\frac{1}{k-1}\right)\left(\frac{x}{k}\right)^{\frac{1}{k-1}} + O(x^{\frac{1}{k}})$$

beweisen. Es soll gezeigt werden, daß man die Abschätzung des Restes zu $O(x^{(k-1)/k^2})$ verbessern kann. Eine weitere Verbesserung der Abschätzung ist nicht möglich. Das wird sich als selbstverständlich erweisen, da gezeigt wird, daß sich in erster Näherung der Rest durch eine Funktion mit genau der genannten Größenordnung darstellen läßt. Es erhebt sich damit das Problem nach der Größenordnung der zweiten Näherung. Die Ergebnisse sind in den Sätzen 1 und 2 dargestellt. Es soll noch darauf hingewiesen werden, daß sich unmittelbare Parallelen zu den Ergebnissen über

$$R_{k,2}(x) = 4 \sum_{\substack{n^k + m^k \leqslant x \\ n,m \geqslant 0}}{}'' 1$$

($n = 0$, $m = 0$ erhalten den Faktor $\frac{1}{2}$), dargestellt in [4], anbieten.