THE RELATION OF THE PERIOD MODULO TO THE RANK OF APPARITION OF m IN THE FIBONACCI SEQUENCE

JOHN VINSON, Aerojet–General Corporation, Sacramento, Calif.

The Fibonacci sequence is defined by the recurrence relation,

(1) $$u_{n+2} = u_{n+1} + u_n\,, \qquad n = 0, 1, 2, \quad ,$$

and the initial values $u_0 = 0$ and $u_1 = 1$. Lucas [2, pp. 297-301] has shown that every integer, m, divides some member of the sequence, and also that the sequence is periodic modulo m for every m. By this we mean there is an integer, k, such that

(2) $$u_{k+n} \equiv u_n \pmod{m}\,, \qquad n = 0, 1, 2, \cdots \;.$$

<u>Definition.</u> The period modulo m, denoted by s(m), is the smallest positive integer, k, for which the system (2) is satisfied.

<u>Definition.</u> The rank of apparation of m, denoted by f(m), is the smallest positive integer, k, for which $u_k \equiv 0 \pmod{m}$.

Wall [3] has shown that

(3) $$u_n \equiv 0 \pmod{m} \text{ iff } f(m) | n.$$

In particular, since $u_{s(m)} \equiv u_0 \equiv 0 \pmod{m}$ we have

(4) $$f(m) \,|\, s(m)\;.$$

<u>Definition.</u> We define a function t(m) by the equation f(m)t(m) = s(m).

We note that t(m) is an integer for all m. The purpose of this paper is to give criteria for the evaluation of t(m).

Now we give some results which will be needed later.

(5) $$u^2_{n-1} = u_n u_{n-2} + (-1)^n \;.$$

This can be proved by induction, using the recurrence relation (1).

This paper was part of a thesis submitted in 1961 to Oregon State University in partial fulfillment of the requirements for the degree of master of Arts.

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad \text{where } \alpha = \frac{1 + \sqrt{5}}{2} \text{ and } \beta = \frac{1 - \sqrt{5}}{2}. \tag{6}$$

This is the well-known "Binet formula." It gives a natural extension of the Fibonacci sequence to negative values of n. By using the relation $\alpha^n\beta^n = (-1)^n$, we find

$$u_{-n} = (-1)^{n+1} u_n . \tag{7}$$

From this we see that the recurrence (1) holds for the extended sequence.

By solving the system

$$\alpha^k - \beta^k = (\alpha - \beta)\, u_k$$

$$\alpha \cdot \alpha^k - \beta \cdot \beta^k = (\alpha - \beta)\, u_{k+1}$$

for α^k and β^k, we obtain

$$\alpha^k = u_{k+1} - \beta u_k = (1 - \beta)u_k + u_{k-1} = \alpha u_k + u_{k-1}$$

and

$$\beta^k = u_{k+1} - \alpha u_k = (1 - \alpha)\, u_k + u_{k-1} = \beta u_k + u_{k-1} .$$

Then

$$(\alpha - \beta)\, u_{nk+r} = \alpha^{nk+r} - \beta^{nk+r} = (\alpha u_k + u_{k-1})^n \alpha^r - (\beta u_k + u_{k-1})^n \beta^r$$

By expanding and recombining we get (for $n \geq 0$)

$$u_{nk+r} = \sum_{j=0}^{n} \binom{n}{j} u_k^j\, u_{k-1}^{n-j}\, u_{r+j} .$$

Now if we set $k = f(m)$, we find

$$u_{nf(m)+r} \equiv u_{f(m)-1}^n\, u_r \pmod{m} . \tag{8}$$

We note that this is valid for negative as well as non-negative integers, r.

Lemma 1. $t(m)$ is the exponent to which $u_{f(m)-1}$ belongs (mod m).

Proof: Suppose $u^n_{f(m)-1} \equiv 1 \pmod m$. Then from (8) we have $u_{nf(m)+r} \equiv u_r \pmod m$ for all r. It follows from the definition of $s(m)$ that $s(m) \leq nf(m)$ and thus $u^n_{f(m)-1} \equiv 1 \pmod m$ implies $t(m) = s(m)/f(m) \leq n$.

Now we set $r = 1$ and $n = t(m)$ in (8) to obtain

$$u^{t(m)}_{f(m)-1} \equiv u_{t(m)f(m)+1} \equiv u_{s(m)+1} \equiv u_1 \equiv 1 \pmod m .$$

Thus $t(m)$ is the smallest positive n for which $u^n_{f(m)-1} \equiv 1 \pmod m$, that is, $u_{f(m)-1}$ belongs to $t(m)$ (mod m).

Theorem 1. For $m > 2$ we have

i) $t(m) = 1$ or 2 if $f(m)$ is even, and

ii) $t(m) = 4$ if $f(m)$ is odd.

Also, $t(1) = t(2) = 1$. Conversely, $t(m) = 4$ implies $f(m)$ is odd, $t(m) = 2$ implies $f(m)$ is even, and $t(m) = 1$ implies $f(m)$ is even or $m = 1$ or 2.

Proof. The cases $m = 1$ and $m = 2$ are easily verified. Now suppose $m > 2$ and set $n = f(m)$ in (5) to get

$$u^2_{f(m)-1} \equiv u_{f(m)}u_{f(m)-2} + (-1)^{f(m)} \equiv (-1)^{f(m)} \pmod m \quad .$$

If $f(m)$ is even we have $u^2_{f(m)-1} \equiv 1 \pmod m$, and i) follows from Lemma 1.

If $f(m)$ is odd we have $u^2_{f(m)-1} \equiv -1 \pmod m$, and since $m > 2, u^2_{f(m)-1} \not\equiv 1 \pmod m$. This implies $u_{f(m)-1} \not\equiv \pm 1 \pmod m$ and then

$$u^3_{f(m)-1} \equiv u^2_{f(m)-1}u_{f(m)-1} \equiv -u_{f(m)-1} \not\equiv \pm 1 \pmod m.$$

Finally, $u^4_{f(m)-1} \equiv (u^2_{f(m)-1})^2 \equiv (-1)^2 \equiv 1 \pmod m$ and, by Lemma 1, $t(m) = 4$.

The converse follows from the fact that the cases in the direct statement of the theorem are all inclusive.

Theorem 2. Let p be an odd prime and let e be any positive integer. Then

i) $t(p^e) = 4$ if $2 \nmid f(p)$,

ii) $t(p^e) = 1$ if $2 \mid f(p)$ but $4 \nmid f(p)$,

iii) $t(p^e) = 2$ if $4 \mid f(p)$, and

iv) $t(2^e) = 2$ for $e \geq 3$ and $t(2) = t(2^2) = 1$.

Conversely, if q represents any prime, then $t(q^e) = 4$ implies $f(q)$ is odd, $t(q^e) = 2$ implies $4 \mid f(q)$ or $q = 2$ and $e \geq 3$, and $t(q^e) = 1$ implies $2 \mid f(q)$ but $4 \nmid f(q)$ or $q^e = 2$ or 4.

Proof. Wall [3, p. 527] has shown that if $p^{n+1} \nmid u_{f(p^n)}$, then $f(p^{n+1}) = pf(p^n)$. It follows by induction that $f(p^e) = p^k f(p)$, where k is some non-negative integer. We emphasize that $f(p^e)$ and $f(p)$ are divisible by the same power of 2, since this fact is used several times in the sequel without further explicit reference.

In case i), $f(p^e)$ is odd and the result is given by setting $m = p^e$ in Theorem 1.

In cases ii) and iii), $f(p^e)$ is even and we may set $m = p^e$, $n = 1$, and $r = \frac{1}{2} f(p^e)$ in (8) to get

$$u_{\frac{1}{2}f(p^e)} \equiv u_{f(p^e)-1} \quad u_{-\frac{1}{2}f(p^e)} \pmod{p^e}$$

which, in view of (7), is the same as

$$u_{f(p^e)-1} \quad u_{\frac{1}{2}f(p^e)} \equiv (-1)^{\frac{1}{2}f(p^e)+1} u_{\frac{1}{2}f(p^e)} \pmod{p^e} \quad .$$

Now $\frac{1}{2}f(p^e) = \frac{1}{2}p^k f(p)$, where k is some non-negative integer, and we see that $f(p) \nmid \frac{1}{2}f(p^e)$. Then from (3) we have $p \nmid u_{\frac{1}{2}f(p^e)}$ so that we may divide the above congruence by $u_{\frac{1}{2}f(p^e)}$. We get

$$u_{f(p^e)-1} \equiv (-1)^{\frac{1}{2}f(p^e)+1} \pmod{p^e} \quad .$$

Now in case ii), $\frac{1}{2}f(p)$ is odd and so is $\frac{1}{2}f(p^e)$, and the last congruence gives $u_{f(p^e)-1} \equiv 1 \pmod{p^e}$ and thus, by Lemma 1, $t(p^e) = 1$.

In case iii) the congruence becomes

$$u_{f(p^e)-1} \equiv -1 \pmod{p^e} \quad ,$$

since

$$\tfrac{1}{2}f(p) \quad \text{and} \quad \tfrac{1}{2}f(p^e)$$

are both even. Then

$$u^2_{f(p^e)-1} \equiv 1 \pmod{p^e}$$

and by Lemma 1 again, $t(p^e) = 2$.

In case iv) we can easily verify $t(2) = t(2^2) = 1$. That $t(2^e) = 2$ for $e \geq 3$ follows from results given by Carmichael [1, p. 42] and Wall [3, p. 527]. These results are, respectively:

A. Let q be any prime and let r be any positive integer such that $(q, r) = 1$. If $q^{\lambda} \mid u_n$ and $q^{\lambda+1} \nmid u_n$, then $q^{\lambda+a} \mid u_{nrq^a}$ and $q^{\lambda+a+1} \nmid u_{nrq^a}$ except when $q = 2$ and $\lambda = 1$.

B. Let q be any prime and let λ be the largest integer such that $s(q^{\lambda}) = s(q)$. Then $s(q^e) = q^{e-\lambda} s(q)$ for $e \geq \lambda$.

The hypotheses of A. are satisfied by $q = 2$, $\lambda = 3$, and $n = f(2^3)$, and we find that $2^{3+a} \mid u_{kf(2^3)}$ iff $2^a \mid k$. It follows from (3) that $f(2^{3+a})$ must be a multiple of $f(2^3)$, hence $f(2^{3+a}) = 2^a f(2^3)$. Since $f(2^3) = 2f(2)$ we have $f(2^e) = 2^{e-2} f(2)$ for $e \geq 3$. Now set $q = 2$ and $\lambda = 1$ in B. We get $s(2^e) = 2^{e-1} s(2)$. Thus for $e \geq 3$ we have

$$t(2^e) = \frac{s(2^e)}{f(2^e)} = \frac{2^{e-1} s(2)}{2^{e-2} f(2)} = 2 .$$

The converse follows from the fact that the cases in the direct statement of the theorem are all inclusive. This completes the proof.

Now we give a lemma which is needed in the proof of the next theorem.

Lemma 2. If m has the prime factorization

$$m = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_n^{\alpha_n} , \text{ then}$$

i) $s(m) = \underset{1 \leq i \leq n}{\text{l.c.m.}} \{s(q_i^{\alpha_i})\}$, and

ii) $f(m) = \underset{1 \leq i \leq n}{\text{l.c.m.}} \{f(q_i^{\alpha_i})\}$.

Wall has given i). The proof of ii) is as follows: Since the $q_i^{\alpha_i}$ are pairwise relatively prime, $m \mid u_k$ is equivalent to $q_i^{\alpha_i} \mid u_k$ $(i = 1, 2, \cdots, n)$, which, by (3), is equivalent to $f(q_i^{\alpha_i}) \mid k$ $(i = 1, 2, \cdots, n)$. The smallest positive k which satisfies these conditions is

$$k = \underset{1 \leq i \leq n}{\text{l.c.m.}} \{f(q_i^{\alpha_i})\} ,$$

which, according to the definition of $f(m)$, gives the desired result.

Theorem 3. We have

i) $t(m) = 4$ if $m > 2$ and $f(m)$ is odd.

ii) $t(m) = 1$ if $8 \nmid m$ and $2 \mid f(p)$ but $4 \nmid f(p)$ for every odd prime, p, which divides m, and

iii) $t(m) = 2$ for all other m.

Proof: From what has already been given in Theorem 1, we see that it suffices to show that the conditions given here in ii) are both necessary and sufficient for $t(m) = 1$. Let m have the prime factorization $m = q_1^{\alpha_1} q_2^{\alpha_2} \quad q_n^{\alpha_n}$ and set

$$f(q_i^{\alpha_i}) = 2^{\gamma_i} K_i \qquad (i = 1, 2, \cdots, n) \quad ,$$

where the K_i are odd integers. By Theorem 1, we may set

$$t(q_i^{\alpha_i}) = 2^{\delta_i} \qquad (i = 1, 2, \cdots, n) \qquad \text{where } \delta_i = 0, 1, \text{ or } 2.$$

Then $s(q_i^{\alpha_i}) = f(q_i^{\alpha_i}) t(q_i^{\alpha_i}) = 2^{\gamma_i + \delta_i} K_i$ $(i = 1, 2, \cdots, n)$. From Lemma 2 we have, where K is an odd integer,

$$s(m) = \underset{1 \le i \le n}{\text{l. c. m.}} \{s(q_i^{\alpha_i})\} = 2^{\max(\gamma_i + \delta_i)} K,$$

$$f(m) = \underset{1 \le i \le n}{\text{l. c. m.}} \ f(q_i^{\alpha_i}) = 2^{\max \gamma_i} K, \text{ and}$$

$$t(m) = s(m)/f(m) = 2^{\max(\gamma_i + \delta_i) - \max \gamma_i}$$

Now suppose $t(m) = 1$. Then $\max(\gamma_i + \delta_i) = \max \gamma_i$. Let $\gamma_k = \max \gamma_i$. We have

$$\gamma_k \le \gamma_k + \delta_k \le \max(\gamma_i + \delta_i) = \max \gamma_i = \gamma_k ,$$

and thus $\delta_k = 0$ and $t(q_k^{\alpha_k}) = 2^{\delta_k} = 1$. It follows from Theorem 2 that $4 \nmid f(q_k^{\alpha_k})$, that is, that $\gamma_k \le 1$. Then for all i,

$$\delta_i \le \max(\gamma_i + \delta_i) = \max \gamma_i = \gamma_k \le 1 \ .$$

Furthermore, $\delta_i = 1$ is impossible, for $\delta_i = 1$ is the same as $t(q_i^{\alpha_i}) = 2$ which implies, by Theorem 2, that $2 \ f(q_i^{\alpha_i})$ and thus $\gamma_i \ge 1$. Then we would have

$\gamma_i + \delta_i \geq 2$, which is contrary to $\max(\gamma_i + \delta_i) \leq 1$. Thus for all i, $\delta_i = 0$ and $t(q_i^{\alpha_i}) = 2^{\delta_i} = 1$, which, by Theorem 2, is equivalent to the conditions given in ii).

Now suppose, conversely, that the conditions given in ii) are satisfied, which, as we have just seen, is equivalent to the condition $t(q_i^{\alpha_i}) = 1$ for all i. Then

$$s(q_i^{\alpha_i}) = f(q_i^{\alpha_i})\, t(q_i^{\alpha_i}) \quad \text{for all } i.$$

Then Lemma 2 gives

$$s(m) = \underset{1 \leq i \leq n}{\text{l. c. m.}} \{s(q_i^{\alpha_i})\} = \underset{1 \leq i \leq n}{\text{l. c. m.}} \{f(q_i^{\alpha_i})\} = f(m)$$

and thus $t(m) = s(m)/f(m) = 1$.

Our last theorem is of rather different character. Once again, we need a preliminary lemma.

Lemma 3. Let p be an odd prime. Then

i) $f(p) \mid (p - 1)$ if $p \equiv \pm 1 \pmod{10}$,

ii) $f(p) \mid (p + 1)$ if $p \equiv \pm 3 \pmod{10}$,

iii) $s(p) \mid (p - 1)$ if $p \equiv \pm 1 \pmod{10}$, and

iv) $s(p) \nmid (p + 1)$ but $s(p) \mid 2(p + 1)$ if $p \equiv \pm 3 \pmod{10}$.

Lucas [2, p. 297] gave the following result:

$$p \mid u_{p-1} \text{ if } p \equiv \pm 1 \pmod{10} \text{ and } p \mid u_{p+1} \text{ if } p \equiv \pm 3 \pmod{10}.$$

We get i) and ii) by applying (3) to this result. Wall [3, p. 528] has given iii) and iv).

Theorem 4. Let p be an odd prime and let e be any positive integer. Then

i) $t(p^e) = 1$ if $p \equiv 11$ or $19 \pmod{20}$,

ii) $t(p^e) = 2$ if $p \equiv 3$ or $7 \pmod{20}$,

iii) $t(p^e) = 4$ if $p \equiv 13$ or $17 \pmod{20}$, and

iv) $t(p^e) \neq 2$ if $p \equiv 21$ or $29 \pmod{40}$.

Proof: Theorem 2 shows that $t(p^e)$ is independent of the value of e, hence is sufficient to consider $e = 1$ throughout the proof.

If follows from the definition of ff(p) that $p \nmid u_{f(p)-1}$ so that by Fermat's theorem,

$$u_{f(p)-1}^{p-1} \equiv 1 \pmod p.$$

Then, since $u_{f(p)-1}$ belongs to $t(p) \pmod p$, it follows that $t(p) \mid (p-1)$. Now if $p \equiv 3 \pmod 4$ we have $4 \nmid (p-1)$ and thus $t(p) \neq 4$.

i) Here $p \equiv 3 \pmod 4$ so $t(p) \neq 4$. Suppose $t(p) = 2$. Then, by Theorem 2, $4 \mid f(p)$. Now $p \equiv \pm 1 \pmod{10}$ and, by Lemma 3 i), $f(p)\ (p-1)$ and thus $4 \mid (p-1)$. But this is impossible when $p \equiv 3 \pmod 4$, hence $t(p) \neq 2$ and we must have $t(p) = 1$.

ii) Again $p \equiv 3 \pmod 4$ and $t(p) \neq 4$. Also $p \equiv \pm 3 \pmod{10}$ and it follows from Lemma 3 that $s(p) \neq f(p)$ and $t(p) = s(p)/f(p) \neq 1$. Hence $t(p) = 2$.

iii) We have just seen that $t(p) \neq 1$ when $p \equiv \pm 3 \pmod{10}$, which is here the case. Also, $f(p) \mid (p+1)$. Now $p \equiv 1 \pmod 4$ so that $4 \nmid (p+1)$ and thus $4 \nmid f(p)$, and it follows from Theorem 2 that $t(p) \neq 2$. Hence $t(p) = 4$.

iv) Suppose $t(p) = 2$. Then by Theorem 2, $4 \mid f(p)$ and thus $8 \mid s(p)$ (since $s(p) = t(p)f(p) = 2f(p)$). Furthermore, $s(p) \mid (p-1)$ since $p \equiv \pm 1 \pmod{10}$. Then $t(p) = 2$ implies $8 \mid (p-1)$. But we have $p - 1 \equiv 20$ or $28 \pmod{40}$ which gives $p - 1 \equiv 4 \pmod 8$, so that $8 \mid (p-1)$ is impossible. Hence $t(p) \neq 2$.

We naturally ask if anything more can be said about $t(p^e)$ for $p \equiv 1, 9, 21, 29 \pmod{40}$. The following examples show that the theorem is "complete":

$p \equiv 1 \pmod{40}$	:	$t(521) = 1$,	$t(41) = 2$,	$t(761) = 4$.
$p \equiv 9 \pmod{40}$	:	$t(809) = 1$,	$t(409) = 2$,	$t(89) = 4$.
$p \equiv 21 \pmod{40}$	:	$t(101) = 1$,	$t(61) = 4$.	
$p \equiv 29 \pmod{40}$	:	$t(29) = 1$,	$t(109) = 4$.	

Now we might ask whether there is a number, m, for which $t(p^e)$ is always determined by the modulo m residue class to which p belongs. The answer to this question is not known. We note that the principles upon which the proof of Theorem 4 is based are not applicable to other moduli.

REFERENCES

1. R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, Ann. of Math. 15 (1913-1914), 30-70.
2. E. Lucas, Théorie des fonctions numériques simplement périodiques, Amer. J. Math. 1 (1878), 184-240, 289-321.
3. D. D. Wall, Fibonacci series modulo m, Amer. Math. Monthly 67 (1960), 525-532.

SPECIAL NOTICE

The Fibonacci Association has on hand 14 copies of Dov Jarden, Recurrent Sequences, Riveon Lematematika, Jerusalem, Israel. This is a collection of papers on Fibonacci and Lucas numbers with extensive tables of factors extending to the 385th Fibonacci and Lucas numbers. The volume sells for $5.00 and is an excellent investment. Check or money order should be sent to Verner Hoggatt at San Jose State College, San Jose, Calif.

REFERENCES TO THE QUARTERLY

Martin Gardner, Editor, Mathematics Games, Scientific American, June, 1963 (Column devoted this issue to the helix.)

A Review of The Fibonacci Quarterly will appear in the Feb. 1963 issue of the Recreational Mathematics Magazine.

FIBONACCI NEWS

Brother U. Alfred reports that he is currently offering a one unit course on Fibonacci Numbers at St. Mary's College.

Murray Berg, Oakland, Calif., reports that he has computed phi to some 2300 decimals by dividing F_{11004} by F_{11003} on a computer. Any inquiries should be addressed to the editor.

Charles R. Wall, Ft. Worth, Texas, reports that he is working on his master's thesis in the area of Fibonacci related topics.

SORTING ON THE B-5000 -- Technical Bulletin 5000-21004P Sept., 1961, Burroughs Corporation, Detroit 32, Michigan.

This contains in Section 3 the use of Fibonacci numbers in the merging of information using three tape units instead of the usual four thus effecting considerable efficiency. (This was brought to our attention by Luanne Anglemyer and the pamphlet was sent to us by Ed Olson of the San Jose office.)

S. L. Basin, Generalized Fibonacci Numbers and Squared Rectangles, American Mathematical Monthly, pp. 372-379, April, 1963.

J. A. H. Hunter and J. S. Madachy, Mathematical Diversions, D. Van Nostrand Company, Inc., Princeton, New Jersey, 1963.

S. K. Stein, The Intersection of Fibonacci Sequences, Michigan Math. Journal, 9 (1962), Dec., No. 4, pp. 399-402. (Correction)

L. Carlitz, Generating Functions for Powers of Certain Sequences of Numbers, Duke Math. Journal, Vol. 29(1962), Dec., No. 4, pp. 521-538. (Correction)

V. E. Hoggatt, Jr. and S. L. Basin, The First 571 Fibonacci Numbers, Recreational Mathematics Magazine, Oct., 1962, pp. 19-31.

A. F. Horadam, Complex Fibonacci Numbers and Fibonacci Quaternions, The American Mathematical Monthly, Mar., 1963, pp. 289-291.

S. L. Basin, The Appearance of Fibonacci Numbers and the Q-matrix in Electrical Network Theory, Math. Magazine, Vol. 36, No. 2, March 1963, pp. 84-97.

J. Browkin and A. Schinzel, On the Equation $2^n - D = y^2$, Bulletin de l'Academie Polonaise des Sciences, Serie des sci. math., astr. et phys. --Vol. VIII, No. 5, 1960, pp. 311-318.

Georges Browkin and Andre Schnizel, Sur les nombres de Mersenne qui sont triangulaires, Comptes rendues des seances de l'Academie des sciences, t. 242, pp. 1780-1781, seance du 4 Avril 1956.

C. D. Olds, Continued Fractions, Random House (New Mathematical Library Series--part of the Monograph Project of SMSG) 1963.

This is an excellent understandable treatment of the subject at a reasonable level with many interesting topics for those devoted to the study of integers with special properties.

L. Zippin, Uses of Infinity, Random House (New Mathematical Library Series, 1962.)

This has no index which makes the Fibonacci topics harder to find but there are several interesting comments there.

Mannis Charosh, Problem Department, Mathematics Student Journal, May, 1963.

In the editorial comment following the solution of Problem 187, there is a little generalized result similar to problem B-2 of the Elementary Problems and Solutions section of the Fibonacci Quarterly, Feb., 1963.

A. Rotkiewicz, On Lucas Numbers with Two Intrinsic Prime Divisors, Bulletin de l'Academie Polonaise des Sciences, Serie des sci. math., astr. et phys. -- Vol. X., No. 5, 1962.