FIBONACCI SEQUENCES OF PERIOD n IN GROUPS

HOWARD J. WILCOX
Wellesley College, Wellesley, MA 02181
(Submitted February 1985)

An unusual application of Fibonacci sequences occurs in a musical composition by Iannis Xenakis. In *Nomos Alpha* the composer uses Fibonacci sequences of group elements to produce "Fibonacci motions," sequences of musical properties such as pitch, volume, and timbre that give the composition its framework (see [1], [4]). This setting suggests some interesting mathematical questions:

1. Given elements a and b in a finite abelian group , what is the period of the Fibonacci sequence $a, b, ab, ab^2, a^2b^3, \ldots$ in G?
2. Given an integer $n > 2$, is there a Fibonacci sequence of period n in a group G, and can such a sequence be readily obtained?

A helpful starting point is the paper entitled "Fibonacci Series Modulo m" by D. D. Wall [3]. With Wall, we let f_n denote the n^{th} member of the sequence of integers $f_0 = a$, $f_1 = b$, ..., where $f_{n+1} = f_n + f_{n-1}$. The symbol $h(m)$ will denote the length of the period of the sequence resulting from reducing each f_n modulo m. The basic Fibonacci sequence will be given by $u_0 = 0$, $u_1 = 1$, ... and the Lucas sequence by $v_0 = 2$, $v_1 = 1$, ... The symbol $k(m)$ will denote the lenght of the period of the basic Fibonacci sequence 0, 1, 2, 3, ... when it is reduced modulo m. Since we will often work in a group setting, we will let $\mathbb{Z}$ and $\mathbb{Z}_m$ represent the group of integers and the group of integers modulo m, respectively.

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

Theorem (Wall): In $\mathbb{Z}_m$, the following hold:

(1) Any Fibonacci sequence is periodic.

(2) If m has prime factorization $\prod p_i^{e_i}$ and if h_i denotes the period of the Fibonacci sequence $f_n \pmod{p_i^{e_i}}$, then $h(m) = \text{lcm}\{h_i\}$.

(3) The terms for which $u_n \equiv 0 \pmod{m}$ have subscripts which form a simple arithmetic progression.

(4) If p is prime and $p = 10x \pm 1$, then $k(p)$ divides $p - 1$.

(5) If p is prime and $p = 10x \pm 3$, then $k(p)$ divides $2p + 2$.

(6) If $k(p^2) \neq k(p)$, then $k(p^e) = p^{e-1}k(p)$ for $e > 1$.

The results in (4) and (5) give upper bounds for $k(p)$, but, as Wall points out, there are many primes for which $k(p)$ is less than the given upper bound. Unfortunately, one must obtain the sequence itself in order to determine $k(p)$. The following theorem provides a method for determining $k(m)$ from the prime factorization of certain u_i and v_i. We note first that in $\mathbb{Z}_2$ the sequence 0, 1, 1, ... has period 3 and in any group G, an element of order 2 yields a sequence 0, a, a, 0, ... of period 3.

Theorem 1: If $m > 2$, the sequence 0, 1, 1, 2, ..., u_n, ... has period $2n$ in $\mathbb{Z}_m$ for $n = \text{minimum}\{n \text{ even and } m|u_n;\ n \text{ odd and } m|v_n\}$.

Proof: Consider the sequence 0, 1, 1, 2, ..., u_n, ... in $\mathbb{Z}_m$. By Wall's Theorem, it is periodic, so we must have

$$0, 1, 1, 2, 3, \ldots, u_n, \ldots, -3, 2, -1, 1, 0, 1, \ldots$$

and the "middle" of the period must have one of the four forms:

(i) $\ldots, u_{n-2}, u_{n-1}, u_{n-1}, -u_{n-2}, \ldots;$

(ii) $\ldots, u_{n-2}, u_{n-1}, -u_{n-1}, u_{n-2}, \ldots;$

(iii) $\ldots, u_{n-2}, u_{n-1}, 0, u_{n-1}, -u_{n-2}, \ldots;$

(iv) $\ldots, u_{n-2}, u_{n-1}, u_n, -u_{n-1}, u_{n-2}, \ldots.$

If (i) occurs, then $u_{n-2} \equiv 0$ and $2u_{n-1} \equiv 0$. Thus, u_{n-1} equals 0 or has order 2 in $\mathbb{Z}_m$, and 0, 0, 0, ... or 0, u_{n-1}, u_{n-1}, 0, ... are the resulting sequences. These cannot occur, since 1 has order m in $\mathbb{Z}_m$.

If (ii) occurs, it is easy to obtain a similar result.

If (iii) occurs, $n - 1$ must be odd (so n is even) and $u_n \equiv 0 \pmod m$ so that $m|u_n$. These two conditions are sufficient to imply repetition after $2n$ terms, since we must then have 1, 1, 2, 3, ..., $2u_{n-1}$, $-u_{n-1}$, u_{n-1}, 0, u_{n-1}, u_{n-1}, $2u_{n-1}$, ..., $u_{n-1}u_{n-1} \equiv 1$, 0, ... by symmetry of the terms of odd index.

In (iv), $n - 1$ must be even (so n is odd) and $u_{n-1} + u_{n+1} \equiv 0 \pmod m$ so that $v_n \equiv 0 \pmod m$ and $m|v_n$. As in (iii), these two conditions imply repetition after $2n$ terms, for they require

$$1, 1, 2, \ldots, u_{n-1}, u_n, -u_{n-1}, u_n - u_{n-1}$$
$$= u_{n-2}, -u_{n-3}, \ldots, -u_2, u_{n-(n-1)}$$
$$= u_1 \equiv 1, 0, \ldots .$$

Thus, to find the period of the sequence 1, 1, 2, 3, ... modulo m, we need only locate the smallest n such that $m|u_n$ for even n or $m|v_n$ for odd n. The period of the sequence will equal $2n$.

Since the period is always $2n$, we easily obtain a result of Wall.

Corollary 1: For $m > 2$, the sequence 1, 1, 2, 3, ... modulo m has even period.

Example: In $\mathbb{Z}_{13}$, the sequence 1, 1, 2, 3, ..., u_n, ... has period 28, since $u_{14} = 377$ is the first eligible u_n or v_n divisible by 13. The index 14 is doubled to obtain the period.

For larger m, our search is narrowed by (2), (4), (5), and (6) of Wall's Theorem. Note that (4) becomes $n|(p - 1)/2$ for $p = 10x \pm 1$ and (5) becomes $n|p+1$ for $n = 10x \pm 3$, since our n represents half the period of the sequence.

Example: In $\mathbb{Z}_{47}$, (5) requires that $n|48$, and Theorem 1 yields $n = 16$, since $u_{16} = 987$ is the first eligible u_n or v_n divisible by 47. The period of 1, 1, 2, ..., u, ... in $\mathbb{Z}_{47}$ is therefore 32.

We remind the reader of three known results (see [2]) which are helpful in the search for a minimal n.

(i) $v_n | v_m$ if and only if $m = (2k - 1)n$ for $n > 1$.

(ii) $v_n | u_m$ if and only if $m = 2kn$ for $n > 1$.

(iii) $u_n | u_m$ if and only if $n | m$.

The following related result completes the picture.

(iv) For $n > 1$, u_{2n} does not divide v_k for k odd.

Proof: If $n = 2$, then $u_4 = 3 = v_2$. Thus, by (i), only those v_x with x even are divisible by u_4.

If $n = 3$, then $u_6 = 8$, and it can be shown that no v_k is divisible by 8. (Use the fact that any number with at least 3 digits is divisible by 8 if and only if the number consisting of its last 3 digits is divisible by 8. Then observe that the set of odd multiples of $v_3 = 4$ yields only a finite set of final 3 digits, none of which is divisible by 8.)

For $n > 3$, assume there exists an odd k such that $u_{2n} | v_k$. Then $u_{2n} | u_{2k}$ by (ii), so $2n | 2k$ and $n | k$ so that $u_n | u_k$ by (iii). Since $u_{2n} | v_k$, it follows that $u_n | v_k$. Hence, u_n is a common divisor of both u_n and v_k and thus u_n must equal 1 or 2. This is impossible for $n > 3$.

These four facts and Wall's Theorem make it quite simple to determine the period of Fibonacci sequences of the form 0, 1, 2, 3, ..., u_n, ... modulo m.

In an arbitrary group G, if we use multiplicative notation, we may apply Theorem 1 to the exponents to obtain

Corollary 2: Let G be any group and a an element of order $m > 2$ in G. Then the sequence $a, a, a^2, a^3, \ldots, a^{u_n}, \ldots$ will have period $2n$ for

$$n = \text{minimum}\{n \text{ even and } m | u_n;\ n \text{ odd and } m | v_n\}.$$

Example: If a is an element of order 4 in a group, then the sequence $a, a, a^2, a^5, \ldots, a^{u_n}, \ldots$ has period 6, since 4 divides $v_3 = 4$ and no previous u_n for n or v_n for n odd.

It is evident from Theorem 1 and Corollary 2 that the process of finding n may be reversed. If we are given $n > 2$, we can construct a Fibonacci sequence of period $2n$. If n is even, we can use any element a of order u_n, and if n is odd, an element of order v_n will suffice. We can often do better, since we need only a factor x of u_n or v_n which is not a factor of any previous u_n of even index or v_n of odd index (i.e., n will be the index of the first qualifying term divisible by x). We state this formally.

Corollary 3: A sequence of the form $a, a, a^2, \ldots, a^{u_n}, \ldots$ in a group G will have period $2n > 5$ if a is chosen to have order u_n for n even or v_n for n odd. Furthermore, a may be chosen to have order x where x divides this u_n or v_n but is not a factor of any previous qualifying u_n or v_n.

Example: To find a sequence of period $16 = 2n$, use $u_8 = 21$. Any element of order 21 in a group G will yield a sequence of the form $a, a, a^2, a^3, \ldots, a^{u_n}$, ... which has period 16. Since 7 is a factor of 21 which divides no previous u_n of even index or v_n of odd index, any element of order 7 will also suffice.

We may use the previous results to present a simple method for obtaining primes p for which $k(p)$ is a proper divisor of $p - 1$ for $p = 10x \pm 1$ or of $2p + 2$ for $p = 10x \pm 3$. As mentioned earlier, our minimal n equals $[k(p)/2]$, so we seek primes p such that n does not equal $(p - 1)/2$ or $p + 1$.

First of all, if we are given a prime $p > 5$, set $n = (p - 1)/2$ or $n = p + 1$, depending on whether $p = 10x \pm 1$ or $p = 10x \pm 3$. Then, using previous results, see whether u_n for n even or v_n for n odd is the smallest such u_n or v_n divisible by p. For example, if $p = 31$, set $n = 15$. Since v_{15} is divisible by 31 and no smaller qualifying u_n or v_n is divisible by 31, $n = (p - 1)/2$ works and $k(31) = 30$. However, if we begin with $p = 47$, set $n = 48$. Since 47 divides $u_{16} < u_{48}$, it follows that $k(47) = 32 \neq 96$.

Another approach begins with N rather than p. Given N, find the prime factors $p_1, \ldots, p_k$ of u_N for N even or v_N for N odd. Proceed as above to set $(p_i - 1)/2$ or $p_i + 1$ equal to n_i for each p_i. If $n_i > N$, then $k(p_i) <$ the given upper bound $p_i - 1$ or $2p_i + 2$. If $n_i = N$, check whether p_i divides a previous u_k of even index or v_k of odd index. If so, then $k(p_i) <$ the given upper bound. If not, $k(p_i) =$ the correct upper bound. (If $n_i < N$, disregard the associated p_i.)

Example: For $N = 44$, the prime factors of u_{44} are 3, 43, 307, 89, and 199. We disregard 3 since $n = 4 < 44$. For $p = 43$, $n = 44$ and, in fact, $k(43) = 88$. For $p = 307$, $n = 308 > 44$, so $k(307) \leqslant 88 \neq 616$. For $p = 89$, $n = 44$ and, in fact, $k(89) = 88$. Finally, for $p = 199$, $n = 99 > 44$, so $k(199) \leqslant 88 \neq 198$.

Two more results follow easily from Theorem 1.

Corollary 4: Any element whose order is a multiple of 5 will yield a sequence $a, a, a^2, \ldots, a^{u_n}, \ldots$ whose period is a multiple of 4.

Proof: No Lucas number is divisible by 5, so n must be even and $2n$ is therefore divisible by 4.

Corollary 5: Any sequence of the form $a, b, ab, ab^2, \ldots, a^{u_{n-1}}b^{u_n}, \ldots$ in an Abelian group G will have odd period > 3 only if it does not contain the identity element.

Proof: By Corollary 2, any sequence of the form $e, a, a, a^2, \ldots, a^{u_n}, \ldots$ for a of order > 2 has even period.

Corollary 3 allows us to construct Fibonacci sequences of period $2n$ for $n > 2$. Corollary 5 requires us to examine sequences not containing the identity element if we wish to obtain sequences of odd period. We first observe that, if the sequence $a, a, a^2, \ldots, a^{u_i}, \ldots$ has period x and the sequence $b, b, b^2, \ldots, b^{u_i}, \ldots$ has period y in an Abelian group G, then the sequence $a, b, ab, ab^2, \ldots, a^{u_{i-1}}b^{u_i}, \ldots$ will repeat after $\operatorname{lcm}\{x, y\}$ terms. Hence, the period of this sequence will be a divisor of $\operatorname{lcm}\{x, y\}$. (Wall [3] gives some sufficient conditions for $h(m)$ to equal $k(m)$ in $\mathbb{Z}_m$.)

Example: In $\mathbb{Z}_5$, both $a = 1$ and $b = 3$ have order 5, and the sequences

$$0, 1, 1, 2, \ldots \quad \text{and} \quad 0, 3, 3, 6, \ldots$$

each have period 20 (since u_{10} is the first qualifying u_n or v_n divisible by 5). However, the sequence 1, 3, 4, 2, 1, ... has period 4.

Our goal is to construct Fibonacci sequences of odd period and the following theorem provides the means to accomplish this.

Theorem 2: Given any integer $n > 2$, there exists a Fibonacci sequence of period n.

Proof: Consider the sequence of integers

$$u_n,\ 1 - u_{n-1},\ 1 + u_{n-2},\ \ldots,\ u_{k-1} + (-1)^{k-1}u_{n-(k-1)},\ \ldots,$$
$$u_n,\ u_{n+1} + (-1)^{n+1},\ \ldots .$$

This is a Fibonacci sequence of period n provided that

$$1 - u_{n-1} \equiv u_{n+1} + (-1)^{n+1} \quad \text{or} \quad v_n = \begin{cases} 0 \pmod{m} \text{ for } n \text{ odd}, \\ 2 \pmod{m} \text{ for } n \text{ even}. \end{cases}$$

Thus, if n is odd, use the given sequence in $\mathbb{Z}_m$ with $m = v_n$ and, if n is even, use the given sequence in $\mathbb{Z}_m$ with $m = v_n - 2$.

Although Theorem 2 establishes the existence of Fibonacci sequences of period n, in practice the calculations often involve large m. To simplify this, observe that we need only a *divisor* of v_n or $v_n - 2$ which has not appeared as a factor of a previous v_k for k odd or $v_k - 2$ for k even.

Example: Given $n = 7$, the resulting sequence is

$$13,\ -7,\ 6,\ -1,\ 5,\ 4,\ 9,\ 13,\ 22,\ \ldots,$$

where $22 \equiv -7 \pmod{m}$, so $m = 29 = v_7$. Other sequences of period 7 may be obtained by multiplication of this sequence by any nonzero element in $\mathbb{Z}_{29}$.

Example: If $n = 9$, the resulting sequence is

$$34,\ -20,\ 14,\ -6,\ 8,\ 2,\ 10,\ 12,\ 22,\ 34,\ 56,\ \ldots,$$

and $m = v_9 = 76 = 2^2 \cdot 19$. Here, we may use the smaller $m = 19$ to obtain the sequence 15, 18, 14, 13, 8, 2, 10, 12, 3, 15, ... in $\mathbb{Z}_{19}$. (Note that if the original sequence is reduced modulo 4, we obtain 2, 0, 2, 2, 0, ... which has period 3 instead of period 9. The problem here is that 4 has appeared in previous v_k for k odd and $v_k - 2$ for k even.) As in the previous example, multiplication of the sequence of period 9 by any number relatively prime to m will yield a sequence of period 9.

Applying Theorem 2 to exponents, we obtain

Corollary 6: Given $n > 2$, an element a of order v_n for n odd or v_{n-2} for n even in an Abelian group G will yield a sequence

$$a^{u_n},\ a^{1-u_{n-1}},\ \ldots,\ a^{u_{(k-1)}+(-1)^{k-1}u_{n-(k-1)}},\ \ldots$$

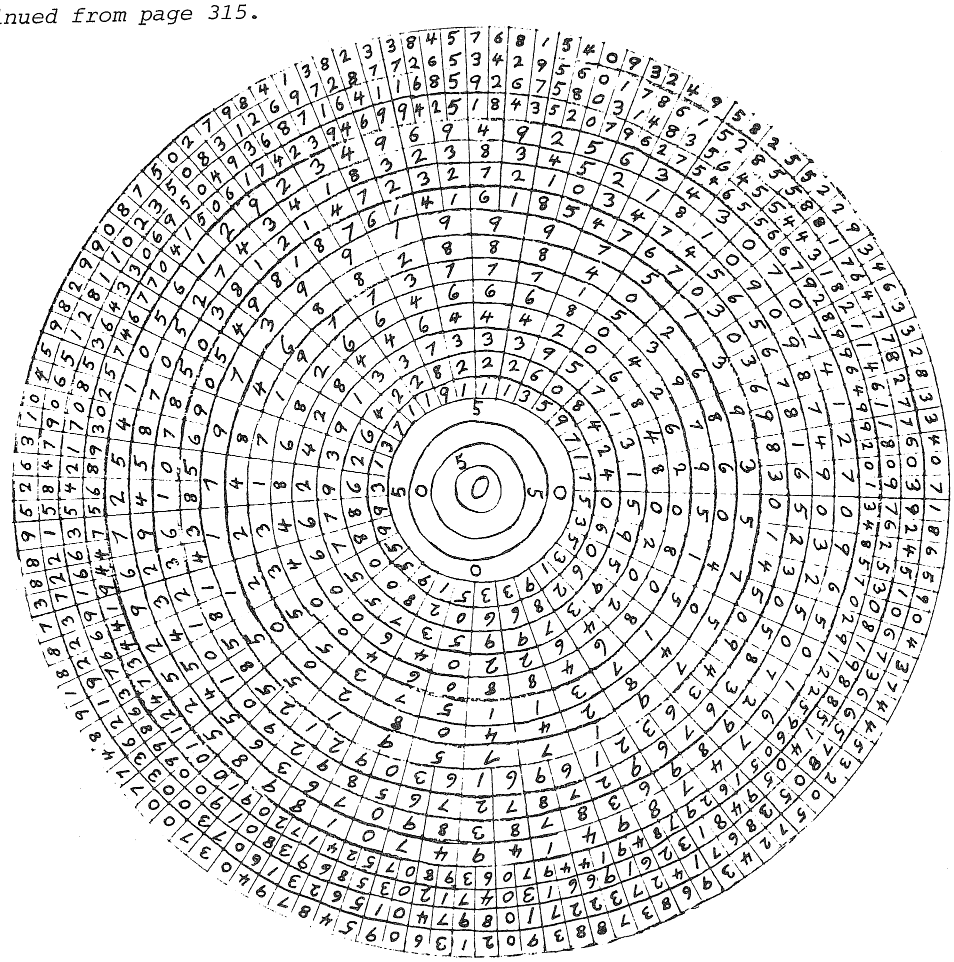
of period n.

REFERENCES

1. Tom DeLio. "Iannis Xenakis' 'Nomos Alpha': The Dialectics of Structure and Materials." *Journal of Music Theory* 24, no. 1 (1980):63-96.
2. Verner E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin, 1969.
3. D. D. Wall. "Fibonacci Series Modulo *m*." *Amer. Math. Monthly* 67 (1960): 525-532.
4. Iannis Xenakis. *Formalized Music*. Bloomington: Indiana University Press, 1971.

◆◇◆◇◆

Continued from page 315.



THE SET OF SERIES BASED ON THREE-DIGIT NUMERALS

◆◇◆◇◆