Iteration of the modular period of a second order linear recurrent sequence

by

DONALD W. ROBINSON (PROVO, UTAH)

O. Introduction. It is well known that the Fibonacci sequence 0, 1, 1, 2, 3, 5, ... reduced modulo a positive integer $m$ is periodic. (See, for example, Dickson [2], Chapter 17, Hardy and Wright [3], pp. 148-150, or Robinson [4].) Let $\pi(m)$ be the period modulo $m$. Fulton and Morris [5] have recently demonstrated two facts about $\pi$ as a function of $m$. The first is a fixed point theorem: if $m > 1$, then $\pi(m) = m$ if and only if $m = 24 \cdot 5^{\lambda-1}$ for some $\lambda \geq 1$. The second is an iteration theorem: for every positive integer $m$ there exists a non-negative integer $\omega$ such that $\pi^{\omega+1}(m) = \pi^\omega(m)$, where $\pi^\omega(m) = m$ and $\pi^n(m) = \pi^{\omega}(m)$ for $n \geq 0$. Thus, if $\omega(m)$ is the smallest such $\omega$, then $\pi^{\omega(m)}(m)$ is a fixed point of $\pi$.

In this note we extend these observations and prove the following:

Theorem. Let $u_0, u_1, u_2, \ldots$ be the sequence given by the integers $u_0, u_1, t$, and $d$ and the recurrence relation $u_{n+2} = tu_{n+1} - du_n$ for $n \geq 0$. For $m$ a positive integer, let $\pi(m)$ be the period of the sequence modulo $m$.

(1) Then there exists a non-negative integer $i$ such that $\pi^{i+1}(m) = \pi^i(m)$.

Let $i(m)$ be the smallest such $i$ and define $g(m) = \pi^{i(m)}(m)$.

(2) Then $\pi^2(m) = m$ if and only if $m$ is the least common multiple of elements drawn from

\[ \{1\} \cup \{g(2), g(3), g(4), g(8)\} \cup \{g(p^s) : p \text{ prime, } e > 0, p^e \mid \pi(p^s)\} \]

In the case of the Fibonacci sequence, the prime power $p^s$ divides $\pi(p^s)$ if and only if $p = 5$. Also,

\[ g(2) = g(3) = g(4) = g(8) = 24, \quad g(5^s) = 24 \cdot 5^s = g(5) \cdot 5^{s-1}, \]

and $m$ is a fixed point of $\pi^s$ if and only if it is a fixed point of $\pi$.

Prior to the proof of the theorem, we comment on the fact that only second order recurrences are considered here. Indeed, in the case of first order linear recurrent sequences, it is easily shown that an iteration theorem is applicable, but that the only fixed point of the period function...
is the trivial value 1. On the other hand, for linear sequences of order exceeding two, the iteration result need not apply. For example, if \( u_0 = 0, u_1 = 0, u_2 = 1, \) and \( u_{n+2} = u_{n+1} + u_n - u_{n-1} \), then \( \pi^2(2) = 2^{k+1} \). Thus, we restrict our attention in this paper to linear recurrent sequences of second order.

1. Preliminaries. Let \( u_0, u_1, u_2, \ldots \) be the sequence of integers that satisfies the linear recurrence

\[
 u_{n+1} = tu_{n+2} - du_n
\]

for \( n \geq 0 \). For convenience, define matrices

\[
 A = \begin{pmatrix} 0 & -d \\ 1 & t \end{pmatrix}
\]

and note that \((u_n, u_{n+1}) = uA^n \). If \( m \) is a positive integer, then there is a term of the sequence \( u, uA, uA^2, \ldots \) that is congruent modulo \( m \) to a preceding term. Specifically, if

\[
 uA^e(m) = uA^e(m) \pmod{m}
\]

is the first such term, then \( uA^e(m), uA^e(m+1), \ldots \) is periodic of period \( \pi(m) \) modulo \( m \). The sequence \( u_0, u_1, u_2, \ldots \) is said to be of index \( \pi(m) \) and period \( \pi(m) \) modulo \( m \). (See also Ward [3], [9] and Hall [4].)

Similarly, there is a term of the sequence \( I, A, A^2, \ldots \) that is congruent modulo \( m \) to a preceding term. If \( A^{(m+1)\pi(m)} = A^{(m)\pi(m+1)} \pmod{m} \) is the first such term, then \( A^{(m)}, A^{(m+1)}, \ldots \) is periodic of period \( \pi(m) \) modulo \( m \). The sequence \( I, A, A^2, \ldots \) is said to be of index \( \pi(m) \) and period \( \pi(m) \) modulo \( m \).

Some well-known facts about these periods are now stated. (For proofs see for example Ward [9].) The least common multiple of the positive integers \( m \) and \( n \) is denoted by \([m,n] \).

**Lemma 1.1.** Let \( \pi(m) \) and \( \pi(n) \) be the periods of \( u_0, u_1, u_2, \ldots \) and \( I, A, A^2, \ldots \) modulo \( m \).

1. If \( m|n \), then \( \pi(m)|\pi(n) \) and \( \pi(n)|\pi(n) \).
2. \( \pi([m,n]) = [\pi(m), \pi(n)] \) and \( \pi([m,n]) = [\pi(m), \pi(n)] \).
3. \( \pi(m)|\pi(n) \).
4. If \( u_0 u_3 - u_1 u_2 \) is relatively prime to \( m \), then \( \pi(m) = \pi(n) \).

In view of property (2), the problem of determining the periods modulo \( m \) is reduced to the problem of determining the periods modulo the prime power factors of \( m \). The next lemma provides a statement of the properties of the period \( \pi(p^e) \) of \( I, A, A^2, \ldots \) modulo a prime power \( p^e \).

**Lemma 1.2.** Let \( \pi(m) \) be the period of \( I, A, A^2, \ldots \) modulo \( m \). Let \( p \) be a prime and let \( D = p - Ad \).

1. If \( p|D \), then \( \pi(p)|(p-1)p \).
provided \( e > 1 \) if \( p = 2 \). Consequently, if also \( \nu(p^{e+2}) = \nu(p^{e+1}) \), then
\[
A^{(p^{e+1})+r(p^e)} = A^{(p^{e+1})+r(p^e)} = A^{(p^{e+1})+r(p^e)B} = A^{(p^{e+1})+r(p^e)}(\mod p^{e+1}),
\]
and
\[
\nu(p^{e+1}) = \nu(p^{e+1}).
\]
In other words, if \( e > 1 \) when \( p = 2 \), then
\[
\nu(p^{e+1}) = \nu(p^e) \implies \nu(p^{e+1}) = \nu(p^{e+1}).
\]

Parts (3), (4), and (4') of the lemma now follow.

For convenience we may substitute the first alternative of part (3) into the second by the convention \( e(p) = +\infty \). Similar agreements may be made for the cases (4) and (4').

We have as a consequence of this lemma and the fact that \( \pi(m) | \nu(m) \).

**Corollary 1.** Let \( \pi(m) \) be the period of \( u_0, u_1, u_2, \ldots \) modulo \( m \).

Let \( p \) be a prime and \( D = p^2 - 4d \). Then

1. \( \pi(2^i) = 2^i \).
2. \( \pi(q) = q \), where \( q \) is a prime, and \( q | \pi(p^e) \), then \( q \equiv p \).
3. \( \pi(p^e) = p^e \), then \( p \equiv e \).
4. \( \pi(p^e) = p^e \), then \( p | D \).

**2. Iteration Theorem.** Let \( m = 2^{a(0)} 3^{b(0)} \cdots p_i^{c(i)} \cdots p_i^{c(i)} \) be the prime power factorization of \( m \), where \( p_i \) is the \( i \)th prime exceeding 3, and \( a(0), b(0), c(0), \ldots, c(0) \) are non-negative with \( c(0) > 0 \). From (1) and (2) of Corollary 1,

\[
\pi(m) = 2^{a(i)} 3^{b(i)} \cdots p_i^{c(i)} \cdots p_i^{c(i)},
\]

where \( a(i), b(i), c(i), \ldots, c(i) \) are non-negative, \( i = 1, 2, \ldots \)

**Lemma 2.1.** If \( \pi(m) = 2^{a(i)} 3^{b(i)} \cdots p_i^{c(i)} \cdots p_i^{c(i)} \) where \( c(0) > 0 \), then there exists an \( i \) such that

\[
c(i + k) = c(i), \quad \ldots \quad c(i + k) = c(i) \quad \text{for} \quad k = 1, 2, \ldots
\]

**Proof.** Let \( m = 2^{a(i)} 3^{b(i)} \cdots p_i^{c(i)} \cdots p_i^{c(i)} \). By part (2) of Lemma 1.1,

\[
\pi(m) = [\pi(x), \pi(p_i^{c(i)})].
\]

Thus, by (2) and (3) of Corollary 1, \( c(1) \leq c(0) \). By repeating this argument, \( c(i + 1) \leq c(i) \) for each \( i \). Thus, there is an \( i \) such that \( c(i + 1) = c(i) \). If \( c(i) = 0 \), then \( c(i + 1) = 0 \) and \( c(i + k) = 0 \) for \( k = 1, 2, \ldots \); if \( c(i) > 0 \), then \( p_i^{c(i)} | \pi(p_i^{c(i)}) \) and \( c(i + k) = c(i) \) for \( k = 1, 2, \ldots \)

Next, suppose that there is an \( i \) such that \( c(i + k) = c(i) \) for \( j = s + 1, \ldots, r \) and all \( k \geq 1 \). Define \( w = 2^{a(s)} 3^{b(s)} \cdots p_i^{c(s)} \cdots p_i^{c(s)} \),

\[
y = p_i^{c(s)} \cdots p_i^{c(s)}, \quad \text{and} \quad n = \pi(m) = x \cdot y. \]

With an obvious extension of this notation, \( \pi(n) = x \cdot y \).

We now show that

\[
\pi(n) = x \cdot y \quad \text{with} \quad o' \leq e'.
\]

Indeed,

\[
\pi(n) = [\pi(x), \pi(y)] = [x, p^e, \pi(y)] = x \cdot p^e \quad \text{yields}
\]

\[
\pi(y) = x \cdot p^e, \quad c_s \leq c_s, \quad \text{and} \quad c_s = \max(c_s, e_s).
\]

Thus,

\[
\pi(n) = [\pi(x), \pi(y)] = [x, p^e, x \cdot p^e] = x \cdot p^e,
\]

where \( c_s \leq c_s \) and \( c_s = \max(c_s, e_s) \). Finally, either \( o' = c_s \leq e_s \) or \( o' = c_s \leq c_s \). That is, \( e' \leq e_s \). Hence, by repetition of the argument, we conclude that for some \( i \), \( \pi^{i+k}(n) = x \cdot p^e \cdot y \) with \( x(i+k) = x(i) \cdot p^e \cdot y \). Again, since \( p^e \cdot y | \pi(p^e \cdot y) \), it follows that \( \pi^{i+k}(n) = x(i+k) \cdot p^e \cdot y \) for \( k \geq 1 \).

That is, using the original notation of the lemma, there is an \( i \) such that \( c(i + k) = c(i) \), \( j = s, \ldots, r \), and \( k = 1, 2, \ldots \). Lemma 2.1 now follows by induction on \( s \).

**Lemma 2.2.** Let \( m = 2^{a(3)} 3^{b(3)} \ldots p_i^{c(i)} \cdots p_i^{c(i)} \) be the prime power factorization of \( m \), where \( p_i \) is the \( i \)th prime exceeding 3, and \( a(3), b(3), c(0), \ldots, c(0) \) are non-negative with \( c(0) > 0 \). From (1) and (2) of Corollary 1,

\[
\pi(m) = 2^{a(i)} 3^{b(i)} \cdots p_i^{c(i)} \cdots p_i^{c(i)},
\]

where \( a(i), b(i), c(i), \ldots, c(i) \) are non-negative, \( i = 1, 2, \ldots \)

**Lemma 2.3.** Let \( m = 2^{a(3)} 3^{b(3)} \cdots p_i^{c(i)} \cdots p_i^{c(i)} \) be the prime power factorization of \( m \), where \( a(3), b(3), c(0), \ldots, c(0) \) are non-negative with \( c(0) > 0 \).

Thus, there is an \( i \) such that \( x(i) = x(i) \cdot p^e \cdot y \).

**Proof.** Since \( \pi(m) = [\pi(2^{a(i)}), \pi(3^{b(i)})] = [2^{a(i)} 3^{b(i)}] \), it is clear that

\[
\pi(y) = 2^{a(i)} 3^{b(i)} \quad \text{where} \quad 2^{a(i)} 3^{b(i)} | \pi(2^{a(i)} 3^{b(i)}).\]

Also, since both \( \pi(3) \) and \( \pi(3) \) divide \( 2^4 \), \( \pi(2^4) \) whenever \( \pi(2^4) \). In particular, \( \pi(m) = \pi(2^4) \cdot \pi(3) \cdot \pi(2^4) \cdot \pi(3) \) for each \( i \).

Since there are only a finite number of divisors of \( 2^4 \cdot 3 \), then \( \pi^{i+1}(m) = \pi(m) \) for some \( i+1 \).

If \( \pi(m) \cdot \pi^{i+1}(m) \) for some \( j \), then \( \pi^{i+1}(m) \cdot \pi^{i+1}(m) \) for all \( h \geq 0 \) and hence \( \pi(m) = \pi^{i+1}(m) \). Similarly, if \( \pi^{i+1}(m) = \pi^{i+1}(m) \) for some \( j \), then \( \pi^{i+1}(m) = \pi^{i+1}(m) \).

Thus, in either case, \( \pi(m) \) is a fixed point of \( \pi \).

Therefore, suppose for all \( j \), \( \pi^{i+1}(m) \) and \( \pi^{i+1}(m) \) for \( i \).

Since \( \pi(m) = \pi(2^4) \cdot \pi(3) \cdot \pi(2^4) \cdot \pi(3) \), this means that for every \( j \), either \( \pi^{i+1}(m) \)
or \( \pi^{i+1}(m) \) is divisible by 3, but not both. Hence, for every \( j \), either \( \pi^{i}(m) \mid \pi^{i+1}(m) \) or \( \pi^{i+2}(m) \mid \pi^{i}(m) \). Again, using the fact that \( \pi^{i+k}(m) = \pi^{i}(m) \), it follows that \( \pi^{i+k}(m) = \pi^{i}(m) \).

**Iteration Theorem.** For each positive integer \( m \) there is a non-negative integer \( i \) such that \( \pi^{i+k}(m) = \pi^{i}(m) \).

**Proof.** We begin with an observation. If \( \pi^{i+k}(m) \mid \pi^{i}(m) \) for some \( i \), then \( \pi^{i+k+1}(m) \mid \pi^{i+k}(m) \) for all \( k \geq 0 \). Hence, \( \pi^{i+k+1}(m) = \pi^{i+k}(m) \) for some \( k \), which means that \( \pi^{i+k}(m) = \pi^{i+k}(m) \) for all \( k \geq 0 \). In particular, \( \pi^{i+k+2}(m) = \pi^{i+k}(m) \).

Let \( m \) be a positive integer. By Lemmas 2.1 and 2.2, either there exists an \( i \) such that \( \pi^{i+k}(m) = 2^{i+k} \cdot 3^{j} \) for all \( k \geq 0 \) or there exists an \( i \) such that \( \pi^{i+k}(m) = 2^{i+k} \cdot 3^{j} \cdot 5 \). If the first case, \( \pi^{i+k}(m) \mid \pi^{i+k+1}(m) \), the conclusion of the theorem follows by the preceding observation. In the second case, \( \pi^{i+k+3}(m) = 2^{i+k+2} \cdot 3^{j} \cdot 5 \cdot 7 \), where \( b' = 1 \) or \( b' = 0 \).

Suppose \( b' = 1 \). If \( a' = a' \), then \( \pi^{i+k+1}(m) \mid \pi^{i+k+1}(m) \), and the conclusion follows. If \( a' > a' \), then \( 2^{i+k} \mid \pi^{i}(m) \) and \( \pi^{i+k+1}(m) = 2^{i+k+1} \cdot 3 \cdot 5 \cdot 7 \). If the second case, \( \pi^{i+k+3}(m) = 2^{i+k+2} \cdot 3^{j} \cdot 5 \cdot 7 \cdot 11 \), where \( c' = 1 \) or \( c' = 0 \).

Suppose \( b'' = 0 \). If \( a'' = a'' \), then \( \pi^{i+k}(m) \mid \pi^{i+k+1}(m) \), and the conclusion follows. Assume \( a'' > a'' \). Then \( \pi^{i+k}(m) = 2^{i+k} \cdot 3 \cdot 5 \cdot 7 \), \( \pi^{i+k+1}(m) = 2^{i+k+1} \cdot 3 \cdot 5 \cdot 7 \cdot 11 \), and \( \pi^{i+k+3}(m) = 2^{i+k+2} \cdot 3^{j} \cdot 5 \cdot 7 \cdot 11 \), with \( a' > a'' > a'' \). Again, by Lemma 2.3, the conclusion follows, and the proof is complete.

**Corollary 2.** For each positive integer \( m \) there is a least non-negative integer \( i \) such that \( \pi^{i+k}(m) = \pi^{i+k}(m) \).

3. **Fixed Point Theorem.** By Corollary 2, let \( i(m) \) be the unique smallest \( i \) such that \( \pi^{i+k}(m) = \pi^{i+k}(m) \).

**Lemma 3.1.** If \( \pi(m) = \pi^{i+k}(m) \), then

1. \( \pi(m) = \pi^{i+k}(m) \) for all \( i \geq i(m) \).
2. \( \pi^{i+k}(m) = \pi^{i+k}(m) \).
3. \( \pi(m, m) = \pi^{i+k}(m) \).

**Proof.** Parts (1) and (2) are obvious from the definition of \( \pi(m) \). Part (3) is a consequence of the fact that by Lemma 1.1(2), \( \pi^{i+k}(m) = \pi^{i+k}(m) \).

The integer \( \pi(m) = \pi^{i+k}(m) \) is called the fixed point of \( \pi^{i+k} \) associated with \( m \). Clearly a fixed point of \( \pi^{i+k+1} \) may also be fixed point of \( \pi^{i+k} \). But if \( \pi(m) = \pi^{i+k}(m) \), then the proof of the iteration theorem above, \( \pi(2) = 3, \pi(3) = 2^{3} \cdot 3 \cdot 5 \), and either \( \pi(m) = 2^{i+k+1} \cdot 3 \cdot 5 \cdot 7 \) or \( \pi(m) = 2^{i+k+1} \cdot 3 \cdot 5 \cdot 7 \), with \( 0 \leq a' < a'' < a'' \).

Next, let \( R \) be the collection of fixed points of \( \pi^{i+k} \), and for \( r \) and \( s \) in \( R \), let \( r \mid s \) mean as usual that \( r \) divides \( s \).

**Lemma 3.2.** \( \{ r \mid s \} \) is a distributive lattice.

**Proof.** We first note that \( r \) is an element of \( R \) if and only if \( \pi(r) = r \). Let \( r, s \in R \). By Lemma 3.1(3), \( \pi(r, s) = \pi(\pi(r), \pi(s)) = \pi(r, s) \) and \( \pi(r, s) \in R \). Thus, \( \pi(r, s) \in R \) is the join \( r \vee s \) of \( r \) and \( s \) in \( R \).

Finally, let \( r, s, t \in R \). Then \( r \vee (s \wedge t) = \pi(\pi(r), \pi(s) \wedge \pi(t)) = \pi(\pi(r), \pi(s) \wedge \pi(t)) = \pi(r, s) \wedge (r \vee t) \), and the lattice is distributive.

As an illustration of this lemma we refer again to the example of the Fibonacci sequence. In this case, the lattice consists simply of the chain 1, 2, 3, 4, 5, ...
4. Properties of the fixed points. In conclusion we mention without proof some properties of the fixed points of $\pi^e$.

If $e = \varphi(p^e) > 1$, where $p$ is a prime and $p^e | \pi(p^e)$, then $p | D$, $\pi(r) = r$, and $r$ is a fixed point in $E$. Furthermore if $p$ is an odd prime, then $\{ \varphi(p^e) : e > 0, p^e | \pi(p^e) \}$ is either the empty set, the singleton $\{ \varphi(p) \}$, or the infinite set $\{ \varphi(p)p^{e-1} : e > 0 \}$. Also, the set $\{ \varphi(2^n) : e > 0, 2^n | \pi(2^n) \}$ is either empty, $\{3, 4\}$, $\{2, 4\}$, or $\{2^e : e > 0\}$.

Each of the integers $\varphi(2), \varphi(3), \varphi(4)$, and $\varphi(8)$ divide 24. Finally, if there is a join irreducible fixed point of $\pi^e$ that is not a fixed point of $\pi$, then there is precisely one pair of such elements. In this case, this pair is either $\{2, 3\}$, $\{4, 3\}$, $\{8, 3\}$, or $\{8, 6\}$.

References


On orthogonal systems and permutation polynomials in several variables

by

R. Lidl (Wien) and H. Niederreiter (Carbondale, Ill.)

1. Introduction. A polynomial $f(a)$ with coefficients in the Galois field $K = GF(q)$ with $q$ elements, $q = p^e$, $p$ prime, $e > 1$, determines a mapping $f : a \mapsto f(a)$ of $K$ into $K$. This mapping is a bijection if and only if the equation $f(a) = a$ has a solution in $K$ for every $a \in K$. In this case, the polynomial $f(a)$ is called a permutation polynomial over $K$. Such polynomials have been studied extensively ([3], [4], [11]). Various papers have also been devoted to extending the notion of a permutation polynomial to polynomials in several variables ([1], [2], [6], [7], [9], [10]). The present paper is meant as a further contribution to this subject matter.

For $n \geq 1$, let $K^n$ denote the cartesian product of $n$ copies of $K$, and let $K[x_1, \ldots, x_n]$ be the ring of polynomials in $n$ variables over $K$.

Definition 1 (Nöbauer [10]). A polynomial $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ is called a permutation polynomial (in $n$ variables over $K$) if the equation $f(x_1, \ldots, x_n) = a$ has $q^{e-1}$ solutions in $K^n$ for each $a \in K$.

Definition 2 (Niederreiter [8]). A system of polynomials $f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)$ from $K[x_1, \ldots, x_n]$ is said to be orthogonal (in $K$) if the system of equations $f_i(x_1, \ldots, x_n) = k_i, 1 \leq i \leq n$, has exactly one solution in $K^n$ for each $(k_1, \ldots, k_n) \in K^n$.

Simple criteria for orthogonality in terms of character sums can be given ([8], Theorem 2). Let $\zeta$ denote a fixed primitive $p$th root of unity over the rationals, and let $tr(\cdot)$ be the trace function relative to the extension $K/QF(q)$. Then the system $f_1, f_2, \ldots, f_n$ is orthogonal if and only if, for all $(b_1, \ldots, b_n) \in K^n$ with $(b_1, \ldots, b_n) \neq (0, \ldots, 0)$, we have

$$\sum_{(a_1, \ldots, a_n) \in K^n} \zeta^{b_1a_1f_1(a_1, \ldots, a_n)+\cdots+b_nf_n(a_1, \ldots, a_n)} = 0.$$ 

We shall now prove another criterion for orthogonality by elementary methods. The following lemma will be useful.