Conspectus materiae tomi XXII, fasciculi 3

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange
Address of the Editorial Board and of the exchange
Die Adresse der Schriftleitung und des Austausches
Адрес редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, 00-950 Warszawa (Poland)

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplare jeder Arbeit
Рукописи статьей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA
XXII (1973)

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

by

DONALD W. ROBINSON (Provo, Utah)

0. Introduction. It is well known that the Fibonacci sequence $0, 1, 1, 2, 3, 5, \ldots$ reduced modulo a positive integer m is periodic. (See for example Dickson [2], Chapter 17, Hardy and Wright [5], pp. 148–150, or Robinson [6].) Let $\pi(m)$ be the period modulo m. Fulton and Morris [3] have recently demonstrated two facts about π 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 $\lambda \geqslant 1$. The second is an iteration theorem: for every positive integer m there exists a non-negative integer ω such that $\pi^{\omega+1}(m) = \pi^{\omega}(m)$, where $\pi^0(m) = m$ and $\pi^{n+1}(m) = \pi(\pi^n(m))$ for $n \geqslant 0$. Thus, if $\omega(m)$ is the smallest such ω, then $\pi^{\omega(m)}(m)$ is a fixed point of π.

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 $n \geqslant 0$. For m a positive integer, let $\pi(m)$ be the period of the sequence modulo m.*

(I) *Then there exists a non-negative integer i such that*

$$\pi^{2(i+1)}(m) = \pi^{2i}(m).$$

Let $i(m)$ be the smallest such i and define $\varrho(m) = \pi^{2(i(m))}(m)$.

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

$$\{1\} \cup \{\varrho(2), \varrho(3), \varrho(4), \varrho(8)\} \cup \{\varrho(p^e):\ p = prime,\ e > 0,\ p^e \mid \pi(p^e)\}.$$

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

$$\varrho(2) = \varrho(3) = \varrho(4) = \varrho(8) = 24, \quad \varrho(5^e) = 24\cdot 5^e = \varrho(5)\cdot 5^{e-1},$$

and m is a fixed point of π^2 if and only if it is a fixed point of π.

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 $u_{n+3} = u_{n+2} + u_{n+1} - u_n$, then $\pi^k(2) = 2^{k+1}$. Thus, we restrict our attention in this paper to linear recurrent sequences of second order.

1. Preliminaries. Let u_0, u_1, t, and d be integers, and let $u_0, u_1, u_2, \ldots$ be the sequence of integers that satisfies the linear recurrence

$$u_{n+2} = tu_{n+1} - du_n$$

for $n \geqslant 0$. For convenience, define matrices

$$u = (u_0, u_1), \qquad A = \begin{pmatrix} 0 & -d \\ 1 & t \end{pmatrix}$$

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

$$uA^{\sigma(m)+\pi(m)} \equiv uA^{\sigma(m)} \pmod{m}$$

is the first such term, then $uA^{\sigma(m)}, uA^{\sigma(m)+1}, \ldots$ is periodic of period $\pi(m)$ modulo m. The sequence $u_0, u_1, u_2, \ldots$ is said to be of index $\sigma(m)$ and period $\pi(m)$ modulo m. (See also Ward [8], [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 $A^{\tau(m)+\nu(m)} \equiv A^{\tau(m)} \pmod{m}$ is the first such term, then $A^{\tau(m)}, A^{\tau(m)+1}, \ldots$ is periodic of period $\nu(m)$ modulo m. The sequence $I, A, A^2, \ldots$ is said to be of index $\tau(m)$ and period $\nu(m)$ 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 $\nu(m)$ be the periods of $u_0, u_1, u_2, \ldots$ and $I, A, A^2, \ldots$ modulo m.*

(1) *If $m \mid n$, then $\pi(m) \mid \pi(n)$ and $\nu(m) \mid \nu(n)$.*

(2) *$\pi([m, n]) = [\pi(m), \pi(n)]$ and $\nu([m, n]) = [\nu(m), \nu(n)]$.*

(3) *$\pi(m) \mid \nu(m)$.*

(4) *If $u_0u_2 - u_1^2$ is relatively prime to m, then $\pi(m) = \nu(m)$.*

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 $\nu(p^e)$ of $I, A, A^2, \ldots$ modulo a prime power p^e.

LEMMA 1.2. *Let $\nu(m)$ be the period of $I, A, A^2, \ldots$ modulo m. Let p be a prime and let $D = t^2 - 4d$.*

(1) *If $p \mid D$, then $\nu(p) \mid (p-1)p$.*

(2) *If $p \nmid D$, then $\nu(p) \mid (p-1)(p+1)$.*

(3) *If p is odd, then either $\nu(p^e) = \nu(p)$ for $e = 1, 2, \ldots$ or there is a positive integer $e(p)$ such that*

$$\nu(p^e) = \nu(p) \cdot p^{\max\{0, e-e(p)\}} \quad \textit{for} \quad e = 1, 2, \ldots$$

(4) *If $\nu(2) = \nu(4)$, then either $\nu(2^e) = \nu(2)$ for $e = 1, 2, \ldots$ or there is an integer $e(2) > 1$ such that*

$$\nu(2^e) = \nu(2) \cdot 2^{\max\{0, e-e(2)\}} \quad \textit{for} \quad e = 1, 2, \ldots$$

(4′) *If $\nu(2) \neq \nu(4)$, then $\nu(4) = 2 \cdot \nu(2)$ and either $\nu(2^e) = \nu(4)$ for $e = 2, 3, \ldots$ or there is a positive integer $e'(2)$ such that*

$$\nu(2^e) = \nu(2) \cdot 2^{\max\{1, e-e'(2)\}} \quad \textit{for} \quad e = 2, 3, \ldots$$

Proof. (1) Since D is the discriminant of the minimum polynomial of A, if $p \mid D$, then A has but one characteristic value λ, and A is similar to the matrix $\begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix}$ modulo p. By Fermat's theorem,

$$A^{p^2} \equiv A^p \equiv \lambda I \pmod{p} \quad \text{and} \quad \nu(p) \mid (p^2 - p) = (p-1)p.$$

(2) Let $p \nmid D$. In this case, either A has two distinct characteristic values or A has no characteristic values modulo p. In the first instance, A is similar to a diagonal matrix, $A^p \equiv A \pmod{p}$, and $\nu(p) \mid (p-1)$. In the second, if $u = (u_0, u_1)$ is not zero modulo p, then $\{u, uA\}$ is linearly independent. Hence, by part (4) of Lemma 1.1, $\pi(p) = \nu(p)$. Since there are $p^2 - 1$ distinct non-zero pairs u modulo p, and each belongs to a cycle of length $\nu(p)$, it follows that $\nu(p) \mid (p^2 - 1)$. (See also Cornwall [1], statement (3.4), p. 105, or Robinson [7].)

We now proceed with the proofs of the next three parts of the lemma. For p a prime, since

$$A^{\tau(p^e)+\nu(p^e)} \equiv A^{\nu(p^e)} \pmod{p^e}$$

implies

$$A^{p\tau(p^e)+p\nu(p^e)} \equiv A^{p\nu(p^e)} \pmod{p^{e+1}},$$

it follows that

$$\tau(p^{e+1}) \leqslant p\,\tau(p^e) \quad \text{and} \quad \nu(p^{e+1}) \mid p\,\nu(p^e).$$

In particular, since $\nu(p^e) \mid \nu(p^{e+1})$, either $\nu(p^{e+1}) = \nu(p^e)$ or $\nu(p^{e+1}) = p\,\nu(p^e)$. Furthermore, since

$$A^{\tau(p^{e+1})+\nu(p^e)} = A^{\tau(p^{e+1})} + p^e B$$

for some integral matrix B,

$$A^{p\tau(p^{e+1})+p\nu(p^e)} \equiv A^{p\tau(p^{e+1})} + p^{e+1} A^{(p-1)\tau(p^{e+1})} B \pmod{p^{e+2}}$$

provided $e>1$ if $p=2$. Consequently, if also $\nu(p^{e+2}) = \nu(p^{e+1})$, then

$$A^{(p-1)\tau(p^{e+1})}B \equiv 0 \pmod{p},$$

$$A^{p\tau(p^{e+1})+\nu(p^e)} = A^{(p-1)\tau(p^{e+1})}A^{\tau(p^{e+1})+\nu(p^e)}$$
$$= A^{p\tau(p^{e+1})} + p^e A^{(p-1)\tau(p^{e+1})}B \equiv A^{p\tau(p^{e+1})} \pmod{p^{e+1}},$$

and

$$\nu(p^{e+1}) = \nu(p^e).$$

In other words, if $e>1$ when $p=2$, then

$$\nu(p^{e+1}) = p\nu(p^e) \quad \text{implies} \quad \nu(p^{e+2}) = p\nu(p^{e+1}).$$

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

For convenience we may subsume 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 $D = t^2-4d$. Then*

(1) $\pi(2^e)|2^e\cdot 3$.

(2) *If $p \neq 2$, q is a prime, and $q|\pi(p^e)$, then $q \leqslant p$.*

(3) *If $p^f|\pi(p^e)$, then $f \leqslant e$.*

(4) *If $p^e|\pi(p^e)$, then $p|D$.*

2. Iteration Theorem. Let $m = 2^{a(0)}3^{b(0)}p_1^{c_1(0)}\ldots p_r^{c_r(0)}$ be the prime power factorization of m, where p_j is the jth prime exceeding 3, and $a(0), b(0), c_1(0), \ldots, c_r(0)$ are non-negative with $c_r(0)>0$. From (1) and (2) of Corollary 1,

$$\pi^i(m) = 2^{a(i)}3^{b(i)}p_1^{c_1(i)}\ldots p_r^{c_r(i)},$$

where $a(i), b(i), c_1(i), \ldots, c_r(i)$ are non-negative, $i = 1, 2, \ldots$

LEMMA 2.1. *If $\pi^i(m) = 2^{a(i)}3^{b(i)}p_1^{c_1(i)}\ldots p_r^{c_r(i)}$ where $c_r(0)>0$, then there exists an i such that*

$$c_1(i+k) = c_1(i), \quad \ldots, \quad c_r(i+k) = c_r(i) \quad \textit{for} \quad k = 1, 2, \ldots$$

Proof. Let $m = x\cdot p_r^{c_r(0)}$. By part (2) of Lemma 1.1,

$$\pi(m) = [\pi(x), \pi(p_r^{c_r(0)})].$$

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

Next, suppose that there is an i such that $c_j(i+k) = c_j(i)$ for $j = s+1, \ldots, r$ and all $k \geqslant 1$. Define $x = 2^{a(i)}3^{b(i)}p_1^{c_1(i)}\ldots p_{s-1}^{c_{s-1}(i)}$, $p^c = p_s^{c_s(i)}$, $y = p_{s+1}^{c_{s+1}(i)}\ldots p_r^{c_r(i)}$, and $n = \pi^i(m) = xp^cy$. With an obvious extension of this notation, $\pi(n) = x'p^{c'}y$. We now show that

$$\pi^2(n) = x''p^{c''}y \quad \text{with} \quad c'' \leqslant c'.$$

Indeed,

$$\pi(n) = [\pi(xp^c), \pi(y)] = [x_*p^{c_*}, \pi(y)] = x'p^{c'}y$$

requires

$$\pi(y) = x^*p^{c^*}y, \quad c_* \leqslant c, \quad \text{and} \quad c' = \max\{c_*, c^*\}.$$

Thus,

$$\pi^2(n) = [\pi(x'p^{c'}), \pi(y)] = [x'_*p^{c'_*}, x^*p^{c^*}y] = x''p^{c''}y,$$

where $c'_* \leqslant c'$ and $c'' = \max\{c'_*, c^*\}$. Finally, either $c'' = c'_* \leqslant c'$ or $c'' = c^* \leqslant c'$. That is, $c'' \leqslant c'$. Hence, by repetition of this argument, we conclude that for some i, $\pi^i(n) = x^{\#}p^{c^{\#}}y$ with $\pi^{i+1}(n) = x^{\#(1)}p^{c^{\#}}y$. Again, since $p^{c^{\#}}y \mid \pi(p^{c^{\#}}y)$, it follows that $\pi^{i+k}(n) = x^{\#(k)}p^{c^{\#}}y$ for $k \geqslant 1$. That is, using the original notation of the lemma, there is an i such that $c_j(i+k) = c_j(i)$, $j = s, \ldots, r$, and $k = 1, 2, \ldots$ Lemma 2.1 now follows by induction on s.

LEMMA 2.2. *Let $m = 2^a3^by$ and $\pi(m) = 2^{a'}3^{b'}y$ where $2 \nmid y$ and $3 \nmid y$. Then $\pi^2(m) = 2^{a''}3^{b''}y$ with $b'' \leqslant b'$ unless $b' = 0$, in which case $b'' = 0$ or $b'' = 1$.*

Proof. $\pi(m) = [\pi(2^a3^b), \pi(y)] = 2^{a'}3^{b'}y$ requires $\pi(2^a3^b) = 2^{a_*}3^{b_*}$, $\pi(y) = 2^{a^*}3^{b^*}y$, $b' = \max\{b_*, b^*\}$ with $b_* \leqslant b$ unless $b = 0$, in which case by Corollary 1(1), b_* may possibly have value 1. Therefore,

$$\pi^2(m) = [\pi(2^{a'}3^{b'}), \pi(y)] = [2^{a'_*}3^{b'_*}, 2^{a^*}3^{b^*}y] = 2^{a''}3^{b''}y$$

where $b'' = \max\{b'_*, b^*\}$ with $b'_* \leqslant b'$ unless $b' = 0$, in which case, $b'_* = 0$ or $b'_* = 1$. Therefore, $b'' = b^* \leqslant b'$ or $b'' = b'_* \leqslant b'$ unless $b' = 0$, in which case, $b^* = 0$ and b'' is either 0 or 1.

LEMMA 2.3. *Let $2 \nmid y$, $3 \nmid y$, $m = 2^a3^by$ with $2^a3^b|24$, and $\pi(m) = 2^{a'}3^{b'}y$ with $2^{a'}3^{b'}|24$. Then there is an i such that $\pi^{i+2}(m) = \pi^i(m)$.*

Proof. Since $\pi(m) = [\pi(2^a3^b), \pi(y)] = 2^{a'}3^{b'}y$, it is clear that

$$\pi(y) = 2^{a^*}3^{b^*}y \quad \text{where} \quad 2^{a^*}3^{b^*}|2^{a'}3^{b'}|24.$$

Also, since both $\pi(3)$ and $\pi(8)$ divide 24, $\pi(d)|24$ whenever $d|24$. In particular, $\pi^i(m) = d(i)\cdot y$ where $d(i)|24$ for each i. Since there are only a finite number of divisors of $24\cdot y$, then $\pi^{i+k}(m) = \pi^i(m)$ for some $i+k > i \geqslant 0$.

If $\pi^j(m)|\pi^{j+1}(m)$ for some j, then $\pi^{j+h}(m)|\pi^{j+h+1}(m)$ for all $h \geqslant 0$ and hence $\pi^i(m) = \pi^{i+1}(m)$. Similarly, if $\pi^{j+1}(m)|\pi^j(m)$ for some j, then $\pi^{i+1}(m) = \pi^i(m)$. Thus, in either case, $\pi^i(m)$ is a fixed point of π.

Therefore, suppose for all j, $\pi^j(m) \nmid \pi^{j+1}(m)$ and $\pi^{j+1}(m) \nmid \pi^j(m)$. Since $\pi^j(m) = d(j)\cdot y|24\cdot y$, this means that for every j, either $\pi^j(m)$

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

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

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

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

Suppose $b'' = 1$. If $a'' \leqslant a'$, then $\pi^{i+2}(m)|\pi^{i+1}(m)$, and the conclusion follows. If $a'' > a'$, then $2^{a''}|\pi(3)$ and $\pi^{i+3}(m) = 2^{a''} \cdot 3 \cdot y$ is a fixed point of π, which again gives the desired conclusion.

Suppose $b'' = 0$. If $a'' \leqslant a'$, then $\pi^{i+2}(m)|\pi^{i+1}(m)$, and the conclusion follows. Assume $a'' > a'$. Then $\pi^i(m) = 2^a \cdot y$, $\pi^{i+1}(m) = 2^{a'} \cdot 3 \cdot y$, $\pi^{i+2}(m) = 2^{a''} \cdot y$, and $\pi(y) = 2^{a^*} \cdot y$, $\pi(3) = 2^{a''}$, with $a^* \leqslant a' < a'' \leqslant 3$. 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 $\pi^{2(i+1)}(m) = \pi^{2i}(m)$.*

3. Fixed Point Theorem. By Corollary 2, let $i(m)$ be the unique smallest i such that $\pi^{2(i+1)}(m) = \pi^{2i}(m)$.

LEMMA 3.1. *If $\varrho(m) = \pi^{2(i(m))}(m)$, then*

(1) $\varrho(m) = \pi^{2i}(m)$ *for all* $i \geqslant i(m)$.

(2) $\pi^2(\varrho(m)) = \varrho(m)$.

(3) $\varrho([m, n]) = [\varrho(m), \varrho(n)]$.

Proof. Parts (1) and (2) are obvious from the definition of $\varrho(m)$. Part (3) is a consequence of the fact that by Lemma 1.1(2), $\pi^i([m, n]) = [\pi^i(m), \pi^i(n)]$.

The integer $\varrho(m) = \pi^{2(i(m))}(m)$ is called the *fixed point* of π^2 associated with m. Clearly a fixed point of π^2 may also be a fixed point of π. But if $\varrho(m)$ is not a fixed point of π, then by the proof of the iteration theorem above, $\pi(2) = 3$, $\pi(3) = 2^{a''}$, and either $\varrho(m) = 2^{a''} \cdot y$ or $\varrho(m) = 2^{a'} \cdot 3 \cdot y$ with $0 \leqslant a' < a'' \leqslant 3$.

Next, let R be the collection of fixed points of π^2, and for r and s in R, let $r|s$ mean as usual that r divides s.

LEMMA 3.2. *$(R, |)$ is a distributive lattice.*

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

We now show that the meet $r \wedge s$ of r and s in R is the fixed point of π^2 associated with the greatest common divisor (r, s) of r and s. Indeed, since $(r, s)|r$, by repeated use of Lemma 1.1(1), $\varrho(r, s)|\varrho(r) = r$. Likewise, $\varrho(r, s)|s$, and $\varrho(r, s) \in R$ is a common divisor of r and s. Also, if $t \in R$ is such that $t|r$ and $t|s$, then $t|(r, s)$. Hence, $t = \varrho(t)|\varrho(r, s)$. That is, $r \wedge s = \varrho(r, s)$. Consequently, $(R, |)$ is a lattice.

Finally, let $r, s, t \in R$. Then $r \wedge (s \vee t) = \varrho((r, [s, t])) = \varrho([(r, s), (r, t)]) = [\varrho(r, s), \varrho(r, t)] = (r \wedge s) \vee (r \wedge t)$, 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 $1, 24, 24 \cdot 5, 24 \cdot 5^2, \ldots$

Each element of R is the join of a finite number of join irreducible elements of R. In the next lemma we identify these elements.

LEMMA 3.3. *Let $r > 1$ be a join irreducible element of R. Then either*

(i) *$r = \varrho(p^e)$ where p is a prime, e is a positive integer, and $p^e|\pi(p^e)$*

or

(ii) *$r = \varrho(2)$, $\varrho(3)$, $\varrho(4)$, or $\varrho(8)$.*

Proof. Let $r > 1$ be join irreducible in R. First, assume there is a prime $p > 3$ such that $p|r$. Let p be the largest such prime and let $r = xp^e$ where $p \nmid x$. Since $r = \varrho(r) = [\varrho(x), \varrho(p^e)]$ is join irreducible and $p \nmid \varrho(x)$, then $r = \varrho(p^e)$. Since it is also clear that $p^e|\pi(p^e)$, r is of type (i).

Next, let $r = 2^a 3^b$ be join irreducible. Since $r = \varrho(r) = [\varrho(2^a), \varrho(3^b)]$, either $r = \varrho(2^a)$ or $r = \varrho(3^b)$.

Suppose $r = \varrho(3^b)$. Since $r > 1$, it follows that $b \geqslant 1$. If $3^b \nmid \pi(3^b)$, then $3^b|\pi(2^a)|2^a \cdot 3$ and $b = 1$. That is, either r is of type (i) or $r = \varrho(3)$.

Suppose $r = \varrho(2^a)$. Since $r > 1$, $a \geqslant 1$. If $2^a \nmid \pi(2^a)$, then $2^a|\pi(3^b)|8 \cdot 3^b$ and $1 \leqslant a \leqslant 3$. That is, either r is of type (i) or $r = \varrho(2)$, $\varrho(4)$, or $\varrho(8)$.

As a corollary of the preceding results we have the following

FIXED POINT THEOREM. *Let m be a positive integer. Then $\pi^2(m) = m$ if and only if m is the least common multiple of elements drawn from the union of the following sets:*

(i) $\{\varrho(p^e)\colon p = \text{prime}, e > 0, p^e|\pi(p^e)\}$,

(ii) $\{\varrho(2), \varrho(3), \varrho(4), \varrho(8)\}$,

(iii) $\{1\}$.

4. Properties of the fixed points. In conclusion we mention without proof some properties of the fixed points of π^2.

If $r = \varrho(p^e) > 1$, where p is a prime and $p^e|\pi(p^e)$, then $p|D$, $\pi(r) = r$, and r is join irreducible in R. Furthermore if p is an odd prime, then $\{\varrho(p^e)\colon e > 0, p^e|\pi(p^e)\}$ is either the empty set, the singleton $\{\varrho(p)\}$, or the infinite set $\{\varrho(p)p^{e-1}\colon e > 0\}$. Also, the set $\{\varrho(2^e)\colon e > 0,\ 2^e|\pi(2^e)\}$ is either empty, $\{2\}$, $\{4\}$, $\{2, 4\}$, or $\{2^e\colon e > 0\}$.

Each of the integers $\varrho(2)$, $\varrho(3)$, $\varrho(4)$, and $\varrho(8)$ divide 24. Finally, if there is a join irreducible fixed point of π^2 that is not a fixed point of π, 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

[1] R. H. Crowell, *Graphs of linear transformations over finite fields*, J. Soc. Indust. Appl. Math. 10 (1962), pp. 103–112.
[2] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, New York 1952.
[3] J. D. Fulton and W. L. Morris, *On arithmetical functions related to the Fibonacci numbers*, Acta Arith. 16 (1969), pp. 105–110.
[4] M. Hall, *An isomorphism between linear recurring sequences and algebraic rings*, Trans. Amer. Math. Soc. 44 (1938), pp. 196–218.
[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Fourth Edition, London 1960.
[6] D. W. Robinson, *The Fibonacci matrix modulo m*, Fib. Q. 1 (1963), pp. 29–36.
[7] — *Solution to problem 5216*, Amer. Math. Monthly 72 (1965), pp. 680–681.
[8] M. Ward, *The characteristic number of a sequence of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. 33 (1931), pp. 153–165.
[9] — *The arithmetical theory of linear recurring series*, Trans. Amer. Math. Soc. 35 (1933), pp. 600–628.

BRIGHAM YOUNG UNIVERSITY
Provo, Utah

Received on 23. 3. 1971 (148)

ACTA ARITHMETICA
XXII (1973)

On orthogonal systems and permutation polynomials in several variables

by

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

1. Introduction. A polynomial $f(x)$ with coefficients in the Galois field $K = \mathrm{GF}(q)$ with q elements, $q = p^e$, p prime, $e \geqslant 1$, determines a mapping $f\colon x \to f(x)$ of K into K. This mapping is a bijection if and only if the equation $f(x) = a$ has a solution in K for every $a \in K$. In this case, the polynomial $f(x)$ 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 $n \geqslant 1$, 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^{n-1} solutions in K^n for each $a \in K$.

Definition 2 (Niederreiter [8]). A system of polynomials $f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)$ from $K[x_1, \ldots, x_n]$ is said to be *orthogonal* (in K) if the system of equations $f_i(x_1, \ldots, x_n) = k_i$, $1 \leqslant i \leqslant n$, 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 ζ denote a fixed primitive pth root of unity over the rationals, and let $\mathrm{tr}(\cdot)$ be the trace function relative to the extension $K/\mathrm{GF}(p)$. Then the system $f_1, \ldots, f_n$ 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

$$\sum_{(a_1, \ldots, a_n) \in K^n} \zeta^{\mathrm{tr}[b_1 f_1(a_1, \ldots, a_n) + \ldots + b_n f_n(a_1, \ldots, a_n)]} = 0.$$

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