Conspectus materiae tomi XXXIX, fasciculi 4

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

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 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-01616-7 ISSN 0065-1036

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XXXIX (1981)

Period of a linear recurrence

by

A. Vince (Ann Arbor, Mich.)

1. Introduction. There is a long history of research involving the period of repeating sequences of integers. The period of decimal fractions was the subject of early investigation by Leibnitz and Gauss. The period modulo n of sequence like $\{ax, ax^2, \ldots\}$ is important in the context of Lehmer's frequently utilized congruential method for computer generation of pseudo-random numbers ([2], [4]). Lucas was a major figure among many investigators into divisibility properties of the Fibonacci and other second order recurrences — and these properties are related to the period of such sequences modulo n [5].

In this article we investigate the period of repetition in a general setting. We first note that the repeating sequences mentioned above fall within the following framework: Let K be an algebraic number field and A its ring of integers. Let T be an $N\times N$ matrix and X_0 an N-column vector, both with entries in A. Define the sequence $X_0, X_1, \ldots$ by the linear recurrence

$$X_{m+1} = TX_m, \quad m = 0, 1, 2, \ldots$$

Let $\mathfrak{a}$ be an ideal in A. Since $A/\mathfrak{a}$ is finite, the sequence must, after a perhaps erratic initial segment, repeat periodically modulo $\mathfrak{a}$. Define $v = v(T, X_0, A/\mathfrak{a})$ to be this *period*. That is, v is the least positive integer for which there is an m_0 giving $X_{m+v} = X_m$ for all $m \geqslant m_0$. Equality here means coordinatewise equality in the ring $A/\mathfrak{a}$. As an example, consider

$$(1.1)\qquad T = \begin{bmatrix} 0 & 1 & \ldots & 0\\ 0 & 0 & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots\\ 0 & 0 & & 1\\ a_N & a_{N-1} & \ldots & a_1\end{bmatrix}, \qquad X_0 = \begin{bmatrix} x_1\\ x_2\\ \vdots\\ x_N\end{bmatrix}.$$

Then $v(T, X_0, A/\mathfrak{a})$ is the period $(\mathrm{mod}\,\mathfrak{a})$ of the general Nth order linear recurrence defined by

$$x_m = a_1x_{m-1} + a_2x_{m-2} + \ldots + a_Nx_{m-N}.$$

T is often referred to as the *companion matrix* of this recurrence.

By looking at the remainders upon division, it is easy to verify that the period of the decimal representation of $1/p$ for p prime is $v([10], [1], Z/pZ)$. When p is not 2 or 5, this is just the multiplicative order of the element 10 in the field Z/pZ of residues mod p. The general situation for a prime ideal $\mathfrak{p}$ is analogous. By our Theorem 1, $v(T, X_0, A/\mathfrak{p})$ is essentially determined by the multiplicative orders of special elements in a finite extension field of the residue class field $A/\mathfrak{p}$. This will enable us to make some new estimates of the value of v and to unify known results, many otherwise proved by complicated recurrence identities.

In Section 2 the problem of determining v is reduced to the case where $\mathfrak{a}$ is a prime ideal and Section 3 deals with a prime. In Section 4 these results are applied to certain second and third order recurrences.

2. Preliminary results. The sequence $\{X_m\}$ is called *simply periodic* if $X_v = X_0$, i.e. X_0 is the first term to repeat. In this case it is apparent that $X_m = X_0$ if and only if m is a multiple of v.

LEMMA 1. *If* $\det T$ *is not a zero divisor of* $A/\mathfrak{p}$ *then* $\{X_m\}$ *is simply periodic.*

Proof. For some integer m, $T^m X_v = X_{m+v} = X_m = T^m X$. When $\det T = 0$ this implies that $X_v = X_0$. ■

The next lemma reduces the problem of determining $v(\mathfrak{a}) = v(T, X_0, A/\mathfrak{a})$ to the case where $\mathfrak{a}$ is a power of a prime ideal.

LEMMA 2. *Let* $\mathfrak{a} = \mathfrak{p}_1^{r_1}\cdot\mathfrak{p}_2^{r_2}\ldots\mathfrak{p}_s^{r_s}$ *be the factorization of* $\mathfrak{a}$ *into prime ideals. Then*

$$v(\mathfrak{a}) = \mathrm{LCM}[v(\mathfrak{p}_1^{r_1}), v(\mathfrak{p}_2^{r_2}), \ldots, v(\mathfrak{p}_s^{r_s})].$$

Proof. The proof is immediate since, for any column vectors X and Y, we have $X \equiv Y (\bmod \mathfrak{a})$ if and only if $X \equiv Y (\bmod \mathfrak{p}_i^{r_i})$ for all i. ■

In considering a power of a prime $\mathfrak{a} = \mathfrak{p}^s$, regard T as a linear transformation on K^N, the vector space of N-tuples of elements of the number field K. Suppose that the minimal polynomial $F(x)$ of T is irreducible over K. Let L be the splitting field of $F(x)$ over K and let C be the integral closure of A in L. Now regard T as a linear transformation on L^N. Since the roots of the minimal polynomial are distinct, there is a diagonal matrix D and an invertible matrix H such that $D = HTH^{-1}$. It is easily seen that the entries of H can be chosen to lie in C; we do so. Let x_0 denote any coordinate of HX_0 and let NX_0 be the norm of x_0 considered as an element of L/K. A short matrix calculation suffices to show that the coordinates of HX_0 are conjugate and therefore NX_0 is independent of the choice of x_0. Finally let p be the rational prime over which $\mathfrak{p}$ lies, i.e. the characteristic of $A/\mathfrak{p}$, and let e be the ramification index of $\mathfrak{p}$ over p. Let s denote the greatest positive integer such that $v(\mathfrak{p}^s) = v(\mathfrak{p})$.

LEMMA 3. *If* (1) *the minimal polynomial for* T *is irreducible over* K, (2) *neither* NX_0 *nor* $\det T$ *is divisible by* $\mathfrak{p}$, (3) $\det H$ *is not divisible by* $\mathfrak{p}C$, (4) $e < s(p-1)$, *then* $v(\mathfrak{p}^r) = p^M v(\mathfrak{p})$ *where* M *is the least non-negative integer greater than or equal to* $(r-s)/e$.

It is not always true that $s = 1$. Take, for example,

$$T = \begin{bmatrix} 0 & 1 \\ 1 & 5 \end{bmatrix}, \quad X_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \text{and} \quad \mathfrak{p} = (3).$$

The assumptions of Lemma 3 are satisfied yet $v(Z/27Z) = v(Z/9Z) = v(Z/3Z) = 8$. Though the hypotheses of the lemma are numerous, note that (2) and (3) can fail for at most a finite number of primes.

Proof of Lemma 3. Consider $\{X_m\}$ as a sequence in $A/\mathfrak{p}^n$. To avoid confusion let $\equiv (\bmod \mathfrak{p}^n)$ signify equality in the ring $A/\mathfrak{p}^n$ and $\equiv (\bmod \mathfrak{p}^n C)$ equality in the ring $C/\mathfrak{p}^n C$. Since $\det T$ is assumed not divisible by $\mathfrak{p}$, $\{X_m\}$ is simply periodic by Lemma 1. Hence there is a positive integer m such that $T^m \equiv I (\bmod \mathfrak{p}^n)$; let $|T|$ denote the least such integer. We first show that $v(T, X_0, A/\mathfrak{p}^n) = |T|$. One direction is easy:

$$T^m \equiv I (\bmod \mathfrak{p}^n) \Rightarrow X_m \equiv T^m X_0 \equiv X_0 (\bmod \mathfrak{p}^n).$$

Conversely assume that $X_m \equiv X_0 (\bmod \mathfrak{p}^n)$. Then we have the following implications:

$$T^m X_0 \equiv X_m \equiv X_0 \Rightarrow D^m H X_0 \equiv H T^m X_0 \equiv H X_0 \Rightarrow D^m \equiv I (\bmod \mathfrak{p}^n C).$$

The last implication is due to that fact that NX_0 not divisible by $\mathfrak{p}$ implies that each coordinate of HX_0 is relatively prime to $\mathfrak{p}^n C$. Furthermore

$$D^m \equiv I \Rightarrow HT^m \equiv D^m H \equiv H \Rightarrow H(T^m - I) \equiv 0 (\bmod \mathfrak{p}^n C).$$

Letting $\tilde{H}$ be the matrix such that $\tilde{H}H = (\det H) I$ we have $(\det H)(T^m - I) \equiv \tilde{H}H(T^m - I) \equiv 0 (\bmod \mathfrak{p}^n C)$. Because $\det H$ is not divisible by $\mathfrak{p}C$, $T^m \equiv I (\bmod \mathfrak{p}^n)$.

Let $v = v(T, X_0, A/\mathfrak{p})$. By the hypotheses of the lemma $T^v = I + \mathfrak{p}^s U$ where not all entries in the matrix U are divisible by $\mathfrak{p}$. A simply calculation using the binomial expansion then substantiates that $(I + \mathfrak{p}^s U)^{p^M} \equiv I (\bmod \mathfrak{p}^r)$ and M is the least integer for which this is true. That $v(\mathfrak{p}) | v(\mathfrak{p}^r)$ and $v(\mathfrak{p}^r) | p^M v(\mathfrak{p})$ and $v(\mathfrak{p}^r) \nmid p^{M-1} v(\mathfrak{p})$ imply that $v(\mathfrak{p}^r) = p^M v(\mathfrak{p})$. ■

3. The period modulo a prime. In this section we are interested in determining $v(T, X_0, A/\mathfrak{p})$ where $\mathfrak{p}$ is a prime ideal in A. Let $\bar{K} = A/\mathfrak{p}$ and now let $F(x)$ be the minimal polynomial for T considered as a linear transformation on $\bar{K}^N$. Then we can write

$$F = (F_1^{e_1})(F_2^{e_2}) \ldots (F_r^{e_r})$$

where each F_i is irreducible over $\bar{K}$. The value of v is highly dependent on this factorization. In order to concisely state the results, we introduce some notation. Within some algebraically closed field containing $\bar{K}$ let a_i be any root of F_i and let $\operatorname{ord}(a_i)$ denote the multiplicative order of a_i in the extension field $\bar{K}(a_i)$. For any integer h with $0 \leqslant h \leqslant e_i$ let $H_i(x, h) = F(x)/(F_i(x))^{e_i-h}$. Then define h_i to be the least integer h for which $H_i(T, h)X_0 = 0$. Finally if $h_i > 0$ let s_i be the unique integer such that $p^{s_i} \geqslant h_i > p^{s_i-1}$. Here p is the characteristic of the field $\bar{K}$. Intuitively, the h_i measure certain "cancellations" due to the initial vector X_0. The maximum possible value of $v(T, X_0, A/\mathfrak{p})$ is the order of the matrix T. Loosely speaking, the smaller the values of the h_i, the greater the variation of $v(T, X_0, A/\mathfrak{p})$ from this maximum. Theorem 1 and its corollaries will make these notions more precise. The proofs follow the statements of the theorem and corollaries.

THEOREM 1. *With notation as above,*

$$v(T, X_0, A/\mathfrak{p}) = \operatorname{LCM}[v_i] \quad \text{where} \quad v_i = \begin{cases} 1 & \text{if} \quad a_i = 0 \text{ or } h_i = 0, \\ p^{s_i}\operatorname{ord}(a_i) & \text{otherwise}. \end{cases}$$

When $F(x)$ is irreducible we have the immediate simplification.

COROLLARY 1. *If* $\det T \neq 0$, $X_0 \neq 0$ *and the minimal polynomial* $F(x)$ *is irreducible over* $\bar{K}$, *then* $v(T, X_0, A/\mathfrak{p}) = \operatorname{ord}(a)$ *where* a *is any root of* $F(x)$.

In the case where T is the companion matrix of a linear recurrence we can define a norm map: $\bar{N}: \bar{K}^N \to \bar{K}$. The norm $\bar{N}X_0$ of the initial vector X_0 is significant in assessing the effect of X_0 on the period of the sequence $\{X_m\} \pmod{\mathfrak{p}}$. To define this norm let $\bar{L}/\bar{K}$ be the splitting field of $F(x)$; let $a_1, a_2, \ldots, a_n$ be all the roots of $F(x)$ in $\bar{L}$; and let $G_i(x) = F(x)/(x-a_i)$. Now consider T as a linear transformation on $\bar{L}^N$. For a matrix of the form (1.1), $G_i(T)$ is a transformation of rank 1. So there is, for each i, a fixed vector Y_i and a linear functional g_i on $\bar{L}^N$ such that $G_i(T)X = g_i(X)Y_i$. If we express X as an N-tuple $X = (x_1, x_2, \ldots, x_N)$ then the g_i may be written in the form $g_i(X) = \sum_{j=1}^{N} c_j x_j$ where the c_j are constants in $\bar{L}$. Now $\prod_{i=1}^{N} g_i(X)$ is a homogeneous polynomial in the variables $x_1, x_2, \ldots, x_N$ and is well defined up to a non-zero multiplicative constant in $\bar{L}$. It is possible to choose this multiplicative constant so that the coefficients of this homogeneous polynomial lie in $\bar{K}$. Letting $g(X)$ be this form with coefficients in $\bar{K}$ (well defined up to a non-zero constant in $\bar{K}$) define the norm as a mapping $\bar{N}: \bar{K}^N \to \bar{K}$ given by $X \mapsto g(X)$. In practice, the norm is easily calculated. For example, consider

$$T = \begin{bmatrix} 0 & 1 \\ a & b \end{bmatrix},$$

the companion matrix of the second order recurrence $x_m = bx_{m-1} + ax_{m-2}$ over the integers. For $X = (x, y)$ a short computation yields $\bar{N}X = (y - a_1x)(y - a_2x) = y^2 - axy - bx^2$. The next corollary states a sufficient condition for v to take its maximum possible value.

COROLLARY 2. *If* $\det T \neq 0$ *and* $\bar{N}X_0 \neq 0$, *then*

$$v(T, X_0, A/\mathfrak{p}) = p^s \operatorname{LCM}[\operatorname{ord}(a_i)]$$

where s is the unique integer such that $p^s \geqslant \max e_i > p^{s-1}$.

The next two corollaries give estimates of v. Since $\bar{K}$ is a finite field, its order is a power of p; say $|\bar{K}| = q$. Let f_i be the degree of the polynomial F_i in the factorization of the minimal polynomial F, and let b_i be the constant term of F_i. Let τ_i denote the multiplicative order of $(b_i)(-1)^{f_i}$ in the field $\bar{K}$.

COROLLARY 3. $v(\mathfrak{p}) | p^s \operatorname{LCM}[\tau_i(q^{f_i}-1)/(q-1)]$ *where s is the unique integer satisfying* $p^s \geqslant \max e_i > p^{s-1}$.

COROLLARY 4. *Assume that* $h_i \neq 0$, $\det T \neq 0$ *and* $\tau_i^u | (q^{f_i}-1)/(q-1)$ *for some integer u. Then* $\tau_i^{u+1} | v(\mathfrak{p})$.

Proof of Theorem 1. In $\bar{L}$ the polynomial $F(x)$ can be factored $F(x) = \prod_{i=1}^{h} (x-a_i)^{n_i}$ where the a_i are distinct. If V_i denotes the kernel of $(T-a_i)^{n_i}$ then $\bar{L}^N = V_1 \oplus V_2 \oplus \ldots \oplus V_k$ and T is the direct sum of the transformations T_i induced by T restricted to the subspace V_i. Let X_0^i be the projection of X_0 on the subspace V_i. It is then apparent that

$$v(T, X_0, \bar{K}) = \operatorname{LCM}[v(T_i, X_0^i, \bar{L})]. \tag{3.1}$$

In order to determine $v(T_i, X_0^i, \bar{L})$ let w_i be the least integer such that $(T-a_i)^{w_i} X_0^i = 0$ but $(T-a_i)^{w_i-1} X_0^i \neq 0$. If $w_i = 0$ or $a_i = 0$, then trivially $v(T_i, X_0^i, \bar{L}) = 1$. Otherwise $a_i \neq 0$ implies that T_i is invertible on V_i and hence $v(T_i, X_0^i, \bar{L})$ is the least integer m such that $T^m X_0^i = X_0^i$. To simplify the notation we drop the subscripts and let a be any of the a_i and let V, w, n and X be the corresponding V_i, w_i, n_i and X_0^i. Then the condition on m stated above is equivalent to

$$(a^m - 1)X + \binom{m}{1} a^{m-1}(T-a)X + \ldots + \binom{m}{w-1} a^{m-w+1}(T-a)^{w-1}X$$
$$= [a + (T-a)]^m X - X = T^m X - X = 0.$$

A short induction using this equation suffices to show that the following conditions must be satisfied:

$$a^m = 1,$$

$$\binom{m}{1} = \binom{m}{2} = \ldots = \binom{m}{w-1} \equiv 0 \pmod{p}$$

where p is the characteristic of $\bar{K}$. For the validity of the set of congruences it is necessary and sufficient that $p^t | m$ where t is the unique integer such that $p^t \geqslant w > p^{t-1}$. Restating equation (3.1) we have $v(T, X_0, \bar{K}) = \mathrm{LMC}[v_i]$ where

$$v_i = \begin{cases} 1 & \text{if } a_i = 0 \text{ or } w_i = 0, \\ p^{t_i}\mathrm{ord}(a_i) & \text{otherwise} \end{cases}$$

and t_i is the unique integer such that $p^{t_i} \geqslant w_i > p^{t_i-1}$. To complete the proof we have only to show that if a_i and a_j are roots of the same factor $f(x)$ of $F(x)$, irreducible over $\bar{K}$, then (1) $\mathrm{ord}(a_i) = \mathrm{ord}(a_j)$ and (2) $w_i = w_j = h$ where we recall that h is the least integer for which $H(T, h)X_0 = 0$ where $H(x, h) = F(x)/(f(x))^{e-h}$. These facts follow easily from the existence of an isomorphism of $\bar{K}(a_i)$ onto $\bar{K}(a_j)$ taking a_i to a_j and leaving the elements of $\bar{K}$ fixed. We omit the details.

Proof of Corollary 2. $\mathrm{Det}\,T \neq 0$ insures that $a_i \neq 0$ for all i. Now assume that $\bar{N}X_0 \neq 0$. Using the notation $G_i(T)$ with the same meaning as in the definition of the norm, we have $G_i(T)X_0 \neq 0$ for all i. As in the proof of the theorem, this implies $H(T, e_i - 1) \neq 0$, which is equivalent to $h_i = e_i$. The result now follows from Theorem 1. ■

Proof of Corollary 3. The norm N of an element γ of $\bar{K}(a_i)$ is defined as the product of the conjugates of γ. Then $N\colon \bar{K}(a_i)^* \to \bar{K}^*$ is a surjective homomorphism of the multiplicative subgroup of $\bar{K}(a_i)$ onto the multiplicative subgroup of $\bar{K}$. Let U_i be the kernel of this homomorphism; then $|U_i| = (q^{f_i}-1)/(q-1)$. Since $Na_i = (-1)^{f_i}b_i$, we have $a_i^{\tau_i} \in U_i$. Therefore $\mathrm{ord}(a_i) \mid [\tau_i(q^{f_i}-1)/(q-1)]$. The corollary then follows from Theorem 1. ■

Proof of Corollary 4. The group $\bar{K}(a_i)^*$ of invertible elements of $\bar{K}(a_i)$ is cyclic; let g be a generator. Then g^{q-1} is a generator of U, the kernel of the norm map $N\colon \bar{K}(a_i)^* \to \bar{K}^*$. Let m be the exponent such that $a_i = g^m$. By definition $g^{m\tau_i} = a_i^{\tau_i} \in U$. Therefore we have the congruence $m\tau_i \equiv j(q-1) \pmod{q^{f_i}-1}$ for some integer j. So there must exist an integer J such that $m = J(q-1)/\tau_i$. In addition we claim that $(J, \tau_i) = 1$. Otherwise we would have

$$a^{\tau_i/(J,\tau_i)} = g^{m\tau_i/(J,\tau_i)} = g^{(q-1)J/(J,\tau_i)} \in U$$

which contradicts the fact that τ_i is the order of Na_i. By Theorem 1 we have $1 = a^v = g^{mv} = g^{J(q-1)v/\tau_i}$ which implies that $q^{f_i}-1 \mid v\cdot J(q-1)/\tau_i$. This in turn implies that $\tau_i^{u+1} \mid vJ$ and Corollary 4 follows. ■

4. Examples. To illustrate the theory let

$$T = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad X_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

and let n be a positive integer. Consider $v(n) = v(T, X_0, Z/nZ)$. We choose this as our first example because $v(n)$ is the period of the Fibonacci sequence ($x_{m+1} = x_m + x_{m-1}$ with $x_0 = 0$ and $x_1 = 1$), and there is an extensive literature on this subject ([1], [3], [8], [9]). The following theorem is a direct consequence of Lemmas 2 and 3 and Corollaries 3 and 4. The usual proof is based on lengthy Fibonacci identities.

THEOREM 2. (i) *If* $n = p_1^{r_1}p_2^{r_2}\ldots p_t^{r_t}$ *then*

$$v(n) = \mathrm{LCM}[v(p_1^{r_1}), \ldots, v(p_t^{r_t})].$$

(ii) *If s is the greatest integer* $\leqslant r$ *such that* $v(p^s) = v(p)$, *then*

$$v(p^r) = p^{r-s}v(p) \quad \textit{for any prime } p.$$

(iii) *If* $p \equiv \pm 3 \pmod{10}$ *then* $v(p) \mid 2(p+1)$ *and* $v(p) \nmid p+1$. *If* $p \equiv \pm 1 \pmod{10}$ *then* $v(p) \mid p-1$ *and* $2 \mid v(p)$.

In part (iii) it is often, but not always, true that $v(p) = 2(p+1)$ or $v(p) = p-1$. For example $v(47) = 32$ and $v(101) = 50$. In Section 2 we gave an example of a matrix for which $v(p^3) = v(p)$. For the Fibonacci matrix, however, it has been an unsolved conjecture for at least 18 years [8] that $v(p^2) = v(p)$. This would imply that always $s = 1$ in part (ii). Penny and Pomerance [6] have verified it by computer for all $p \leqslant 177\,409$. By the methods of this paper, the conjecture is equivalent to $a^{p^2-1} \not\equiv 1 \pmod{p^2B}$ where B is the set of algebraic integers in $Q(\sqrt{5})$ and $a = (1+\sqrt{5})/2$. A similar congruence $2^{p-1} \not\equiv 1 \pmod{p^2}$ has been studied extensively. The first counterexample is $p = 1093$. The analogy between the two congruences makes the existence of a large counterexample to $v(p^2) = v(p)$ seem likely. Finally we note that for arbitrary initial vector Y_0 we do not necessarily have $v(Y_0) = v\begin{pmatrix}0\\1\end{pmatrix}$. For example $v\begin{pmatrix}3\\1\end{pmatrix} = 5$ while $v\begin{pmatrix}0\\1\end{pmatrix} = 10$. However, it can be shown via Theorem 1 that either $v(Y_0) = v\begin{pmatrix}0\\1\end{pmatrix}$ or $v(Y_0) = \frac{1}{2}v\begin{pmatrix}0\\1\end{pmatrix}$.

As a second example consider the sequence of integers $x_1, x_2, \ldots$ defined by the integral second order recurrence

$$x_{m+1} = ax_m + bx_{m-1}, \quad x_0 = 0;\ x_1 = 1.$$

Historically more attention has been focused on the rank than on the period. The *rank* $\mu(n)$ of an integer n is defined as the least positive integer m such that n divides x_m. We will assume that the recurrence is non-degenerate, i.e. $a, b \not\equiv 0 \pmod{n}$. Then for a prime p

$$\mu(p) = v(S, X_0, Z/pZ) \quad \text{where} \quad S = \begin{bmatrix} 0 & 1 \\ -1 & -(2+a/b) \end{bmatrix} \text{ and } X_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

(We leave the proof to the reader.) The following theorem has occured in the literature in various forms. It is a special case of our Corollary 3. Here $\left(\frac{q}{p}\right)$ denotes the Legendre symbol.

THEOREM 3. *Let p be an odd prime. If $a^2+4b \equiv 0 \pmod p$ then $\mu(p) = p$. If $a^2+4b \not\equiv 0 \pmod p$ then*

$$\mu(p) \mid p-1 \quad \textit{when} \quad \left(\frac{a^2+4b}{p}\right) = 1$$

and

$$\mu(p) \mid p+1 \quad \textit{when} \quad \left(\frac{a^2+4b}{p}\right) = -1.$$

As a final example consider the recurrence $x_m = x_{m-1}+x_{m-2}+x_{m-3}$ with the initial values $x_0 = x_1 = 0$ and $x_2 = 1$. This is a likely third order generalization of the Fibonacci sequence. The companion matrix is

$$U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad X_0 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

The minimal polynomial for U over Z/pZ for any prime p is $F(x) = x^3 - x^2 - x - 1$. Modulo Lemmas 2 and 3, the determination of $v(U, X_0, Z/nZ)$ is reduced to the case of n prime. The Newton formulas can be used to calculate the discriminant of $F(x)$: $d(F) = -44$. Hence the only primes for which $F(x)$ has a multiple root are 2 and 11. For all other primes we apply a long known criteria for the factorability of cubics mod p and Corollary 3 to derive the following theorem. $v(p)$ means $v(U, X_0, Z/pZ)$.

THEOREM 4. *Assume that p is a prime other than 2 or 11.*

If $\left(\frac{p}{11}\right) = 1$ then

$$\begin{cases} v(p) \mid p^2+p+1 & \textit{if } F(x) \textit{ is irreducible} \bmod p, \\ v(p) \mid p-1 & \textit{otherwise}. \end{cases}$$

If $\left(\frac{p}{11}\right) = -1$ then $v(p) \mid p^2-1$.

References

[1] D. M. Bloom, *On periodicity in generalized Fibonacci sequences*, Amer. Math. Monthly 72 (1965), pp. 856–861.

[2] I. J. Good and R. A. Gaskins, *Some relationships satisfied by additive and multiplicative recurrent congruential sequences with inplications for pseudo random number generation*, in: *Computers in Number Theory*, Atkin and Birch, ed., Academic Press, London 1971, pp. 125–136.

[3] L. I. Gor'kov, *Certain properties of Fibonacci numbers*, Leningrad. Gos. Ped. Inst., Učen. Zap. (1971), čast' 2, pp. 3–15.

[4] D. H. Lehmer, *Mathematical methods in large scale computing units*, Amm. Comp. Lab. Harvard Univ. 26 (1951), pp. 141–146.

[5] E. Lucas, *Sur la théorie des nombres premiers*, Atti. R. Accad. Sc. Torino (Math.) 11 (1875), pp. 928–937.

[6] Penny and Pomerance, *Solution to Problem E2539*, Amer. Math. Monthly 83 (1976), pp. 742–743.

[7] D. W. Robinson, *The rank and period of a linear recurrent sequence over a ring*, Fibonacci Quart. 14 (1976), pp. 210–214.

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

[9] M. Ward, *The prime divisors of Fibonacci numbers*, Pacific J. Math. 11 (1961), pp. 379–386.

[10] O. Wyler, *On second order recurrences*, Amer. Math. Monthly 72 (1965), pp. 500–506.

Received on 18.2.1978
and in revised form on 27.10.1978 (1045)