FIBONACCI SPACES

E.D. Cashwell and C.J. Everett
University of California, Los Alamos Scientific Laboratory
Los Alamos, New Mexico

INTRODUCTION

The Fibonacci sequence $\{F_j\} = 0, 1, 1, 2, \ldots$, with $F_j + F_{j+1} = F_{j+2}$, $j \geq 0$, may be regarded as one element of a certain space of sequences associated with the quadratic polynomial $f(x) = -1 - x + x^2$, from which its remarkable properties derive. In the following pages, we present first, in modern algebraic terminology, an exposition of those parts of the general theory of such spaces of linear recurring sequences which form a background for this point of view. The spaces arising from quadratic polynomials are then considered in this setting, with some applications to number theory, in particular to various tests for primality of the Mersenne and Fermat numbers.

It is hoped that the paper may thus serve as an introduction and source of reference for these aspects of the subject. [1] **

1. THE SPACE OF A POLYNOMIAL

Let $f(x) = -a_0 - a_1 x - \ldots - a_{n-1} x^{n-1} + x^n = (x - r_1) \ldots (x - r_n)$ be an arbitrary monic polynomial of degree n in $Z[x]$, i.e., with coefficients a_j in the domain Z of rational integers, its (complex) zeros being therefore algebraic integers. With $f(x)$ we associate the set $C(f)$ of all sequences $S = \{s_0, s_1, \ldots\}$ with components s_j in the complex field [2] C, in which $s_0, \ldots, s_{n-1}$ are arbitrary but having

$$(R) \qquad a_0 s_j + a_1 s_{j+1} + \ldots + a_{n-1} s_{j+n-1} = s_{j+n}$$

for all $j \geq 0$. Clearly, $C(f)$ is a vector space of order n over C. An obvious basis consists of the integral sequences [3] (i.e., with components in Z):

$$U_0 = \{u_{0j}\} = \{1, \ldots, 0, a_0, \ldots\}, \ldots, U_{n-1} = \{u_{n-1,j}\} = \{0, \ldots, 1, a_{n-1}, \ldots$$

*Worked performed under the auspices of the United States Atomic Energy Commission.

**Refer to footnotes at end of article.

of C(f), in terms of which every sequence S of the space may be expressed uniquely, in the form

$$S = s_0U_0 + \ldots + s_{n-1}U_{n-1},\ s_j \in C \quad .$$

A "Geometric" sequence $\{1, r, r^2, \ldots\}$ with $r \in C$ is in C(f) if and only if $f(r) = 0$. Thus

$$R_i = \{1, r_i, r_i^2, \ldots\}, \quad i = 1, \ldots, n$$

constitute the geometric sequences of C(f). Every element

$$c_1R_1 + \ldots + c_nR_n,\ c_i \in C \quad ,$$

of the space they span is therefore in C(f), in particular the integral sequence $V = R_1 + \ldots + R_n = \{v_j\} = \{n, a_{n-1}, \ldots\}$, with $v_j = r_1^j + \ldots + r_n^j$, $j \geq 0$. Being in C(f), its components v_{j+n} satisfy the relations (R); these, together with the less obvious recursions

$$(a_{n-m})m + a_{n-m+1}v_1 + \ldots + a_{n-1}v_{m-1} = v_m,\ 1 \leq m < n$$

are "Newton's formulas".

The geometric sequences R_i also form a basis for C(f) over C if and only if the zeros of f(x) are distinct. For, the matrix $R = [r_i^j]$, $i = 1, \ldots, n$; $j = 0, \ldots, n-1$, has the Vandermonde determinant $\pi_{k>i}(r_k - r_i)$. When the latter is not zero, the inverse matrix $R^{-1} = [r_{ij}]$ exists [4] (over C) with $I = R^{-1}R$, from which it follows that

(B) $$U_i = r_{i1}R_1 + \ldots + r_{in}R_n, \quad i = 0, \ldots, n-1$$

By means of these equations, which may be regarded as the "Binet formulas" for the general case, every sequence

$$S = \{s_j\} = \{s_0U_0 + s_{n-1}U_{n-1}\} \text{ of } C(f)$$

is expressible uniquely in the form

$$S = c_1R_1 + \ldots + c_nR_n,\ c_i \in C$$

with $s_j = c_1r_1^j + \ldots + c_nr_n^j$, $j \geq 0$,

when the r_i are distinct. This underlying structure of the sequences of C(f), particularly of the integral sequences, is one of the most curious features of the subject.

For example, if all zeros of f(x) are h-th roots of unity, it is clear that every $S = \Sigma c_i R_i$ is pure periodic, with period [5]** dividing h. When $a_0 \neq 0$ and the r_i are distinct, the existence of a sequence S, with all the $c_i \neq 0$, of period k, implies that all r_i are k-th roots of unity. For, $a_0 \neq 0$ insures, via (R), that S is pure periodic, and we should then have a linear system $\Sigma r_i^j (r_i^k - 1)c_i = 0$, $j = 0, \ldots, n-1$, with determinant $\det R \neq 0$. Thus $(r_i^k - 1)c_i = 0$ for each i, and either $c_i = 0$ or r_i is a k-th root of unity. Consequently, if f(x) has distinct zeros which are roots of unity, and h is the least positive integer for which all $r_i^h = 1$, then every $S = \Sigma c_i R_i$ of C(f) with all $c_i \neq 0$ is pure periodic of period k equal to h. For, by the first remark, $k \mid h$, and by the second, $h \leq k$, hence, every period $k = h$.

Note: The following generalization of the "geometric basis" theorem was suggested by the referee: If r is a zero of multiplicity m for f(x), then r is a zero of the first m-1 derivatives of f(x). From this one may show that the m sequences

$$s_j^{(h)} = \binom{j}{h} r^j; \quad j \geq 0, \quad h = 0, 1, \ldots, m-1 \ ,$$

are in C(f), where $\binom{j}{h} = 1$ for $h = 0$, and $\binom{j}{h} = (j)(j-1)\ldots(j-h+1)/h!$ for $h \geq 1$. Moreover, if f(x) has the <u>distinct</u> zeros $r_1, \ldots, r_k$, $1 \leq k \leq n$, of multiplicities $m_1, \ldots, m_k$ respectively, then the set of n sequences consisting of k subsets such as that above, one for each zero r_i, are linearly independent, and so form a basis for C(f) in the general case, provided only that zero, if it occurs among the r_i, has multiplicity 1. The linear independence follows from the non-singularity of the "confluent Vandermonde matrix." Cf. ref. [1].

2. LIMIT THEOREMS

If $\lim s_{j+1}/s_j = r$ exists for a terminally non-zero sequence S of C(f), then r must be one of the zeros of f(x). For, the

recursion (R) implies $a_0 + a_1(s_{j+1}/s_j) + \ldots + a_{n-1}(s_{j+n-1}/s_j) = s_{j+n}/s_j$. Since $s_{j+2}/s_j = (s_{j+2}/s_{j+1})(s_{j+1}/s_j)$, and so on, we have $f(r) = 0$ in the limit. As a partial answer to the questions arising here we include

Theorem 1. (A). If one zero r_1 of $f(x)$ exceeds all others in absolute value, then $S = \{s_j\} = \Sigma c_i R_i$ has $\lim s_j/r_1^j = c_1$. Hence if $c_1 \neq 0$, S is terminally non-zero, and $\lim s_{j+1}/s_j = r_1$.

(B). If $|r_i| < 1$ for all $i \geq 2$, the sequence S has $\lim (s_j - c_1 r_1^j) = 0$. Hence, if S is an integral sequence, s_j is the closest integer to $c_1 r_1^j$ for large j, and, if $a_0 \neq 0$, no other integral sequence $\Sigma c_i R_i$ has the same c_1.

Proof. (A). $s_j/r_1^j = c_1 + c_2(r_2/r_1)^j + \ldots + c_n(r_n/r_1)^j \to c_1$.

If $c_1 \neq 0$, then $s_j \neq 0$, $j \geq J$, and so $s_{j+1}/s_j =$

$$r_1(s_{j+1}/r_1^{j+1})/(s_j/r_1^j) \to r_1 c_1/c_1 = r_1 \ .$$

(B). $s_j - c_1 r_1^j = c_2 r_2^j + \ldots + c_n r_n^j \to 0$. Two integral sequences with the same c_1 are therefore terminally identical, and hence identical, if $a_0 \neq 0$. Indeed, it is clear from (R) that two sequences are equal if they agree on any n consecutive corresponding indices.

3. INTEGRAL SEQUENCES

The integral sequences $F = \{f_j\}$ of $C(f)$ form a module $Z(f)$, with integral basis $U_0, \ldots, U_{n-1}$, every such sequence being uniquely expressible, with integral coefficients, in the form

$$F = f_0 U_0 + \ldots + f_{n-1} U_{n-1}, \quad f_j \in Z \ .$$

The sequences of $Z(f)$ with $f_0 = 0$ form a sub-module of $Z(f)$, and have remarkable divisibility properties, as we shall see.

The sequences of $Z(f)$, considered modulo m, form a finite module $Z_m(f)$ of exactly m^n sequences with components in the modular ring $Z_m = Z/Zm$, the first n arbitrary, the rest governed by the recursion (R) mod m.

Suppose now that $m \geq 2$ is an integer prime to a_0, and let $F = \{f_j\}$ be a sequence of $Z_m(f)$. It is clear from (R) that F is pure

periodic if it is periodic at all, hence that F is periodic if and only if its n-tuples

$$(f_0, \ldots, f_{n-1}) \text{ and } (f_k, \ldots, f_{k+n-1})$$

are identical for some positive k, the least such k being its period. Since F = 0, of period k = 1, is the only sequence of $Z_m(f)$ containing the zero n-tuple, a non-zero sequence F can contain at most m^{n-1} different n-tuples, and so must be pure periodic of period $k \leq m^n - 1$.

Moreover, F has period $k = m^n - 1$ if and only if its first $m^n - 1$ n-tuples

$$(f_0, \ldots, f_{n-1}), (f_1, \ldots, f_n), \ldots, (f_{m^n-2}, \ldots, f_{m^n+n-3})$$

are all distinct. In such a case, each of the $m^n - 1$ non-zero sequences of $Z_m(f)$ is a terminal sub-sequence of F, and so also has this period. The situation cannot arise for a composite modulus m = ab, $a \geq 2$, $b \geq 2$. For, such an F contains the n-tuples (1, 0, ..., 0) and (b, 0, ..., 0), hence aF is in the space and contains the n-tuples (a, 0, ..., 0) $\neq$ (0, 0, ..., 0), which is impossible.

The maximum period $m^n - 1$ is attainable in case of a prime modulus, which may be seen from the theory of Galois fields [7]. Let p be a prime in Z, and suppose $f(x) = -a_0 - a_1 x - \ldots - a_{n-1} x^{n-1} + x^n$ is an irreducible polynomial in $Z_p[x]$. Such an f(x) exists for every p and n. The sequences of $Z_p(f)$ may then be regarded not only as the integral sequences, mod p, of the space C(f), but also in a quite different light. For there exists a field $C^* \supset Z_p$, the "root-field" of f(x) (abstractly, the Galois field GFp^n)) of exactly p^n elements, uniquely expressible in the form

$$s = f_0 + f_1 r + \ldots + f_{n-1} r^{n-1}, \quad f_j \in Z_p$$

in terms of which we may write

$$f(x) = (x - r)(x - r^p) \ldots (x - r^{p^{n-1}})$$

with n distinct zeros in C*.

Following the plan of § 1, we find that the set $C^*(f)$ of all sequences $S = \{s_j\}$, with $s_j \in C^*$ governed by the recursion (R) in C^*, is a vector space of order n over C^*, consisting of exactly $(p^n)^n$ sequences, and containing the original module $Z_p(f)$ of p^n sequences $F = \{f_j\}$, $f_j \in Z_p$.

The zeros of $f(x)$ being distinct in C^*, the geometric sequences R_i which they generate form a basis for $C^*(f)$, in terms of which every sequence of the space may be uniquely expressed:

$$S = c_1 R_1 + \ldots + c_n R_n, \quad c_j \in C^*$$

with components $s_j = c_1 r_1^j + \ldots + c_n r_n^j$, $j \geq 0$, where the r_i are now the zeros of $f(x)$ displayed above.

This sub-structure of the sequences S reveals their periodic character. For, the multiplicative group G of C^* is cyclic, with a generator s of period $p^n - 1$. If h is the period of r in G, then $h \mid p^n - 1$, and the element r^{p^i} has period $h/(h, p^i) = h$, which is therefore the period of every zero of $f(x)$. An obvious modification of the argument at the end of § 1 shows that every non-zero sequence S of $C^*(f)$ has period h.

The element r itself need not have period $p^n - 1$; however, some element $s \neq 0$ of C^* does generate the full group G, and its minimal polynomial mod p is irreducible of degree n in $Z_p[x]$. Hence there exists, for every p and n, an irreducible $f(x)$ of degree n in $Z_p[x]$ for which the zero r in C^* generates G, and every sequence $S \neq 0$ of the corresponding space $C^*(f)$ has period $p^n - 1$. We summarize these results in more conventional terms in

Theorem 2. If $m \geq 2$ is an integer prime to a_0, then, modulo m, every integral sequence $F = \{f_j\}$ of $C(f)$ is pure periodic of period $k \leq m^n - 1$. Hence, if $m \mid f_0$, then also $m \mid f_k, f_{2k}, f_{3k}, \ldots$. If m is composite, every period is less than $m^n - 1$. If p is a prime, and $f(x)$ is irreducible [6] mod p, all integral sequences F of $C(f)$ are pure periodic with the same period h, where $h \mid p^n - 1$. For every p and n, there exists an $f(x)$ such that $h = p^n - 1$.

Example 1. For $f(x) = -2 - x + x^3 \bmod 3$,

$$V = \{\dot{0}0202122102220010121120111\dot{0}0, \ldots\},$$

the period [7] being $h = 26$.

If an integer $m \geq 1$ divides some f_j, $j \geq 1$, of an integral sequence F, the least positive such j is called the rank of m in F.

Corollary 1. If F is an integral sequence of C(f), with $f_0 = 0$, every positive integer m prime to a_0 has a rank $r \leq k \leq m^n - 1$ in F.

4. THE SPACE OF A QUADRATIC

For $f(x) = -a_0 - a_1 x + x^2 = (x-r_1)(x-r_2)$, the associated space C(f) of all sequences $S = \{s_j\}$, $s_j \in C$, satisfying

$$a_0 s_j + a_1 s_{j+1} = s_{j+2}, \quad j \geq 0 \tag{R}$$

has the basis $U_0 = \{1, 0, a_0, \ldots\}$, $U_1 = \{0, 1, a_1, \ldots\}$, and contains the sub-space of vectors $c_1 R_1 + c_2 R_2$, where $R_i = \{1, r_i, r_i^2, \ldots\}$, $i = 1, 2$ are its geometric sequences. The particular sequence

$$V = R_1 + R_2 = \{v_j\} = \{2, a_1, 2a_0 + a_1^2, \ldots\}$$

consisting of the integers $v_j = r_1^j + r_2^j$, $j \geq 0$, is of special importance.

The geometric sequences R_i form a basis for C(f) if and only if $r_1 \neq r_2$, in which case the matrix R^{-1} of § 1 is

$$\frac{1}{r_1 - r_2} \begin{bmatrix} -r_2 & r_1 \\ 1 & -1 \end{bmatrix}$$

The corresponding "Binet formulas" are accordingly

$$U_0 = (-r_2 R_1 + r_1 R_2)/(r_1 - r_2), \tag{B}$$

$$U_1 = (R_1 - R_2)/(r_1 - r_2),$$

or explicitly,

$$u_{0j} = (-r_2 r_1^j + r_1 r_2^j)/(r_1 - r_2), \quad u_{1j} = (r_1^j - r_2^j)/(r_1 - r_2)$$

The relation $u_{0j} = a_0 u_{1,j-1}$ is here manifest.

We know from § 2 that, if $|r_1| > |r_2|$, $\lim u_{1j}/r_1^j = 1/(r_1 - r_2)$, $\lim v_j/r_1^j = 1$, and $\lim u_{1,j+1}/u_{1j} = \lim v_{j+1}/v_j = r_1$.

Again, if $|r_2| < 1$, then, for example, $\lim (v_j - r_1^j) = 0$ and v_j is the nearest integer to r_1^j, $j \geq J$; moreover if $a_0 \neq 0$, V is the only integral sequence $R_1 + c_2 R_2$.

The integral sequences $F = \{f_j\}$ of C(f) form a module, with integral basis U_0, U_1, and, modulo an integer m prime to a_0, are all pure periodic with periods less than m^2. For a prime modulus p, if f(x) is irreducible mod p, these periods are equal, and divide $p^2 - 1$, and there exists an f(x) such that every period is exactly $p^2 - 1$.

The sub-module of sequences $F = f_1 U_1$ (i.e., with $f_0 = 0$) has the single basic sequence U_1, which is hereafter denoted simply by $U = \{u_j\} = \{0, 1, a_1, \ldots\}$. For $f(x) = -1-x+x^2$, it is of course the Fibonacci sequence.

Every integer m prime to a_0 has a rank $r \leq k < m^2$ in U, where k is the period of U mod m; indeed $m | u_k, u_{2k}, \ldots$; similar statements may be made for every $F = f_1 U$, and $F = f_0 U_0$.

It is interesting that every sequence of C(f) is expressible in terms of U alone. For example, from $V = 2U_0 + a_1 U$ follows

$$v_j = a_0 u_{j-1} + u_{j+1}, \quad j \geq 1 .$$

Example 2. For

$$f(x) = 1 - 2x + x^2 = (x - 1)^2, \quad U = 0, 1, 2, 3, 4, \ldots \quad V = 2, 2, 2, 2, 2, \ldots .$$

Example 3. For

$$f(x) = 2 - 3x + x^2 = (x - 2)(x - 1), \quad u_j = 2^j - 1, \quad v_j = 2^j + 1$$

satisfy the simple recursions $u_{j+1} = 2u_j + 1$, $v_{j+1} = 2v_j - 1$. Note that $u_p = 2^p - 1$, $v_{2^k} = 2^{2^k} + 1$. The sequence U mod u_j has period j.

Example 4. For

$$f(x) = -2 - x + x^2 = (x - 2)(x + 1), \quad u_p = (2^p + 1)/3, \quad v_p = 2^p - 1 ,$$

for odd p, and $v_{2k} = 2^{2k} + 1$, $k \geq 1$.

5. THE SEQUENCE U

Even for the general quadratic [8], the sequence

$$U = \{0, 1, a_1, a_0 + a_1^2, \ldots\}$$

has some remarkable properties, which flow from the

Lemma 1. For all

$$j \geq 0,\ t \geq 0,\ a_0 u_j u_t + u_{j+1} u_{t+1} = u_{j+t+1} \quad .$$

The statement is easily proved, for fixed $t \geq 0$, by induction from j, j+1 to j+2, being obvious for $j = 0, 1$. The induction step reads

$$a_0 u_{j+2} u_t + u_{j+3} u_{t+1} = a_0(a_0 u_j + a_1 u_{j+1}) u_t + (a_0 u_{j+1} + a_1 u_{j+2}) u_{t+1} =$$
$$a_0 u_{j+t+1} + a_1 u_{j+t+2} = u_{j+t+3} \quad .$$

From this follows

Theorem 3. The correspondence $j \to u_j$ preserves divisibility i.e., $j \mid k$ implies $u_j \mid u_k$, or $u_j \mid u_j, u_{2j}, u_{3j}, \ldots$.

Since $u_0 = 0$, $u_1 = 1$, the final statement is trivial for $j = 0, 1$. Fixing $j \geq 2$, we prove $u_j \mid u_{jq}$ by induction on $q \geq 1$. This is trivial for $q = 1$. Fix $q \geq 1$, and assume $u_j \mid u_{jq}$. Setting $t = jq - 1$ (≥ 1) in the Lemma shows that $u_j \mid u_{j(q+1)}$.

Lemma 2. If a prime p divides any two consecutive u_k, then p divides a_0.

If $p \mid u_{j+1}, u_{j+2}$ but not a_0, then from (R) follows $p \mid u_j, u_{j+1}$ and ultimately $p \mid u_0 = 0, u_1 = 1$, which is false.

Theorem 4. Let m be a positive integer prime to a_0. Then, modulo m, U is pure periodic of period $k < m^2$, and $m \mid u_0, u_k, u_{2k}, \ldots$. Thus m has a rank $r \leq k$ in U. Moreover, $m \mid u_0, u_r, u_{2r}, \ldots$ and no other u_j, i.e., $m \mid u_\ell$ if and only if $r \mid \ell$. In particular, $r \mid k$.

We have only to prove $m \mid u_\ell$ implies $r \mid \ell$, which is obvious for $\ell = 0$. For $\ell \geq 1$, we have $r \leq \ell$, by the minimality of r. Write $\ell = rq + j$, $0 \leq j < r$, $q \geq 1$. For $t = rq - 1$ (≥ 0), Lemma 1 reads

$$a_0 u_j u_{rq-1} + u_{j+1} u_{rq} = u_\ell \quad .$$

Since $m \mid u_\ell, u_r, u_{rq}$ (Th. 3), we have $m \mid a_0 u_j u_{rq-1}$. Now m is prime to a_0, and hence also to u_{rq-1}, since a prime common to

this and m is also in u_{rq}, contradicting Lemma 2. It follows that $m \mid u_j$, where $0 \leq j < r$. Hence $j = 0$ and $\ell = rq$. We turn to the special case of

Lemma 3. If $(a_0, a_1) = 1$, the sequence U has the properties:

(a) $(a_0, u_j) = 1$, for all $j \geq 1$,

(b) $(u_j, u_{j+1}) = 1$, for all $j \geq 0$,

(c) $(u_j, u_k) = (u_k, u_{j+k})$ for all $j, k \geq 0$.

Proof. (a) Induction on $j \geq 1$. For $j = 1$, trivial. Assuming $(a_0, u_{j+1}) = 1$ for fixed $j \geq 0$, we see from (R) that $(a_0, u_{j+2}) = 1$ also. For, a prime common to these divides $a_1 u_{j+1}$ and hence u_{j+1}, since $(a_0, a_1) = 1$, violating the induction hypothesis.

(b) is clear from Lemma 2 and (a).

(c) is trivial when j or k is zero.

For $j, k \geq 1$, we have from Lemma 1, $a_0 u_j u_{k-1} + u_{j+1} u_k = u_{j+k}$. Clearly $(u_j, u_k) \mid u_k, u_{j+k}$ and hence $(u_j, u_k) \mid (u_k, u_{j+k})$. Conversely,

$$(u_k, u_{j+k}) \mid a_0 u_j u_{k-1} \quad .$$

The former is prime to a_0 by (a) and to u_{k-1} by (b). Thus it divides u_j, u_k, and so it divides (u_j, u_k).

Note: It is clear from (a) that the only integers m dividing components u_j of U are prime to a_0.

Theorem 5(A). If $\{g_j\}$ is an arbitrary sequence of integers with $g_0 = 0$, then the correspondence $j \to g_j$ preserves g.c.d.'s, that is, $(g_\ell, g_k) = g_{(\ell, k)}$ if and only if $(g_j, g_k) = (g_k, g_{j+k})$ for all $j, k \geq 0$.

(B) In particular, the sequence U has this property whenever $(a_0, a_1) = 1$.

Proof: (A) The necessity is obvious. In proving the sufficiency we may suppose $\ell \geq k$. The conclusion is clear for $k = 0$, since $g_0 = 0$. If $\ell \geq k > 0$ and $k \mid \ell = qk$, we have

$g_{(\ell, k)} = g_k = (g_k, g_k) = (g_k, g_{2k}) = \ldots = (g_k, g_\ell)$.

In the remaining case, $\ell > k > 0$, $k \nmid \ell$, we write $\ell = kq + j$, $0 < j < k < \ell$, and obtain $(g_j, g_k) = (g_k, g_{j+k}) = \ldots = (g_k, g_\ell)$. It is then clear how the Euclidean algorithm, proceeding from this relation through a sequence of similar steps and terminating in an equation such as $L = KQ + J$, $0 < J < K < L$, with $(\ell, k) = J \mid K$, leads to the conclusion $(g_\ell, g_k) = \ldots = (g_L, g_K) = (g_K, g_J) = g_J$.

(B) The application of (A) to U is now clear from Lemma 3(c).

Note: The non-trivial part of Th. 4 follows elegantly from Th. 5(B) when $(a_0, a_1) = 1$. For, if r is the rank of m, and $m \mid u_\ell$, then

$$m \mid (u_r, u_\ell) = u_{(r, \ell)},\ r \leqq (r, \ell) \mid r, \text{ and } r = (r, \ell) \mid \ell .$$

Corollary 2. If $r_1 \neq r_2$ are relatively prime integers the correspondence $j \to u_j = (r_1^{\,j} - r_2^{\,j})/(r_1 - r_2)$ is g.c.d.-preserving.

For, $f(x) = (x - r_1)(x - r_2) = -a_0 - a_1 x + x^2$ has $a_1 = r_1 + r_2$ and $a_0 = -r_1 r_2$ relatively prime.

Note: It is clear that the set of all g.c.d.-preserving functions g(j) on the integers is a closed associative system (semi-group) with identity under the composition f(g(j)). Theorem 5(A), suggested by the referee, characterizes these functions. The sequences U resulting from quadratics with $(a_0, a_1) = 1$ are non-trivial functions of the kind. As a "trivial" example consider $g(2j - 1) = 1$, $g(2j) = 2j$. Although "well-known" we include the seldom fully stated

Corollary 3. For integers $r_1 \neq r_2$ with $(r_1, r_2) = 1$ and difference $d = r_1 - r_2$, let $u_j = (r_1^{\,j} - r_2^{\,j})/(r_1 - r_2)$, $j \geqq 1$.

(a) $(d, u_j) = (d, j)$

(b) A prime $p \mid u_p$ if and only if $p \mid d$. Such a prime p has rank p in U.

(c) If $p \nmid d$, then $p \nmid u_p$ and $(d, u_p) = 1$.

(d) If $p \mid d$, then $p \mid u_p$, $(d, u_p) = p$, and if p is odd, $p^2 \nmid u_p$.

(e) Every prime factor $q \neq p$ of u_p is of form $1 + hp$.

(f) If $r_1 > r_2 > 0$, then for every odd prime p there exists a prime $q = q(p)$ dividing u_p, of form $1 + hp$, and $q(p)$ is one-one.

Proof. (a) is trivial for $j = 1$, and follows for $j \geq 2$ from

$$u_j = (d+r_2)^j - r_2^j)/d = (d^{j-2} + C^j_1 d^{j-3} r_2 + \ldots + C^j_{j-2} r_2^{j-2})d + j r_2^{j-1} \quad (a^*)$$

since $(d, r_2) = 1$.

(b) From (a*), $u_p \equiv d^{p-1} \bmod p$. The statement about the rank of p follows from (a).

(c) follows from (b) and (a).

(d) follows from (b), (a), and the congruence $u_p \equiv p r_2^{p-1} \bmod p^2$ implied by (a*) for a prime $p \geq 3$.

(e) If $q \mid u_p$, $q \neq p$, then $r_1^p \equiv r_2^p \bmod q$, $r_1 \not\equiv r_2 \bmod q$, since (d, u_p) is 1 or p; and $q \nmid r_1, r_2$. We present two proofs: (1) Letting $r_2 r_2' \equiv 1 \bmod q$, we have $(r_1 r_2')^p \equiv 1$, $r_1 r_2' \not\equiv 1 \bmod q$ implies $p = \text{period } (r_1 r_2' \bmod q) \mid \Phi(q) = q - 1 = hp$. (2) $r_1^{q-1} \equiv 1 \equiv r_2^{q-1} \bmod q$, $q \mid (u_{q-1}, u_p) = u_{(q-1, p)}$, by Cor. 2. Hence $p \mid (q - 1) = hp$, otherwise $(q - 1, p) = 1$, $q \mid u_1 = 1$.

(f) Since $u_p = r_1^{p-1} + \ldots + r_2^{p-1} > p r_2^{p-1} \geq p$, it follows that there exists a prime $q = q(p)$ of form $1 + hp \geq 7$ dividing u_p for p odd, and by Cor. 2, this function is one-one. Of course the construction is valid for every pair r_1, r_2 covered by the corollary, the simplest being 2, 1 with $u_p = 2^p - 1$. It is not known whether an infinity of primes $1 + 2p$ exist.

Corollary 4. If

$$(a_0, a_1) = 1 \text{ and } a_0, a_1 \geq 1, \text{ then } u_0 = 0 < u_1 = 1 \leq u_2 = a_1 < u_3 < u_4 \ldots,$$

and

(a) j composite implies u_j composite, (b) $u_j \mid u_k$ implies $j \mid k$, except in the single case $a_1 = 1$. If $a_1 = 1$, (a) is false only when

$j = 4$ and u_4 is prime, while (b) is false only when $j = 2$ and k is odd.

Proof. It is clear from (R) that u_j is increasing as stated.

(a) Let $j = hi$, $h \geq 2$, $i \geq 2$. By Th. 3, $u_h, u_k \mid u_j$, where $u_h, u_i < u_j$, since $2 \leq h$, $i < j$. If u_h or u_i exceeds 1, u_j is composite. Suppose both are 1. Then clearly $h = i = 2$, and $1 = u_h = u_i = u_2 = a_1$, $j = hi = 4$, $u_j = u_4$, and (a) follows with its proviso.

(b) If $u_j \mid u_k$, then $u_j = (u_j, u_k) = u_{(j,k)}$ (Th. 5), where $(j, k) \leq j$. If equality holds, $j \mid k$; if inequality, we must have $(j, k) = 1$, $j = 2$, $1 = u_1 = u_2 = a_1$, k odd, and (b) follows.

6. THE LUCASIAN SEQUENCES U, V

The integral sequences

$$U = \{u_j\} = \{0, 1, a_1, \ldots\} \quad \text{and} \quad V = \{v_j\} = \{2, a_1, 2a_0 + a_1^2, \ldots\},$$

with

$$u_j = (r_1^j - r_2^j)/(r_1 - r_2), \quad v_j = r_1^j + r_2^j,$$

of the space $C(f)$ associated with the quadratic

$$f(x) = -a_0 - a_1 x + x^2 = (x - r_1)(x - r_2),$$

where

$$r_1 = \tfrac{1}{2}(a_1 + Q^{\frac{1}{2}}), \quad r_2 = \tfrac{1}{2}(a_1 - Q^{\frac{1}{2}}), \quad Q = a_1^2 + 4a_0,$$

$$r_1 + r_2 = a_1, \quad r_1 r_2 = -a_0, \quad r_1 - r_2 = Q^{\frac{1}{2}}, \quad a_0 Q \neq 0,$$

have curious interrelations, which have been exploited by Lucas [4; p. 223], and Lehmer [5], (in even more general form) in the design of various "tests for primality". We present here some old and new aspects of this.

The following relations are easily verified using the above formulas for u_j, v_j:

(1) $u_j v_k + u_k v_j = 2u_{j+k}$ (1a) $u_j v_j = u_{2j}$

(2) $u_j v_k - u_k v_j = -2(-a_0)^j u_{k-j}$ $(k \geq j)$

(3) $v_j v_k + Q u_j u_k = 2v_{j+k}$ (3a) $v_j^2 + Q u_j^2 = 2v_{2j}$

(4) $v_j v_k - Q u_j u_k = 2(-a_0)^j v_{k-j}$ $(k \geq j)$

(4a) $v_j^2 - Q u_j^2 = 4(-a_0)^j$

(5) $v_{2j} = v_j^2 - 2(-a_0)^j$

(6) $u_1 = 1,\ v_1 = a_1$

(7) $u_p \equiv Q^{(p-1)/2} \bmod p$, for every odd prime p.

For example, we compute

$$2^p Q^{\frac{1}{2}} u_p = (a_1 + Q^{\frac{1}{2}})^p - (a_1 - Q^{\frac{1}{2}})^p = \Sigma_0^p (1-(-1)^i) C^p{}_i a_1^{p-i} Q^{i/2},$$

so

$$2^{p-1} u_p = \Sigma_{0,\ i \text{ odd}}^p C^p{}_i a_1^{p-i} Q^{(i-1)/2}, \quad \text{from which}$$

$$u_p \equiv Q^{(p-1)/2} \bmod p.$$

A prime is said to be <u>regular</u> (relative to $f(x)$) in case $p \nmid 2a_0 Q$. We know from Th. 4 such a prime has rank $r = r(p) \mid k(p) \leq p^2 - 1$ in U, where $k(p)$ is the period of U mod p, and $p \mid u_0, u_r, u_{2r}, \ldots$ and no other u_j. More remarkably, we see now, from (2), (1), (6), and (7), that

$$a_1 - Q^{(p-1)/2} a_1 \equiv 2a_0 u_{p-1} \quad \text{and} \quad a_1 + Q^{(p-1)/2} a_1 \equiv 2u_{p+1} \bmod p.$$

Lemma 4. If p is a regular prime, then $p \mid u_{p-1}$ if $(Q/p) = 1$, where $p \mid u_{p+1}$ if $(Q/p) = -1$ (Legendre symbol!), so that always $r(p) \leq p + 1$ in U.

Lemma 5. If p is a regular prime, then $p \mid v_{2k}$ if and only if $r(p) = 2^{k+1}$ in U.

Proof. If $p \mid v_{2k}$ then $p \mid u_{2k+1}$ by (1a), but $p \nmid u_{2k}$ by (4a), hence $r(p) = 2^{k+1}$. Conversely, if $p \mid u_{2k+1}$ but not u_{2k}, then $p \mid v_{2k}$ by (1a).

These are the basic lemmas. For computational reasons, we note that the sequence $\{v_{2k}\}$, with $v_2 = 2a_0 + a_1^2$, $v_{2k+1} = (v_{2k})^2 - 2a_0^{2k}$, $k \geq 1$ (cf. [5]) is related to the auxiliary sequence $\{S_k\}$ defined by

$$S_1 = 2 + (a_1^2/a_0), \quad S_{k+1} = S_k^2 - 2, k \geq 1 \quad ,$$

via the simple equation $v_{2k} = a_0^{2k-1} S_k$, $k \geq 1$. Thus, whenever $a_0 \mid a_1^2$, $\{S_k\}$ is an integral sequence, and a regular prime p divides v_{2k} if and only if $p \mid S_k$.

We may state one of Lehmer's results as

Theorem 6. Let $M = 2^q - 1$, where q is an odd prime, and suppose a_0, a_1 are integers with the properties

(a) If p is a prime divisor of M, then $p \nmid 2a_0Q$ where $Q = a_1^2 + 4a_0$.

(b) M prime implies $(Q/M) = -1$ and $(a_0/M) = 1$.

Then M is prime if and only if $M \mid v_{(M+1)/2}$, (equivalently S_{q-1}, if $a_0 \mid a_1^2$).

Proof. If prime $p \mid M \mid v_{(M+1)/2}$, p is regular by (a); hence, in U, $r(p) = M+1 \leq p+1$ by Lemmas 5, 4. Thus $p \mid M \leq p$, and $M = p$, prime. Conversely, if M is prime, it is regular by (a), and from (b), (3), (6), and (7) follows $a_1^2 - Q \equiv 2v_{M+1}$, or $v_{M+1} \equiv -2a_0 \bmod M$. Then from (5) and (b), $-2a_0 \equiv (v_{(M+1)/2})^2 - 2a_0^{(M+1)/2}$, and M divides the stated v_j.

Example 5. For $a_0 = a_1 = 2$, $Q = 12$, (a) and (b) are satisfied. For, only the primes 2 and 3 divide $2a_0Q$, and $M \equiv 1 \bmod 2$ and $M \equiv 1 \bmod 3$. Moreover, if M is a prime $(Q/M) = (3/M) = -1$, and

$(a_0/M) = (2/M) = 1$, since $M \equiv -1 \mod 8$. Since $a_0 | a_1^2$, the sequence $\{S_k\}$ is integral with $S_1 = 4$, and M is prime if and only if $M | S_{q-1}$.

In the same fashion one may prove

Theorem 7. Let $F = 2^{2^t} + 1$, $t \geq 1$, and suppose a_0, a_1 are integers with the properties

(a) If p is a prime divisor of F, then $p \nmid 2a_0Q$.

(b) F prime implies $(Q/F) = 1$, $(a_0/F) = -1$.

Then F is prime if and only if $F | V_{(F-1)/2}$, (equivalently S_{2^t-1}, if $a_0 | a_1^2$).

Proof. Suppose prime $p | F | V_{(F-1)/2}$. Then p is regular and in U has $r(p) = F - 1 \leq p + 1$, so $p | F \leq p + 2$. Clearly $F = p$, otherwise $2p \leq F \leq p + 2$, $p \leq 2$. If F is prime, it is regular by (a), and from (b), (6), (7), (4), $a_1^2 - Q \equiv -2a_0 V_{F-1} \mod F$ or $V_{F-1} \equiv 2 \mod F$. From (5) and (b), $2 \equiv (V_{(F-1)/2})^2 + 2 \mod F$ and the theorem follows.

Example 6. For $a_0 = a_1 = 3$, $Q = 21$, only the primes 2, 3, and 7 divide $2a_0Q$, whereas $F \equiv 1 \mod 2$, $F \equiv 2 \mod 3$; as for 7, note that either $2^t = 1 + 3h$, and then $F \equiv 3 \mod 7$, or $2^t = 2 + 3h$, and then $F \equiv 5 \mod 7$. Hence (a) holds. If F is prime, we have $(3/F) = (F/3) = (2/3) = -1$, and also $(7/F) = (F/7) = -1$, since $(3/7) = -1 = (5/7)$. Hence $(Q/F) = (3/F)(7/F) = 1$, and $(a_0/F) = (3/F) = -1$, as required. The auxiliary S_k are integers, with $S_1 = 5$.

Note: The tests indicated in Th. 7 have no computational advantage over the orthodox N and S condition $3^{(F-1)/2} \equiv -1 \mod F$. Indeed, the latter is a special case of Th. 7, with $a_0 = 3$, $a_1 = 2$. For the latest computational results see the relevant articles in Math. Comp. 18 (Jan. 1964) and Scientific American (Nov. 1964, p. 12). The least undecided Fermat number is F_{17}.

7. THE SPACE $Z_p(f)$

Let p be a prime of Z, and $f(x) = -a_0 - a_1 x + x^2 \in Z_p[x]$. The

regularity condition $p \nmid 2a_0Q$, which we here assume, insures that p is odd, and the zeros r_i of f(x) in its root field are non-zero and distinct.

Since $f(x) = (x-2'a_1)^2 - (2')^2Q$, where $2'$ is the inverse of 2 mod p, we see that this root field is Z_p if $(Q/p) = 1$, or the Galois field $C^* \cong GF(p^2)$ of $\not\in 3$ if $(Q/p) = -1$.

(I.) If $(Q/p) = 1$, there is a $b \in Z$ such that $b^2 \equiv Q \bmod p$, and f(x) is reducible in $Z_p[x]$. Indeed, in Z_p, $f(x) = (x - 2'(a_1+b))(x - 2'(a_1 - b))$ has the distinct zeros indicated. The space $Z_p(f)$ itself has basis R_1, R_2 over Z_p, each of its sequences being expressible in the form $s_j = c_1r_1^j + c_2r_2^j$, $c_i, r_i \in Z_p$. Since $r_i^{p-1} \equiv 1 \bmod p$, every S is pure periodic of period dividing p-1. By an argument now familiar, if h is the least exponent for which both $r_i^h \equiv 1$, every sequence with both $c_i \neq 0$ (e.g., U_0, U, and V) has period h.

This case is of special interest when $p = 2^{2^t} + 1$ is a prime. The conditions $(Q/p) = 1$, $(a_0/p) = -1$ then hold if and only if f(x) has zeros in Z_p with (say) r_2 a quadratic residue, and r_1 a non-residue. In such a case, r_1 has period p-1, and r_2 may have any period $m \mid \frac{1}{2}(p-1)$, in Z_p. From the above expression of s_j in terms of the r_i it is clear that one sequence $(S = 0)$ has period 1, exactly p-1 (those with $c_1 = 0$, $c_2 \neq 0$) have period m, and the (p-1)p remaining sequences (with $c_1 \neq 0$, c_2 arbitrary) have period p-1.

(II.) If $(Q/p) = -1$, f(x) is irreducible in $Z_p[x]$, with zeros r, r^p in C*, where, in the cyclic group G of order $p^2 - 1$, r and r^p have a period $h \mid p^2 - 1$. The geometric sequences R_i are now in C*(f) and form a basis for the latter space over C*. All sequences $S \neq 0$ of C*(f), in particular those of $Z_p(f)$, have period h. Since $(r)^{p+1} - (r^p)^{p+1} = r^{p+1}(1 - r^{p^2-1}) = 0$, $p \mid u_{p+1}$.

For every $p \geq 3$, there exists an irreducible quadratic (relative to which p is necessarily regular) for which r has period p^2-1. Every sequence of the corresponding space has period p^2-1. Since $p \mid u_{p+1}$, and every pair (0, 1), ..., (0, p-1), indeed every pair $\neq (0, 0)$,

must appear exactly once as an adjacent pair in the sequence $\{u_0, \ldots, u_{p^2-1}\}$ mod p, it is clear that p+1 is itself the rank of p in U, and the above sequence consists of the terminal element and p-1 blocks of p+1 elements each. Moreover, each block arises from the first by renaming its elements, since each is the beginning of a sequence of the space which is a multiple of U itself.

Such a sequence thus provides a solution of very special type for the m = p, n = 2 problem (Cf. footnote [7]). Lehmer's quadratic (Ex. 5) $f(x) = -2-2x+x^2$ mod $p = 2^3 - 1 = 7$ has a root r of period $7^2 - 1 = 48$, and mod 7 we find

$$U = \{01262216\ 05323352\ 04131143\ 06515561\ 02454425\ 03646634\ 0\ldots\} .$$

FOOTNOTES

1. Most of the ideas presented may be found elsewhere, sometimes in less general form. See for example references [3, 6, 10].

2. A parallel version is obtained if C is everywhere replaced by the "root field" of f(x) over the rational field, or by the abstract root field of f(x) mod p. See [7].

3. Although linearly independent, one may note, among others, the relation $u_{oj} = a_o u_{n-1, j-1}$, $j \geq 1$.

4. Explicitly, for $i = 0, 1, \ldots, n-1$; $j = 1, \ldots, n$,

$$r_{ij} = (-1)^i \sigma(n-1-i; j) / \prod_{k \neq j} (r_k - r_j)$$

where the σ denotes the elementary symmetric function of degree n-1-i in the n-1 roots r_k other than r_j. (Here $\sigma \equiv 1$ when n-1-i = 0). Cf. ref. [8].

5. Period always means minimal period, while pure periodic means that periodicity obtains from the beginning of the sequence.

6. The root field for a reducible f mod p exists, but the periodicity properties are more complicated.

7. The method indicated (with suitable insertion of a zero) provides

an algebraic construction of a sequence of integers mod m, of length m^n+n-1, containing no repeated n-tuple, in the case of prime m. The existence of such sequences for arbitrary m, n is a well-known corollary of a theorem on graphs [2, 9]. (Remark of referee.)

8. For the Fibonacci case, see [10], on which the present section is modelled.

REFERENCES

1. J. W. Archbold, Algebra, 1958, Pitman, London, p. 419.
2. C. Berge, Theory of Graphs, 1962, Wiley, N. Y., p. 167, Th. 2.
3. E. B. Dynkin, Problems in the theory of numbers, Survey of recent East European math. literature, 1963.
4. G. H. Hardy, E. M. Wright, Introduction to the theory of numbers, 3rd ed'n., 1954, Oxford, p. 223.
5. D. H. Lehmer, An extended theory of Lucas functions, Annals of Math. (2) 31, 1930, 419-448. On Lucas's test for the primality of Mersenne's numbers, Jour. London Math. Soc., X, 1935, 162-165.
6. E. Lucas, Théorie des nombres, 1961, Blanchard, Paris, Ch. XVII, XVIII.
7. C. C. MacDuffee, Introduction to abstract algebra, 1940, Wiley, N. Y., p. 174 ff.
8. L. Mirsky, An introduction to linear algebra, 1955, Oxford, p. 36.
9. O. Ore, Theory of graphs, Am. Math. Soc. Colloq. Pub. XXXVIII, 1962, p. 40, Th. 3.1.3.
10. N. N. Vorob'ev, Fibonacci numbers, Popular lectures in mathematics, v. 2., Blaisdell, N. Y.

XXXXXXXXXXXXXXX