Journal of Integer Sequences, Vol. 5 (2002),
Article 02.2.3

INTEGER SEQUENCES AND PERIODIC POINTS

G. Everest[1], A. J. van der Poorten[2], Y. Puri[1], and T. Ward[1]

[1] School of Mathematics, University of East Anglia, Norwich NR4 7TJ, United Kingdom
g.everest@uea.ac.uk, puri@hotmail.com, t.ward@uea.ac.uk

[2] ICS, Macquarie University, NSW 2109, Australia
alf@math.mq.edu.au

Abstract. Arithmetic properties of integer sequences counting periodic points are studied, and applied to the case of linear recurrence sequences, Bernoulli numerators, and Bernoulli denominators.

1. Introduction

An existing dialogue between number theory and dynamical systems is advanced. A combinatorial device gives necessary and sufficient conditions for a sequence of non-negative integers to count the periodic points in a dynamical system. This is applied to study linear recurrence sequences which count periodic points. Instances where the p-parts of an integer sequence themselves count periodic points are studied. The Mersenne sequence provides one example, and the denominators of the Bernoulli numbers provide another. The methods give a dynamical interpretation of many classical congruences such as Euler-Fermat for matrices, and suggest the same for the classical Kummer congruences satisfied by the Bernoulli numbers.

Let X denote a set, and $T : X \to X$ a map. An element $x \in X$ is a periodic point of period $n \in \mathbb{N}$ if it is fixed under T^n, that is $T^n(x) = x$. Let $\mathrm{Per}_n(T)$ denote the set of points of period n under T. Following [13], call a sequence $u = (u_n)_{n\geq 1}$ of non-negative integers *realizable* if there is a set X and a map $T : X \to X$ such that $u_n = |\,\mathrm{Per}_n(T)|$.

This subject is example-driven so we begin our account with several of these. Throughout, examples will be referenced as they appear in the Encyclopedia of Integer Sequences.

Example 1.1. (1) Let $M_n = 2^n - 1, n \geq 1$ denote the n-th term of the Mersenne sequence A000225. This sequence is of interest in number theory because it is conjectured to contain infinitely many prime terms, and in dynamics because it counts the periodic points in the simplest expanding dynamical system. Let

$$\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

denote the complex unit circle. Then the map $T : \mathbb{S}^1 \to \mathbb{S}^1$, $T(z) = z^2$, has $|\,\mathrm{Per}_n(T)| = M_n$.

(2) Let L_n denote the n-th term of the Lucas sequence A000204. Let X denote the set of all doubly-infinite strings of 0's and 1's in which every 0 is followed by a 1, and let $T : X \to X$ be the left shift defined by $(Tx)_n = x_{n+1}$. Then $|\operatorname{Per}_n(T)| = L_n$.

(3) The Lehmer-Pierce sequences (generalizing the Mersenne sequence; see [4]) also arise in counting periodic points. Let $f(x)$ denote a monic, integral polynomial with degree $d \geq 1$ and roots $\alpha_1, \dots, \alpha_d$. Define

$$\Delta_n(f) = \prod_i |\alpha_i^n - 1|,$$

which is non-zero for $n \geq 1$ under the assumption that no α_i is a root of unity. When $f(x) = x - 2$, we obtain $\Delta_n(f) = M_n$. Sequences of the form $(\Delta_n(f))$ were studied by Pierce and Lehmer with a view to understanding the special form of their factors, in the hope of using them to produce large primes. One such, is sequence A001945 corresponding to $f(x) = x^3 - x - 1$. In dynamics they arise as sequences of periodic points for toral endomorphisms: Let $X = \mathbb{T}^d$ denote the d-dimensional additive torus. The companion matrix A_f of f acts on X by multiplication mod 1, $T(x) = A_f x \bmod 1$. It requires a little thought to check that $|\operatorname{Per}_n(T)| = \Delta_n(f)$ under the same *ergodicity* condition that no α_i is a root of unity (see [4]). Notice that the Lehmer-Pierce sequences are the absolute values of integer sequences which could have mixed signs.

The next two examples illuminate the same issue of signed sequences whose absolute value counts periodic points.

(4) The Jacobsthal-Lucas sequence A014551 $R_n = |(-2)^n - 1|$ counts points of period n for the map $z \mapsto z^{-2}$ on $\mathbb{S}^1$.

(5) The sequence $S_n = |2^n + (-3)^n|$ counts periodic points in a certain continuous automorphism of a 1-dimensional solenoid, see [3] or [10].

(6) For $a \geq 1$, the shift map T on $\{0, 1, \dots, a-1\}^{\mathbb{Z}}$ has $|\operatorname{Per}_n(T)| = a^n$.

(7) If B denotes a square matrix with non-negative integral entries then $(\operatorname{trace}(B^n))$ is a realizable sequence. To see this, let G_B be the labelled graph with adjacency matrix B and T_B the edge-shift on the set of labels of infinite paths on G_B. Then the number of points of period n for this system is $\operatorname{trace}(B^n)$ (see [11] for the details).

The sequences above are realizable by continuous maps of compact spaces; it turns out that any realizable sequence is in fact realizable by such a map.

It is natural to ask what is required of a sequence in order that it be realizable. For example, could the Fibonacci sequence A000045, the more illustrious cousin of the Lucas sequence, be realized in this way? The answer is no, and a simple proof will follow in Section 3. In fact a sequence of non-negative integers satisfying the Fibonacci recurrence is realizable if and only if it is a non-negative integer multiple of the Lucas sequence (see [13], [14], [15] and Theorem 2.1 below). However, we will see in Theorem 2.6 that in a precise sense, the Fibonacci sequence is semi-realizable.

2. Statements of Results

If $u = (u_n)$ is any sequence of integers, then it is reasonable to ask if the sequence $|u| = (|u_n|)$ of absolute values is realizable. For example, the sequence $(1, -3, 4, -7, \dots)$ is a signed linear recurrence sequence whose absolute values are realizable. A signed sequence u will also be called realizable if $|u|$ is realizable.

Theorem 2.1 recasts [14, Theorem 2.5], concerning realizable binary linear recurrence sequences, in a form that generalizes. The definitions are standard but they will be recalled later. Recall that the $\mathbb{C}$-space of all solutions of a binary recurrence relation has dimension 2. The *realizable subspace* is the subspace spanned by the realizable solutions. Thus, for the Fibonacci recurrence, the realizable subspace has dimension 1 and is spanned by the Lucas sequence.

Theorem 2.1. *Let Δ denote the discriminant of the characteristic polynomial associated to a non-degenerate binary recurrence relation. Then the realizable subspace has*

(1) *dimension 0 if $\Delta < 0$,*
(2) *dimension 1 if $\Delta = 0$ or $\Delta > 0$ and non-square,*
(3) *dimension 2 if $\Delta > 0$ is a square.*

Example 2.2. (cf. [14, Example 2.6(2)]) As an example of the third condition, consider the recurrence relation

$$u_{n+2} = 3u_{n+1} - 2u_n, \tag{1}$$

which is satisfied by the Mersenne sequence. The recurrence sequences $a2^n + b$ with $a, b \in \mathbb{N}$ all satisfy (1) and are realizable — see Corollary 3.2.

Theorem 2.1 is proved in [14] using essentially quadratic methods — but it surely has a generalization to higher degree, characterizing the realizable subspace in terms of the factorization of the characteristic polynomial of the recurrence. The second theorem is a partial result in that direction, giving a restriction on the dimension of the realizable subspace under the assumption that the characteristic polynomial has a dominant root.

Theorem 2.3. *Let f denote the characteristic polynomial of a non-degenerate linear recurrence sequence with integer coefficients. If f is separable, with ℓ irreducible factors and a dominant root then the dimension of the realizable subspace cannot exceed ℓ. If $f(0) \neq 0$ then equality holds if either the dominant root is not less than the sum of the absolute values of the other roots or the dominant root is strictly greater than the sum of the absolute values of its conjugates.*

It is not clear if there is an exact result but the deep result of Kim, Ormes and Roush [8] on the Spectral Conjecture of Boyle and Handelman [1] gives a checkable criterion for a given linear recurrence sequence to be realized *by an irreducible subshift of finite type.*

Example 2.4. Consider the sequences which satisfy the Tribonacci relation

$$u_{n+3} = u_{n+2} + u_{n+1} + u_n. \tag{2}$$

The sequence A001644 satisfies (2) and is realizable, since it is the sequence $\left(\mathrm{trace}(A_f^n)\right)$, where A_f is the companion matrix to $f(x) = x^3 - x^2 - x - 1$. Theorem 2.3 says that any realizable sequence which satisfies (2) is a multiple of this one.

Example 2.5. Suppose g denotes a polynomial with $\ell - 1$ distinct irreducible factors (possibly repeated). For an integer K, consider the linear recurrence relation with characteristic polynomial

$$f(x) = (x - K)g(x).$$

For all sufficiently large K, f has ℓ distinct irreducible factors and the realizable subspace has dimension ℓ.

The third theorem consists of a triple of examples. Given a sequence u and a prime p, write $[u_n]_p$ for the p-part of u_n. Notice that $[u]_p$ is always non-negative. A sequence u is *locally realizable at* p if $[u]_p$ is itself realizable, and is *everywhere locally realizable* if it is locally realizable at p for all primes p. If a sequence is everywhere locally realizable and non-negative then it is realizable by Corollary 3.2 below. Moss has shown [12] that the converse is true for any endomorphism of a locally nilpotent group.

Consider the Bernoulli numbers B, defined by the relation

$$\frac{t}{e^t-1}=\sum_{n=0}^{\infty}B_n\frac{t^n}{n!};$$

$B_n\in\mathbb{Q}$ for all n, and $B_n=0$ for all odd $n>1$.

Theorem 2.6. *Any Lehmer–Pierce sequence is everywhere locally realizable, and hence realizable. The Fibonacci sequence is locally realizable at primes $\equiv\pm1$ modulo 5. Let b_n denote the denominator of B_{2n} for $n\geq1$. Then $b=(b_n)$ is everywhere locally realizable, and hence realizable.*

The sequence b is A002445, a much-studied sequence. The maps in Theorem 2.6 are endomorphisms of groups. Theorem 2.6 and Lemma 3.1 suggest a dynamical interpretation of composite versions of the classical Kummer congruences; see Section 4 below.

3. Combinatorics of periodic points

As pointed out in [14, Example 2.2(1)], the Fibonacci sequence is not realizable. No map can have 1 fixed point and 2 points of period 3 — the image under the map of the non-fixed point of period 3 would have to be a distinct non-fixed point of period 3, and there are no others. More generally, for any prime p, the number of non-fixed points of period p must be divisible by p because their orbits occur in cycles of length p. From this kind of reasoning, the following characterization emerges (see [14, Lemma 2.1]).

Lemma 3.1. *Let u be a sequence of non-negative integers, and let $u*\mu$ denote the Dirichlet convolution of u with the Möbius function μ. Then u is realizable if and only if $(u*\mu)_n\equiv0$ mod n and $(u*\mu)_n\geq0$ for all $n\geq1$.*

Corollary 3.2. *The sum and product of two realizable sequences are both realizable.*

Proof. This may be seen either using elementary properties of the Dirichlet convolution or using the realizing maps: if u and v are realizable, then the Cartesian product of the realizing maps realizes (u_nv_n), while the disjoint union realizes (u_n+v_n). □

Notice that if $n=p^r$, for a prime p and $r>0$ an integer, Lemma 3.1 requires that

$$u_{p^r}\equiv u_{p^{r-1}}\mod p^r \tag{3}$$

for any realizable sequence u.

Corollary 3.3. *Let a denote a positive integer and let p and r be as above. Then*

$$a^{p^r}\equiv a^{p^{r-1}}\mod p^r.$$

Proof. This is the statement of the Euler-Fermat Theorem; a dynamical proof applies (3) to Example 1.1(6). □

This kind of observation — that periodic points in full shifts give simple proofs of many elementary congruences — is folklore; indeed the paper [2] gives a rather complicated proof of Euler–Fermat using a dynamical system.

Lemma 3.1 does more with no additional effort. The following is a generalization of the Euler-Fermat Theorem for integral matrices which will be used in the proof of Theorem 2.1.

Corollary 3.4. *Let A denote a square matrix with integer entries and let p and r be as above. Then*

$$\mathrm{trace}(A^{p^r}) \equiv \mathrm{trace}(A^{p^{r-1}}) \mod p^r.$$

Proof. It is sufficient to assume A has non-negative entries, since any matrix has such a representative mod p^r. The result follows at once from Example 1.1(7). □

We now state the consequences of Lemma 3.1 in their most general form for matrix traces.

Corollary 3.5. *Let A denote a square matrix with integer entries and let A_n denote the sequence* $\mathrm{trace}(A^n)$. *Then for all $n \geq 1$*

$$\sum_{d|n} A_d \mu(n/d) \equiv 0 \mod n.$$

4. Proofs

Before the proof of Theorem 2.1, we begin with some notation (for a lively account of the general properties of linear recurrence sequences, see [16]). Let u be a binary recurrence sequence. This means that u_1 and u_2 are given as initial values, with all subsequent terms defined by a recurrence relation

$$u_{n+2} = Bu_{n+1} - Cu_n. \tag{4}$$

The polynomial $f(x) = x^2 - Bx + C$ is the *characteristic polynomial* of the recurrence relation. Write

$$A_f = \begin{pmatrix} 0 & 1 \\ -C & B \end{pmatrix}$$

for the companion matrix of f. The zeros α_1 and α_2 of f, are the *characteristic roots* of the recurrence relation. The sequence is non-degenerate if α_1/α_2 is not a root of unity. The *discriminant* of the recurrence relation is $\Delta = B^2 - 4C$. The general solution of the recurrence relation is $u_n = (\gamma_1 + \gamma_2 n)\alpha_1^n$ if $\Delta = 0$, and $u_n = \gamma_1\alpha_1^n + \gamma_2\alpha_2^n$ if $\Delta \neq 0$.

Proof of Theorem 2.1. Assume first that $\Delta = 0$, and let p denote any prime which does not divide α_1 or γ_2. Then the congruence (3) is violated at $n = p$ unless $\gamma_2 = 0$. In that case, $|\gamma_1\alpha_1^n|$ is realizable and the space this generates is 1-dimensional.

If $\Delta > 0$ is a square, then the roots are rationals and, plainly, must be integers. We claim that for any integers γ_1 and γ_2, the sequence $|\gamma_1\alpha_1^n + \gamma_2\alpha_2^n|$ is realizable. In fact (up to multiplying and adding full shifts) this sequence counts the periodic points for an automorphism on a one-dimensional solenoid, see [4] or [10].

The two cases where $\Delta \neq 0$ is not a square are similar. Write $\alpha = s + t\sqrt{\Delta}$, with $s, t \in \mathbb{Q}$, for one of the roots of f and let $K = \mathbb{Q}(\alpha)$ denote the quadratic number field generated by α. Write $\mathrm{T}_{K|\mathbb{Q}} : K \to \mathbb{Q}$ for the usual field trace. The general integral solution to the recurrence is $u_n = \mathrm{T}_{K|\mathbb{Q}}((a + b\sqrt{\Delta})\alpha^n)$, where a and b are both integers or both half-odd integers. Write $v_n = \mathrm{T}_{K|\mathbb{Q}}(a\alpha^n)$ and $w_n = \mathrm{T}_{K|\mathbb{Q}}(b\sqrt{\Delta}\alpha^n)$. Now $v_n = a\,\mathrm{trace}(A_f^n)$, where A_f denotes the companion matrix of f. Hence it satisfies $v_p \equiv v_1 \bmod p$ for all primes p by Corollary 3.4.

Let p denote any inert prime for K. The residue field is isomorphic to the field $\mathbb{F}_{p^2}$. Moreover, the non-trivial field isomorphism restricts to the Frobenius at the finite field level. Reducing mod p gives the congruence

$$\sqrt{\Delta}\alpha^p - \sqrt{\Delta}\alpha \equiv \sqrt{\Delta}\alpha - \sqrt{\Delta}\alpha^p \mod p.$$

Thus $w_p \equiv -w_1 \bmod p$ for all inert primes p. On the other hand, $v_p \equiv v_1 \bmod p$ for all inert primes p.

If $|u_n|$ is realizable then $|u_p| \equiv |u_1| \bmod p$ by (3). If $u_p \equiv -u_1 \bmod p$ for infinitely many primes p then $v_p + w_p \equiv v_1 - w_1 \equiv -v_1 - w_1 \bmod p$. We deduce that $p|v_1$ for infinitely primes and hence $v_1 = 2as = 0$. We cannot have $s = 0$ by the non-degeneracy, so $a = 0$. If $u_p \equiv u_1 \bmod p$ then, by a similar argument, we deduce that $bt = 0$. We cannot have $t = 0$ again, by the non-degeneracy so $b = 0$. This proves that when $\Delta \neq 0$ is not a square, the realizable subspace must have rank less than 2.

Suppose firstly that $\Delta > 0$. We will prove that the rank is precisely 1. In this case, there is a dominant root. If this root is positive then all the terms of u_n are positive. If the dominant term is negative then the sequence of absolute values agrees with the sequence obtained by replacing α by $-\alpha$ and the dominant root is now positive. In the recurrence relation (4) $C = \mathrm{N}_{K|\mathbb{Q}}(\alpha)$, the field norm, and $B = \mathrm{T}_{K|\mathbb{Q}}(\alpha)$. We are assuming $B > 0$. If $C < 0$ then the sequence $u_n = \mathrm{trace}(A_f^n)$ is realizable using Example 1.1(7), because the matrix A_f has non-negative entries. If $C > 0$ the matrix A_f may be conjugated to a matrix with non-negative entries (this leaves the sequence of traces invariant). To see this, let E denote the matrix

$$E = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}.$$

Then

$$E^{-1}A_fE = \begin{pmatrix} k & 1 \\ Bk - k^2 - C & B - k \end{pmatrix}.$$

If B is even, take $k = B/2$. Then the lower entries in $E^{-1}A_fE$ are $(B^2 - 4C)/4 = \Delta/4 > 0$ and $B/2 > 0$. If B is odd, take $k = (B+1)/2$. Then the lower entries are $(B^2 - 1 - 4C)/4 = (\Delta - 1)/4 \geq 0$ and $(B - 1)/2 \geq 0$. In both cases we have conjugated A_f to a matrix with non-negative entries.

Finally, we must show that when $\Delta < 0$, both sequences v_n and w_n are not realizable in absolute value. Assume $a \neq 0$, and then note that $v_1 = 2as \neq 0$ by the non-degeneracy assumption. For all primes p we have $v_p \equiv v_1$ by the remark above. Since the roots α_1 and α_2 are complex conjugates, $|\alpha_1| = |\alpha_2|$. Let $\beta = \frac{1}{2\pi}\arg(\alpha_1/\alpha_2)$; β is irrational by the non-degeneracy assumption. The sequence of fractional parts of $p\beta$, with p running through the primes, is dense in $(0, 1)$ (this was proved by Vinogradov [19]; see [18] for a modern treatment). It follows that there are infinitely many primes p for which $v_pv_1 < 0$. Therefore, if $|v_n|$ is realizable then it satisfies $v_p \equiv v_1 \bmod p$ and $-v_p \equiv v_1 \bmod p$ for infinitely many primes. We deduce that $v_1 = 0$ which is a contradiction. With w_n we may argue in a similar way to obtain a contradiction to $w_1 \neq 0$. If $|w_n|$ is realizable then Lemma 3.1 says $|w_{p^2}| \equiv |w_p| \equiv |w_1|$ for all primes p. Arguing as before, $w_{p^2} \equiv w_1$ for both split and inert primes. However, the sequence $\{p^2\beta\}$, p running over the primes, is dense in $(0,1)$. (Again, this is due to Vinogradov in [19] or see [5] for a modern treatment. The general case of $\{F(p)\}$, where F is a polynomial can be found in [7].) We deduce that $w_{p^2}w_1 < 0$ for infinitely many primes. This means $w_{p^2} \equiv w_1 \bmod p$ and $w_{p^2} \equiv -w_1 \bmod p$ infinitely often. This forces $w_1 = 0$ — a contradiction.

Proof of Theorem 2.3. Let d denote the degree of f. In the first place we assume $\ell = 1$, thus f is irreducible. The irreducibility of f implies that the rational solutions of the recurrence are given by $u_n = \mathrm{T}_{K|\mathbb{Q}}(\gamma\alpha^n)$, where $K = \mathbb{Q}(\alpha)$, and $\gamma \in K$. We write $\gamma_i, \alpha_i, i = 1, \dots, d$ for the algebraic conjugates of γ and α. The dominant root hypothesis says, after re-labelling, $|\alpha_1| > |\alpha_i|$ for $i = 2, \dots, d$. We will show that if u is realizable then $\gamma \in \mathbb{Q}$.

Let p denote any inert prime. If p is sufficiently large, the dominant root hypothesis guarantees that $u_p, \dots, u_{p^d}$ will all have the same sign. Using Lemma 3.1 several times, we deduce that

$$u_p \equiv u_{p^2} \equiv \cdots \equiv u_{p^d} \equiv \pm u_1 \mod p.$$

Therefore $u_p + \cdots + u_{p^d} \equiv \pm d u_1 \bmod p$, the sign depending upon the sign of u_1. However,

$$u_p + \cdots + u_{p^d} \equiv \mathrm{T}_{K|\mathbb{Q}}(\gamma)\,\mathrm{T}_{K|\mathbb{Q}}(\alpha) \mod p.$$

We deduce a fundamental congruence

$$\mathrm{T}_{K|\mathbb{Q}}(\gamma)\,\mathrm{T}_{K|\mathbb{Q}}(\alpha) \equiv \pm d\,\mathrm{T}_{K|\mathbb{Q}}(\gamma\alpha) \mod p.$$

Since this holds for infinitely many primes p, the congruence is actually an equality,

$$\mathrm{T}_{K|\mathbb{Q}}(\gamma)\,\mathrm{T}_{K|\mathbb{Q}}(\alpha) = \pm d\,\mathrm{T}_{K|\mathbb{Q}}(\gamma\alpha). \tag{5}$$

The next step comes with the observation that if u_n is realizable then u_{rn} is realizable for every $r \geq 1$. Thus equation (5) now reads

$$\mathrm{T}_{K|\mathbb{Q}}(\gamma)\,\mathrm{T}_{K|\mathbb{Q}}(\alpha^r) = \pm d\,\mathrm{T}_{K|\mathbb{Q}}(\gamma\alpha^r). \tag{6}$$

Dividing equation (6) by α_1^r and letting $r \to \infty$ we obtain the equation

$$\mathrm{T}_{K|\mathbb{Q}}(\gamma) = \pm d\gamma_1.$$

This means that one conjugate of γ is rational and hence γ is rational.

The end of the proof in the case $\ell = 1$ can be re-worked in a way that makes it more amenable to generalization. The trace is a $\mathbb{Q}$-linear map on K so its kernel has rank $d-1$. Thus every element γ of K can be written $q + \gamma_0$ where $q \in \mathbb{Q}$ and $\mathrm{T}_{K|\mathbb{Q}}(\gamma_0) = 0$. Noting that $\mathrm{T}_{K|\mathbb{Q}}(q) = dq$ and cancelling d, this simply means equation (6) can be written

$$u_r = \pm q\,\mathrm{T}_{K|\mathbb{Q}}(\alpha^r),$$

for all $r \geq 1$ confirming that the realizable subspace has rank ≤ 1.

The general case is similar. Each of the irreducible factors of f generates a number field $K_j, j = 1, \dots, \ell$ of degree $d_j = [K_j : \mathbb{Q}]$. The solutions of the recurrence look like

$$u_n = \sum_{j=1}^{\ell} \mathrm{T}_{K_j|\mathbb{Q}}(\gamma_j \alpha_j^n),$$

where each $\gamma_j \in K_j$. Let L denote the compositum of the K_j. Using the inert primes of L and noting that each is inert in each K_j, we deduce an equation

$$\sum_{j=1}^{\ell} \frac{d}{d_j} \mathrm{T}_{K_j|\mathbb{Q}}(\gamma_j)\, \mathrm{T}_{K_j|\mathbb{Q}}(\alpha_j) = \pm d \sum_{j=1}^{\ell} \mathrm{T}_{K_j|\mathbb{Q}}(\gamma_j \alpha_j). \tag{7}$$

As before, replace α_j by α_j^r, and cancel d so that

$$u_r = \pm \sum_{j=1}^{\ell} \frac{1}{d_j} \mathrm{T}_{K_j|\mathbb{Q}}(\gamma_j)\, \mathrm{T}_{K_j|\mathbb{Q}}(\alpha_j^r)$$

Each γ_j can be written $\gamma_j = q_j + \gamma_{0j}$, where $\mathrm{T}_{K_j|\mathbb{Q}}(\gamma_{0j}) = 0$. Noting that $\mathrm{T}_{K_j|\mathbb{Q}}(q_j) = d_j q_j$ we deduce that

$$u_r = \pm \sum_{j=1}^{\ell} q_j\, \mathrm{T}_{K_j|\mathbb{Q}}(\alpha_j^r)$$

which proves that the realizable subspace has rank $\leq \ell$.

Finally, show that equality holds in the two cases stated. Write $u_n^{(j)} = \mathrm{T}_{K_j|\mathbb{Q}}(\alpha_j^n)$, which is not identically zero because no $\alpha_j = 0$. Each sequence $u_n^{(j)}$ satisfies the congruence part of Lemma 3.1 and hence any $\mathbb{Z}$-linear combination also satisfies the congruence. This is because $u_n^{(j)}$ is identical to trace$(A_{f_j}^n)$, where A_{f_j} denotes the companion matrix for f_j - hence we can invoke Corollary 3.5. To obtain l linearly independent realizable sequences, suppose α_1 is the dominant root and take $u_n^{(1)}$ together with $u_n^{(1)} + u_n^{(j)}$ for $j = 2, \dots, l$. The non-negativity part of Lemma 3.1 follows from the condition on the dominant root. For the second case, a similar argument shows that for sufficiently large $M > 0$, the independent sequences $u_n^{(1)}$ and $Mu_n^{(1)} + u_n^{(j)}$ are realizable.

Proof of Theorem 2.6. It is sufficient to construct local maps $T_p : X_p \to X_p$ for each prime p. Then Corollary 3.2 guarantees a global realization by defining

$$T = \prod_p T_p \text{ on } X = \prod_p X_p.$$

If the maps T_p are group endomorphisms then the map T is a group endomorphism.

As motivation, consider the Mersenne sequence. For each prime p, let $\mathbb{U}_p \subset \mathbb{S}^1$ denote the group of all pth power roots of unity. Define the local endomorphism $S_p : x \mapsto x^2$ on $\mathbb{U}_p$. Then $|\operatorname{Per}_n(S_p)| = [2^n - 1]_p$ so S_p gives a local realization of the Mersenne sequence. Using the same method of proof, we can easily verify the claim about the Fibonacci sequence. Let F_n denote the n-th term and let X denote the group of all p-th power roots of 1. This is naturally a $\mathbb{Z}_p$-module. Let u denote the golden-mean, thought of as lying in $\mathbb{Z}_p$ by the congruence property on p. Then the map $x \mapsto x^{-u^2}$ has precisely $[F_n]_p$ points of period p.

An alternative proof in the Mersenne case uses the S-integer dynamical systems from [3]: for each prime p, define T_p to be the automorphism dual to $x \mapsto 2x$ on $\mathbb{Z}_{(p)}$ (the localization at p). Then by [3],

$$|\operatorname{Per}_n(T_p)| = \prod_{q \leq \infty; q \neq p} |2^n - 1|_q = [2^n - 1]_p$$

by the product formula. This approach gives a convenient proof for Lehmer-Pierce sequences in general. We may assume that the polynomial f is irreducible; let $K=\mathbb{Q}(\xi)$ for some zero of f. Then for each prime p, let S comprise all places of K expect those lying above p, and let T_p be the S-integer map dual to $x\mapsto\xi x$ on the ring of S-integers in K. Then by the product formula

$$|\operatorname{Per}_n(T_p)| = \Big(\prod_{v|p} |\xi^n-1|_v\Big)^{-1} = [\Delta_n(f)]_p$$

as required.

For the Bernoulli denominators, define $X_p=\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$. For $p=2$ define T_p to be the identity. For $p>2$, let g_p denote an element of (multiplicative) order $(p-1)/2$. Define $T_p : X_p\to X_p$ to be the endomorphism $T_p(x)=g_px \bmod p$. Plainly $|\operatorname{Per}_n(T_p)|=p$ if and only if $p-1|2n$; for all other n, $|\operatorname{Per}_n(T_p)|=1$. The Clausen von Staudt Theorem ([6], [9]) states that

$$B_{2n}+\sum\frac{1}{p}\in\mathbb{Z},$$

where the sum ranges over primes p for which $p-1|2n$. Thus $|\operatorname{Per}_n(T_p)|=\max\{1,|B_{2n}|_p\}$ and this shows the local realizability of the Bernoulli denominators.

5. Epilogue

A result similar to the one in Theorem 2.6 for the Fibonacci sequence can be proved for any binary linear recurrence sequence, using the primes which split in the corresponding quadratic field.

Using the same ideas as in the proof of Theorem 2.6 one can prove that the sequence A006953, the denominators of $B_{2n}/2n$, is everywhere locally realizable. A much more subtle result, due to Moss [12], is that the sequence A001067, the numerators of $B_{2n}/2n$, is a realizable sequence that is not locally realizable exactly at the irregular primes A000928. Taking these remarks together with $n=p^r$ in Lemma 3.1, suggests a dynamical interpretation of the Kummer congruences. These are stated now, for a proof see [9].

Theorem 5.1. *If p denotes a prime and $p-1$ does not divide n then $n\equiv n' \bmod (p-1)p^r$ implies*

$$(1-p^{n-1})\frac{B_n}{n}\equiv(1-p^{n'-1})\frac{B_{n'}}{n'} \mod p^{r+1}.$$

Finally, experimental evidence suggests the sequence A006863, the denominators of $B_{2n}/4n$ forms a realizable sequence that is not locally realizable at the primes $2,3,5,7,11,13$ but seems to be locally realizable for all large primes.

6. Acknowledgments

The second author acknowledges the support of EPSRC visiting fellowship award GR/R70200. The third author acknowledges the support of EPSRC postgraduate award 96001638.

References

[1] M. Boyle and D. Handelman. The spectra of nonnegative matrices via symbolic dynamics. *Ann. of Math.* (2), **133**, 249–316 (1991); MR 92d:58057.

[2] Humberton Carillo Calvet and José Ramón Guzmán. A dynamical systems proof of Euler's generalization of the little theorem of Fermat. *Aportaciones Mat. Comun.* , **25**, 199–202, 1999. XXXI National Congress of the Mexican Mathematical Society; MR 2001i:11005.

[3] Vijay Chothi, Graham Everest and Thomas Ward. S-integer dynamical systems: periodic points. *J. Reine Angew. Math.*, **489**, 99-132 (1997); MR 99b:11089.

[4] Graham Everest and Thomas Ward. *Heights of polynomials and entropy in algebraic dynamics*, Springer-Verlag London Ltd., London, 1999; MR 2000e:11087.

[5] A. Ghosh. The distribution of αp^2 modulo one *Proc. London Math. Soc.* (3) **42**, 225-269 (1981); MR 82j:10067.

[6] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* The Clarendon Press Oxford University Press, New York, fifth edition, 1979; MR 81i:10002.

[7] G. Harman. Trigonometric sums over primes I *Mathematika*, **28**, 249-254 (1981); MR 83j:10045.

[8] Ki Hang Kim, Nicholas S. Ormes and Fred W. Roush. The spectra of nonnegative integer matrices via formal power series. *J. Amer. Math. Soc.*, **13**, 773–806 (2000); MR 2001g:15013.

[9] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* Springer-Verlag, New York, 1977; MR 57#5964.

[10] D. A. Lind and T. Ward. Automorphisms of solenoids and p-adic entropy. *Ergodic Theory Dynamical Systems*, **8**(3), 411–419, 1988; MR 90a:28031.

[11] Douglas Lind and Brian Marcus. *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, Cambridge, 1995; MR 97a:58050.

[12] Patrick Moss *The Arithmetic of Realizable Sequences* PhD Thesis, University of East Anglia, 2003.

[13] Y. Puri. *Arithmetic of Numbers of Periodic Points*. PhD. thesis, Univ. East Anglia, (2001), www.mth.uea.ac.uk/admissions/graduate/phds.html

[14] Y. Puri and T. Ward. Arithmetic and growth of periodic orbits *Journal of Integer Sequences*, **4**, 01.2.1 (2001); MR 2002i:11026.

[15] Y. Puri and T. Ward. A dynamical property unique to the Lucas sequence *Fibonnaci Quarterly*, **39**(5), 398-402 (2001).

[16] A. J. van der Poorten. Some facts that should be better known, especially about rational functions. *Number theory and applications (Banff, AB, 1988)*, 497–528 (1989). Kluwer Acad. Publ., Dordrecht; MR 92k:11011.

[17] N. J. A. Sloane *The On-Line Encyclopedia of Integer Sequences*; MR 95b:05001.

[18] R. Vaughan. On the distribution of $p\alpha$ modulo one *Mathematika*, **24**, 135-141 (1977); MR 57#12423.

[19] I. M. Vinogradov. A new estimation of a trigonometric sum involving primes *Bull. Acad. Sc. URSS Ser. Math.*, **2**, 1–13 (1938).

2000 *Mathematics Subject Classification*: 11G07, 37B40 .
Keywords: periodic points, dynamical systems, linear recurrences, Bernoulli numbers, realizable sequences

---

(Concerned with sequences A000225, A000204, A001945, A000045, A001644, A002445, A006953, A001067, A000928.)

Received October 18, 2002; revised version received November 12, 2002. Published in *Journal of Integer Sequences* November 13, 2002.

Return to Journal of Integer Sequences home page.