Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Computing the Cycle Structure of Finite Linear Systems ⋆

Eva Zerz * **and Hermann Giese** *

* *Lehrstuhl D für Mathematik, RWTH Aachen University, 52062 Aachen, Germany (e-mail: eva.zerz@math.rwth-aachen.de)*

Abstract: Consider a linear difference equation with constant coefficients in the ring of integers modulo m. If the leading coefficient and the constant term are both units, then all trajectories are (purely) periodic. Moreover, the finite state set can be decomposed into disjoint cycles of various lengths. The following problems will be addressed: computing the cycle partition and determining the period w.r.t. a specific initial state. The latter question can often be reduced to calculating the order of an invertible matrix. If the prime factorization of m is known, then it suffices to consider prime powers, by the Chinese remainder theorem. For primes, an efficient algorithm due to Leedham-Green may be used, which is available in group-theoretic computer algebra systems such as Magma or GAP. This approach will be extended to prime powers. Finally, we will discuss how to relax the assumptions guaranteeing periodicity.

Keywords: Linear systems, algebraic systems theory, cycle length, periodicity, finite rings.

1. INTRODUCTION

The Fibonacci equation

$$y(t+2) = y(t+1) + y(t),$$

where t is a nonnegative integer, is usually considered in characteristic zero. Choosing $y(0) = 0$ and $y(1) = 1$ as initial values, one obtains the famous sequence

$$y = (0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots).$$

In positive characteristic however, the sequence becomes (purely) periodic, that is, it returns to its initial values and thus runs into a loop.

Example: In characteristic 2, we obtain

$$y = (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, \ldots)$$

and the length of the period is 3. In characteristic 3,

$$y = (0, 1, 1, 2, 0, 2, 2, 1, 0, 1, \ldots)$$

and the length of the period is 8. In characteristic 4,

$$y = (0, 1, 1, 2, 3, 1, 0, 1, \ldots)$$

and the length of the period is 6.

The sequence of period lengths is known as the Pisano sequence

$$\pi = (1, 3, 8, 6, 20, 24, 16, 12, 24, 60, \ldots).$$

Its properties have been studied by several authors, see e.g. Wall (1960), and it is popular in recreational mathematics. However, it is also related to "serious" mathematical problems. A Wall-Sun-Sun prime is a prime p such that $\pi(p) = \pi(p^2)$. It has been checked experimentally that such a prime (if it exists) must be greater than 10^{14}. On the other hand, we have $\pi(n) = \pi(n^2)$ for $n \in \{6, 12\}$. A proof of the nonexistence of Wall-Sun-Sun primes would yield an alternative proof of the first case of Fermat's last theorem, see Sun and Sun (1992).

⋆ This work was supported by DFG-SFB/TRR 195.

In the present paper, we will study general monic difference equations of order n, that is,

$$y(t+n) + a_{n-1}y(t+n-1) + \ldots + a_1 y(t+1) + a_0 y(t) = 0$$

with $a_i \in \mathbb{Z}$. The case where all solutions modulo m are (purely) periodic will be characterized by the condition $\gcd(a_0, m) = 1$. We will then turn to computing the period of the solution evolving from specific initial values $y(0), \ldots, y(n-1)$. Next, we study when this period coincides with the (group-theoretic) order of the companion matrix A of the polynomial $s^n + \sum_{i=0}^{n-1} a_i s^i$, if A is considered as an element of $\mathbb{Z}_m^{n\times n}$, where $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$. Note that $A \in \mathbb{Z}_m^{n\times n}$ is invertible if and only if $\gcd(\det(A), m) = 1$. Due to the companion matrix structure, $\det(A) \in \{\pm a_0\}$. The state set $X := \mathbb{Z}_m^n$ can be decomposed into disjoint cycles and we will show how to compute this partition. Finally, the assumption of monicity ($a_n = 1$) will be relaxed.

2. MONIC EQUATIONS

Let $\mathbb{Z}$ denote the ring of integers, and let $\mathbb{N}$ denote the set of nonnegative integers. Let n be a positive integer, and let $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ be given. Consider the linear difference equation

$$y(t+n)+a_{n-1}y(t+n-1)+\ldots+a_1 y(t+1)+a_0 y(t) = 0, \quad (1)$$

where $t \in \mathbb{N}$. Let $y_0, \ldots, y_{n-1} \in \mathbb{Z}$ be given. Together with the initial condition

$$y(0) = y_0, \quad \ldots, \quad y(n-1) = y_{n-1} \quad (2)$$

the initial value problem (1), (2) has a unique solution $(y(t))_{t\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$. For each integer $m > 1$, one obtains an induced sequence $(y(t))_{t\in\mathbb{N}} \in \mathbb{Z}_m^{\mathbb{N}}$, where $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ denotes the ring of integers modulo m. In the following, we will make no notational distinction between an integer and its residue class modulo m, or between a polynomial in $\mathbb{Z}[s]$ and its residue class in $\mathbb{Z}_m[s]$.

Copyright lies with the authors

Theorem 1. For each $m > 0$, there exist integers $k \geq 0$ and $p > 0$ such that

$$y(t+p) = y(t) \quad \text{for all } t \geq k.$$

If $\gcd(a_0, m) = 1$, then k can be taken to be zero.

Proof: Define

$$x(t) := [y(t), \ldots, y(t+n-1)]^T.$$

Then $x(t+1) = Ax(t)$, where

$$A = \begin{bmatrix} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ -a_0 & -a_1 & \ldots & -a_{n-1} \end{bmatrix}$$

is the companion matrix of the polynomial $\chi_A = s^n + \sum_{i=0}^{n-1} a_i s^i$. Since the ring $\mathbb{Z}_m$ is finite, the sequence y, and hence also x, can only take finitely many values. Thus there exists $k \geq 0$ and $p > 0$ such that $x(k+p) = x(k)$. This implies that $x(t+p) = x(t)$ for all $t \geq k$.

If $\gcd(a_0, m) = 1$, then a_0 is a unit in $\mathbb{Z}_m$. This implies that the polynomial indeterminate s is a unit in the finite ring $R := \mathbb{Z}_m[s]/\langle \chi_A \rangle$. Hence it has finite order, that is, there exists $p > 0$ such that $s^p = 1$ holds in R. This means that the polynomial $s^p - 1$ is a multiple of χ_A in $\mathbb{Z}_m[s]$ and thus $y(t+p) = y(t)$ holds for all $t \in \mathbb{N}$. □

Given m with $\gcd(a_0, m) = 1$, we will address the computation of the smallest number $p > 0$ such that

(1) $x(p) = x(0)$. Since this implies that $x(t+p) = x(t)$ for all $t \in \mathbb{N}$, this number will be called the *period* of x with respect to the initial value $x_0 := [y_0, \ldots, y_{n-1}]^T$. It is the smallest $p > 0$ with $A^p x_0 = x_0$ and will be denoted by $\pi_m(x_0)$.
(2) $A^p = I$. This p is the order of the invertible matrix $A \in \mathbb{Z}_m^{n \times n}$, denoted by $\mathrm{ord}_m(A)$.

We observe that $\pi_m(x_0)$ must be a divisor of $\mathrm{ord}_m(A)$. Moreover,

$$\mathrm{ord}_m(A) = \mathrm{lcm}\{\pi_m(x_0) \mid x_0 \in \mathbb{Z}_m^n\}.$$

By the Chinese remainder theorem, it suffices to consider the case where m is a prime power.

Example: Consider

$$y(t+3) = y(t+2) + y(t+1) + y(t), \quad y(0) = y(1) = y(2) = 1.$$

- Modulo 2, we obtain the constant sequence 1, and hence $\pi_2([1,1,1]^T) = 1$, but $\mathrm{ord}_2(A) = 4$. Indeed, we have

x_0^T	$\pi_2(x_0)$
$[0,0,0]$	1
$[0,0,1]$	4
$[0,1,0]$	2
$[0,1,1]$	4
$[1,0,0]$	4
$[1,0,1]$	2
$[1,1,0]$	4
$[1,1,1]$	1.

  Adopting the notation used by Deng (2015), the cycle structure is $X = \mathbb{Z}_2^3 = 2C_1 \cup C_2 \cup C_4$. This means that there are two fixed points (i.e., cycles of length one), one cycle of length two, and one cycle of length four, corresponding to a partition of the state set into cycles according to 8=1+1+2+4.
- Modulo 3, we obtain a sequence of period 13, that is, $\pi_3([1,1,1]^T) = 13$, and we also have $\mathrm{ord}_3(A) = 13$. Indeed, all $x_0 \neq 0$ yield $\pi_3(x_0) = 13$.
- Modulo 4, we obtain a sequence of period 4, that is, $\pi_4([1,1,1]^T) = 4$, but $\mathrm{ord}_4(A) = 8$.

Theorem 2. Given $x_0 = [y_0, \ldots, y_{n-1}]^T \in \mathbb{Z}^n$, compute $y_n, \ldots, y_{2n-2} \in \mathbb{Z}$ according to (1) and define the Hankel matrix

$$H = \begin{bmatrix} y_0 & y_1 & \cdots & y_{n-1} \\ y_1 & & & y_n \\ \vdots & & \iddots & \vdots \\ y_{n-1} & y_n & \cdots & y_{2n-2} \end{bmatrix} \in \mathbb{Z}^{n \times n}.$$

If $\gcd(\det(H), m) = 1$, then $\pi_m(x_0) = \mathrm{ord}_m(A)$. Since $x_0 = e_n = [0, \ldots, 0, 1]^T$ yields a matrix H with $\det(H) \in \{\pm 1\}$, we conclude that there always exists x_0 with $\pi_m(x_0) = \mathrm{ord}_m(A)$.

Proof: Suppose that $A^p x_0 = x_0$. Let H_{-i} denote the i-th column of H. Noting that $x_0 = H_{-1}$ and $AH_i = H_{-(i+1)}$, we may conclude that $A^p H = H$. By assumption, H is invertible as a matrix over $\mathbb{Z}_m$, and hence $A^p = I$ holds over $\mathbb{Z}_m$. □

The prime divisors of $\det(H)$ are called bad primes of the initial value problem (1),(2).

Example: For $y(t+3) = y(t+2) + y(t+1) + y(t)$ and $x_0 = [1,1,1]^T$, the only bad prime is 2. For odd m, we have $\pi_m(x_0) = \mathrm{ord}_m(A)$.

3. COMPUTING THE ORDER

We will now discuss how to compute $\mathrm{ord}_m(A)$ for a matrix $A \in \mathbb{Z}^{n \times n}$ that is invertible when considered as an element of $\mathbb{Z}_m^{n \times n}$. Note that we do not restrict to companion matrices. If the prime factorization of m is known, the problem can be reduced to the case where m is prime power, by the Chinese remainder theorem. For primes p, an efficient algorithm by Celler and Leedham-Green (1997) can be used to compute $\mathrm{ord}_p(A)$.

Theorem 3. Let $A \in \mathbb{Z}^{n \times n}$ and a prime p with $p \nmid \det(A)$ be given. Then A is invertible over $\mathbb{Z}_{p^k}$ for all $k \geq 1$. We have

$$\mathrm{ord}_{p^k}(A) \mid \mathrm{ord}_p(A) p^{k-1}.$$

Proof: Since $A^r = I$ implies that the order of A divides r, it suffices to show that

$$A^{\mathrm{ord}_p(A) p^{k-1}} \equiv I \pmod{p^k}.$$

Set $B := A^{\mathrm{ord}_p(A)}$. Then we have

$$B \equiv I \pmod{p}.$$

We need to prove that

$$B^{p^{k-1}} \equiv I \pmod{p^k}$$

for all $k \geq 1$. This will be done by induction on k. The statement is clearly true for $k = 1$. Let's assume that it holds for k. This means that

$$B^{p^{k-1}} = I + p^k C$$

for some matrix $C \in \mathbb{Z}^{n \times n}$. By the binomial theorem,

$$\begin{aligned} B^{p^k} &= (B^{p^{k-1}})^p \\ &= (I + p^k C)^p \\ &= I + \binom{p}{1} p^k C + \sum_{i=2}^{p} \binom{p}{i} p^{ki} C^i. \end{aligned}$$

Considering the right hand side modulo p^{k+1}, all terms vanish except for the identity matrix: In the second summand, this is due to the binomial coefficient, and for the sum over i, we use $ki \geq k+1$ (since $i \geq 2$). Thus

$$B^{p^k} \equiv I \pmod{p^{k+1}},$$

which completes the inductive step. □

Corollary 4. In the situation of the previous theorem, we have

$$\operatorname{ord}_p(A) \mid \operatorname{ord}_{p^2}(A) \mid \operatorname{ord}_{p^3}(A) \dots$$

and

$$\operatorname{ord}_{p^k}(A) = \operatorname{ord}_p(A) p^i \quad \text{for some} \quad 0 \leq i \leq k-1. \tag{3}$$

Proof: Since $A^r \equiv I \pmod{p^{l+1}}$ implies $A^r \equiv I \pmod{p^l}$, we have

$$\operatorname{ord}_{p^l}(A) \mid \operatorname{ord}_{p^{l+1}}(A)$$

for all $l \geq 1$. In particular, $\operatorname{ord}_p(A)$ is a divisor of $\operatorname{ord}_{p^k}(A)$ for all $k \geq 1$. Combining this with the statement of the theorem, we obtain (3). □

Theorem 5. Let $t \geq 1$ be such that $\operatorname{ord}_{p^t}(A) \neq \operatorname{ord}_{p^{t+1}}(A)$. If $t = 1$, assume additionally that p is odd. Then we have

$$\operatorname{ord}_{p^k}(A) = \operatorname{ord}_{p^t}(A) p^{k-t}$$

for all $k \geq t$.

Proof: Set $B := A^{\operatorname{ord}_{p^t}(A)}$. By assumption, we have

$$B \equiv I \pmod{p^t} \quad \text{and} \quad B \not\equiv I \pmod{p^{t+1}}.$$

Claim: For all $k \geq t$, we have

$$B^{p^{k-t}} \equiv I \pmod{p^k} \quad \text{and} \quad B^{p^{k-t}} \not\equiv I \pmod{p^{k+1}}.$$

We will prove this by induction on k. The claim is true for $k = t$. Let's assume that it is true for k. Then $B^{p^{k-t}} = I + p^k C$ with $p \nmid C$, that is, there exists i, j such that $p \nmid C_{ij}$. By the binomial theorem, this implies

$$\begin{aligned} B^{p^{k-t+1}} &= (I + p^k C)^p \\ &= I + \binom{p}{1} p^k C + \binom{p}{2} p^{2k} C^2 + \sum_{i=3}^{p} \binom{p}{i} p^{ki} C^i. \end{aligned}$$

Considering the right hand side modulo p^{k+1} shows that $B^{p^{k-t+1}} \equiv I \pmod{p^{k+1}}$. Considering the right hand side modulo p^{k+2}, all terms vanish in the sum over i, because $ki \geq k+2$ (since $i \geq 3$). The term containing C^2 vanishes if p is odd (because then $p \mid \binom{p}{2}$) or if $t \geq 2$, because then $k \geq 2$ and thus $2k \geq k+2$. Due to $p \nmid C$, the term containing C does not vanish. Therefore, we have $B^{p^{k-t+1}} \not\equiv I \pmod{p^{k+2}}$, which completes the inductive step.

Now let $k > t$. According to the claim, we have

$$B^{p^{k-t}} \equiv I \pmod{p^k} \quad \text{and} \quad B^{p^{k-t-1}} \not\equiv I \pmod{p^k}.$$

This implies that $\operatorname{ord}_{p^k}(A) = \operatorname{ord}_{p^t}(A) p^{k-t}$. For $k = t$, this statement is trivially true. □

The following example shows that the theorem does not hold if $t = 1$ and $p = 2$.

Example: Consider

$$A = \begin{bmatrix} 0 & 3 & 0 \\ 0 & 0 & 3 \\ 3 & 0 & 0 \end{bmatrix} \in \mathbb{Z}^{3\times 3}.$$

The order of A modulo $m = 2^k$ is given by

k	$\operatorname{ord}_{2^k}(A)$
1	3
2	6
3	6
4	12.

By the theorem, we may conclude that $\operatorname{ord}_{2^k}(A) = 6 \cdot 2^{k-3}$ for $k \geq 3$.

A crucial ingredient for calculating $\operatorname{ord}_p(A)$ is the *a priori* computation of a number N with $A^N = I$. Then $\operatorname{ord}_p(A)$ must be a divisor of N. The following result can be found in Celler and Leedham-Green (1997), where it is shown using the Jordan form of A over the algebraic closure of the field $\mathbb{Z}_p$. Below, we provide an alternative proof.

Theorem 6. (Celler and Leedham-Green (1997)). Let $A \in \mathbb{Z}^{n\times n}$ be given and let p be a prime with $p \nmid \det(A)$. Let $f_A \in \mathbb{Z}_p[s]$ be the minimal polynomial of A and let

$$f_A = \prod_{i=1}^{l} f_i^{\mu_i}$$

be its prime factorization in $\mathbb{Z}_p[s]$, that is, the polynomials f_i are prime and pairwise coprime, and the μ_i are positive integers. Let $d_i := \deg(f_i)$ and let $\mu = \max\{\mu_1, \dots, \mu_l\}$. Then the order of A as an element of $\mathbb{Z}_p^{n\times n}$ divides

$$N := \operatorname{lcm}(p^{d_1} - 1, \dots, p^{d_l} - 1) \cdot p^\nu,$$

where ν is the smallest integer such that $p^\nu \geq \mu$, that is, $\nu = \lceil \log_p(\mu) \rceil$.

Proof: Consider the evaluation homomorphism

$$\Phi_A : \mathbb{Z}_p[s] \to \mathbb{Z}_p^{n\times n}, \quad h \mapsto h(A).$$

We have $\ker(\Phi_A) = \langle f_A \rangle$ and $\operatorname{im}(\Phi_A) = \mathbb{Z}_p[A]$. We obtain an isomorphism

$$R := \mathbb{Z}_p[s]/\langle f_A \rangle \leftrightarrow \mathbb{Z}_p[A], \quad s \leftrightarrow A.$$

Thus the order of A coincides with the order of s in R. By the Chinese remainder theorem, we have

$$R \cong \bigoplus_{i=1}^{l} \mathbb{Z}_p[s]/\langle f_i^{\mu_i} \rangle.$$

Thus, it suffices to determine N_i such that $s^{N_i} = 1$ holds in $R_i := \mathbb{Z}_p[s]/\langle f_i^{\mu_i} \rangle$. We claim that

$$N_i := (p^{d_i} - 1) \cdot p^{\nu_i}$$

is an appropriate choice, where $\nu_i = \lceil \log_p(\mu_i) \rceil$. Setting $\nu := \max\{\nu_1, \dots, \nu_l\}$, we have $N_i \mid N$ for all i and this proves the theorem.

To prove the claim, let r denote the order of s in $F_i := \mathbb{Z}_p[s]/\langle f_i \rangle$. Since f_i is irreducible, F_i is a field with $|F_i| = p^{d_i}$. Its unit group has $p^{d_i} - 1$ elements and hence we must have $r \mid p^{d_i} - 1$. Since $s^r = 1 + f_i g_i$ holds in $\mathbb{Z}_p[s]$, we conclude that

$$s^{rp^\nu} = (1 + f_i g_i)^{p^\nu} = 1 + f_i^{p^\nu} g_i^{p^\nu},$$

using that $(a+b)^p = a^p + b^p$ holds in characteristic p. Thus $s^{rp^\nu} = 1$ holds in R_i provided that $p^\nu \geq \mu_i$.

Let $\nu_i = \lceil \log_p(\mu_i) \rceil$. Then the order of s in R_i is a divisor of rp^{ν_i} and thus of $(p^{d_i}-1)p^{\nu_i}$. □

Example: Let $p = 157$ and

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \in \mathbb{Z}^{3\times 3}.$$

Its minimal polynomial $f_A = x^3 - x^2 - x - 1$ is irreducible over $\mathbb{Z}_p$ and hence we obtain $N = p^3 - 1 = 2^2 \cdot 3^2 \cdot 13 \cdot 8269$, which has 36 divisors, i.e., candidates for $\mathrm{ord}_p(A)$.

Using the computer algebra system MAGMA, see Bosma et al. (1997), we compute the order of A modulo $m = p^k$ for $k = 1, \ldots, 4$. The timings (in seconds) were taken on an Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz:

k	time
1	0.00
2	0.42
3	59.60
4	*

The star indicates that the process terminated with an error message after about 8 hours. This test was performed using MAGMA V2.24-10. The support team has been informed and they fixed this issue in V2.25. The computer algebra system GAP, see GAP (2019), currently seems to perform even worse than MAGMA V2.24-10. Using Corollary 4, we only need to compute $\mathrm{ord}_p(A) = 8269$ and to test whether $A^{8269 \cdot p^i}$ is equal to the identity matrix for $i = 0, \ldots, k-1$.

4. COMPUTING THE CYCLE STRUCTURE

Let $A \in \mathbb{Z}^{n\times n}$ be given and let $m > 1$ be such that $\gcd(\det(A), m) = 1$. Let $r := \mathrm{ord}_m(A)$ denote the order of A when considered as an element of $\mathbb{Z}_m^{n\times n}$. For each divisor d of r, define

$$a_d := |\{x \in \mathbb{Z}_m^n \mid A^d x = x\}|,$$

and let b_d be defined recursively by

$$b_d := a_d - \sum_{e|d, e\neq d} b_e$$

Then there are exactly b_d states in $X = \mathbb{Z}_m^n$ that belong to a cycle of length d. Hence $c_d := \frac{b_d}{d}$ is the number of cycles of length d. The cycle structure of $x(t+1) = Ax(t)$ is therefore given by $X = \bigcup_{d|r} c_d C_d$, see also Deng (2015), Wei et al. (2016). Note that a is the summatory function of b, that is, $a_d = \sum_{e|d} b_e$. Hence b can be computed from a via the Möbius inversion formula

$$b_d = \sum_{e|d} a_e \mu(\frac{d}{e}),$$

where μ denotes the Möbius function.

Lemma 7. The numbers a_d can be read off the Smith form $S_d = \mathrm{diag}(s_1, \ldots, s_n)$ of $I - A^d$ over $\mathbb{Z}^{n\times n}$. We have

$$a_d = \prod_{i=1}^{n} |\mathrm{ann}_m(s_i)|,$$

where $\mathrm{ann}_m(s_i) = \{l \in \mathbb{Z}_m \mid s_i l = 0\}$. We have

$$|\mathrm{ann}_m(s_i)| = \gcd(m, s_i).$$

In particular, if $m = p$ is prime, then each a_d is a power of p. (This can also be seen from the fact that a_d is the cardinality of a vector space over $\mathbb{Z}_p$.)

Example: Considering $y(t+3) = y(t+2) + y(t+1) + y(t)$ again, the cycle structure

- modulo 3 is a partition of 27 into 1's and 13's, where both summands must appear and the number of 1's has to be a power of 3. Thus we must have $27 = 1 + 13 + 13$ corresponding to $X = C_1 \cup 2C_{13}$.
- modulo 4 equals $X = 2C_1 \cup C_2 \cup 3C_4 \cup 6C_8$, because

$$S_1 = \mathrm{diag}(1,1,2), \quad S_2 = \mathrm{diag}(1,2,2),$$
$$S_4 = \mathrm{diag}(2,2,4), \quad S_8 = \mathrm{diag}(4,4,8).$$

Hence

d	a_d	b_d	c_d
1	2	2	2
2	4	2	1
4	16	12	3
8	64	48	6.

5. NONMONIC CASE

In the previous sections, the difference equation (1) was supposed to be monic, that is, $a_n = 1$. Now let $0 \neq a_n \in \mathbb{Z}$ be arbitrary. Consider

$$a_n y(t+n) + a_{n-1} y(t+n-1) + \ldots + a_1 y(t+1) + a_0 y(t) = 0$$

modulo a prime power $m = p^k$. First, assume that $p \mid a_i$ from all $0 \leq i \leq n$. Then we cannot expect a periodic behavior. For example, $2y(t+1) = 2y(t)$ with $m = 4$ admits solutions such as $(0, 2, 0, 0, 2, 0, 0, 0, 2, 0, 0, 0, 0, 2, \ldots)$. Thus, let's assume that $p \nmid a_i$ for some $0 \leq i \leq n$. We will show that this case can be reduced to the monic situation.

Recall that elements of $\mathbb{Z}_{p^k}$ are either units or nilpotent. Thus a polynomial $f = \sum_{i=0}^{n} a_i s^i \in \mathbb{Z}_{p^k}[s]$ is (Atiyah and Macdonald, 1969, Ch. 1, Ex. 2)

- a unit if and only if a_0 is a unit and $a_1, \ldots, a_n$ are nilpotent,
- a zerodivisor if and only if it is nilpotent,
- nilpotent if and only if $a_0, \ldots, a_n$ are nilpotent.

In any commutative ring, the sum of a unit and a nilpotent element is a unit. Two ring elements r_1, r_2 are called associated if there exists a unit u with $r_1 = ur_2$.

Theorem 8. Let $m = p^k$ be a prime power, and let $f = \sum_{i=0}^{n} a_i s^i \in \mathbb{Z}[s]$ be a nonzerodivisor when considered as an element of $\mathbb{Z}_{p^k}[s]$. This means that there exists $0 \leq i \leq n$ such that $p \nmid a_i$. Let t be maximal with $p \nmid a_t$. Then f is associated (in $\mathbb{Z}_m[s]$) to a monic polynomial f' of degree t, where the constant terms of f and f' are associated (in $\mathbb{Z}_m$).

Proof: Without loss of generality, let $a_t = 1$. We will show by induction on l that there exist monic polynomials $f_l \in \mathbb{Z}[s]$ of degree t and polynomials $g_l \in p\mathbb{Z}[s]$ such that

$$f \equiv (1 + g_l) f_l \pmod{p^l}.$$

Then $f = (1 + g_k) f_k$ holds in $\mathbb{Z}_{p^k}[s]$, where f_k is monic of degree t and g_k is nilpotent in $\mathbb{Z}_{p^k}[s]$, that is, $1 + g_k$ is a unit. Moreover, $f(0) = (1 + g_k(0)) f_k(0)$ shows that $f(0)$ and $f_k(0)$ are associated. Thus we may put $f' := f_k$.

We set $f_1 := \sum_{i=0}^{t} a_i s^i$ and $g_1 := 0$. Assume that $f_1, \ldots, f_l$ and $g_1, \ldots, g_l$ with the desired properties have been constructed. Set $h := f - (1 + g_l) f_l$. Since f_l is monic, we may perform a division with remainder to obtain $h = q f_l + r$, where $r = 0$ or $\deg(r) < t$.

Set $f_{l+1} := f_l + r$ and $g_{l+1} := g_l + q$. Then f_{l+1} is monic of degree t. Since $h \equiv 0 \pmod{p^l}$ and f_l is monic, we have $q \equiv 0 \pmod{p^l}$ and hence $r = h - qf_l \equiv 0 \pmod{p^l}$. In particular, g_{l+1} belongs to $p\mathbb{Z}[s]$. Finally,

$$\begin{aligned} f &= (1+g_l)f_l + h \\ &= (1+g_l)f_l + qf_l + r \\ &= f_{l+1} + g_{l+1}f_l \\ &= f_{l+1} + g_{l+1}(f_{l+1} - r) \\ &= (1+g_{l+1})f_{l+1} - g_{l+1}r \\ &\equiv (1+g_{l+1})f_{l+1} \pmod{p^{l+1}}. \end{aligned}$$

This completes the inductive step. □

Example: Let $m = 16$ and $f = 2s^4 + s^3 + 4s^2 + 3s + 8$. We set

$$f_1 := s^3 + 4s^2 + 3s + 8 \quad \text{and} \quad g_1 := 0.$$

Thus $h = 2s^4$ and the division with remainder yields $q = 2s + 8$ and $r = 10s^2 + 8s$. (All intermediate results are reduced modulo m.) We set

$$f_2 := s^3 + 14s^2 + 11s + 8 \quad \text{and} \quad g_2 := 2s + 8.$$

Thus $h = 12s^3$ and the division with remainder yields $q = 12$ and $r = 8s^2 + 12s$. We set

$$f_3 := s^3 + 6s^2 + 7s + 8 \quad \text{and} \quad g_3 := 2s + 4.$$

Thus $h = 8s^2$, $r = 8s^2$, $q = 0$ and we set

$$f_4 := s^3 + 14s^2 + 7s + 8 \quad \text{and} \quad g_4 := 2s + 4.$$

We put $f' = f_4$, $g' = g_4$ and obtain $f = (1 + g')f'$.

6. LAURENT POLYNOMIALS

Next, we will consider

$$a_n y(t+n) + a_{n-1} y(t+n-1) + \ldots + a_1 y(t+1) + a_0 y(t) = 0$$

as an equation defined for all $t \in \mathbb{Z}$. Correspondingly, we will treat $f := \sum_{i=0}^{n} a_i s^i$ as a Laurent polynomial, that is, as an element of $\mathbb{Z}[s, s^{-1}]$ or $\mathbb{Z}_m[s, s^{-1}]$ with a prime power $m = p^k$.

A polynomial $f = \sum_{i=0}^{n} a_i s^i \in \mathbb{Z}_{p^k}[s, s^{-1}]$ is

- a unit if and only if there exists t such that a_t is a unit and all a_i with $i \neq t$ are nilpotent,
- a zerodivisor if and only if it is nilpotent,
- nilpotent if and only if $a_0, \ldots, a_n$ are nilpotent.

The proof of the second and the third statement is analogous to the case of ordinary polynomials. The "if" part of the first statement is clear, since $f = a_t s^t + (f - a_t s^t)$ is the sum of a unit and a nilpotent polynomial.

Lemma 9. Let $f = \sum_{i=0}^{n} a_i s^i$ be a unit in $\mathbb{Z}_{p^k}[s, s^{-1}]$. Then there exists t such that a_t is a unit and all a_i with $i \neq t$ are nilpotent.

Proof: If all a_i were nilpotent, then f would be nilpotent, and hence not a unit. Thus there exists i such that a_i is a unit. Let t be the maximal index such that a_t is a unit. Then all a_i with $i > t$ are nilpotent and hence also $h := a_n s^n + \ldots + a_{t+1} s^{t+1}$. Thus $f_1 := f - h = \sum_{i=0}^{t} a_i s^i$ is a unit. We need to show that all a_i with $i < t$ are nilpotent. If $t = 0$, we're finished. Assume that $t > 0$.

Let $g \in \mathbb{Z}_{p^k}[s, s^{-1}]$ be the inverse of f_1. There exists $l \in \mathbb{Z}$ such that $g_1 := s^l g = \sum_{j=0}^{m} b_j s^j \in \mathbb{Z}_{p^k}[s]$ with $b_m \neq 0$ and $b_0 \neq 0$. We have $f_1 g_1 = s^l$.

Since a_t is a unit and $b_m \neq 0$, we have $a_t b_m \neq 0$. Thus we must have $a_t b_m = 1$ and $l = t + m > 0$. Then $a_0 b_0 = 0$, which implies (since $b_0 \neq 0$) that a_0 is not a unit, hence nilpotent. If $t = 1$, we're finished. Assume that $t > 1$. Then $s^{-1}(f_1 - a_0) = \sum_{i=0}^{t-1} a_{i+1} s^i$ is a unit and we may conclude that a_1 is nilpotent. Inductively, we obtain that all a_i with $i < t$ are nilpotent. □

Lemma 10. Let R be an arbitrary commutative ring. Let $f = \sum_{i=0}^{n} a_i s^i \in R[s]$ be such that $a_n \neq 0$. Then the reciprocal polynomial of f is defined by

$$f^* = \sum_{i=0}^{n} a_i s^{n-i}.$$

Let $g = \sum_{j=0}^{m} b_j s^j \in R[s]$ be such that $b_m \neq 0$ and $g^* = \sum_{j=0}^{m} b_j s^{m-j}$. Then there exists $l \geq 0$ such that

$$f^* g^* = s^l (fg)^*.$$

In particular, $f^* g^*$ and $(fg)^*$ are associated when considered as elements of $R[s, s^{-1}]$.

Proof: Let $N := \deg(fg)$. We have

$$f^* g^* = \sum_{k=0}^{n+m} \Big(\sum_{i+j=k} a_i b_j \Big) s^{n+m-k} = \sum_{k=0}^{N} \Big(\sum_{i+j=k} a_i b_j \Big) s^{n+m-k}$$

and

$$(fg)^* = \sum_{k=0}^{N} \Big(\sum_{i+j=k} a_i b_j \Big) s^{N-k}.$$

Thus $f^* g^* = s^{n+m-N} (fg)^*$ and we're finished by putting $l := n + m - N$. □

Theorem 11. Let $f \in \mathbb{Z}_{p^k}[s, s^{-1}]$ be given. Without loss of generality, write $f = \sum_{i=0}^{n} a_i s^i$ with $a_n \neq 0$ and $a_0 \neq 0$. Assume that f is a nonzerodivisor, that is, there exists i such that a_i is a unit in $\mathbb{Z}_{p^k}$. Then f is associated to a polynomial whose leading coefficient and constant term are both units.

Proof: From Theorem 8, we know that $f = ug$, where g is monic and u is a unit in $\mathbb{Z}_{p^k}[s]$ and thus, a unit in $\mathbb{Z}_{p^k}[s, s^{-1}]$. We also know that $f(0)$ is associated to $g(0)$ and hence $g(0) \neq 0$. Consider g^*, which is a polynomial with constant term 1. Again by Theorem 8, we obtain $g^* = vh$, where h is monic, and v is a unit in $\mathbb{Z}_{p^k}[s]$. Moreover, $1 = g^*(0)$ is associated to $h(0)$, that is, $h(0)$ is a unit. Since $g(0) \neq 0$, we have $(g^*)^* = g$. Thus $g = (g^*)^* = (vh)^* = s^{-l} v^* h^*$ for some l. But v^* is a unit in $\mathbb{Z}_{p^k}[s, s^{-1}]$. Thus f is associated (over $\mathbb{Z}_{p^k}[s, s^{-1}]$) to h^*, which is a polynomial whose leading coefficient and constant term are both units. □

Example: Let $m = 16$ and $f = 2s^4 + s^3 + 4s^2 + 3s + 8$. We have already computed $f = ug$ with $u = 2s + 5$ and $g = s^3 + 14s^2 + 7s + 8$. Now we consider $g^* = 8s^3 + 7s^2 + 14s + 1$ and obtain $7g^* = 8s^3 + s^2 + 2s + 7 = vh$ with $v = 1 + 8s$ and $h = s^2 + 10s + 7$. Thus $g = (g^*)^* = 7(vh)^* = 7v^* h^*$ and $f = 7uv^* h^*$ with $7uv^* = 8 + 3s + 14s^2$ and $h^* = 7s^2 + 10s + 1$. Thus f is associated to h^*.

7. CONCLUSION

The results of the previous two sections can also be tackled using Gröbner bases over coefficient rings, see Adams and Loustaunau (1994), Kuijper and Pinto (2017). A principal ideal $\langle f \rangle$ in $\mathbb{Z}_{p^k}[s]$, where f is a nonzerodivisor, possesses a Gröbner basis of the form $\{g\}$, where g is a monic polynomial associated to f. The Laurent polynomial case can be treated using the ideal $\langle f, st-1 \rangle$ in $\mathbb{Z}_{p^k}[s,t]$.

Using the theory developed in Zerz (2015), we plan to extend the results of this paper from scalar equations to systems of equations $R(\sigma)w = 0$. Here, σ denotes the shift operator, and R is a $g \times q$ matrix with entries in $\mathcal{D} = \mathbb{Z}_m[s]$ with $m > 1$. If $\mathrm{ann}(\mathcal{M})$ contains a monic polynomial, where $\mathcal{M} := \mathcal{D}^{1\times q}/\mathcal{D}^{1\times g}R$, then $\mathcal{M}$ is finitely generated as a module over $\mathbb{Z}_m$, the system has an equivalent first order representation, and all trajectories are (eventually) periodic. If $\mathrm{ann}(\mathcal{M})$ contains even a polynomial whose constant term is a unit, then all trajectories are (purely) periodic, see Zerz (2010), Zerz and Wagner (2012).

The authors would like to thank D. Ulmer for inspiration.

REFERENCES

Adams, W.W. and Loustaunau, P. (1994). *An Introduction to Gröbner Bases*. American Mathematical Society.

Atiyah, M.F. and Macdonald, I.G. (1969). *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company.

Bosma, W., Cannon, J., and Playoust, C. (1997). The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24, 235–265.

Celler, F. and Leedham-Green, C.R. (1997). Calculating the order of an invertible matrix. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 28, 55–60.

Deng, G. (2015). Cycles of linear dynamical systems over finite local rings. *Journal of Algebra*, 433, 243–261.

Kuijper, M. and Pinto, R. (2017). An iterative algorithm for parametrization of shortest length linear shift registers over finite chain rings. *Designs, Codes and Cryptography*, 83, 283–305.

McDonald, B.R. (1974). *Finite Rings with Identity.* Marcel Dekker, Inc.

Sun, Z.-H., and Sun, Z.-W. (1992). Fibonacci numbers and Fermat's last theorem. *Acta Arithmetica*, 60, 371–388.

The GAP Group (2019). *GAP – Groups, Algorithms, and Programming, Version 4.10.2.* (`https://www.gap-system.org`).

Wall, D.D. (1960). Fibonacci series modulo m. *The American Mathematical Monthly*, 67, 525–532.

Wei, Y., Xu, G., and Zou, Y.M. (2016). Dynamics of linear systems over finite commutative rings. *Applicable Algebra in Engineering, Communication and Computing*, 27, 469–479.

Zerz, E. (2010). On periodic solutions of linear difference equations. *Proc. 19th Int. Symposium on Mathematical Theory of Networks and Systems (MTNS)*, 1567–1570.

Zerz, E. and Wagner, L. (2012). Finite multidimensional behaviors. *Multidimensional Systems and Signal Processing*, 23, 5–15.

Zerz, E. (2015). State representations of finitely generated nD behaviors over rings. *Proc. IEEE 9th Int. Workshop on Multidimensional (nD) Systems (nDS),* 4 pages.