#A56 INTEGERS 16 (2016)

NEW EXAMPLES OF DIVISIBILITY SEQUENCES

Krzysztof Górnisiewicz
Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Poznań, Poland
krisgorn@amu.edu.pl

Received: 9/5/14, Revised: 2/20/16, Accepted: 7/11/16, Published: 7/22/16

Abstract

We show that if a full group of invertible matrices is embedded in an affine space, then the determinant divisibility sequence associated with the set of endomorphisms given by taking nth powers of matrices is a product of Lucas sequences.

1. Introduction

By a *divisibility sequence* we shall mean a sequence $\{d_n\}_{n\in\mathbb{N}}$ of integers such that if $n|m$, then $d_n|d_m$. One of the most famous divisibility sequences is the Fibonacci sequence: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34,... which arises from the linear recurrence $F_n = F_{n-1} + F_{n-2}$. This is an example of the Lucas sequences: $L_n = \frac{\alpha^n-\beta^n}{\alpha-\beta}$, where α, β are the roots of a quadratic polynomial over $\mathbb{Z}$. See [1] for a complete classification of linear recurrence divisibility sequences and [4], [5], [6] for an introduction to other divisibility sequences. In this paper we discuss properties of certain matrix divisibility sequences. We follow the approach initiated in [3].

2. Matrix Divisibility Sequence

Let S be a commutative ring with 1. Let $M_r(S)$ be the ring of $r \times r$ matrices with entries in S. By the divisor class of a matrix $M \in M_r(S)$ we mean the coset $GL_r(S) \cdot M$ of M with respect to the natural left action of $GL_r(S)$. We say that a matrix $M \in M_r(S)$ divides a matrix $N \in M_r(S)$ if there exists a matrix $Q \in M_r(S)$ such that $N = QM$. If M divides N, then any element of the divisor class of M also divides N. Let $(\Gamma, \cdot)$ denote a semigroup. A *divisibility sequence of matrices* over a commutative ring S, indexed by Γ, is a collection of matrices $\{M_\alpha\}_{\alpha\in\Gamma}$ in $M_r(S)$, such that if α divides β in Γ, then M_α divides M_β in $M_r(S)$. If $\{M_\alpha\}_{\alpha\in\Gamma}$ is a divisibility sequence of matrices, then by the multiplicativity of the determinant

$\{det(M_\alpha)\}_{\alpha\in\Gamma}$ is a divisibility sequence of elements of the ring S.
We fix a faithful representation:

$$[\cdot] : \Gamma \hookrightarrow \mathrm{End}(\mathbb{A}^r_S) : \alpha \mapsto [\alpha]$$

of Γ into the group of endomorphisms of the affine r-dimensional space $\mathbb{A}^r_S$ over S.

Definition 1. Let $x \in \mathbb{A}^r_S$. The *matrix divisibility sequence* associated with $(\Gamma, [\cdot])$ is the sequence of Jacobians $\{J_\alpha(x)\}_{\alpha\in\Gamma}$ which are $r \times r$ matrices with $(i,j)-$entry given by partial differentials:

$$[J_\alpha(x)]_{i,j} := \partial(([\alpha](x))_i)/\partial x_j,$$

where $([\alpha](x))_i$ is the ith entry of the value of the endomorphism $[\alpha]$ on x. The associated *determinant divisibility sequence* is defined by $\{\det(J_\alpha(x)\}_{\alpha\in\Gamma}$.

3. Main Result

From now on we fix $\Gamma = \mathbb{N}$. Consider the group G of all invertible $r \times r$ matrices with the embedding:

$$G \to \mathbb{A}^{r^2} : \begin{bmatrix} X_{11} & \cdots & X_{1s} \\ \vdots & \ddots & \vdots \\ X_{s1} & \cdots & X_{rr} \end{bmatrix} \mapsto (X_{11}, \ldots, X_{1r}, \ldots, X_{r1}, \ldots, X_{rr})$$

We define the endomorphism $[n]$ for $n \in \mathbb{N}$. Let $X := [X_{ij}] \in G$ and respectively $X^n := [\bar{X}_{kl}] \in G$, where we treat $\bar{X}_{kl}$ as functions of X_{ij}, for $1 \le i,j,k,l \le r$. We define $[n] : \mathbb{A}^{r^2} \to \mathbb{A}^{r^2}$ as

$$[n]\,(X_{11}, \ldots, X_{1r}, \ldots, X_{r1}, \ldots, X_{rr}) = \left(\bar{X}_{11}, \ldots, \bar{X}_{1r}, \ldots, \bar{X}_{r1}, \ldots, \bar{X}_{rr}\right).$$

Then, the Jacobian J_n of the nth power of the matrix X has the form:

$$J_n = \frac{d(X^n)}{dX} \qquad D_n = \det J_n.$$

Theorem 2. *Let $X \in GL_r(\mathbb{Z})$ and $\lambda_1, \ldots, \lambda_r$ be the eigenvalues of X. Then for every $n \ge 1$:*

$$D_n = \prod_{1\le i,j\le r} \left(\lambda_j^{n-1} + \lambda_i\lambda_j^{n-2} + \lambda_i^2\lambda_j^{n-3} + \ldots + \lambda_i^{n-2}\lambda_j + \lambda_i^{n-1}\right) \tag{1}$$

is an integer and the sequence $\{D_n\}_{n\in\mathbb{N}}$ is a determinant divisibility sequence.

Proof. Let X, Y, Z be square $r \times r$ matrices. Assume that the entries of matrices Y and Z are functions of the entries of the matrix X. Then, the following matrix derivative formula holds ([2]):

$$\frac{d(YZ)}{dX} = (I \otimes Y)\frac{dZ}{dX} + (Z^t \otimes I)\frac{dY}{dX}, \tag{2}$$

where $\otimes$ denotes the Kronecker product, I is the identity matrix of rank r, and A^t denotes the transpose matrix of A. In addition we will use the following property of the Kronecker product:

$$(A \otimes C)(B \otimes D) = AB \otimes CD \tag{3}$$

for any square matrices A, B, C, D of the size $r \times r$.

Using (2) we compute the Jacobians of the nth power of the matrix X

$$J_n = \frac{d(X^n)}{dX} = \frac{d(X^{n-1}X)}{dX} = (I \otimes X^{n-1})\frac{dX}{dX} + (X^t \otimes I)\frac{dX^{n-1}}{dX}.$$

By induction and the property (3) of the Kronecker product we get:

$$J_n = \sum_{k=0}^{n-1} (X^t)^k \otimes X^{n-1-k}.$$

Let $N := J_X$ be the Jordan normal form of $X \in GL_r(\mathbb{Z})$. Then, $X = PNP^{-1}$, for some invertible matrix $P \in \mathrm{GL}_r(\mathbb{C})$. Hence,

$$J_n = \sum_{k=0}^{n-1} ((PNP^{-1})^t)^k \otimes (PNP^{-1})^{n-1-k} = \sum_{k=0}^{n-1} (P^{-1})^t (N^t)^k (P)^t \otimes PN^{n-1-k}P^{-1} =$$

$$= ((P^{-1})^t \otimes P)\left[\sum_{k=0}^{n-1} ((N^t)^k \otimes N^{n-1-k})\right](P^t \otimes P^{-1})$$

and the determinant divisibility sequence is of the form:

$$D_n = \det J_n = \det\left[\sum_{k=0}^{n-1} ((N^t)^k \otimes N^{n-1-k})\right].$$

The matrix $(N^t)^k$ is a lower triangular matrix whose diagonal consists of the eigenvalue powers λ_i^k. Hence, the Kronecker product $(N^t)^k \otimes N^{n-1-k}$ is a lower triangular block matrix whose blocks are upper triangular matrices with diagonals composed of terms $\lambda_i^k \lambda_j^{n-1-k}$. Therefore we can conclude that:

$$D_n = \prod_{1 \le i,j \le r} \left(\lambda_j^{n-1} + \lambda_i \lambda_j^{n-2} + \lambda_i^2 \lambda_j^{n-3} + \ldots + \lambda_i^{n-2}\lambda_j + \lambda_i^{n-1}\right).$$

The right hand side is the product of the values of symmetric polynomials computed at eigenvalues of the matrix X. The Galois group of the splitting field of the characteristic polynomial of X acts trivially on these algebraic integers, hence $D_n \in \mathbb{Z}$. For any $n, m \in \mathbb{N}$ such that n divides m we have $n\lambda_i^{(n-1)} | m\lambda_i^{(m-1)}$ (for $\lambda_j = \lambda_i$) and $(\lambda_i^n - \lambda_j^n)|(\lambda_i^m - \lambda_j^m)$ (for $\lambda_j \neq \lambda_i$) . Therefore, the sequence D_n is a divisibility sequence. □

Remark 3. If the matrix X has distinct eigenvalues then the integer D_n can be simplified to the form:

$$D_n = n^r [detX]^{n-1} \prod_{1 \leq i \neq j \leq r} \left(\frac{\lambda_i^n - \lambda_j^n}{\lambda_i - \lambda_j} \right)^2 .$$

4. Examples

1) Let $X \in \mathrm{GL}_2(\mathbb{Z})$ and $a = \mathrm{tr}X, b = \mathrm{tr}^2 X - 4\mathrm{det}X$. Then, using Theorem 2 we obtain the sequence presented in [3], Example 4.3:

$$D_n = \frac{n^2}{b} [\mathrm{det}X]^{n-1} \left(\left(\frac{a + \sqrt{b}}{2} \right)^n - \left(\frac{a - \sqrt{b}}{2} \right)^n \right)^2 .$$

2) Let $X \in \mathrm{GL}_3(\mathbb{Z})$ and $b = -\mathrm{tr}X$, $c = X_{11} + X_{22} + X_{33}$, $d = -\det X$. The discriminant of the characteristic polynomial of X is $\Delta = (4\Delta_0^3 - \Delta_1^2)/27$, where $\Delta_0 = b^2 - 3c$ and $\Delta_1 = 2b^3 - 9bc + 27d$. We obtain the divisibility sequence defined by:

$$D_n = \frac{n^3(-d)^{n-1}}{\Delta} \prod_{i=1}^{3} \left[\left(\frac{b + \epsilon^i A + \epsilon^{2i} \bar{A}}{3} \right)^n - \left(\frac{b + \epsilon^{i+1} A + \epsilon^{2i+2} \bar{A}}{3} \right)^n \right]^2 ,$$

where $A = \sqrt[3]{(\Delta_1 + \sqrt{-27\Delta})/2}$, $\bar{A} = \sqrt[3]{(\Delta_1 - \sqrt{-27\Delta})/2}$ and ϵ is a fixed primitive cube root of unity.

3) It is easy to compute values of D_n for any square matrix X. The matrix $X = \begin{bmatrix} 1 & -2 & -6 \\ 0 & 1 & 3 \\ -1 & 0 & 1 \end{bmatrix} \in Gl_3(\mathbb{Z})$ gives the following divisibility sequence:

n	D_n	factorization of D_n
1	1	1
2	800	$2^5 5^2$
3	177147	3^{11}
4	12390400	$2^{12} 5^2 11^2$
5	101025125	$5^3 29^2 31^2$
6	40956386400	$2^5 3^{11} 5^2 17^2$
7	17195158625743	$7^3 41^2 43^2 127^2$
8	2097446912000000	$2^{21} 5^6 11^2 23^2$
9	116366997680401329	$3^{20} 53^2 109^2$
10	1865976489302500000	$2^5 5^7 29^2 31^6$
11	42038200804419417851	$11^3 131^2 857^2 1583^2$
12	37991519596669194547200	$2^{12} 3^{11} 5^2 11^2 17^2 71^2 109^2$
13	5207914793773442748752677	$13^3 1637^2 4057^2 7331^2$
14	323985952722322674280901600	$2^5 5^2 7^3 41^2 43^6 83^2 127^2$
15	7972611872817713189931453375	$3^{11} 5^3 29^2 31^2 2969^2 7109^2$
16	347979934553230802944000000	$2^{30} 5^6 11^2 23^2 47^2 383^2$

Acknowledgments: The author thanks Wojciech Gajda for suggesting the problem and fruitful discussions. He was supported by the research grant UMO-2012 / 07 / B / ST1 / 03541 of the National Centre of Sciences of Poland. He would also like to thank the anonymous referee for helpful remarks which improved exposition of the paper.

References

[1] J.P. Bezivin, A. Ptheo, A.J. van der Poorten. A full characterization of divisibility sequences, *Amer. J. Math.* **112** (1990), 985-1001.

[2] M. Brooks. The Matrix Reference Manual, *http://www.ee.ic.ac.uk/hp/staff/dmb/matrix/intro.html*.

[3] G. Cornelissen, J. Reynolds. Matrix divisibility sequences, *Acta Arith.* **156** (2012),177-188.

[4] P. Ingram. Elliptic divisibility sequences over certain curves, *J. Number Theory* **123** (2007), no. 2, 473-486.

[5] Rachel Shipsey. Elliptic divisibility sequences, Ph.D. thesis, Goldsmiths College, University of London, (2000), *http://homepages.gold.ac.uk/rachel*.

[6] J. H. Silverman. Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups, *Monatsh. Math.*, **145** (2005), 333-350.