

## Matrix divisibility sequences

by

GUNTHER CORNELISSEN and JONATHAN REYNOLDS (Utrecht)

**1. Introduction.** The most famous divisibility sequence is probably the Fibonacci sequence  $\{F_n\}_{n \geq 1}$ : if  $m$  divides  $n$ , then  $F_m$  divides  $F_n$ . This property is shared by other linear recurrent sequences [3], such as any other Lucas sequence, and by higher degree recurrent sequences known as elliptic divisibility sequences [13, 24]. Recent years have witnessed a revived and increasing interest in such sequences [11, 12, 14, 15, 16], alongside applications in cryptography [19, 17] and undecidability [8, 10]. In the current paper, we argue that—in a non-tautological way—behind each of these divisibility sequences lies hidden a naturally defined divisibility sequence of matrices, such that the given divisibility sequence occurs as the determinant of the sequence of matrices.

The plan for the paper is as follows: we shall first introduce the general notion of a matrix divisibility sequence indexed by a semigroup. Then we will see how a faithful representation of the semigroup by endomorphisms of an affine space gives rise to a matrix divisibility sequence, by considering the Jacobian matrices of the endomorphisms. We will show how most of the commonly known divisibility sequences (mentioned briefly above) arise as determinants of matrix divisibility sequences through interesting semigroups of endomorphisms of affine spaces, often associated to a representation of addition in an algebraic group. For example, Lucas sequences are associated to the  $2 \times 2$  Borel group. We also construct the *elliptic matrix divisibility sequence* that underlies the usual elliptic divisibility sequences, and prove that it has primitive right matrix divisor classes.

**2. Matrix divisibility sequences.** In this section, we introduce general matrix divisibility sequences over a ring  $S$ , indexed by a semigroup  $\Gamma$ , and we define primitive divisor classes of matrix divisibility sequences.

---

2010 *Mathematics Subject Classification*: Primary 11B37, 11G05; Secondary 11C20, 11G30, 16U30.

*Key words and phrases*: divisibility sequences, divisibility of matrices, Lucas sequences, elliptic divisibility sequences, Jacobian matrix, algebraic group.

DEFINITIONS 2.1. Let  $S$  denote a commutative unital ring and  $\text{Mat}_d(S)$  the ring of  $d \times d$  matrices over  $S$ . A (right) *divisor class of a matrix*  $M \in \text{Mat}_d(S)$  is a coset  $\text{GL}_d(S) \cdot M$  of  $M$  in the left quotient of  $\text{Mat}_d(S)$  by the invertible matrices  $\text{GL}_d(S)$  over  $S$ . A matrix  $M$  is said to (right) *divide* a matrix  $N$  if there exists a matrix  $Q$  such that  $N = QM$ . If  $M$  (right) divides  $N$ , then any element of the divisor class of  $M$  also right divides  $N$ .

EXAMPLE 2.2. An interesting special case of matrix divisibility is that of integer matrices (i.e.,  $S = \mathbb{Z}$ ). In this case, the right divisor classes of a matrix  $M$  are in bijection with subgroups of the cokernel  $\mathbb{Z}^d/M^\top\mathbb{Z}^d$  of left multiplication by the transpose  $M^\top$  of  $M$  (cf. [4]).

We will only consider right division from now on, and hence frequently leave out “right” from the terminology.

DEFINITIONS 2.3. Let  $(\Gamma, \cdot)$  denote a (not necessarily commutative) semi-group. A divisibility sequence of matrices over a commutative ring  $S$ , indexed by  $\Gamma$ , is a collection of matrices

$$\{M_\alpha\}_{\alpha \in \Gamma}$$

in  $\text{Mat}_d(S)$ , such that if  $\alpha$  right divides  $\beta$  in  $\Gamma$ , then  $M_\alpha$  right divides  $M_\beta$  in  $\text{Mat}_d(S)$ . A *primitive divisor class* of a term  $M_\alpha$  of such a sequence is a right divisor class of  $M_\alpha$  that is not a right divisor class of any  $M_\beta$  for  $\beta$  a right divisor of  $\alpha$ .

If  $\{M_\alpha\}_{\alpha \in \Gamma}$  is a matrix divisibility sequence, then

$$\{\det(M_\alpha)\}_{\alpha \in \Gamma}$$

is a divisibility sequence consisting of elements from the ring  $S$ . This is obvious from the multiplicativity of the determinant.

In general, divisibility of matrices is strictly stronger than divisibility of their determinants. For example, the matrices  $\text{diag}(1, 2)$  and  $\text{diag}(2, 1)$  are not right or left divisors of each other over the integers, although of course, their determinants are. Thus, it appears that the theory presented here is a strict superset of the existing one. Over a PID, divisibility of matrices is in general also stronger than divisibility of their individual elementary divisors in the Smith Normal Form.

### 3. Matrix divisibility sequences arising from endomorphisms.

We produce a natural source of matrix divisibility sequences, as Jacobian matrices of endomorphisms of affine space.

DEFINITIONS 3.1. As before, let  $(\Gamma, \cdot)$  denote a semigroup, and  $S$  a commutative unital ring. Now let

$$[\cdot]: \Gamma \hookrightarrow \text{End}(\mathbf{A}_S^d): \alpha \mapsto [\alpha]$$

denote a faithful representation of  $\Gamma$  into the group (under composition) of endomorphisms of affine  $d$ -space  $\mathbf{A}_S^d$  over  $S$  (i.e., morphisms  $\mathbf{A}_S^d \rightarrow \mathbf{A}_S^d$ ). Let  $x \in \mathbf{A}^d(S')$  be a point in some ring extension  $S \rightarrow S'$ . The *matrix divisibility sequence associated to*  $(\Gamma, [\cdot])$  is the sequence of Jacobians  $\{J_\alpha\}_{\alpha \in \Gamma}(x)$ , with  $J_\alpha$  being the  $d \times d$  matrix whose  $(i, j)$ -entry is given by

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

The associated *determinantal divisibility sequence* is given by

$$\{\det(J_\alpha)(x)\}_{\alpha \in \Gamma}.$$

EXAMPLE 3.2. A trivial example: set  $\Gamma = (\mathbb{Z}_{\geq 0}, \cdot)$ , and  $[n]: \mathbf{A}_{\mathbb{Z}}^1 \rightarrow \mathbf{A}_{\mathbb{Z}}^1: x \mapsto x^n$ . Then indeed  $[mn] = [m] \circ [n]$ , and the associated (matrix) divisibility sequence is  $nx^{n-1}$ . At  $x = 1$ , this is just the divisibility sequence of integers  $1, 2, 3, \dots$

The following facts are obvious, but they represent the basic idea in our definition: *derivatives turn composition into multiplication*.

PROPOSITION 3.3. *A matrix divisibility sequence associated to  $(\Gamma, [\cdot])$  as before is indeed a matrix divisibility sequence: if  $\alpha$  right divides  $\beta$  in  $\Gamma$ , then for any  $x \in \mathbf{A}^d(S')$ , the matrix  $J_\alpha(x)$  right divides  $J_\beta(x)$  in the semigroup of  $d \times d$  matrices  $\text{Mat}_d(S)$ , and  $\det(J_\alpha(x))$  divides  $\det(J_\beta(x))$  in  $S$ .*

*Proof.* Write  $\beta = \gamma \cdot \alpha$  in  $\Gamma$ . Then  $[\beta] = [\gamma] \circ [\alpha]$ . The chain rule for the Jacobian matrix implies that for any  $x \in \mathbf{A}^d(S')$ , we have

$$J_\beta(x) = J_\gamma([\alpha]x) \cdot J_\alpha(x)$$

in  $\text{Mat}_d(S)$ . One can then simply take determinants of this identity. ■

REMARK 3.4. We have included the case of a general semigroup  $\Gamma$ , instead of focussing on the (positive) integers as index set for the sequence, because some natural examples arise from elliptic curves with complex multiplication [23], and even noncommutative semigroups occur naturally from supersingular elliptic curves over infinite fields of positive characteristic.

REMARK 3.5. A more general case would arise when one replaces affine space  $\mathbf{A}^d$  by an algebraic variety  $X$ . If  $[\cdot]: \Gamma \hookrightarrow \text{End}(X)$  is a representation, then one may consider the pullback of  $[\alpha]$  to the tangent bundle

$$d[\alpha]: TX \rightarrow TX,$$

which then satisfies the chain rule

$$d[\alpha\beta](x) = d[\alpha](\beta x) \circ d[\beta](x).$$

Instead of taking a determinant, one may construct the highest exterior power

$$\det(d[\alpha]): \bigwedge^d TX \rightarrow \bigwedge^d TX$$

as automorphisms of the canonical bundle  $\bigwedge^d TX$ . In general, however, there is no canonical choice for compatible coordinates in tangent spaces at different points (as there is on affine space), so that this does not lead to a “numerical” divisibility sequence. Therefore, we will not consider this more general setting here.

**4. A construction of endomorphisms from algebraic groups.**

A natural context for endomorphism representations is one that arises from the endomorphisms of a linear algebraic group, as follows. Let  $(\mathbf{G}, +)$  denote an affine algebraic group over a field  $k$ , and let  $\Gamma \subseteq \text{End}_k(\mathbf{G})$  denote a finitely generated semisubgroup of the algebraic group endomorphisms of  $\mathbf{G}$ . Fix an affine embedding of  $\mathbf{G}$  into  $\mathbf{A}^d$ . Choose generators  $\gamma_1, \dots, \gamma_n$  for the group, and fix an algebraic formula  $\langle \gamma_i \rangle$  for the action of the generators on the affine embedding, and fix an algebraic formula for the product and inverse in the group in the given embedding. Now define a representation  $[\cdot]: \Gamma \rightarrow \text{End}(\mathbf{A}^d)$  by  $[\sum a_i \gamma_i](x_1, \dots, x_d) := \sum a_i \langle \gamma_i \rangle(x_1, \dots, x_d)$ , where  $\sum a_i$  is computed using the given formulas for  $+$  and  $-$  in the group.

EXAMPLE 4.1. Example 3.2 fits into this framework, if we consider  $x \mapsto x^m$  as iterates of the multiplication map on the multiplicative group  $\mathbf{G}_m$ . A more interesting example is the following:

EXAMPLE 4.2 (Borel group and Lucas sequences). Consider the Borel group  $\mathbf{B}$  of  $2 \times 2$  matrices with the affine embedding

$$\mathbf{B} \rightarrow \mathbf{A}^3: \begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix} \mapsto (X, Y, Z),$$

and the multiplication formula

$$(X_1, Y_1, Z_1) \odot (X_2, Y_2, Z_2) := (X_1 X_2, X_1 Y_2 + Y_1 Z_2, Z_1 Z_2),$$

corresponding to the product of matrices, and a similar one for the inverse. Now, for  $n \in \mathbb{N} = \Gamma$ , consider the endomorphisms given by

$$[n](X, Y, Z) = \underbrace{(X, Y, Z) \odot \dots \odot (X, Y, Z)}_{n \text{ times}} = \left( X^n, Y \frac{X^n - Z^n}{X - Z}, Z^n \right).$$

The associated matrix divisibility sequences of Jacobians of  $[n]$  is

$$J_n(X, Y, Z) = \begin{pmatrix} nX^{n-1} & 0 & 0 \\ YP(X, Z) & \frac{X^n - Z^n}{X - Z} & YP(Z, X) \\ 0 & 0 & nZ^{n-1} \end{pmatrix},$$

with

$$P(X, Z) = \frac{nX^{n-1}(X - Z) - (X^n - Z^n)}{(X - Z)^2},$$

and the associated determinant sequence is

$$\det(J_n)(X, Y, Z) = n^2 X^{n-1} Z^{n-1} \frac{X^n - Z^n}{X - Z},$$

an innocuous modification of the Lucas sequence for  $X$  and  $Z$  (and independent of  $Y$ ).

EXAMPLE 4.3. Similarly, assuming that the base ring  $S$  has characteristic  $\neq 2$ , taking powers of matrices  $M \in \text{GL}(2)$  leads to a determinantal divisibility sequence of the form

$$n \mapsto \frac{n^2}{\beta} \cdot \det(M)^{n-1} \cdot \left( \left( \frac{\alpha - \sqrt{\beta}}{2} \right)^n - \left( \frac{\alpha + \sqrt{\beta}}{2} \right)^n \right)^2$$

with  $\alpha = \text{tr}(M)$  and  $\beta = \text{tr}^2(M) - 4\det(M)$ . Here, when  $\beta = 0$  (i.e., the matrix has two identical eigenvalues), the formula should be understood in the limit as  $\beta \rightarrow 0$ , which gives  $n^4(\alpha/2)^{4(n-1)}$ .

It could be interesting to consider the determinantal divisibility sequence of more exotic linear algebraic groups.

One might wonder whether for Lucas sequences, one can do with one dimension less, but this is not even true for Mersenne sequences and general sets of endomorphisms of the affine line, as a simple integration proves:

PROPOSITION 4.4. *A generalized Mersenne sequence  $\{x^n - 1\}_{n \geq 1}$  cannot occur as a matrix divisibility sequence associated to a set of endomorphisms of  $\mathbf{A}^1$ , i.e., in dimension  $d = 1$ .*

*Proof.* If so, then there are polynomials  $f_n$  such that

$$x^n - 1 = \frac{df_n}{dx}(x).$$

By integration, we find that

$$f_n(x) = \frac{x^{n+1}}{n+1} - x + c_n$$

for some constants  $c_n$ , but then  $n \mapsto f_n$  cannot be a representation, because it already fails to satisfy  $f_{mn} = f_m \circ f_n$  (for example,  $\deg(f_m(f_n(x))) = (m+1)(n+1) \neq mn+1 = \deg(f_{mn})$ ). ■

In connection with applications of divisibility sequences in logic, we record the following. Recall that a subset  $X \subseteq \mathbb{Z}^d$  is called *Diophantine* if there exists an algebraic variety  $V$  defined over  $\mathbb{Z}$  and a morphism  $\pi: V \rightarrow \mathbf{A}^d$  defined over  $\mathbb{Z}$ , such that the image of the set of integral points of  $X$  is the given set:  $\pi(V(\mathbb{Z})) = X$ .

PROPOSITION 4.5. *Suppose  $\{M_n\}_{n \in \mathbb{N}}$  is a matrix divisibility sequence that arises as above from an affine algebraic group  $\mathbf{G}/\mathbb{Z}$ , evaluated at a*

point  $P \in \mathbf{G}(\mathbb{Z})$ . Then  $\{M_n\}_{n \in \mathbb{N}}$  is a Diophantine subset of  $\mathbb{Z}^{d^2}$ , and the associated determinant sequence  $\{\det(M_n)\}$  is a Diophantine subset of  $\mathbb{Z}$ .

*Proof.* By the David–Putnam–Robinson–Matiyasevich theorem (see, e.g., [18]), Diophantine sets over  $\mathbb{Z}$  are the same as recursively enumerable sets over  $\mathbb{Z}$ . We prove that the set  $\{M_n\}$  is recursively enumerable. The formula that expresses  $[n]x$  in algebraic terms, for a general point  $x \in \mathbf{G}$ , is computable in finite time on a Turing machine. The same holds for its Jacobian matrix. Hence also the values of the Jacobian matrices at  $P$  are computable in finite time. Now the set  $\{M_n\}$  can be enumerated by running through  $n$ . The same holds for the determinant sequence, since determinants are computable in finite time. ■

REMARK 4.6. For a set of endomorphisms of a projective algebraic group (e.g., an abelian variety), one can use the general construction from Remark 3.5. One may also try to adapt the previous method from affine groups, by fixing an equation for addition in homogeneous coordinates and consider it on the affine cone over the group. (A particularly simple example of such a formula arises from the complete group law on the representation of an elliptic curve in Edwards form, cf. [9], [2].) However, in general one will then only have a projective composition formula

$$[\alpha\beta](P) = \lambda_{\alpha,\beta}(P)[\alpha]([\beta]P),$$

for some functions  $\lambda_{\alpha,\beta}$  on  $G$ —from which the associated Jacobian matrix divisibility sequence will not in general be multiplicative, but rather satisfy

$$J_{\alpha\beta}(P) = \lambda_{\alpha,\beta}(P)J_{\alpha}([\beta]P)J_{\beta}(P) + (\nabla\lambda_{\alpha,\beta}(P))^{\top} \cdot [\beta]P.$$

If  $P \in \mathbf{G}(S')$  is a point whose  $\Gamma$ -orbit stays within a fixed affine chart, then it is possible to extend the previous method.

Another approach to general divisibility sequences, based on generalized GCD's, is due to Silverman [21]. For a further approach to (non-divisibility!) sequences in higher genus, see Cantor [6] (where the  $r$ th division polynomial is zero at a point  $P$  if and only if  $rP$  is in the theta-divisor—compare with [5] for another interpretation of these sequences).

In the next section, we will use a slightly different method for elliptic curves, based on the theory of division polynomials.

## 5. Matrix elliptic divisibility sequences: formal construction.

We will now show how elliptic divisibility sequences fit into the matrix divisibility picture, using division polynomials. Let  $E$  denote a cubic curve with projective equation

$$Y^2Z = X^3 + AXZ^2 + BZ^6$$

over the ring  $S = \mathbb{Z}[A, B]$ . The non-singular points of  $E$  over any field containing  $S$  form a group. Multiplication on the non-singular points of this cubic curve can be expressed using classical division polynomials:

$$n \cdot (x, y) = \left( \frac{\phi_n(x)}{\psi_n^2(x, y)}, \frac{\omega_n(x, y)}{\psi_n^3(x, y)} \right).$$

We refer to [7], [1] and [22, Ex. III.3.7] for the definition of these polynomials. Here,  $\phi_n$  and

$$\tilde{\psi}_n := \psi_n^2$$

only depend on  $x$ .

We now consider the following map of affine 2-space:

$$[n]: \mathbf{A}^2 \rightarrow \mathbf{A}^2: (X, Z) \mapsto (f(X, Z), g(X, Z)),$$

where

$$f(X, Z) = Z^{n^2} \phi_n(X/Z) \text{ and } g(X, Z) = Z^{n^2} \tilde{\psi}_n(X/Z).$$

The multiplicative property  $(mn)P = m(nP)$  translates to  $[mn] = [m] \circ [n]$  (compare [7, formula (5)], so that  $[\cdot]$  indeed defines a faithful representation of  $\Gamma = \mathbb{N}$  as a group of endomorphisms of affine 2-space  $\mathbf{A}^2$ . Hence the associated sequence of Jacobian matrices is a matrix divisibility sequence, and its determinant is a divisibility sequence in the usual sense. We now establish a formula for these sequences in terms of known division polynomials. For this, we first compute some partial derivatives:

$$\begin{aligned} \frac{\partial f}{\partial X} &= Z^{n^2-1} \phi'_n(X/Z), \\ \frac{\partial f}{\partial Z} &= -X Z^{n^2-2} \phi'_n(X/Z) + n^2 Z^{n^2-1} \phi_n(X/Z) \\ &= Z^{n^2-2} (n^2 Z \phi_n(X/Z) - X \phi'_n(X/Z)). \end{aligned}$$

Also

$$\frac{\partial g}{\partial X} = Z^{n^2-1} \tilde{\psi}'_n(X/Z), \quad \frac{\partial g}{\partial Z} = Z^{n^2-2} (n^2 Z \tilde{\psi}_n(X/Z) - X \tilde{\psi}'_n(X/Z)).$$

We conclude:

PROPOSITION 5.1. Denoting as before  $\tilde{\psi}_n = \psi_n^2$ , the sequence

$$J_n(X, Z) := Z^{n^2-2} \begin{pmatrix} Z \phi'_n(X/Z) & n^2 Z \phi_n(X/Z) - X \phi'_n(X/Z) \\ Z \tilde{\psi}'_n(X/Z) & n^2 Z \tilde{\psi}_n(X/Z) - X \tilde{\psi}'_n(X/Z) \end{pmatrix}$$

is a matrix divisibility sequence, which we call a matrix elliptic divisibility sequence, with associated so-called determinant elliptic divisibility sequence

$$\det(J_n)(X, Z) = n^2 Z^{2(n^2-1)} W(\phi_n, \tilde{\psi}_n)(X/Z),$$

where  $W(\phi, \tilde{\psi}) = \phi' \tilde{\psi} - \phi \tilde{\psi}'$  is the Wronskian determinant of two functions  $\phi$  and  $\tilde{\psi}$ . ■

REMARK 5.2. By Cassels' Theorem I in [7], the polynomial derivatives  $\phi'_n(x)$  and  $\tilde{\psi}'_n(x)$  have all their coefficients divisible by  $n$ ; we conclude that the matrix  $J_n(X, Z)$  is divisible by the diagonal matrix  $\text{diag}(n, n)$ .

We can further simplify the Wronskian determinant in Proposition 5.1, as follows: by taking derivatives on both sides of

$$x(n \cdot (x, y)) = \frac{\phi_n(x)}{\tilde{\psi}_n(x)}$$

we find that

$$\frac{dx(n \cdot (x, y))}{dx} = \frac{W(\phi_n, \tilde{\psi}_n)}{\tilde{\psi}_n^2}.$$

To use  $\wp$ -functions, we switch to classical Weierstrass form, by writing  $x = x_1/36$  and  $y = y_1/432$ , so that  $(x_1, y_1)$  satisfies the Weierstrass equation in traditional form  $y_1^2 = 4x_1^3 - g_2x_1 - g_3$  for  $g_2 = -5184A$  and  $g_3 = -186624B$ , and we can write  $x_1 = \wp(z)$ ,  $y_1 = \wp'(z)$  for  $\wp$  the Weierstrass  $\wp$ -function of the corresponding lattice. Then

$$\frac{dx(n \cdot (x, y))}{dx} = \frac{1}{36} \frac{d\wp(nz)}{dx} = \frac{n}{36} \wp'(nz) \frac{dz}{dx} = n \frac{\wp'(nz)}{\wp'(z)},$$

which we further simplify to

$$n \frac{y(n \cdot (x, y))}{y} = \frac{2n}{\psi_2} y(n \cdot (x, y)) = \frac{1}{\psi_n^4} \left( \frac{n\psi_{2n}}{\psi_2} \right),$$

so that we finally find

PROPOSITION 5.3. *The determinant elliptic divisibility sequence from Proposition 5.1 equals*

$$\det J_n(X, Z) = n^3 Z^{2(n^2-1)} \frac{\psi_{2n}}{\psi_2}(X/Z) = 2n^3 Z^{2(n^2-1)} \frac{\psi_n \omega_n}{\psi_2}(X/Z). \blacksquare$$

This result shows that every elliptic divisibility sequence occurs (up to passing to a field extension to divide a given point by 2) as a determinant divisibility sequence.

REMARK 5.4. We have already seen how Lucas sequences arise from the  $2 \times 2$  Borel group. Since all Lucas sequences also occur as elliptic divisibility sequence for singular cubics, we immediately find from the previous section that they, too, fit into this framework ([24, Thm. 22.1]).

**6. Matrix elliptic divisibility sequences: integral values and primitive divisors.** We now turn to the issue of actually substituting a rational point on the curve into these new sequences.

PROPOSITION 6.1. *Suppose that  $P = (x, y)$  is a rational point of infinite order on an elliptic curve  $E/\mathbb{Q}$  with chosen short Weierstrass equation*

with integral coefficients, and write  $x = a/b^2$  in coprime integers  $a, b$ . The determinantal divisibility sequence

$$\det(J_n(a, b^2))$$

is integer-valued, and has primitive prime divisors for  $n$  sufficiently large.

*Proof.* First of all, we quote a result of Ayad ([1]) to the effect that if we write

$$nP = \left( \frac{A_n}{B_n^2}, y_n \right),$$

with  $A_n, B_n$  coprime integers, then

$$b^{2n^2} \psi_n^2(a/b^2) = B_n^2 Q_n,$$

where  $Q_n$  is only divisible by primes  $p$  for which  $P$  is singular modulo  $p$  on the given model (so in particular,  $Q_n$  has only prime factors from the divisors of the discriminant  $\Delta_E$  of the given curve). This means that

$$\det J_n(a, b^2) = n^3 b^{4(n^2-1)} \frac{\psi_{2n}}{\psi_2}(a/b^2) = n^3 \frac{B_{2n}}{B_2} \cdot Q'_n,$$

where  $Q'_n$  has only prime divisors from  $\Delta_E$ .

Now, Silverman [20] has proven the elliptic analogue of Zsigmondy's theorem, implying that  $B_{2n}/B_2$  has a primitive prime divisor, say  $p$ , for sufficiently large  $n$  (since  $P$  has infinite order in  $E(\mathbb{Q})$ ). We claim that  $p$  is coprime to  $n$  for  $n$  sufficiently large. Indeed, suppose  $p | n$ . Since  $p$  is prime and primitive,  $P \pmod p$  has order  $2n$  in  $E(\mathbb{F}_p)$ , so that by the Hasse–Weil bound

$$2n < p + 1 + 2\sqrt{p} < n + 1 + 2\sqrt{n},$$

leading to  $n < 6$ . Hence for  $n$  sufficiently large ( $n > 6$ ,  $n$  large enough for Silverman's result to hold and for  $2nP$  not to be an  $S$ -integer, where  $S$  contains the primes dividing  $\Delta_E$ ),  $p$  is also primitive for  $\det(J_n(a, b))$ . ■

We finish this section by proving a matrix version of the existence of primitive divisors, based on the following general lemma:

LEMMA 6.2. *Let  $\{M_n\}_{n \in \mathbb{N}}$  denote a matrix divisibility sequence in integral matrices  $M_n \in \text{Mat}_n(\mathbb{Z})$ . If the associated determinantal divisibility sequence  $\{\det(M_n)\}_{n \in \mathbb{N}}$  has primitive prime divisors, then the matrix divisibility sequence has primitive right divisor classes.*

*Proof.* A nice way to organize the proof is by using the correspondence from Example 2.2, which implies that  $M_n$  has a primitive right divisor if and only if  $\mathbb{Z}^d/M_n^\top \mathbb{Z}^d$  has a subgroup that is not in the image of any of the natural reduction maps  $\mathbb{Z}^d/M_m^\top \mathbb{Z}^d \rightarrow \mathbb{Z}^d/M_n^\top \mathbb{Z}^d$  for any  $m | n$  with  $m \neq n$ . But since we assume that  $\det(M_n)$  has a prime divisor  $p$  that does not divide any  $\det(M_m)$  for any  $m | n$  with  $m \neq n$ , it follows that  $p$  divides one

of the elementary divisors of  $M_n$ , but none of those of such  $M_m$ . This implies that the subgroup  $\mathbb{Z}^d/p\mathbb{Z}^d$  corresponding to  $p$  has non-trivial reduction, so corresponds to a primitive right divisor class. ■

**COROLLARY 6.3** (Elliptic matrix Zsigmondy theorem). *Suppose that  $P = (x, y)$  is a rational point on an elliptic curve  $E/\mathbb{Q}$  with chosen short Weierstrass equation with integral coefficients, and write  $x = a/b^2$  in coprime integers  $a, b$ . There exists an integer  $N$  such that all the terms of a matrix elliptic divisibility sequence  $\{J_n(a, b^2)\}_{n \in \mathbb{N}}$  with  $n > N$  have primitive right matrix divisors.*

*Proof.* This follows from the previous lemma since the associated determinantal sequence (cf. Proposition 5.1) has primitive prime divisors by Proposition 6.1. ■

**REMARK 6.4.** One may also ask for “converse theorems” in the following style: if the height of the entries of the matrices  $\{M_n\}$  has a specific growth behaviour in  $n$ , does it follow (at least generically) that its determinant sequence has a “related” growth behaviour?

**REMARK 6.5.** Linear and elliptic divisibility sequences satisfy recurrence relations (provided their terms are chosen with the right sign), so we ask: Is there a choice of representatives for the divisor classes corresponding to a Lucas or elliptic *matrix* divisibility sequence as in Proposition 5.1, such that these representative matrices themselves satisfy a polynomial recurrence relation (i.e., with coefficients that do not depend on the index of the term of the sequence)? We have checked by direct computation that it is *not* the case that the “Borel” matrix sequence  $J_n(X, Y, Z)$  from Example 4.2 satisfies a second order linear recurrence in matrices of the form

$$J_n = A \cdot J_{n-1} + B \cdot J_{n-2}$$

for matrices  $A = A(X, Y, Z)$  and  $B = B(X, Y, Z)$  independent of  $n$ . One might argue that in the non-commutative ring of matrices, a second order linear recurrence should be of the form

$$J_n = A \cdot J_{n-1} \cdot B + C \cdot J_{n-2} \cdot D$$

for matrices  $A, B, C, D$  independent of  $n$ , but we did not investigate this possibility any further.

**Acknowledgments.** The idea of this paper arose after a discussion between the first named author and Thanases Pheidas in the early years of the 21st century. It was revived again through discussions and computer calculations with Graham Everest and Shaun Stevens during a visit to Norwich some time later—and forgotten again. We thank all these people, along

with Marco Streng and Tom Ward, for their stimulating interest. The second named author is supported by a Marie Curie Intra-European Fellowship (PIEF-GA-2009-235210).

### References

- [1] M. Ayad, *Points  $S$ -entiers des courbes elliptiques*, Manuscripta Math. 76 (1992), 305–324.
- [2] D. J. Bernstein and T. Lange, *Inverted Edwards coordinates*, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-1), Lecture Notes in Comput. Sci. 4851, Springer, Berlin, 2007, 20–27.
- [3] J.-P. Bézivin, A. Pethő, and A. J. van der Poorten, *A full characterisation of divisibility sequences*, Amer. J. Math. 112 (1990), 985–1001.
- [4] G. Bhowmik and O. Ramaré, *Algebra of matrix arithmetic*, J. Algebra 210 (1998), 194–215.
- [5] H. W. Braden, V. Z. Enolskii, and A. N. W. Hone, *Bilinear recurrences and addition formulae for hyperelliptic sigma functions*, J. Nonlinear Math. Phys. 12 (2005), Suppl. 2, 46–62.
- [6] D. G. Cantor, *On the analogue of the division polynomials for hyperelliptic curves*, J. Reine Angew. Math. 447 (1994), 91–145.
- [7] J. W. S. Cassels, *A note on the division values of  $\wp(u)$* , Proc. Cambridge Philos. Soc. 45 (1949), 167–172; Corrigendum, *ibid.* 71 (1972), 431.
- [8] G. Cornelissen and K. Zahidi, *Elliptic divisibility sequences and undecidable problems about rational points*, J. Reine Angew. Math. 613 (2007), 1–33.
- [9] H. M. Edwards, *A normal form for elliptic curves*, Bull. Amer. Math. Soc. (N.S.) 44 (2007), 393–422.
- [10] K. Eisenträger and G. Everest, *Descent on elliptic curves and Hilbert’s tenth problem*, Proc. Amer. Math. Soc. 137 (2009), 1951–1959.
- [11] G. Everest and H. King, *Prime powers in elliptic divisibility sequences*, Math. Comp. 74 (2005), 2061–2071.
- [12] G. Everest, V. Miller, and N. Stephens, *Primes generated by elliptic curves*, Proc. Amer. Math. Soc. 132 (2004), 955–963.
- [13] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence Sequences*, Math. Surveys Monogr. 104, Amer. Math. Soc., Providence, RI, 2003.
- [14] P. Ingram, *Elliptic divisibility sequences over certain curves*, J. Number Theory 123 (2007), 473–486.
- [15] P. Ingram, V. Mahé, J. H. Silverman, K. E. Stange, and M. Streng, *Algebraic divisibility sequences over function fields*, J. Austral. Math. Soc. 92 (2012), 99–126.
- [16] P. Ingram and J. H. Silverman, *Uniform estimates for primitive divisors in elliptic divisibility sequences*, in: Number Theory, Analysis and Geometry (in Memory of Serge Lang), Springer, Berlin, 2012, 243–271.
- [17] K. E. Lauter and K. E. Stange, *The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences*, in: Selected Areas in Cryptography, Lecture Notes in Comput. Sci. 5381, Springer, Berlin, 2009, 309–327.
- [18] Y. V. Matiyasevich, *Hilbert’s Tenth Problem*, Foundations of Computing Series, MIT Press, Cambridge, MA, 1993.
- [19] R. Shipsey, *Elliptic divisibility sequences*, Ph.D. thesis, Goldsmiths College, Univ. of London, 2000; [homepages.gold.ac.uk/rachel](http://homepages.gold.ac.uk/rachel).

- [20] J. H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory 30 (1988), 226–237.
- [21] J. H. Silverman, *Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups*, Monatsh. Math. 145 (2005), 333–350.
- [22] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, 2009.
- [23] M. Streng, *Divisibility sequences for elliptic curves with complex multiplication*, Algebra Number Theory 2 (2008), 183–208.
- [24] M. Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. 70 (1948), 31–74.

Gunther Cornelissen, Jonathan Reynolds  
Mathematisch Instituut  
Universiteit Utrecht  
Postbus 80.010  
3508 TA Utrecht, The Netherlands  
E-mail: g.cornelissen@uu.nl  
jonathan.reynolds@gmx.com

*Received on 9.8.2011  
and in revised form on 27.3.2012*

(6790)