Bull. Korean Math. Soc. **55** (2018), No. 3, pp. 763–776
https://doi.org/10.4134/BKMS.b170227
pISSN: 1015-8634 / eISSN: 2234-3016

OPERATIONS ON ELLIPTIC DIVISIBILITY SEQUENCES

Osman Bi̇zi̇m and Betül Gezer

Abstract. In this paper we consider the element-wise (Hadamard) product (or sum) of elliptic divisibility sequences and study the periodic structure of these sequences. We obtain that the element-wise product (or sum) of elliptic divisibility sequences are periodic modulo a prime p like linear recurrence sequences. Then we study periodicity properties of product sequences. We generalize our results to the case of modulo p^l for some prime $p > 3$ and positive integer l. Finally we consider the p-adic behavior of product sequences and give a generalization of [9, Theorem 4].

1. Introduction

Linear recurrence sequences have played crucial roles in number theory for many years. These sequences also appear in other mathematical disciplines and fields including cryptography, coding theory, approximation theory, and several branches of electrical engineering. But there are also recurrence sequences satisfying a nonlinear recurrence relation which arise as values of the division polynomials of an elliptic curve. Elliptic divisibility sequences (EDSs) were first introduced by M. Ward [14] and these are integer sequences (s_n) satisfying a nonlinear recurrence relation of the form

$$s_{m+n}s_{m-n} = s_{m+1}s_{m-1}s_n^2 - s_{n+1}s_{n-1}s_m^2 \tag{1.1}$$

and divisibility property

$$s_n | s_m \text{ whenever } n|m$$

for all $m \geq n \geq 1$. A solution of (1.1) is called proper if $s_0 = 0$, $s_1 = 1$ and $s_2s_3 \neq 0$. A proper solution will be an EDS if and only if s_2, s_3, s_4 are integers with $s_2|s_4$. It is also easy to prove that $s_{-n} = -s_n$ for all $n \in \mathbb{N}$.

Elliptic divisibility sequences are quite interesting because of the close relation with elliptic curves. These sequences are useful for solving the elliptic curve discrete logarithm problem in cryptography, at least in special cases; see [4], [7].

Received March 14, 2017; Revised February 22, 2018; Accepted March 8, 2018.
2010 *Mathematics Subject Classification.* 11B37, 11B83, 11G07.
Key words and phrases. elliptic divisibility sequences, operations on bilinear sequences, periodicity properties of product sequences, elliptic curves.

Elliptic divisibility sequences are generalizations of a class of linear recurrence sequences. Furthermore, a great many questions about linear recurrence sequences — for instance, prime factorization of their terms, appearance of prime terms, primitive divisors, and powers — have been asked for elliptic divisibility sequences. For more details, about elliptic divisibility sequences, see [3], [4], [8], [13], [14]. Various authors have also considered the behavior of linear recurrence sequences under the element-wise product (Hadamard) or sum of linear recurrence sequences [2], [5], [15], see also [4], [6]. In this work, in analogy with the element-wise product or sum of linear recurrence sequences we consider similar problems for elliptic divisibility sequences.

Both linear sequences and elliptic divisibility sequences belong to a larger class of sequences called bilinear sequences; see [4] for more details. It is well known that every linear sequence of order k is also a bilinear sequence of order k. Let (s_n) and (t_n) be bilinear recurrence sequences. The element-wise product sequence (u_n) (or sum sequence (v_n)) of (s_n) and (t_n) is defined by $u_n = s_n t_n$ (or $v_n = s_n + t_n$) for all $n \in \mathbb{N}$. It can easily be seen that the set of bilinear recurrence sequences is closed under this multiplication. Furthermore, if (s_n) and (t_n) are elliptic divisibility sequences, then (u_n) is a quaternary bilinear recurrence sequence which satisfies the recurrence relation

$$u_{n+4}u_{n-4} = \lambda_1 u_{n+3}u_{n-3} + \lambda_2 u_{n+2}u_{n-2} + \lambda_3 u_{n+1}u_{n-1} + \lambda_4 u_n^2, \tag{1.2}$$

where $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ are constants. Moreover, although the product and sum sequences are not elliptic divisibility sequences many similar results can be obtained for these sequences, for example, they are periodic sequences. In Section 2, it is shown that the product and sum sequences are periodic modulo a prime p, and the periodicity properties of product sequences are studied in Section 3. In Section 4, we generalize our results to the case of reduction modulo prime powers. Finally, in Section 5, the p-adic behavior of product sequences is considered and a generalization of [9, Theorem 4] is given.

2. Periodicity modulo p

A sequence (s_n) of rational integers is said to be *numerically periodic* modulo m if there exists a positive integer π such that

$$s_{n+\pi} \equiv s_n \pmod m \tag{2.1}$$

for all sufficiently large n. If (2.1) holds for all n, then (s_n) is said to be *purely periodic* modulo m. The smallest integer π for which (2.1) is true is called the *period* of (s_n) modulo m, and all other periods are multiples of it. An integer m said to be a *divisor* of the sequence (s_n) if it divides some term s_k with $k > 0$. If m divides s_k but does not divide s_l when l is a proper divisor of k, then k is called a *rank of apparition* of m in (s_n).

M. Ward showed that elliptic divisibility sequences modulo a prime are periodic, indeed EDSs are numerically periodic for any prime p and purely periodic for all primes which do not divide both s_3 and s_4 and the period is some multiple of the rank of apparition. Ward also proved that every prime p has exactly one rank of apparition r in (s_n) if and only if $\gcd(s_3, s_4) = 1$ and it satisfies $r \leq 2p + 1$.

The following theorem shows that if (s_n) and (t_n) are proper elliptic divisibility sequences, then the product and sum of these sequences is purely periodic for all primes which do not divide the terms s_3, s_4 and t_3, t_4. The proof of the theorem is similar to the proofs of [6, Theorems 6.61 and 6.70] for linear sequences.

Theorem 2.1. *Let (s_n) and (t_n) be purely periodic elliptic divisibility sequences modulo a prime p with periods π_1 and π_2, respectively. Then*

(i) *the element-wise product sequence (u_n) is also purely periodic modulo p, and its period π is a divisor of* $\operatorname{lcm}[\pi_1, \pi_2]$. *Furthermore if* $\gcd(\pi_1, \pi_2) = 1$, *then $\pi = \pi_1\pi_2$.*

(ii) *the element-wise sum sequence (v_n) is also purely periodic modulo p, and its period π is a divisor of* $\operatorname{lcm}[\pi_1, \pi_2]$. *Furthermore if* $\gcd(\pi_1, \pi_2) = 1$, *then $\pi = \pi_1\pi_2$.*

Proof. (i) If (s_n) and (t_n) are purely periodic elliptic divisibility sequences modulo a prime p with periods π_1 and π_2, respectively, then $\operatorname{lcm}[\pi_1, \pi_2]$ is a period of the sequences (s_n) and (t_n). Let $\rho = \operatorname{lcm}[\pi_1, \pi_2]$, then

$$u_{n+\rho} = s_{n+\rho}t_{n+\rho} \equiv s_n t_n = u_n \pmod p$$

for all n. It follows that the element-wise product sequence (u_n) is also purely periodic modulo p and moreover $\operatorname{lcm}[\pi_1, \pi_2]$ is a period of (u_n). Therefore the least period π of (u_n) divides $\operatorname{lcm}[\pi_1, \pi_2]$.

Let $\pi = k_1k_2$ where k_1 and k_2 are divisors of π_1, π_2 respectively. It is clear that $k_1\pi_2$ is a period of (u_n), that is,

$$u_{n+k_1\pi_2} = s_{n+k_1\pi_2}t_{n+k_1\pi_2} \equiv s_n t_n = u_n \pmod p$$

for all n. From the last congruence we have

$$s_{n+k_1\pi_2}t_n \equiv s_n t_n \pmod p \tag{2.2}$$

for all n, since $t_n \equiv t_{n+k_1\pi_2} \pmod p$ for all n. On the other hand there exists an integer k with $t_r \neq 0$ for all $r \equiv k \pmod{\pi_2}$, therefore

$$s_{r+k_1\pi_2} \equiv s_r \pmod p$$

for all such r by (2.2). Now let $\gcd(\pi_1, \pi_2) = 1$. Then we can choose an integer $m \geq n$ with $m \equiv n \pmod{\pi_1}$ and $m \equiv k \pmod{\pi_2}$ by the Chinese remainder theorem. Thus,

$$s_n \equiv s_m \equiv s_{m+k_1\pi_2} \equiv s_{n+k_1\pi_2} \pmod p$$

and hence $k_1\pi_2$ is a period of (s_n). It follows that $\pi_1 | k_1\pi_2$ and so $\pi_1 | k_1$ since $\gcd(\pi_1, \pi_2) = 1$. Therefore $k_1 = \pi_1$. Similarly, one can obtain that $k_2 = \pi_2$. Thus we derive that if $\gcd(\pi_1, \pi_2) = 1$, then $\pi = \pi_1\pi_2$.

(ii) As in the proof of part (i), one can show that the element-wise sum sequence (v_n) is also purely periodic modulo p and moreover $\operatorname{lcm}[\pi_1, \pi_2]$ is a period of (v_n). Hence, the least period π of (v_n) divides $\operatorname{lcm}[\pi_1, \pi_2]$.

Let $\pi = k_1 k_2$ where k_1 and k_2 are divisors of π_1, π_2 respectively. Now $k_1\pi_2$ is a period of (v_n), that is,

$$v_{n+k_1\pi_2} = s_{n+k_1\pi_2} + t_{n+k_1\pi_2} \equiv s_n + t_n = v_n \pmod p$$

for all n. On the other hand $t_n \equiv t_{n+k_1\pi_2} \pmod p$ for all n, and so $s_n \equiv s_{n+k_1\pi_2} \pmod p$ for all n. It follows that $\pi_1 | k_1\pi_2$ and if $\gcd(\pi_1, \pi_2) = 1$, then $\pi_1 | k_1$ and so $k_1 = \pi_1$. Similarly, one can show that $k_2 = \pi_2$. Thus we derive that if $\gcd(\pi_1, \pi_2) = 1$, then $\pi = \pi_1\pi_2$. □

In general, the finite product (or sum) of proper elliptic divisibility sequences is periodic modulo a prime.

Theorem 2.2. *Let $(s_{1n}), \ldots, (s_{mn})$ be purely periodic elliptic divisibility sequences modulo a prime p with periods $\pi_1, \ldots, \pi_m$ respectively. Then*

(i) *the element-wise product sequence (u_n) is also purely periodic modulo p, and its period π is a divisor of* $\operatorname{lcm}[\pi_1, \ldots, \pi_m]$. *Furthermore if $\pi_1, \ldots, \pi_m$ are pairwise relatively prime, then $\pi = \pi_1 \cdots \pi_m$.*

(ii) *the element-wise sum sequence (v_n) is also purely periodic modulo p, and its period π is a divisor of* $\operatorname{lcm}[\pi_1, \ldots, \pi_m]$. *Furthermore if $\pi_1, \ldots, \pi_m$ are pairwise relatively prime, then $\pi = \pi_1 \cdots \pi_m$.*

Proof. As a consequence of the above argument, we proved the theorem for the case $n = 2$ and the general case of the theorem follows easily by induction. □

3. Periodicity properties of product sequences

In this section we study the periodicity properties of product of two elliptic divisibility sequences and give some formulas for computing the least period of these sequences. Elliptic divisibility sequences possess certain periodicity properties named symmetry properties after M. Ward. These properties are given by Ward [14, Theorems 8.1, 8.2, and 9.2] in the following theorem.

Theorem 3.1. *Let (s_n) be an elliptic divisibility sequence, let p be an odd prime and suppose* $\gcd(p, s_2 s_3) = 1$. *Let r denote the rank of apparition of p in (s_n). Then there exist integers a, b, c with $ac \equiv 1 \pmod p$ such that for all non-negative integers n and k*

$$s_{r-n} \equiv a^n b s_n, \ s_{r+n} \equiv -bc^n s_n \pmod p \tag{3.1}$$

and

$$s_{rk+n} \equiv (-1)^k b^{k^2} c^{kn} s_n \pmod p. \tag{3.2}$$

Furthermore, the integers a and b satisfy the congruences

$$a \equiv \frac{s_{r-2}}{s_{r-1}s_2}, \ b \equiv \frac{s_{r-1}^2 s_2}{s_{r-2}} \text{ and } a^r b^2 \equiv 1 \pmod p.$$

As an immediate consequence of the above theorem we deduce the following corollary which will be used later.

Corollary 3.2. *Let (s_n) be an elliptic divisibility sequence. With the notation of Theorem 3.1, the following congruence holds for all non-negative integers n and k*

$$s_{rk-n} \equiv (-1)^{k+1} a^{kn} b^{k^2} s_n \pmod{p}. \tag{3.3}$$

Proof. We proceed by induction on k. If $k = 1$, then the result is true by Theorem 3.1. Now suppose that the result is true for $k = q$. Then the first congruence in (3.1) implies that

$$s_{(q+1)r-n} = s_{r-(n-rq)} \equiv a^{n-rq} b s_{n-rq} \pmod{p}$$

and hence

$$s_{(q+1)r-n} \equiv (-1) a^{n-rq} b s_{rq-n} \pmod{p}$$

since $s_{-n} = -s_n$ for all $n \in \mathbb{N}$. Then by the induction hypothesis we have

$$(-1)a^{n-rq} b (-1)^{q+1} a^{qn} b^{q^2} s_n \equiv (-1)^{q+2} a^{(q+1)n} a^{-rq} b^{q^2+1} s_n \pmod{p}.$$

Now as $a^r b^2 \equiv 1 \pmod{p}$ it follows that $a^{-rq} \equiv b^{2q} \pmod{p}$. Therefore

$$s_{(q+1)r-n} \equiv (-1)^{q+2} a^{(q+1)n} b^{(q+1)^2} s_n \pmod{p}.$$

Thus we proved the congruence (3.3) is true for $k = q + 1$. □

Now we study periodicity properties of product sequences. We give some congruences, theorems, and a simple useful lemma that will be needed. Let (s_n) and (t_n) be elliptic divisibility sequences, let p be an odd prime, and suppose that $\gcd(p, s_2 s_3) = 1$ and $\gcd(p, t_2 t_3) = 1$. Let r_1 and r_2 be the ranks of apparition of p in (s_n) and (t_n) respectively. Then by Theorem 3.1, there exist integers a_1, b_1 and a_2, b_2 with $a_1 c_1 \equiv 1$, $a_2 c_2 \equiv 1 \pmod{p}$ such that for all non-negative integers n and k_1, k_2

$$s_{r_1 k_1 + n} \equiv (-1)^{k_1} c_1^{k_1 n} b_1^{k_1^2} s_n \pmod{p}$$

and

$$t_{r_2 k_2 + n} \equiv (-1)^{k_2} c_2^{k_2 n} b_2^{k_2^2} t_n \pmod{p}.$$

Furthermore these integers satisfy the following congruences

$$a_1 \equiv \frac{s_{r_1-2}}{s_{r_1-1} s_2}, \ b_1 \equiv \frac{s_{r_1-1}^2 s_2}{s_{r_1-2}} \text{ and } a_1^{r_1} b_1^2 \equiv 1 \pmod{p} \tag{3.4}$$

and

$$a_2 \equiv \frac{t_{r_2-2}}{t_{r_2-1} t_2}, \ b_2 \equiv \frac{t_{r_2-1}^2 t_2}{t_{r_2-2}} \text{ and } a_2^{r_2} b_2^2 \equiv 1 \pmod{p}. \tag{3.5}$$

We will see that an element-wise product sequence of two purely periodic elliptic divisibility sequences is also periodic modulo a prime p and similar symmetry properties hold for the product sequences in the following theorems.

Theorem 3.3. *Let (u_n) denote the element-wise product sequence of the elliptic divisibility sequences (s_n) and (t_n). Suppose p is an odd prime which divides neither s_2t_2 nor s_3t_3. Let r_1 and r_2 be the ranks of apparition of p in (s_n) and (t_n), respectively and write $\operatorname{lcm}[r_1, r_2] = r^*$. Then there exist integers A, B, C with*

$$AC \equiv 1 \pmod p \tag{3.6}$$

such that for all non-negative integers n and k

$$u_{r^*-n} \equiv A^n B u_n, \; u_{r^*+n} \equiv BC^n u_n \pmod p \tag{3.7}$$

and

$$u_{r^*k+n} \equiv B^{k^2} C^{kn} u_n \pmod p. \tag{3.8}$$

The integers can be computed from the congruences

$$A \equiv a_1^{k_1} a_2^{k_2} \text{ and } B \equiv (-1)^{k_1+k_2} b_1^{k_1^2} b_2^{k_2^2} \pmod p,$$

where a_1, a_2 and b_1, b_2 are the integers specified in (3.4) and (3.5) for the elliptic divisibility sequences (s_n) and (t_n), respectively and $k_1 = r^*/r_1$, $k_2 = r^*/r_2$. Furthermore, the following congruences hold

$$A \equiv \frac{u_{r^*-2}}{u_{r^*-1}u_2}, \; B \equiv \frac{u_{r^*-1}^2 u_2}{u_{r^*-2}} \text{ and } A^{r^*} B^2 \equiv 1 \pmod p. \tag{3.9}$$

Proof. By Corollary 3.2 and Theorem 3.1, we have

$$s_{r^*-n} \equiv (-1)^{k_1+1} a_1^{k_1 n} b_1^{k_1^2} s_n \text{ and } s_{r^*+n} \equiv (-1)^{k_1} c_1^{k_1 n} b_1^{k_1^2} s_n \pmod p$$

and

$$t_{r^*-n} \equiv (-1)^{k_2+1} a_2^{k_2 n} b_2^{k_2^2} t_n \text{ and } t_{r^*+n} \equiv (-1)^{k_2} c_2^{k_2 n} b_2^{k_2^2} t_n \pmod p,$$

where $r^* = \operatorname{lcm}[r_1, r_2]$ and $k_1 = r^*/r_1$, $k_2 = r^*/r_2$. Therefore

$$u_{r^*-n} \equiv (-1)^{k_1+k_2} a_1^{k_1 n} a_2^{k_2 n} b_1^{k_1^2} b_2^{k_2^2} u_n \equiv A^n B u_n \pmod p$$

and

$$u_{r^*+n} \equiv (-1)^{k_1+k_2} c_1^{k_1 n} c_2^{k_2 n} b_1^{k_1^2} b_2^{k_2^2} u_n \equiv BC^n u_n \pmod p,$$

where

$$A \equiv a_1^{k_1} a_2^{k_2}, \; B \equiv (-1)^{k_1+k_2} b_1^{k_1^2} b_2^{k_2^2} \text{ and } C \equiv c_1^{k_1} c_2^{k_2} \pmod p.$$

Thus we have proved (3.7). The values A and B for the element-wise product sequence (u_n) can be obtained by setting $n = 1$ and then $n = 2$ in the first congruence of (3.7) which gives the first part of (3.9). By setting $n = 1$ and then $n = r^* - 1$ in the first congruence of (3.7) we obtain $A^{r^*} B^2 \equiv 1 \pmod p$ which gives the second part of (3.9). Finally, the last congruence of (3.9) and the congruence (3.6) implies that $B^2 \equiv C^{r^*} \pmod p$, so the congruence (3.8) can be proved by induction on k and using the fact that $B^2 \equiv C^{r^*} \pmod p$. □

Theorem 3.4. *Let (u_n) denote the element-wise product sequence of the elliptic divisibility sequences (s_n) and (t_n). Let p be an odd prime which divides neither s_2t_2 nor s_3t_3. Let r_1 and r_2 be the ranks of apparition of p in (s_n) and (t_n), respectively and write* $\operatorname{lcm}[r_1, r_2] = r^*$. *Let τ be the least integer such that*

$$B^{\tau^2} \equiv 1,\ C^{\tau} \equiv 1 \pmod p. \tag{3.10}$$

Then (u_n) is purely periodic modulo p with period τr^*.

Proof. If τ is the defined as in the theorem and if k is an integer such that

$$B^{k^2} \equiv 1,\ C^{k} \equiv 1 \pmod p,$$

then it can easily be seen that τ divides k. The congruence (3.8) implies that

$$u_{r^*\tau+n} \equiv B^{\tau^2} C^{\tau n} u_n \pmod p$$

and hence (u_n) is purely periodic modulo p with period dividing τr^*.

Now since $u_n \equiv 0 \pmod p$ if and only if $n \equiv 0 \pmod{r^*}$, the period must be a multiple of r^*. For instance, if $\pi = mr^*$, then $m|\tau$. On the other hand, by (3.8) we have

$$u_n \equiv u_{mr^*+n} \equiv B^{m^2} C^{mn} u_n \pmod p$$

and hence $B^{m^2} C^{mn} \equiv 1 \pmod p$ for all non-negative integers n. By putting $n = 1$ and then $n = 2$ in the last congruence we obtain $C^m \equiv 1 \pmod p$ and so $B^{m^2} \equiv 1 \pmod p$. Therefore $m \geq \tau$ and hence $m = \tau$. □

The intimate relation between the rank of apparition and period of an EDS is given by the following periodicity theorem.

Theorem 3.5 ([14]). *Let (s_n) be an EDS and p be an odd prime whose rank of apparition r is greater than 3. Let e be an integral solution of the congruence $e \equiv s_2/s_{r-2} \pmod p$ and let ε and κ be the least positive integers such that $e^{\varepsilon} \equiv 1$ and $s_{r-1}^{\kappa} \equiv 1 \pmod p$, respectively. Then (s_n) is purely periodic modulo p, and its period π is given by the formula $\pi(s_n) = \tau r$ where $\tau = 2^{\alpha} \operatorname{lcm}[\varepsilon,\ \kappa]$ and the exponent α is determined as follows*:

$$\alpha = \begin{cases} +1 & \text{if } \varepsilon \text{ and } \kappa \text{ are both odd,} \\ -1 & \text{if } \varepsilon \text{ and } \kappa \text{ are both even and both divisible} \\ & \text{by exactly the same power of } 2, \\ 0 & \text{otherwise.} \end{cases}$$

We state a lemma to prove the main periodicity theorem for the product sequences.

Lemma 3.1 ([14]). *Let p be an odd prime and d be an integer with* $\gcd(p, d) = 1$. *Let δ be the least positive integer such that $d^{\delta} \equiv 1 \pmod p$. Then if δ is odd, there exists no integer x such that the congruence $d^x \equiv -1 \pmod p$ is satisfied. But if δ is even the last congruence is satisfied if and only if x is an odd multiple of $\delta/2$.*

In the following theorem we see that periodicity properties similar to those in Theorem 3.5 hold for product sequences, moreover the period of a product sequence is determined by the relation between the ranks and periods of the given elliptic divisibility sequences.

Theorem 3.6. *Let (u_n) denote the element-wise product sequence of the elliptic divisibility sequences (s_n) and (t_n). Let p be an odd prime which divides neither s_2t_2 nor s_3t_3. Let r_1 and r_2 be the ranks of apparition of p in (s_n) and (t_n), respectively and write* $\operatorname{lcm}[r_1, r_2] = r^*$. *Let E be an integral solution of the congruence*

$$E \equiv \frac{u_2}{u_{r^*-2}} \pmod{p} \tag{3.11}$$

and let ε and κ be the least positive integers such that $E^\varepsilon \equiv 1, u_{r^*-1}^{\kappa} \equiv 1$ $(\bmod\, p)$, respectively. Then (u_n) is purely periodic modulo p with period τr^* where $\tau = 2^\alpha \operatorname{lcm}[\varepsilon, \kappa]$ and

$$\alpha = \begin{cases} -1 & \text{if } \varepsilon \text{ and } \kappa \text{ are both even and both divisible} \\ & \text{by } 2^x \text{ with exactly the same power } x \geq 2, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. First observe that the congruences (3.6), (3.9) and (3.11) imply that

$$E \equiv \frac{C}{u_{r^*-1}} \equiv \frac{C^2}{B} \pmod{p} \tag{3.12}$$

and hence

$$B \equiv C u_{r^*-1} \pmod{p}. \tag{3.13}$$

Then by (3.12) and (3.13) we obtain

$$E^\tau u_{r^*-1}^\tau \equiv 1 \pmod{p} \tag{3.14}$$

and

$$B^\tau \equiv u_{r^*-1}^\tau (\bmod\, p) \tag{3.15}$$

since τ is the smallest integer such that $C^\tau \equiv 1 \pmod{p}$ by (3.10). On the other hand, as $C^\tau \equiv 1 \pmod{p}$, we have $C^{\tau r^*} \equiv 1 \pmod{p}$. Then we derive that

$$C^{\tau r^*} \equiv B^{2\tau} \equiv 1 \pmod{p},$$

since $C^{r^*} \equiv B^2 \pmod{p}$ by (3.9) and (3.6). It follows that $B^\tau \equiv 1$ or $B^\tau \equiv -1$ $(\bmod\, p)$.

Now suppose that $B^\tau \equiv 1 \pmod{p}$. Then by (3.15)

$$u_{r^*-1}^\tau \equiv 1 \pmod{p} \tag{3.16}$$

and hence

$$E^\tau \equiv 1 \pmod{p} \tag{3.17}$$

by (3.14). Now let ε and κ be the least positive integers such that $E^\varepsilon \equiv 1$, $u_{r^*-1}^{\kappa} \equiv 1 \pmod{p}$, and let $\sigma = \operatorname{lcm}[\varepsilon, \kappa]$. Then the congruences (3.16) and

(3.17) imply that $\varepsilon|\tau$ and $\kappa|\tau$, and hence $\sigma|\tau$. Furthermore, $u_{r^*-1}^{\sigma} \equiv 1$ and $E^{\sigma} \equiv 1 \pmod{p}$. Then by (3.12) and (3.13) we have

$$C^{\sigma} \equiv 1 \text{ and } B^{\sigma} \equiv 1 \pmod{p}.$$

The last congruence implies that $B^{\sigma^2} \equiv 1 \pmod{p}$. Then $\tau|\sigma$ since τ is the smallest integer such that $B^{\tau^2} \equiv 1$, $C^{\tau} \equiv 1 \pmod{p}$. Hence $\tau = \sigma$.

Now suppose that $B^{\tau} \equiv -1 \pmod{p}$. Then by (3.10), $B^{\tau^2} \equiv (B^{\tau})^{\tau} \equiv (-1)^{\tau} \equiv 1 \pmod{p}$. Therefore τ must be even. On the other hand (3.15) implies that $u_{r^*-1}^{\tau} \equiv -1 \pmod{p}$, and so $E^{\tau} \equiv -1 \pmod{p}$ by (3.14). By Lemma 3.1, ε and κ are both even and τ is an odd multiple of both $\varepsilon/2$ and $\kappa/2$. Therefore ε and κ are both even and both divisible by 2^x with exactly the same power $x \geq 2$ since τ is even. Now write $\sigma = \frac{1}{2}\operatorname{lcm}[\varepsilon, \kappa]$ then $\sigma|\tau$. By Lemma 3.1, σ is an odd multiple of both $\varepsilon/2$ and $\kappa/2$, that is, $\sigma = \frac{\varepsilon}{2}m$ and $\sigma = \frac{\kappa}{2}n$ for odd integers m, n. Conversely, if ε and κ are both even and both divisible by 2^x with exactly the same power $x \geq 2$, then σ is an odd multiple of both $\frac{\varepsilon}{2}$ and $\frac{\kappa}{2}$. Then by Lemma 3.1,

$$u_{r^*-1}^{\sigma} \equiv -1, \; E^{\sigma} \equiv -1 \pmod{p}.$$

Thus by (3.12) and (3.13)

$$C^{\sigma} \equiv 1, \; B^{\sigma} \equiv -1 \pmod{p}.$$

As σ is always even, $B^{\sigma^2} \equiv 1 \pmod{p}$ and so it can easily be seen that $\tau|\sigma$. Hence $\tau = \sigma$. □

4. Periodicity modulo p^l

In [13], Ward considers elliptic divisibility sequences modulo p^l for primes p greater than three with ranks of apparition greater than three and positive integers l. Ward called such primes *regular* and proved that if $r > 3$ is the rank of a regular prime in an elliptic divisibility sequence (s_n) and p^k is the highest power of p dividing s_r, then the rank of apparition of p^l in (s_n) is r or $p^{l-k}r$ according as $l \leq k$ or $l > k$ by using the elliptic function theory.

Shipsey [7] considers periodicity properties of elliptic divisibility sequence (s_n) modulo p^2 for some prime $p > 3$. She gave a symmetry formula for the value of s_{mr} modulo p^2 for $m \geq 1$, where r is the rank of apparition of p in (s_n) [7, Theorem 3.5.4]. Then she obtains the periodicity of the sequence $(s_{mr})_{m\geq 1}$ modulo p^2 by using the symmetry formula. Ayad [1] and Swart [12], generalize Shipsey's symmetry properties to the case of modulo p^l for some prime $p > 3$ and positive integer l.

Theorem 4.1 ([1], [12]). *Let (s_n) be an elliptic divisibility sequence and let $p > 3$ be a regular prime whose rank of apparition in (s_n) is $r > 3$. Let the rank of apparition of p^l in (s_n) be r_l. Then there exist integers b_l, c_l such that for all non-negative integers n and k*

$$s_{r_l+n} \equiv -b_l c_l^n s_n \pmod{p^l}$$

and

$$s_{r_l k+n} \equiv (-1)^{k^2} b_l^{k^2} c_l^{kn} s_n \pmod{p^l},$$

where

$$b_l \equiv \frac{s_{r_l-1}^2 s_2}{s_{r_l-2}},\ c_l \equiv \frac{s_{r_l-1} s_2}{s_{r_l-2}} \pmod{p^l}.$$

In this section we consider the element-wise product of two elliptic divisibility sequences modulo p^l for some prime $p > 3$ and positive integer l and obtain similar periodicity properties for the element-wise product sequences. The proofs are elementary and are based on the proofs of Theorems 3.3, 3.4 and 3.6.

Theorem 4.2. *Let (u_n) denote the element-wise product sequence of the elliptic divisibility sequences (s_n) and (t_n). Suppose p is a regular prime greater than three. Let r_1, $r_2 > 3$ be the ranks of apparition of p in (s_n) and (t_n), respectively and write $p^{l-1}\operatorname{lcm}[r_1, r_2] = r_l^*$. Then there exist integers B_l, C_l such that for all non-negative integers n and k*

$$u_{r_l^*+n} \equiv B_l C_l^n u_n \pmod{p^l}$$

and

$$u_{r_l^* k+n} \equiv B_l^{k^2} C_l^{kn} u_n \pmod{p^l}.$$

Furthermore the integers can be computed from the congruences

$$B_l \equiv \frac{u_{r_l^*-1}^2 u_2}{u_{r_l^*-2}} \text{ and } C_l \equiv \frac{u_{r_l^*-1} u_2}{u_{r_l^*-2}} \pmod{p^l}.$$

Theorem 4.3. *Let (u_n) denote the element-wise product sequence of the elliptic divisibility sequences (s_n) and (t_n). Suppose p is a regular prime greater than three. Let r_1, $r_2 > 3$ be the ranks of apparition of p in (s_n) and (t_n), respectively and write $p^{l-1}\operatorname{lcm}[r_1, r_2] = r_l^*$. Let τ_l be the least integer such that*

$$B_l^{\tau_l^2} \equiv 1,\ C_l^{\tau_l} \equiv 1 \pmod{p^l}.$$

Then (u_n) is purely periodic modulo p^l with period $\tau_l r_l^*$.

Theorem 4.4. *Let (u_n) denote the element-wise product sequence of the elliptic divisibility sequences (s_n) and (t_n). Suppose p is a regular prime greater than three. Let r_1, $r_2 > 3$ be the ranks of apparition of p in (s_n) and (t_n), respectively and write $p^{l-1}\operatorname{lcm}[r_1, r_2] = r_l^*$. Let E_l be an integral solution of the congruence*

$$E_l \equiv \frac{u_2}{u_{r_l^*-2}} \pmod{p^l} \tag{4.1}$$

and let ε_l and κ_l be the least positive integers such that $E_l^{\varepsilon} \equiv 1$, $u_{r_l^*-1}^{\kappa} \equiv 1$ $(\operatorname{mod} p^l)$, respectively. Then (u_n) is purely periodic modulo p^l with period $\tau_l r_l^*$ where $\tau_l = 2^{\alpha_l}\operatorname{lcm}[\varepsilon_l, \kappa_l]$ and

$$\alpha_l = \begin{cases} -1 & \text{if } \varepsilon \text{ and } \kappa \text{ are both even and both divisible} \\ & \text{by } 2^x \text{ with exactly the same power } x \geq 2, \\ 0 & \text{otherwise.} \end{cases}$$

We can generalize Theorems 2.1 and 2.2 to the case of modulo p^l for some prime $p > 3$ and positive integer l. The proofs are elementary and are similar to that of Theorems 2.1 and 2.2.

Theorem 4.5. *Let (s_n) and (t_n) be purely periodic elliptic divisibility sequences modulo a prime power p^l with periods π_1 and π_2, respectively. Then*

(i) *the element-wise product sequence (u_n) is also purely periodic modulo p^l, and its period π is a divisor of* $\operatorname{lcm}[\pi_1, \pi_2]$. *Furthermore if* $\gcd(\pi_1, \pi_2) = 1$, *then $\pi = \pi_1\pi_2$.*

(ii) *the element-wise sum sequence (v_n) is also purely periodic modulo p^l with period* $\operatorname{lcm}[\pi_1, \pi_2]$. *Furthermore if* $\gcd(\pi_1, \pi_2) = 1$, *then $\pi = \pi_1\pi_2$.*

In general, the finite product (or sum) of proper elliptic divisibility sequences is periodic modulo a prime power.

Theorem 4.6. *Let $(s_{1n}), \dots, (s_{mn})$ be purely periodic elliptic divisibility sequences modulo a prime p^l with periods $\pi_1, \dots, \pi_m$, respectively. Then*

(i) *the element-wise product sequence (u_n) is also purely periodic modulo p^l and its period π is a divisor of* $\operatorname{lcm}[\pi_1, \dots, \pi_m]$. *Furthermore if $\pi_1, \dots, \pi_m$ are pairwise relatively prime, then $\pi = \pi_1 \cdots \pi_m$.*

(ii) *the element-wise sum sequence (v_n) is also purely periodic modulo p^l with period* $\operatorname{lcm}[\pi_1, \dots, \pi_m]$. *Furthermore if $\pi_1, \dots, \pi_m$ are pairwise relatively prime, then $\pi = \pi_1 \cdots \pi_m$.*

5. *p*-adic convergence of product sequences

Consider an elliptic curve $E(K)$ defined over a field K by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The *division polynomials* $\psi_n \in \mathbb{Z}[a_1, \dots, a_6, x, y]$ for the curve E are defined using the initial values

$$\psi_1 = 1,$$

$$\psi_2 = 2y + a_1x + a_3,$$

$$\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,$$

$$\psi_4 = \psi_2(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)),$$

where b_i are the usual quantities [10, Chapter III.1] and by the formulas

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \qquad \text{for } m \geq 2,$$

$$\psi_{2m}\psi_2 = \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^3 \quad \text{for } m \geq 3.$$

The n-th division polynomial ψ_n has divisor

$$\sum_{T \, \in \, E[n]} (T) - n^2(\mathcal{O}),$$

where $E[n]$ is the n-torsion subgroup of $E(K)$. The basic properties of division polynomials can be found in [10]. These polynomials arises in expressing the coordinates of nP in terms of a point $P \in E(K)$. Ward [14] proved that a proper elliptic divisibility sequence (s_n) is associated an elliptic curve E and a point $P \in E(\mathbb{Q})$. Furthermore, he showed that these sequences arise as values of the division polynomials $\psi_n(P)_{n\geq 1}$ where $\psi_n(P)_{n\geq 1}$ is evaluated at the point $P = (x, y)$ of ψ_n. Silverman [9] considered the sequence of values $\psi_n(P)_{n\geq 1}$ of division polynomials. Silverman [9, Theorem 1] used a lift to characteristic zero and the Lefschetz principle to prove that the division polynomials over finite fields form a purely periodic sequence, which is inspired by a similar result of Ward for elliptic divisibility sequences. Theorem 2 of [9] uses the Mazur-Tate p-adic σ-function to prove that there is a power $q = p^e$ for which the sequence $(\psi_{mq^k}(P))$ converges as $k \to \infty$ in $\mathbb{Z}_p$ for all $m \geq 1$, in addition, if E and P are defined over $\mathbb{Q}$, then the limit of this sequence is algebraic over $\mathbb{Q}$, and in an addendum Silverman connects this result with Ayad's work [1]. In [9, Theorem 3], the periodicity of these sequences modulo prime powers is proved by using similar techniques in the proof of [9, Theorem 2]. As an application, Silverman partially answered a question, which was raised in [11], about the p-adic behavior of elliptic divisibility sequences [9, Theorem 4]. More precisely; Theorem 4 of [9] says that if (s_n) is a proper elliptic divisibility sequence and the associated elliptic curve E is non-singular, and does not have complex multiplication, then for almost all primes p, in the sense of density, the following two statements are true.

(i) There is an exponent $N = N_p \geq 1$ so that for every $m \geq 1$, the limit

$$\lim_{k\to\infty} s_{mp^{kN}} \quad \text{converges in } \mathbb{Z}_p.$$

(ii) The limit given by (i) is algebraic over $\mathbb{Q}$.

Theorems 4.5 and 4.6 show that an element-wise product sequence of proper elliptic divisibility sequences is purely periodic modulo p^l for some prime $p > 3$ and positive integer l. The periodicity of the product sequences modulo prime powers raises a question about the p-adic behavior of product sequences. The following theorem is a generalization of [9, Theorem 4] to the case of a product of proper elliptic divisibility sequences.

Theorem 5.1. *Let (s_n) and (t_n) be proper elliptic divisibility sequences and let (u_n) be element-wise product of (s_n) and (t_n). Let S and T be sets of primes such that the associated elliptic curves to these sequences are non-singular and do not have complex multiplication, respectively. Then for almost all primes $p \in S \cap T$, in the sense of arithmetic density, the following statements are true.*

(i) *There is an exponent $N = N_p \geq 1$ so that for every $m \geq 1$, the limit*

$$\lim_{k\to\infty} u_{mp^{kN}} \quad \textit{converges in } \mathbb{Z}_p.$$

(ii) *The limit is algebraic over $\mathbb{Q}$.*

Proof. Let $P(k)$ be the set of all primes less than k and let $S(k)$ be the subset of $P(k)$ such that the statements (i) and (ii) are true. Then the expression "almost all primes in S, in the sense of arithmetic density" means that

$$\lim_{k\to\infty} \frac{|S(k)|}{|P(k)|} = 1.$$

If the statements (i) and (ii) are true for almost all primes in S and T, in the sense of arithmetic density, then the statements (i) and (ii) are true for almost all primes in $S \cap T$. Indeed,

$$\lim_{k\to\infty} \frac{|S(k) \cup T(k)|}{|P(k)|} = 1$$

since $\lim_{k\to\infty} \frac{|S(k)|}{|P(k)|} = \lim_{k\to\infty} \frac{|T(k)|}{|P(k)|} = 1$, and therefore

$$\lim_{k\to\infty} \frac{|S(k) \cap T(k)|}{|P(k)|} = 1$$

since $|S(k) \cup T(k)| = |S(k)| + |T(k)| - |S(k) \cap T(k)|$.

On the other hand, it can easily be seen that if (x_n) and (y_n) are any convergent sequences in $\mathbb{Z}_p$, then the product sequence $(x_n y_n)$ is a convergent sequence in $\mathbb{Z}_p$, and the equation

$$\lim_{n\to\infty} (x_n y_n) = \lim_{n\to\infty} (x_n) \lim_{n\to\infty} (y_n)$$

holds in $\mathbb{Z}_p$. Moreover if the limits $\lim_{n\to\infty}(x_n)$ and $\lim_{n\to\infty}(y_n)$ are algebraic numbers, then the limit $\lim_{n\to\infty}(x_n y_n)$ is an algebraic number since the product of two algebraic numbers is algebraic.

By Theorem 4.5, the product sequence (u_n) is purely periodic modulo a prime power and so the proof follows from the choice of the primes and [9, Theorem 4]. □

As a consequence of the above theorem we have the following corollary.

Corollary 5.2. *Let $(s_{1n}), \ldots, (s_{mn})$ be proper elliptic divisibility sequences and let (u_n) be element-wise product of these sequences. Let $S_1, \ldots, S_m$ be sets of primes such that the associated elliptic curves to these sequences are non-singular and do not have complex multiplication, respectively. Then for almost all primes $p \in S_1 \cap \cdots \cap S_m$, in the sense of arithmetic density, the following statements are true.*

(i) *There is an exponent $N = N_p \geq 1$ so that for every $m \geq 1$, the limit*

$$\lim_{k\to\infty} u_{mp^{kN}} \quad \textit{converges in } \mathbb{Z}_p.$$

(ii) *The limit is algebraic over $\mathbb{Q}$.*

Acknowledgements. The authors would like to thank the anonymous reviewer for valuable comments and suggestions to improve the quality of the paper.

References

[1] M. Ayad, *Périodicité* (*mod q*) *des suites elliptiques et points S-entiers sur les courbes elliptiques*, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 3, 585–618.

[2] U. Cerruti and F. Vaccarino, *R-algebras of linear recurrent sequences*, J. Algebra **175** (1995), no. 1, 332–338.

[3] D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Adv. in Appl. Math. **7** (1986), no. 4, 385–434.

[4] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs, **104**, American Mathematical Society, Providence, RI, 2003.

[5] R. Göttfert and H. Niederreiter, *On the minimal polynomial of the product of linear recurring sequences*, Finite Fields Appl. **1** (1995), no. 2, 204–218.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, **20**, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983.

[7] R. Shipsey, *Elliptic divisibility sequences*, Ph. D. thesis, Goldsmith's (University of London), 2000.

[8] J. H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237.

[9] ———, *p-adic properties of division polynomials and elliptic divisibility sequences*, Math. Ann. **332** (2005), no. 2, 443–471, and addendum 473–474.

[10] ———, *The Arithmetic of Elliptic Curves*, second edition, Graduate Texts in Mathematics, **106**, Springer, Dordrecht, 2009.

[11] J. H. Silverman and N. Stephens, *The sign of an elliptic divisibility sequence*, J. Ramanujan Math. Soc. **21** (2006), no. 1, 1–17.

[12] C. S. Swart, *Elliptic curves and related sequences*, Ph. D. thesis, Royal Holloway (University of London), 2003.

[13] M. Ward, *The law of repetition of primes in an elliptic divisibility sequence*, Duke Math. J. **15** (1948), 941–946.

[14] ———, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948), 31–74.

[15] N. Zierler and W. H. Mills, *Products of linear recurring sequences*, J. Algebra **27** (1973), 147–157.

Osman Bizim
Uludag University
Faculty of Science
Department of Mathematics
Görükle, 16059, Bursa-Turkey
Email address: `obizim@uludag.edu.tr`

Betül Gezer
Uludag University
Faculty of Science
Department of Mathematics
Görükle, 16059, Bursa-Turkey
Email address: `betulgezer@uludag.edu.tr`