Publ. Math. Debrecen
Manuscript (August 26, 2013)

On common factors within a series of consecutive terms of an elliptic divisibility sequence

By Lajos Hajdu[1] and Márton Szikszai[2]

Dedicated to Professor Lajos Tamássy on the occasion of his 90th birthday

Abstract. We prove that for any elliptic divisibility sequence and any sufficiently large integer k, one can find k consecutive terms of the sequence such that none of these terms is coprime to all the others. In other words, elliptic divisibility sequences are *Pillai sequences*, named for a problem posed originally by Pillai for the sequence of integers. In fact we give an upper bound for the smallest value k_0 past which this property is valid. We also provide a more general theorem where the coprimality condition is severely relaxed. In case of some particular sequences we give the values of k_0, as well.

1. Introduction

Elliptic divisibility sequences have a long history and a large literature. Already the definition of such sequences has several variants. We shall use the

Mathematics Subject Classification: Primary 11B39.
Key words and phrases: Elliptic divisibility sequences, greatest common divisor, Pillai's problem.
[1]Research supported in part by the OTKA grants K75566, K100339 and NK101680, and by the TÁMOP 4.2.1./B-09/1/KONV-2010-0007 project. The project is implemented through the New Hungary Development Plan, cofinanced by the European Social Fund and the European Regional Development Fund. The publication is supported by the TÁMOP-4.2.2.C-11/1/KONV-2012-0001 project. The project has been supported by the European Union, co-financed by the European Social Fund.
[2]The work/publication is supported by the TÁMOP-4.2.2/B-10/1-2010-0024 project. The project is co-financed by the European Union and the European Social Fund.

version from a paper of Everest, Mclaren and Ward [9]. That is, by an elliptic divisibility sequence we mean the following. Take an elliptic curve E over $\mathbb{Q}$ given in generalized Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ with } a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}, \qquad (1)$$

and let $P = (x(P), y(P))$ be a non-torsion rational point on E. (For the background and basic properties of elliptic curves see e.g. [5, 13, 26, 31]). For any non-zero integer n write $x(nP) = A_n/B_n$ in lowest terms, with $A_n \in \mathbb{Z}$ and $B_n \in \mathbb{N}$. Throughout the paper the sequence $B = B(E, P) = (B_n)_{n=1}^{\infty}$ is called an elliptic divisibility sequence. As noted in [9], this terminology follows a suggestion of Silverman. The term has also been used for more general sequences related to rational points on elliptic curves (see e.g. Ward [36] and Silverman [30]). Furthermore, note that as is well-known, B_n is a full square for all $n \geq 1$. We would like to emphasize that in several papers the sequence $\pm\sqrt{B_n}$ is considered as an elliptic divisibility sequence, where the sign is chosen in an appropriate way (which is itself of particular interest - see the paper of Silverman and Stephens [32]). However, since for our purposes only the prime divisors of B_n are important and their powers are in fact irrelevant, we stick to the above definition of elliptic divisibility sequences throughout the paper.

The arithmetic properties of elliptic divisibility sequences were first studied in detail by Ward [36, 37]. Since then several authors achieved many interesting results, concerning various properties of such sequences. Instead of trying to survey the related literature (which would be an enormous task), we only refer the interested reader to the papers [6, 7, 8, 10, 11, 12, 15, 23, 25, 28, 29, 30, 32, 34, 35] and the references therein.

In this paper we investigate a new property of elliptic divisibility sequences. Let $u = (u_n)_{n=1}^{\infty}$ be a sequence of integers. Write g_u for the smallest $k \geq 2$ (if it exists) such that there exist k consecutive terms of u with the property that none of them is coprime to all the others. Further, write G_u for the smallest $k_0 \geq 2$ (if it exists) such that for any $k \geq k_0$ one can find k consecutive terms of u with the above property. Obviously, these quantities do not always exist. However, if G_u exists then so does g_u, and we have $g_u \leq G_u$. Sequences u for which G_u exists are called Pillai sequences (see [17]) after Pillai, who was the first to investigate this property in $\mathbb{N}$ (i.e. in the increasing sequence of positive integers). Due to Pillai's classical result from [22] and by a nice theorem of Brauer [3], we have that $\mathbb{N}$ is a Pillai sequence, with $g_{\mathbb{N}} = G_{\mathbb{N}} = 17$. Later, Ohtomo and Tamari [21] proved that for any coprime integers a, b the arithmetic progression $an+b$ $(n \geq 1)$ is also a Pillai sequence. Recently, Hajdu and Szikszai [17] together with other

related results proved that Lucas and Lehmer sequences of the first kind are Pillai sequences, as well. However, they also demonstrated that being a Pillai sequence is a special property, at least Lucas and Lehmer sequences of the second kind do not have this property in general. In the present paper we show that elliptic divisibility sequences are also Pillai sequences. Further, we prove a more general theorem about the so-called T-Pillai property of such sequences. (We provide the precise definitions in the next section.) Moreover, we explicitly give the values g_B and G_B for several particular elliptic divisibility sequences B. Our results rely on divisibility properties of elliptic divisibility sequences shown by Everest, Mclaren and Ward [9], a classical theorem of Baker [2] bounding the solutions of elliptic diophantine equations, a theorem of Ingram and Silverman [19] concerning the existence of primitive prime divisors of B, and results and algorithms of Hajdu and Saradha [16] and Hajdu and Szikszai [17] concerning the T-Pillai property.

We organize the paper in the following way. In the next section we give our results (together with some new notions and notation). Since we need several lemmas to prove our theorems, we give them separately, in the third section. Then in the final section we provide the proofs of our theorems.

2. New results

Our principal result is the following.

Theorem 2.1. *Every elliptic divisibility sequence $B = B(E, P) = (B_n)_{n=1}^{\infty}$ is a Pillai sequence. Further, we have $G_B \leq C_1(E)$, where $C_1(E)$ is an explicitly computable constant depending only on E.*

Remark 1. As one can notice, the upper bound $C_1(E)$ is independent of the point P. It is an interesting question how far this "uniformity" can be extended. In our arguments the critical point is to give a bound for the number N of integral points on an elliptic curve. Already the classical result of Baker [2] implies the finiteness of such points, in terms of the coefficients a_1, a_2, a_3, a_4, a_6, appearing in (1). Hence in fact one could replace $C_1(E)$ by $C_1(a_1, a_2, a_3, a_4, a_6)$. Further, by a conjecture of Lang (see [20], p. 140), N should be bounded in terms of the rank of E only, provided that the above model for E is so-called quasiminimal. This conjecture has been proved to be true by Silverman [27] if E has integral j-invariant, while Hindry and Silverman [18] showed that Lang's conjecture is implied by the ABC conjecture. So if we assume that E is given by a quasiminimal model and it has integral j-invariant, then $C_1(E)$ can be replaced by $C_1(r)$, where

r denotes the rank of E. The same is true if we assume Lang's conjecture or the ABC-conjecture.

Our next theorem provides the exact values of G_B for certain "interesting" elliptic divisibility sequences B from the literature. More precisely, we consider the sequences given in Examples 2-5 in [32], as the "simplest" examples of elliptic divisibility sequences. Note that in [32] in our notation the authors work with the sequence $\pm\sqrt{B_n}$. However, as we have already mentioned, this does not yield any difference from our viewpoint. We also mention that the background data (that is the corresponding elliptic curve E and point P) indicated in Table 1 are given in [32]. In fact in [32] two more examples are given. However, Example 1 and Example 2 coincide, while Example 6 concerns a "degenerate" situation, so we do not include it here. Finally, we mention that our method would work for other elliptic divisibility sequences, as well. We just pick up these sequences because they appear in the literature, and they are the "simplest" ones in some sense.

Theorem 2.2. *Table 1 gives the explicit values of g_B and G_B for elliptic divisibility sequences $B = B(E, P)$ for the indicated specific choices for E and P.*

E	$P = (x(P), y(P))$	g_B	G_B
$y^2 + y = x^3 - x$	$(0, 0)$	79	79
$y^2 + y = x^3 + x^2$	$(0, 0)$	81	81
$y^2 + xy = x^3 - x^2 - x + 1$	$(1, 0)$	47	47
$y^2 + xy = x^3 - 2x + 1$	$(1, 0)$	81	81

Table 1. The values of g_B and G_B for certain elliptic divisibility sequences.

Remark 2. Note that for the four sequences B appearing in Theorem 2.2 we have $g_B = G_B$. The coincidence of these parameters seems to be a common behavior; see [16] and [17] for related situations. However, we are pretty sure that there are elliptic divisibility sequences B with $g_B < G_B$, similarly to the cases considered in [16] and [17].

Our last result concerns a much more general case. For its formulation we need to introduce some new notation.

Let T be an arbitrary set of positive integers. The integers a and b are called T-coprime if $\gcd(a, b) \in T$. Observe that in case of $T = \{1\}$, T-coprimality just coincides with the ordinary notion of coprimality. Let $u = (u_n)_{n=1}^{\infty}$ be a sequence of integers. As in the original case, we write $g_u(T)$ for the smallest $k \geq 2$ (if it

exists) such that there exist k consecutive terms of u with the property that none of them is T-coprime to all the others. Further, we write $G_u(T)$ for the smallest $k_0 \geq 2$ (if it exists) such that for any $k \geq k_0$ one can find k consecutive terms of u with the above property. As before, if $G_u(T)$ exists then so does $g_u(T)$, and we have $g_u(T) \leq G_u(T)$. A sequence u for which $G_u(T)$ exists is called a T-Pillai sequence (see [17]). Obviously, for $T = \{1\}$ we get back the notion of Pillai sequences.

In the literature there are several results concerning the problem whether $\mathbb{N}$ is a T-Pillai sequence or not for various choices of T, see e.g. the papers of Caro [4], Saradha and Thangadurai [24] and Hajdu and Saradha [16], and the references there. Further, there are also theorems concerning the T-Pillai property of other sequences for certain types of T, cf. results of Hajdu and Saradha [16] for arithmetic progressions, and of Hajdu and Szikszai [17] for Lucas, Lehmer and general linear recurrence divisibility sequences.

Now we give an answer to this question for elliptic divisibility sequences in the case when T consists of integers with prime factors coming from a fixed finite set. Note that a similar choice for T was considered in [16] and [17], for $\mathbb{N}$ and for Lucas-Lehmer sequences, respectively.

Theorem 2.3. *Let S be an arbitrary finite set of primes with $|S| = s$, and T be an arbitrary set of integers having no prime divisors outside S. Then every elliptic divisibility sequence $B = B(E, P) = (B_n)_{n=1}^{\infty}$ is a T-Pillai sequence. Moreover, we have $G_B(T) \leq C_2(E, s)$, where $C_2(E, s)$ is an explicitly computable constant depending only on E and s.*

Remark 3. As one can easily check, Theorem 2.1 is in fact an immediate consequence of Theorem 2.3. However, beside being a simpler statement, Theorem 2.1 can be proved by more classical tools than Theorem 2.3. So we prefer to state and prove these theorems separately.

3. Some lemmas

To prove our results, we need two types of lemmas. The first branch of them concerns various properties of elliptic divisibility sequences. The other class of lemmas provide certain information about T-Pillai sequences.

3.1. Lemmas concerning elliptic divisibility sequences. The first result we use is due to Everest, Mclaren and Ward [9], and reveals a vital property of elliptic divisibility sequences - in fact it justifies their name in a strong form.

Lemma 3.1. *Every elliptic divisibility sequence $B = (B_n)_{n=1}^{\infty}$ is a strong divisibility sequence. That is, for any $m, n \in \mathbb{N}$ we have*

$$\gcd(B_m, B_n) = B_{\gcd(m,n)}.$$

PROOF. See Lemma 3.2 in [9]. □

Our second lemma is a classical result of Baker [2], providing an upper bound for the integral solutions of elliptic diophantine equations.

Lemma 3.2. *Let $B = B(E, P) = (B_n)_{n=1}^{\infty}$ be an elliptic divisibility sequence. There exists a positive explicit constant $C_3(E)$ depending only on E such that we have*

$$\{n \ : \ B_n = 1\} \leq C_3(E).$$

PROOF. Observe that $B_n = 1$ means that the underlying point nP is an integral point of E. Hence the statement immediately follows from the main result of [2]. □

The next result we need is a theorem of Ingram and Silverman [19], concerning primitive prime divisors of elliptic divisibility sequences $B = (B_n)_{n=1}^{\infty}$. A prime p is called a primitive prime divisor of the term B_n, if $p \mid B_n$, and furthermore, whenever $1 \leq m < n$, one has $p \nmid B_m$.

Lemma 3.3. *Let $B = B(E, P) = (B_n)_{n=1}^{\infty}$ be an elliptic divisibility sequence. There exists an explicitly computable positive integer $N(E)$ depending only on E such that the number of terms B_n having no primitive prime divisor is at most $N(E)$.*

PROOF. The assertion is a simple and immediate consequence of Theorem 1 (a) of [19]. □

3.2. Lemmas concerning the T-Pillai property. Our first lemma of this type is due to Hajdu and Saradha [16]. It implies that if T is finite then the original Pillai function $G(T) = G_{\mathbb{N}}(T)$ (and hence also $g(T) = g_{\mathbb{N}}(T)$) exists. For any set T of positive integers let $T(X)$ denote the set of elements t of T with $t \leq X$.

Lemma 3.4. *Suppose that*

$$|T(X)| \leq \frac{X}{10 \log X} \tag{2}$$

holds for all $X \geq X_1$. Then $G(T)$ exists and

$$g(T) \leq G(T) \leq \max(425, 2X_1 + 1).$$

PROOF. This is Theorem 2.1 of [16]. □

The next lemma provides the values of $g(T)$ and $G(T)$ for certain special choices of T. In fact two of the cases considered are covered by a previous result of the present authors [17].

Lemma 3.5. *For the sets T occurring in the first column of Table 2, the values of $g(T)$ and $G(T)$ are those occurring in the second and third columns of the table, respectively.*

T	$g(T)$	$G(T)$
$\{1,2,3,4,6\}$	79	79
$\{1,2,3,4,7\}$	81	81
$\{1,2,4\}$	47	47
$\{1,2,3,5\}$	81	81

Table 2. The values of $g(T)$ and $G(T)$ for some particular sets T.

PROOF. The second and third cases are included in Lemma 4.4 of [17]. In the first and last cases we use the algorithm developed in [16], see Section 5 there. As the precise explanation of the procedure would need a lot of preparation, we only indicate the most important steps of the method, and refer to [16] for details. In giving this short description, we follow the proof of Lemma 4.4 from [17].

We consider only the case $T = \{1,2,3,4,6\}$, the choice $T = \{1,2,3,5\}$ can be similarly treated. As it has been explained in [16], the property that there exists a set S_k of k consecutive integers such that none of them is T-coprime to all the others is equivalent to the following assertion: the set $K := \{1,2,\dots,k\}$ can be "covered" by the set $L := \{p \ : \ p \text{ prime}, \ p \neq 2,3, \ p < k\} \cup \{8,9,12\}$. That is, there exists a function $f : \ L \to K$ with the following properties:

• for every $\ell \in L$ we have $f(\ell) \leq \ell$,

• $4 \mid (f(8) - f(12))$ and $3 \mid (f(9) - f(12))$,

• for every $i \in K$ there exists a $j \in K$ with $i \neq j$ and an $\ell \in L$ such that $i \equiv j \equiv f(\ell) \pmod{\ell}$.

Indeed, assume that such a function f is given. (One can consider f such that it defines the places $f(\ell)$ of the elements of $\ell \in L$ in K. Then $\ell \mid i \in K$ precisely when $\ell \mid (i - f(\ell))$.) Using the Chinese Remainder Theorem, we can find a set $S_k = \{n+1,\dots,n+k\}$ of k consecutive integers such that for any $\ell \in L$ and $i \in K$, we have $\ell \mid i$ if and only if $\ell \mid (n+i)$. So for any $n+i \in S_k$ we can find an $n+j \in S_k$ such that $n+i \neq n+j$, and $\gcd(n+i, n+j)$ has a divisor

from L, implying that it is not in T. This shows that $g(T) \neq k$ and certainly also $G(T) > k$. On the other hand, if we can find a set $S_k = \{n+1, \dots, n+k\}$ such that none of its elements is T-coprime to all the others, then for any $n+i \in S_k$ we can find an $n+j \in S_k$ such that $n+i \neq n+j$, and $\gcd(n+i, n+j) \notin T$, i.e., it has a divisor from L. Putting now $f(\ell) = i$ for any $\ell \in L$ where $i \in K$ is the first element such that $\ell \mid (n+i)$, we just get a function f with the properties required above.

Thus to find $g(T)$, we need to check all k-s from $k_0 = 17$ up. (Since by the results of Pillai [22] and Brauer [3] we know that $g(T) \geq g(\{1\}) = 17$.) This is done by applying the corresponding algorithm from [16]. This gives $g(T) = 79$. Now since $|T| = 5$, by Lemma 3.4 we obtain $X_1 = 283$ so that $G(T) \leq 567$. Thus we need to check for coverings of K for the values of k in the interval $79 < k < 567$. For $k < 90$ one can easily and quickly find coverings just as previously. For the larger values of k, the algorithm becomes less efficient. Thus for these values of k we use a heuristic algorithm from [16], to find a covering for K. Note that this algorithm is heuristic only in the sense that there is no preliminary guarantee that it will work. However, it worked efficiently in all cases considered in [16], and also in all the present instances. In this way, we could produce a covering for all k with $79 < k < 567$, which gives $G(T) = 79$, too. Hence the statement is proved in this case. As we mentioned, in the other case a similar method has been used, and we have just obtained the values of $g(T)$ and $G(T)$ occurring in Table 2. □

4. Proofs of the theorems

Now we are ready to give the proofs of our theorems. We start with the proof of Theorem 2.1. Then the proof of Theorem 2.3 follows, since it is of similar nature. We conclude this section with the proof of Theorem 2.2.

Proof of Theorem 2.1. Let $B = B(E,P) = (B_n)_{n=1}^{\infty}$ be an elliptic divisibility sequence. Put

$$T = \{n \ : \ B_n = 1\},$$

and note that by Lemma 3.2 we have $|T| \leq C_4(E)$ where $C_4(E)$ is an explicitly computable constant depending only on E. Consider k consecutive terms $B_{n+1}, \dots, B_{n+k}$ of B. In view of Lemma 3.1 we obtain that

$$\gcd(B_{n+i}, B_{n+j}) = B_{\gcd(n+i,n+j)} = 1$$

if and only if $\gcd(n+i, n+j) \in T$. In other words, a term B_{n+i} is coprime to all the other terms B_{n+j} $(i \neq j)$ if and only if $n+i$ is T-coprime to all the other indices $n+j$. Since T is finite, by Lemma 3.4 we know that $\mathbb{N}$ is a T-Pillai sequence. This implies that B is a Pillai sequence. Further, we also have that $g_B = g(T)$ and $G_B = G(T)$. Since $|T| \leq C_4(E)$, by Lemma 3.4 we have that $G(T) \leq C_1(E)$ with some explicitly computable constant $C_1(E)$, and the theorem follows. □

Proof of Theorem 2.3. Let S be an arbitrary finite set of primes with $|S| = s$ and T be an arbitrary set of integers having no prime divisors outside S. Further, let $B = B(E,P) = (B_n)_{n=1}^{\infty}$ be an elliptic divisibility sequence. Put

$$T' := \{n \ : \ B_n \in T\}.$$

Lemma 3.3 yields that there exists an explicitly computable positive integer $N(E)$ such that there exist at most $N(E)$ terms B_n having no primitive prime divisor. Thus $|T'| \leq C_5(E,s)$ holds, where $C_5(E,s)$ is some constant depending only on E and s. Thus by Lemma 3.4, $\mathbb{N}$ is a T'-Pillai sequence, and in particular, $G(T') \leq C_2(E,s)$ with some explicitly computable constant $C_2(E,s)$ depending only on E and s. Now by a similar argument as in the proof of Theorem 2.1 we get that B is a T-Pillai sequence, and $G_B(T) = G(T')$. Hence the statement immediately follows. □

Proof of Theorem 2.2. For any of the sequences $B = B(E,P)$ from Table 1, put

$$T_B := \{n \ : \ B_n = 1\}.$$

By a simple calculation e.g. using the function `IntegralPoints` of Magma [1] (which is based upon the deterministic and efficient method of Stroeker and Tzanakis [33] and Gebel, Pethő and Zimmer [14]) we can easily find all integral points on the corresponding elliptic curves E, and check that the sets T_B are precisely those indicated in Table 3.

Thus recalling from the proof of Theorem 2.1 that $g_B = g(T)$ and $G_B = G(T)$, the statement instantly follows from Lemma 3.5. □

4.1. Acknowledgements. The authors are grateful to the referees for their helpful and motivating remarks and suggestions.

References

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

E	$P=(x(P),y(P))$	T_B
$y^2+y=x^3-x$	$(0,0)$	$\{1,2,3,4,6\}$
$y^2+y=x^3+x^2$	$(0,0)$	$\{1,2,3,4,7\}$
$y^2+xy=x^3-x^2-x+1$	$(1,0)$	$\{1,2,4\}$
$y^2+xy=x^3-2x+1$	$(1,0)$	$\{1,2,3,5\}$

Table 3. The sets T_B for certain elliptic divisibility sequences.

[2] A. Baker, *The diophantine equation* $y^2=ax^3+bx^2+cx+d$, J. London Math. Soc. **43** (1968), 1-9.

[3] A. T. Brauer, *On a property of consecutive integers*, Bull. Amer. Math. Soc. **47** (1941), 328–331.

[4] Y. Caro, *On a division property of consecutive integers*, Israel J. Math. **33** (1979), 32–36.

[5] J. W. S. Cassels, *Lectures on Elliptic Curves*, London Math. Soc. Stud. Texts **24**, Cambridge Univ. Press, Cambridge, 1991.

[6] L. K. Durst, *The apparition problem for equianharmonic divisibility*, Proc. Nat. Acad. Sci. U. S. A. **38** (1952), 330-333.

[7] M. Einsiedler, G. Everest and T. Ward, *Primes in elliptic divisibility sequences*, LMS J. Comput. Math. **4** (2001), 1-13.

[8] G. Everest and H. King, *Prime powers in elliptic divisibility sequences*, Math. Comp. **74** (2005), 2061–2071.

[9] G. Everest, G. Mclaren and T. Ward, *Primitive divisors of elliptic divisibility sequences*, J. Number Theory **118** (2006), 71-89.

[10] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs **104**, AMS, Providence, RI, 2003.

[11] G. Everest and T. Ward, *The canonical height of an algebraic point on an elliptic curve*, New York J. Math. **6** (2000), 331–342.

[12] G. Everest and T. Ward, *Primes in divisibility sequences*, Cubo Mat. Educ. **3** (2001), 245-259.

[13] G. Everest and T. Ward, *An Introduction to Number Theory*, Springer-Verlag, New York, 2005.

[14] J. Gebel, A. Pethő and H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. **68** (1994), 171–192.

[15] B. Gezer and O. Bizim, *Elliptic divisibility sequences associated to elliptic curves with torsion points*, arXiv:1101.3839v1 [math.NT] 20 Jan 2011.

[16] L. Hajdu and N. Saradha, *On a problem of Pillai and its generalizations*, Acta Arith. **144** (2010), 323–347.

[17] L. Hajdu and M. Szikszai, *On the GCD-s of k consecutive terms of Lucas sequences*, J. Number Theory **132** (2012), 3056–3069.

[18] M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. **93** (1988), 419-450.

[19] P. Ingram and J. H. Silverman, *Uniform estimates for primitive divisors in elliptic divisibility sequences*, Number Theory, Analysis and Geometry: In Memory of Serge Lang, D.

Goldfeld, J. Jorgenson, P. Jones, D. Ramakrishnan, K. Ribet, J. Tate eds., Springer-Verlag, 2012, pp. 243-271.

[20] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften **231**, Springer-Verlag, Berlin, 1978.

[21] M. Ohtomo and F. Tamari, *On relative prime number in a sequence of positive integers*, J. Stat. Plan. Inf. **106** (2002), 509–515.

[22] S. S. Pillai, *On M consecutive integers - I*, Proc. Indian Acad. Sci., Sect. A. **11** (1940), 6–12.

[23] J. Reynolds, *Perfect powers in elliptic divisibilty sequences*, J. Number Theory **132** (2012), 998–1015.

[24] N. Saradha and R. Thangadurai, *Pillai's problem on consecutive integers*, Proceedings of the conference on Number Theory and Cryptography at HRI, Allahabad, 2007, pp. 176–188.

[25] R. Shipsey, *Elliptic divisibility sequences*, Ph.D. thesis, Goldsmiths College (University of London), 2000.

[26] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[27] J. H. Silverman, *A quantitative version of Siegels theorem: integral points on elliptic curves and Catalan curves*, J. Reine Angew. Math. **378** (1987), 60-100.

[28] J. H. Silverman, *Wieferichs criterion and the abc-conjecture*, J. Number Theory **30** (1988) 226-237.

[29] J. H. Silverman, *Common divisors of elliptic divisibility sequences over function fields*, Manuscripta Math. **114** (2004), 432-446.

[30] J. H. Silverman, *p-adic properties of division polynomials and elliptic divisibility sequences*, Math. Ann. **332** (2005), 443-471.

[31] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergrad. Texts Math., Springer-Verlag, New York, 1992.

[32] J. H. Silverman and N. Stephens, *The sign of an elliptic divisibility sequences*, Journal of Ramanujan Math. Soc. **21** (2006), 1-17.

[33] R. J. Stroeker and N. Tzanakis, *On the Elliptic Logarithm Method for Elliptic Diophantine Equations: Reflections and an Improvement*, Experimental Math. **8** (1999), 135–149.

[34] C. S. Swart, *Elliptic divisibility sequences*, Ph.D. thesis, Royal Holloway (University of London), 2003.

[35] P. Voutier and M. Yabuta, *Primitive prime divisors of certain elliptic divisibilty sequences*, arXiv:1009.0872v2 [math.NT] 24 Apr 2011.

[36] M. Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948), 31-74.

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

UNIVERSITY OF DEBRECEN
INSTITUTE OF MATHEMATICS
P.O. BOX 12
H-4010 DEBRECEN
HUNGARY

E-mail: hajdul@science.unideb.hu

UNIVERSITY OF DEBRECEN
INSTITUTE OF MATHEMATICS
P.O. BOX 12
H-4010 DEBRECEN
HUNGARY

E-mail: szikszaimarton@gmail.com