Journal of Integer Sequences, Vol. 25 (2022),
Article 22.9.2

Some Divisibility Properties Concerning Lucas and Elliptic Divisibility Sequences

Chatchawan Panraksa and Aram Tangboonduangjit
Mahidol University International College
Mahidol University
Salaya, Nakhon Pathom 73170
Thailand
chatchawan.pan@mahidol.edu
aram.tan@mahidol.edu

Abstract

We consider sequences of integers formed by a quotient of the Lucas sequences or elliptic divisibility sequences. We then investigate some divisibility properties of these quotient sequences. Additionally, we prove that elliptic divisibility sequences possess a divisibility property that is analogous to a generalization of Matijasevich's lemma involving the Fibonacci numbers, which contributed to the solution to Hilbert's tenth problem.

1 Introduction

Let P and Q be relatively prime integers. The Lucas sequence $\big(U_n(P,Q)\big)_{n\geq 0}$ is defined by $U_0(P,Q)=0$, $U_1(P,Q)=1$, and

$$U_n(P,Q)=P\cdot U_{n-1}(P,Q)-Q\cdot U_{n-2}(P,Q) \quad \text{for } n\geq 2.$$

For example, the Fibonacci sequence $(F_n)_{n\geq 0}$ corresponds to $U_n(1,-1)$ and the sequence $(M_n)_{n\geq 0}$ of Mersenne numbers, where $M_n=2^n-1$, corresponds to $U_n(3,2)$. Each Lucas sequence $(U_n(P,Q))_{n\geq 0}$ is associated with a characteristic polynomial of the form x^2-Px+Q. In this work, if not stated otherwise, $(U_n)_{n\geq 0}$ denotes a sequence $(U_n(P,Q))_{n\geq 0}$ for

some relatively prime integers P and Q. We also assume that the sequence $(U_n)_{n\geq 0}$ is nondegenerate in the sense that $Q \neq 0$ and the ratio of the two roots of the associated characteristic polynomial is not a root of unity. Therefore, the discriminant $D = P^2 - 4Q$ satisfies $D \neq 0$, and the two roots α, β of the characteristic polynomial are distinct so that we can express U_n explicitly as

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\sqrt{D}}.$$

Another sequence of integers that we consider in this work is called the *elliptic divisibility sequence* (EDS). It is defined as a sequence of integers $(h_n)_{n\geq 0}$ satisfying the recurrence

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \tag{1}$$

for all integers $m \geq n \geq 0$ and being a divisibility sequence; that is, $h_m \mid h_n$ whenever $m \mid n$. Examples [14] include the sequence of nonnegative integers $(n)_{n\geq 0}$ and the sequence $((-1)^{(n-1)(n-2)/2}F_n)_{n\geq 0}$. We can see the latter by realizing the following identity of the Fibonacci numbers:

$$F_{m+n}F_{m-n} = (-1)^{n+1}(F_{m+1}F_{m-1}F_n^2 - F_{n+1}F_{n-1}F_m^2) \tag{2}$$

for all $m \geq n \geq 0$. (We can readily verify the identity (2) by appealing to the well-known Catalan identity $F_{n+r}F_{n-r} = F_n^2 + (-1)^{n+r+1}F_r^2$ for all integers n and r.) This means EDS gives us a natural way to generalize the Fibonacci sequence. It also gives examples of divisibility sequences that do not satisfy linear recurrences. A sequence $(h_n)_{n\geq 0}$ with $h_0 = 0$, $h_1 = 1$, and $h_2h_3 \neq 0$ is said to be *proper*. Ward [14] was the first to study arithmetic properties of proper elliptic divisibility sequences. One of his results states that a proper sequence $(h_n)_{n\geq 0}$ satisfying (1) is an elliptic divisibility sequence if and only if h_2, h_3, h_4 are integers and $h_2 \mid h_4$.

However, we can give an alternative definition of EDS via elliptic curves. We recall some theories of elliptic curves. In particular, we consider a curve with the Weierstrass equation given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3}$$

with integer coefficients. Non-singular rational points on the projective closure of this curve form a group $E(\mathbb{Q})$; see, for instance, [11]. Let P be a non-identity element in this group. For a positive integer n, we denote the addition of point P to itself $P + P + \cdots + P$ up to n terms by nP. Then the corresponding coordinate point $(x(nP), y(nP))$ on the curve can be expressed by

$$(x(nP), y(nP)) = \left(\frac{A_{nP}}{B_{nP}^2}, \frac{C_{nP}}{B_{nP}^3}\right)$$

where A_{nP} and C_{nP} are integers, B_{nP} is a positive integer, and the fractions in the coordinates are in reduced forms.

It is now conventional to define an elliptic divisibility sequence as follows.

Definition 1. Let $E/\mathbb{Q}$ be an elliptic curve with the Weierstrass equation given by (3). Let $P \in E(\mathbb{Q})$ be a non-torsion point. For each positive integer n, denote the integer B_{nP} by B_n. Then the sequence $(B_n)_{n\geq 1}$ is said to be an *elliptic divisibility sequence (EDS)*. An EDS $(B_n)_{n\geq 1}$ is said to be *normalized* if $B_1 = 1$. We can normalize an EDS by a change of variables in the defining Weierstrass equation. The obtained sequence $(B_n/B_1)_{n\geq 1}$ is then an EDS.

In this work, we follow Definition 1 for the definition of the elliptic divisibility sequence. If not stated otherwise, all elliptic divisibility sequences are assumed to be normalized. See, for example, [15, 10] for the connection between the two definitions of the elliptic divisibility sequence. Elliptic divisibility sequences have gained popularity recently due to their application in cryptography; see, for example, [13]. In Section 2, we define a new sequence as a ratio of Lucas sequences and study specific arithmetic properties this sequence possesses. In Section 3, we do the same for elliptic divisibility sequences. In 1970, Matijasevich [4] completed the theorem (based on combined work by Davis, Putnam, and Robinson) that solved Hilbert's tenth problem. Part of the proof of this theorem used specific arithmetic properties of the Fibonacci numbers. Onphaeng and Pongsriiam [5] generalized one of these properties to the Lucas sequences. The final result of this paper (Theorem 16) generalizes the exact property to elliptic divisibility sequences.

2 Lucas sequences

A sequence (u_n) of integers is said to be a *strong divisibility sequence* if $\gcd(u_m, u_n) = u_{\gcd(m,n)}$ for all m, n. Let N be a positive integer. A sequence (u_n) of rational numbers is said to be an *N-almost strong divisibility sequence* if for all m and n where u_m and u_n are integers we have $\gcd(u_m, u_n) = u_{\gcd(m,n)}$ whenever $\gcd(mn, N) = 1$. Let the sequence $(T_n)_{n\geq 1}$ be defined by

$$T_n = \left| \frac{U_{n\Delta}}{U_n U_\Delta} \right|, \tag{4}$$

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial associated with the Lucas sequence $(U_n)_{n\geq 0}$. In general, some of the terms of this sequence might not be integers. For example, for the sequence $U(4, -7)$, we have $\Delta = 12$ and the first five terms of the sequence

$$T_n = \left| \frac{U_{12n}}{U_{12} U_n} \right|$$

are

$$1, \frac{76751}{2}, \frac{3240525601}{3}, \frac{158095946378449}{2}, 7471977820027132645$$

while for the Fibonacci sequence $F_n = U_n(1, -1)$, we have $\Delta = 5$ and the first five terms of the sequence

$$T_n = \frac{F_{5n}}{5F_n} \tag{5}$$

are

$$1,\ 11,\ 61,\ 451,\ 3001.$$

We can show that each term of the sequence (5) is an integer [6]. Filipponi and Freitag [1] gave the Zeckendorf decomposition of the sequence (5). The present authors [6] also studied and gave certain curious arithmetic properties of the sequence (5) . In particular, we proved that T_n^k divides $T(nT(nT(\cdots(nT(n)))))$ exactly, where n appears k times in this composition of indices. For example, for $k = 4$, we have

$$T_n^4 \parallel T(nT(nT(nT(n)))),$$

where $a^n \parallel b$ means a^n divides b exactly, that is, a^n divides b but a^{n+1} does not. In this work, we generalize this result to the sequence $(T_n)_{n\geq 1}$ defined in terms of the Lucas sequences in (4) (Corollary 11). We also prove that this sequence $(T_n)_{n\geq 1}$ is a Δ-almost strong divisibility sequence (Theorem 7).

2.1 p-adic valuations of Lucas sequences

If p is a prime such that $p \nmid Q$, then the *rank of apparition of* p in the sequence $(U_n)_{n\geq 0}$, denoted $\tau(p)$, is defined to be the least positive integer such that $p \mid U_{\tau(p)}$. The following basic facts about $\tau(p)$ are well-known: $\tau(p)$ exists for each p, and $p \mid U_n$ if and only if $\tau(p) \mid n$. Sanna [9] gave an explicit formula for the p-adic valuation $\nu_p(U_n)$ of nondegenerate Lucas sequences in terms of the prime p, the index n, and the rank of apparition $\tau(p)$, generalizing the result by Lengyel [3] who gave the same formula but only for the Fibonacci sequence. We quote this result by Sanna [9, Thm. 1.5, Cor. 1.6] as Theorem 2 below.

Theorem 2. *Let p be a prime such that $p \nmid Q$. Then, for each positive integer n,*

$$\nu_p(U_n) = \begin{cases} \nu_p(n) + \nu_p(U_p) - 1, & p \mid D \text{ and } p \mid n; \\ 0, & p \mid D \text{ and } p \nmid n; \\ \nu_p(n) + \nu_p(U_{p\tau(p)}) - 1, & p \nmid D,\ \tau(p) \mid n, \text{ and } p \mid n; \\ \nu_p(U_{\tau(p)}), & p \nmid D,\ \tau(p) \mid n, \text{ and } p \nmid n; \\ 0, & p \nmid D \text{ and } \tau(p) \nmid n. \end{cases}$$

In particular, if p is an odd prime such that $p \nmid Q$, then, for each positive integer n,

$$\nu_p(U_n) = \begin{cases} \nu_p(n) + \nu_p(U_p) - 1, & p \mid D \text{ and } p \mid n; \\ 0, & p \mid D \text{ and } p \nmid n; \\ \nu_p(n) + \nu_p(U_{\tau(p)}), & p \nmid D \text{ and } \tau(p) \mid n; \\ 0, & p \nmid D \text{ and } \tau(p) \nmid n. \end{cases}$$

Remark 3. If p is a prime and $p \mid Q$ then since $\gcd(P, Q) = 1$, we can prove by induction that $\nu_p(U_n) = 0$ for all $n \geq 1$. In fact, since $U_1 = 1$, we have $p \nmid U_1$. Assume that $p \nmid U_{n-1}$ for some $n \geq 2$. If $p \mid U_n$, then since $PU_{n-1} = U_n + QU_{n-2}$, $p \mid Q$, and $p \nmid U_{n-1}$, it follows that $p \mid P$ contradicting the assumption that $\gcd(P, Q) = 1$. Hence $p \nmid U_n$.

We also need the following result by the present authors [7, Lem. 2.3] for p-adic valuation of Lucas sequence with integer-multiple index.

Lemma 4. *Let $n, k \geq 1$ and p a prime factor of U_k such that $p \nmid Q$. Then*

1. *if (i) p is odd, or (ii) $p = 2$ and k is even, or (iii) $p = 2$ and n is odd, we have*

$$\nu_p(U_{kn}) = \nu_p(n) + \nu_p(U_k);$$

2. *if k and D are odd and n is even, we have*

$$\nu_2(U_{kn}) = \nu_2(n) + \nu_2(U_k) + \big(\nu_2(U_{2\tau(2)}) - \nu_2(U_{\tau(2)}) - 1\big) \geq \nu_2(n) + \nu_2(U_k).$$

We now state some properties of the sequence $(T_n)_{n\geq 1}$.

Lemma 5. *Suppose* $\gcd(n, \Delta) = 1$. *Then T_n is an integer.*

Proof. Since $\gcd(P, Q) = 1$, it follows that $(U_n)_{n\geq 0}$ is a strong divisibility sequence. From the definition of T_n, it suffices to show that $\gcd(U_n, U_\Delta) = 1$. Indeed, we have $\gcd(U_n, U_\Delta) = U_{\gcd(n,\Delta)} = U_1 = 1$. □

Lemma 6. *Suppose* $\gcd(n, \Delta) = 1$. *Then* $\gcd(T_n, \Delta) = 1 = \gcd(T_n, U_n)$.

Proof. To prove $\gcd(T_n, \Delta) = 1$, suppose p is a prime factor of Δ. Then by Theorem 2, since $\gcd(n, \Delta) = 1$ and $p \mid \Delta$, we have

$$\begin{aligned}\nu_p(U_{n\Delta}) &= \nu_p(n\Delta) + \nu_p(U_p) - 1 = \nu_p(n) + \nu_p(\Delta) + \nu_p(U_p) - 1\\ &= \nu_p(\Delta) + \nu_p(U_p) - 1\end{aligned}$$

and

$$\begin{aligned}\nu_p(U_nU_\Delta) &= \nu_p(U_n) + \nu_p(U_\Delta) = 0 + \nu_p(\Delta) + \nu_p(U_p) - 1\\ &= \nu_p(\Delta) + \nu_p(U_p) - 1.\end{aligned}$$

We see that $\nu_p(U_{n\Delta}) = \nu_p(U_nU_\Delta)$. Therefore, $\gcd(T_n, \Delta) = 1$.

To prove $\gcd(T_n, U_n) = 1$, suppose p is a prime divisor of U_n. If $p \mid \Delta$, then since $\gcd(n, \Delta) = 1$, we have $p \nmid n$. By Theorem 2, it follows that $\nu_p(U_n) = 0$, contradicting the fact that p is a prime divisor of U_n. Thus $p \nmid \Delta$. By case (1) of Lemma 4, we have

$$\nu_p(U_{n\Delta}) = \nu_p(\Delta) + \nu_p(U_n) = 0 + \nu_p(U_n) = \nu_p(U_n).$$

This implies $\nu_p(T_n) = 0$ and therefore $\gcd(T_n, U_n) = 1$. □

2.2 Almost strong divisibility property

Theorem 7. *The sequence $(T_n)_{n\geq 1}$ is a Δ-almost strong divisibility sequence.*

Proof. Suppose m and n satisfy $\gcd(mn, \Delta) = 1$. Let p be a prime such that $p \mid T_m$ and $p \mid T_n$. By Lemma 6, $p \nmid U_m$, $p \nmid U_n$, and $p \nmid \Delta$. If p is odd, by Theorem 2 we have

$$\begin{aligned}\nu_p(T_m) &= \nu_p(U_{m\Delta}) - \nu_p(U_\Delta) = \nu_p(m\Delta) + \nu_p(U_{\tau(p)}) - \nu_p(U_\Delta)\\ &= \nu_p(m) + \nu_p(U_{\tau(p)}) - \nu_p(U_\Delta).\end{aligned}$$

Similarly, we have $\nu_p(T_n) = \nu_p(n) + \nu_p(U_{\tau(p)}) - \nu_p(U_\Delta)$. Let $\ell = \gcd(m, n)$. Then

$$\begin{aligned}\nu_p(T_\ell) &= \nu_p(U_{\ell\Delta}) - \nu_p(U_\Delta) = \nu_p(\ell) + \nu_p(U_{\tau(p)}) - \nu_p(U_\Delta)\\ &= \min\{\nu_p(m), \nu_p(n)\} + \nu_p(U_{\tau(p)}) - \nu_p(U_\Delta).\end{aligned}$$

For $p = 2$, we consider four cases.
Case 1: Suppose $p \mid m$ and $p \mid n$. We have

$$\begin{aligned}\nu_p(T_m) &= \nu_p(U_{m\Delta}) - \nu_p(U_\Delta) = \nu_p(m\Delta) + \nu_p(U_{p\tau(p)}) - 1 - \nu_p(U_\Delta)\\ &= \nu_p(m) + \nu_p(U_{p\tau(p)}) - 1 - \nu_p(U_\Delta).\end{aligned}$$

Similarly, we have $\nu_p(T_n) = \nu_p(n) + \nu_p(U_{p\tau(p)}) - 1 - \nu_p(U_\Delta)$. Let $\ell = \gcd(m, n)$ so that $p \mid \ell$. Then

$$\begin{aligned}\nu_p(T_\ell) &= \nu_p(U_{\ell\Delta}) - \nu_p(U_\Delta) = \nu_p(\ell) + \nu_p(U_{p\tau(p)}) - 1 - \nu_p(U_\Delta)\\ &= \min\{\nu_p(m), \nu_p(n)\} + \nu_p(U_{p\tau(p)}) - 1 - \nu_p(U_\Delta).\end{aligned}$$

Case 2: Suppose $p \nmid m$ and $p \mid n$. We have

$$\nu_p(T_m) = \nu_p(U_{m\Delta}) - \nu_p(U_\Delta) = \nu_p(U_{\tau(p)}) - \nu_p(U_\Delta)$$

and

$$\begin{aligned}\nu_p(T_n) &= \nu_p(n) + \nu_p(U_{p\tau(p)}) - 1 - \nu_p(U_\Delta) \geq \nu_p(U_{p\tau(p)}) - \nu_p(U_\Delta)\\ &\geq \nu_p(U_{\tau(p)}) - \nu_p(U_\Delta).\end{aligned}$$

Let $\ell = \gcd(m, n)$ so that $p \nmid \ell$. Then

$$\nu_p(T_\ell) = \nu_p(U_{\ell\Delta}) - \nu_p(U_\Delta) = \nu_p(U_{\tau(p)}) - \nu_p(U_\Delta) = \min\{\nu_p(T_m), \nu_p(T_n)\}.$$

Case 3: Suppose $p \mid m$ and $p \nmid n$. This is analogous to Case 2.
Case 4: Suppose $p \nmid m$ and $p \nmid n$. This is also analogous to Case 2.

We have shown that $\nu_p(\gcd(T_m, T_n)) = \nu_p(T_{\gcd(m,n)})$ for all primes p. Hence

$$\gcd(T_m, T_n) = T_{\gcd(m,n)},$$

as we wish to show. □

2.3 Nested exact divisibility property

Let n be a positive integer. Define the sequence $(H_k(n))_{k\geq 1}$ by $H_1(n) = T_n$ and $H_k(n) = T_{nH_{k-1}(n)}$ for $k \geq 2$. The first few terms of the sequence $(H_k(n))_{k\geq 1}$ are

$$T(n), \quad T(nT(n)), \quad T(nT(nT(n))), \quad T(nT(nT(nT(n)))).$$

We see that this forms a subsequence of $(T_m)_{m\geq 1}$ for each n, and the sequence of nested indices is increasing very rapidly. We first observe the following property of the sequence $(H_k(n))_{k\geq 1}$.

Lemma 8. *Suppose* $\gcd(n, \Delta) = 1$. *Then* $\gcd(U_{nH_k(n)}, T_n) = 1$ *for all positive integers* k.

Proof. We prove that $\gcd(H_k(n), \Delta) = 1$ for all positive integers k by induction. For $k = 1$, by Lemma 6, we have

$$\gcd(H_k(n), \Delta) = \gcd(H_1(n), \Delta) = \gcd(T_n, \Delta) = 1.$$

Assume that $\gcd(H_k(n), \Delta) = 1$ for some $k \geq 1$. Then $\gcd(nH_k(n), \Delta) = 1$ and by Lemma 6, we have

$$\gcd(H_{k+1}(n), \Delta) = \gcd(T_{nH_k(n)}, \Delta) = 1.$$

Now since $(U_n)_{n\geq 0}$ is a strong divisibility sequence, we have

$$\gcd(U_{nH_k(n)}, U_{n\Delta}) = U_{\gcd(nH_k(n),n\Delta)} = U_{n\cdot\gcd(H_k(n),\Delta)} = U_n.$$

Hence

$$\gcd(U_{nH_k(n)}, T_n) = \gcd\left(U_{nH_k(n)}, \frac{U_{n\Delta}}{U_n U_\Delta}\right) = 1.$$

□

Lemma 9. *Suppose* $\gcd(n, \Delta) = 1$. *If* $2 \mid T_n$, *then* $2 \mid n\Delta$.

Proof. We proceed by contradiction. Assume that $n\Delta$ is odd. Then both n and Δ are odd. Since $2 \mid T_n$, we have $2 \mid U_{n\Delta}$ so that $\nu_2(U_{n\Delta}) \geq 1$. Consequently, Theorem 2 implies that $\nu_2(U_{n\Delta}) = \nu_2(U_{\tau(2)})$ and $\tau(2) \mid n\Delta$. Since Δ is odd, we have that P is odd and thus, by Remark 3, $\tau(2) = 3$. Therefore $\nu_2(U_{n\Delta}) = \nu_2(U_3)$ and $3 \mid n\Delta$. This implies $3 \mid \Delta$ or $3 \mid n$. If $3 \mid \Delta$, by the fact that $(U_n)_{n\geq 0}$ is a divisibility sequence, we have

$$\nu_2(U_3) = \nu_2(U_{n\Delta}) \geq \nu_2(U_\Delta) \geq \nu_2(U_3).$$

This yields $\nu_2(U_\Delta) = \nu_2(U_3)$. Similarly, if $3 \mid n$, then $\nu_2(U_n) = \nu_2(U_3)$. Consequently, $\max\{\nu_2(U_\Delta), \nu_2(U_n)\} = \nu_2(U_3)$, and we have

$$\begin{aligned} 0 \leq \nu_2(T_n) &= \nu_2\Big(\frac{U_{n\Delta}}{U_n U_\Delta}\Big) \\ &\leq \min\Big\{\nu_2\Big(\frac{U_{n\Delta}}{U_n}\Big), \nu_2\Big(\frac{U_{n\Delta}}{U_\Delta}\Big)\Big\} \\ &= \nu_2(U_{n\Delta}) - \nu_2(U_3) = \nu_2(U_3) - \nu_2(U_3) = 0. \end{aligned}$$

Hence, $\nu_2(T_n) = 0$, contradicting the assumption that $2 \mid T_n$. □

We have the following theorem about the exact divisibility property of the sequence $(H_k(n))_{k\geq 1}$.

Theorem 10. *Suppose* $\gcd(n,\Delta)=1$. *Let* p *be a prime such that* $\nu_p(T_n)>0$. *Then* $\nu_p(H_k(n))=k\nu_p(T_n)$ *for all positive integers* k.

Proof. We prove by induction on k. The case when $k=1$ is obvious. Assume that the statement holds for some positive integer k. Let p be a prime such that $p \mid T_n$. Put $a=\nu_p(T_n)\geq 1$. Then

$$\nu_p(T_n^k)=ka=\nu_p(H_k(n)).$$

Since $p \mid T_n$, it follows from Lemma 6 that $p \nmid U_n$ and from Lemma 8 that $p \nmid U_{nH_k(n)}$. Thus,

$$\nu_p(H_{k+1}(n))=\nu_p(T_{nH_k(n)})=\nu_p\left(\frac{U_{nH_k(n)\cdot\Delta}}{U_{nH_k(n)}U_\Delta}\right)=\nu_p(U_{nH_k(n)\cdot\Delta})-\nu_p(U_\Delta).$$

If p is odd, then, by Theorem 2 and Lemma 4, we have

$$\begin{aligned}\nu_p(U_{nH_k(n)\cdot\Delta})-\nu_p(U_\Delta)&=\nu_p(H_k(n))+\nu_p(U_{n\Delta})-\nu_p(U_\Delta)\\&=ka+\nu_p\left(\frac{U_{n\Delta}}{U_\Delta}\right)=ka+\nu_p\left(\frac{U_{n\Delta}}{U_nU_\Delta}\right)\\&=ka+\nu_p(T_n)=ka+a=(k+1)a.\end{aligned}$$

If $p=2$, then by Lemma 9, we have that $n\Delta$ is even and by case 1 (ii) of Lemma 4, we have the same result as above.
Hence, for all primes p, we have

$$\nu_p(H_{k+1}(n))=(k+1)a=(k+1)\nu_p(T_n).$$

□

We conclude this section with an immediate corollary.

Corollary 11. *Suppose* $\gcd(n,\Delta)=1$ *and* $T_n\neq 1$. *Then, for each positive integer* k,

$$T_n^k \parallel H_k(n).$$

3 Elliptic divisibility sequences

We have the following result summarized by Reynolds [8, Lem. 2.1] for specific basic arithmetic properties of elliptic divisibility sequences.

Lemma 12. *Let* $(B_n)_{n\geq 1}$ *be an elliptic divisibility sequence corresponding to an elliptic curve* E *with the Weierstrass equation* (3) *and a non-torsion point* P *in* $E(\mathbb{Q})$.

(i) *Let p be a prime. There exists a smallest positive integer n_0 such that $p \mid B_{n_0}$. Moreover, for every positive integer n,*

$$p \mid B_n \quad \text{if and only if} \quad n_0 \mid n.$$

(ii) *Let p be an odd prime. For every pair of positive integers m, n, if $\nu_p(B_n) > 0$ then*

$$\nu_p(B_{mn}) = \nu_p(B_n) + \nu_p(m).$$

(iii) *For every pair of positive integers m, n, if $\nu_2(B_n) > 0$ then*

$$\nu_2(B_{mn}) = \nu_2(B_n) + \nu_2(m)$$

if the coefficient a_1 is even and

$$\left|\nu_2(B_{mn}) - (\nu_2(B_n) + \nu_2(m))\right| \leq \epsilon$$

otherwise, where the constant ϵ depends only on E and P.

(iv) *For all positive integers m, n,*

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

Now we define a sequence similar in the form to sequence (5) but in the context of elliptic divisibility sequences. Let τ be a positive integer and $(B_n)_{n\geq 1}$ an elliptic divisibility sequence corresponding to an elliptic curve with the Weierstrass equation (3) and a non-torsion point P. We define the sequence $(K_n)_{n\geq 1}$ as follows. For each positive integer n, let

$$K_n = \frac{B_{\tau n}}{B_\tau B_n}.$$

Then we have the following result.

Theorem 13. *Let $(K_n)_{n\geq 1}$ be a sequence defined as above with the coefficient a_1 in the Weierstrass equation (3) being even and $\tau \mid B_\tau$. Then $(K_n)_{n\geq 1}$ is a τ-almost strong divisibility sequence. That is, for all positive integers m, n, if $\gcd(mn, \tau) = 1$, then*

$$\gcd(K_m, K_n) = K_{\gcd(m,n)}.$$

Proof. Let m and n be positive integers that are relatively prime to τ. By Lemma 12(iv), we have $B_\tau \mid B_{\tau n}$ and $B_n \mid B_{\tau n}$. Since $\gcd(n, \tau) = 1$, it follows that K_n is an integer. Similarly, we have that K_m is an integer. Let p be a prime. We consider two cases.

Case 1: Suppose $\nu_p(B_\tau) > 0$. Since $\gcd(\tau, mn) = 1$, by Lemma 12(iv), we have $\nu_p(B_n) = 0 = \nu_p(B_m)$. By Lemma 12(ii, iii), we have $\nu_p(B_{\tau n}) = \nu_p(B_\tau) + \nu_p(n)$ and $\nu_p(B_{\tau m}) = \nu_p(B_\tau) + \nu_p(m)$. This implies that

$$\begin{aligned}\nu_p(K_n) &= \nu_p(B_{\tau n}) - \nu_p(B_\tau) - \nu_p(B_n)\\ &= \nu_p(B_\tau) + \nu_p(n) - \nu_p(B_\tau) - 0\\ &= \nu_p(n).\end{aligned}$$

Similarly, we have $\nu_p(K_m) = \nu_p(m)$. Consequently,

$$\nu_p(\gcd(K_m, K_n)) = \min\{\nu_p(K_m), \nu_p(K_n)\} = \min\{\nu_p(m), \nu_p(n)\}.$$

Now, we consider $\nu_p(K_{\gcd(m,n)})$. By Lemma 12(iv), we observe that

$$\nu_p(B_{\gcd(m,n)}) = \nu_p(\gcd(B_m, B_n)) = \min\{\nu_p(B_m), \nu_p(B_n)\} = 0.$$

By Lemma 12(ii, iii), we obtain that

$$\begin{aligned}\nu_p(K_{\gcd(m,n)}) &= \nu_p(B_{\tau\cdot\gcd(m,n)}) - \nu_p(B_\tau) - \nu_p(B_{\gcd(m,n)})\\ &= \nu_p(B_\tau) + \nu_p(\gcd(m,n)) - \nu_p(B_\tau) - \nu_p(B_{\gcd(m,n)})\\ &= \nu_p(\gcd(m,n)) = \min\{\nu_p(m), \nu_p(n)\}.\end{aligned}$$

Comparing the values, we conclude that

$$\nu_p(\gcd(K_m, K_n)) = \nu_p(K_{\gcd(m,n)}).$$

Case 2: Suppose $\nu_p(B_\tau) = 0$. We consider three subcases.
Case 2.1: Suppose $\nu_p(B_m) = 0$ and $\nu_p(B_n) = 0$. We have,

$$\nu_p(K_n) = \nu_p(B_{\tau n}) - \nu_p(B_\tau) - \nu_p(B_n) = \nu_p(B_{\tau n}).$$

Similarly, we have $\nu_p(K_m) = \nu_p(B_{\tau m})$. Consequently, by Lemma 12(iv),

$$\nu_p(\gcd(K_m, K_n)) = \nu_p(\gcd(B_{\tau m}, B_{\tau n})) = \nu_p(B_{\gcd(\tau m, \tau n)}) = \nu_p(B_{\tau\cdot\gcd(m,n)}).$$

On the other hand, since $\min\{\nu_p(B_m), \nu_p(B_n)\} = 0$, we have, by Lemma 12(iv),

$$\nu_p(B_{\gcd(m,n)}) = \nu_p(\gcd(B_m, B_n)) = \min\{\nu_p(B_m), \nu_p(B_n)\} = 0.$$

Hence,

$$\nu_p(K_{\gcd(m,n)}) = \nu_p(B_{\tau\cdot\gcd(m,n)}) - \nu_p(B_\tau) - \nu_p(B_{\gcd(m,n)}) = \nu_p(B_{\tau\cdot\gcd(m,n)}).$$

Comparing the values, we conclude that

$$\nu_p(\gcd(K_m, K_n)) = \nu_p(K_{\gcd(m,n)}).$$

Case 2.2: Suppose $\nu_p(B_m) > 0$ and $\nu_p(B_n) > 0$. By Lemma 12(ii, iii), we have $\nu_p(B_{\tau n}) = \nu_p(B_n) + \nu_p(\tau)$. Therefore,

$$\begin{aligned}\nu_p(K_n) &= \nu_p(B_{\tau n}) - \nu_p(B_\tau) - \nu_p(B_n) \\ &= \nu_p(B_n) + \nu_p(\tau) - \nu_p(B_\tau) - \nu_p(B_n) \\ &= \nu_p(\tau).\end{aligned}$$

Similarly, we have $\nu_p(K_m) = \nu_p(\tau)$. Thus,

$$\nu_p(\gcd(K_m, K_n)) = \min\{\nu_p(K_m), \nu_p(K_n)\} = \nu_p(\tau).$$

On the other hand, since $\nu_p(B_m) > 0$ and $\nu_p(B_n) > 0$, by Lemma 12(iv), it follows that $\nu_p(B_{\gcd(m,n)}) > 0$. By Lemma 12(ii), we have

$$\begin{aligned}\nu_p(K_{\gcd(m,n)}) &= \nu_p(B_{\tau\cdot\gcd(m,n)}) - \nu_p(B_\tau) - \nu_p(B_{\gcd(m,n)}) \\ &= \nu_p(B_{\gcd(m,n)}) + \nu_p(\tau) - \nu_p(B_\tau) - \nu_p(B_{\gcd(m,n)}) \\ &= \nu_p(\tau).\end{aligned}$$

Again, for this case, we have

$$\nu_p(\gcd(K_m, K_n)) = \nu_p(K_{\gcd(m,n)}).$$

Case 2.3: Suppose $\nu_p(B_m) > 0$ and $\nu_p(B_n) = 0$. By following the same argument as in Case 2.1 and Case 2.2, we have $\nu_p(K_m) = \nu_p(\tau)$ and $\nu_p(K_n) = \nu_p(B_{\tau n})$. Since $\tau \mid B_\tau$, by Lemma 12(iv), we have

$$\nu_p(\gcd(K_m, K_n)) = \nu_p(\gcd(\tau, B_{\tau n})) \leq \nu_p(\gcd(B_\tau, B_{\tau n})) = \nu_p(B_\tau) = 0.$$

Hence, $\nu_p(\gcd(K_m, K_n)) = 0$. Now we claim that $\nu_p(K_{\gcd(m,n)}) = 0$. Since, by Lemma 12(iv), $\nu_p(B_{\gcd(m,n)}) = \nu_p(\gcd(B_m, B_n)) = \min\{\nu_p(B_m), \nu_p(B_n)\} = 0$, it follows that

$$\nu_p(K_{\gcd(m,n)}) = \nu_p(B_{\tau\cdot\gcd(m,n)}) - \nu_p(B_\tau) - \nu_p(B_{\gcd(m,n)}) = \nu_p(B_{\tau\cdot\gcd(m,n)}).$$

Assume that $\nu_p(B_{\tau\cdot\gcd(m,n)}) > 0$. Since $\nu_p(B_m) > 0$, by Lemma 12(i), there exists a smallest positive integer m_0 such that $\nu_p(B_{m_0}) > 0$ and $m_0 \mid m$. Since $p \mid B_{\tau\cdot\gcd(m,n)}$, by Lemma 12(i), $m_0 \mid \tau \cdot \gcd(m, n)$. Since $\gcd(mn, \tau) = 1$ and $m_0 \mid m$, we have $\gcd(m_0, \tau) = 1$. Consequently, $m_0 \mid \gcd(m, n)$. This implies $m_0 \mid n$, so that, by Lemma 12(i), $\nu_p(B_n) > 0$, which is a contradiction. Hence, $\nu_p(B_{\tau\cdot\gcd(m,n)}) = 0 = \nu_p(K_{\gcd(m,n)})$. We conclude for this case that

$$\nu_p(\gcd(K_m, K_n)) = \nu_p(K_{\gcd(m,n)}).$$

Combining all cases, we have proved that for every prime p, we have

$$\nu_p(\gcd(K_m, K_n)) = \nu_p(K_{\gcd(m,n)}).$$

Hence

$$\gcd(K_m, K_n) = K_{\gcd(m,n)},$$

as desired. □

We point out that the condition in Theorem 13 on integer τ dividing B_τ is not particularly restrictive. This condition is investigated extensively in [2, 10].

Example 14. [10] The elliptic divisibility sequence $(B_n)_{n\geq 1}$ corresponding to elliptic curve $E : y^2 + y = x^3 - x$ and non-torsion point $P = (0, 0)$ is

$$(1, 1, 1, 1, 2, 1, 3, 5, 7, 4, 23, 29, 59, 129, 314, 65, 1529, 3689, 8209, 16264, 83313, \dots).$$

(See [12, A006769].) The indices τ with the property $\tau \mid B_\tau$ are

$$1, 40, 53, 63, 80, 127, 160, 189, 200, 320, 400, 441, 443, \dots.$$

According to Theorem 13 with $\tau = 40$, the sequence $(K_n)_{n\geq 1}$ defined by

$$K_n = \frac{B_{40n}}{B_{40}B_n} = \frac{B_{40n}}{(40 \cdot 13526278251270010)B_n}$$

for all $n \geq 1$ satisfies $\gcd(K_m, K_n) = K_{\gcd(m,n)}$ whenever $\gcd(mn, 40) = 1$.

The following result is an analog to Theorem 10 for p-adic valuation of sequence with nested indices. Here again, to describe the nth term of a sequence (a_n), we use the function notation $a(n)$ interchangeably with the subscript notation a_n.

Theorem 15. *Let $(B_n)_{n\geq 1}$ be an elliptic divisibility sequence corresponding to an elliptic curve whose Weierstrass equation (3) has coefficient a_1 even. Let n be a positive integer. Define a sequence $(G_k(n))_{k\geq 1}$ as follows: $G_1(n) = B_n$ and $G_{k+1}(n) = B(nG_k(n))$ for $k \geq 1$. Let p be a prime number. If $\nu_p(B_n) > 0$, then*

$$\nu_p(G_k(n)) = k\nu_p(B_n).$$

Therefore, if $B_n \neq 1$, then $B_n^k \parallel G_k(n)$ for all positive integers k.

Proof. We prove by induction on k. For $k = 1$, we have $G_1(n) = B_n$. Hence the statement holds. Assume that the statement holds for some positive integer k. Then, Lemma 12(ii, iii), we have

$$\begin{aligned}\nu_p(G_{k+1}(n)) &= \nu_p(B(nG_k(n))) = \nu_p(G_k(n)) + \nu_p(B_n)\\ &= k\nu_p(B_n) + \nu_p(B_n) = (k+1)\nu_p(B_n).\end{aligned}$$

By mathematical induction, the statement holds for all positive integers k. □

The final result is a generalization of Matijasevich's lemma [4, Lem. 17] for elliptic divisibility sequences. Matijasevich's lemma states that for $n > 2$ we have $F_n^2 \mid F_m$ if and only if $nF_n \mid m$ where $(F_n)_{n\geq 0}$ is the Fibonacci sequence.

Theorem 16. *Let $(B_n)_{n\geq 1}$ be an elliptic divisibility sequence corresponding to an elliptic curve whose Weierstrass equation (3) has coefficient a_1 even. Moreover, suppose that there exists a positive integer N such that all terms of the sequence $(B_n)_{n\geq N}$ are distinct and none of the terms $B_1, \ldots, B_{N-1}$ appears in $(B_n)_{n\geq N}$. Then, for all integers n, $r \geq N$ and for all positive integers k, we have $B_n^k \mid B_r$ if and only if $nB_n^{k-1} \mid r$.*

Proof. Let n, r be at least N and k a positive integer. Assume that $B_n^k \mid B_r$. Since $B_n \mid B_r$, by Lemma 12(iv), we have $B_{\gcd(n,r)} = \gcd(B_n, B_r) = B_n$. Since all terms of the sequence $(B_n)_{n\geq N}$ are distinct and none is equal to any $B_1, \ldots, B_{N-1}$, it follows that $\gcd(n, r) = n$ and therefore $n \mid r$. Write $r = ns$ for some positive integer s and let p be a prime dividing nB_n. We consider two cases.

Case 1: Suppose $p \mid B_n$. Let $\nu_p(B_n) = \ell \geq 1$. Then $k\ell = \nu_p(B_n^k) \leq \nu_p(B_r)$. By Lemma 12(ii, iii), we have

$$k\ell \leq \nu_p(B_r) = \nu_p(B_{ns}) = \nu_p(B_n) + \nu_p(s) = \ell + \nu_p(s).$$

Thus, $\nu_p(s) \geq (k-1)\ell$. Consequently,

$$\begin{aligned}\nu_p(nB_n^{k-1}) &= \nu_p(n) + \nu_p(B_n^{k-1}) = \nu_p(n) + (k-1)\ell \\ &\leq \nu_p(n) + \nu_p(s) = \nu_p(ns) = \nu_p(r).\end{aligned}$$

Case 2: Suppose $p \nmid B_n$. Then $p \mid n$ and we have $\nu_p(nB_n^{k-1}) = \nu_p(n) \leq \nu_p(r)$.

Combining all cases, we have $nB_n^{k-1} \mid r$.

For the converse, we assume that $nB_n^{k-1} \mid r$. Let p be a prime dividing B_n. Let $\nu_p(B_n) = \ell \geq 1$. Then Lemma 12(ii, iii, iv) implies

$$\begin{aligned}\nu_p(B_r) &\geq \nu_p(B_{nB_n^{k-1}}) = \nu_p(B_n) + \nu_p(B_n^{k-1}) \\ &= \ell + (k-1)\ell = k\ell = \nu_p(B_n^k).\end{aligned}$$

Since this is true for all primes p dividing B_n, it follows that $B_n^k \mid B_r$. □

4 Acknowledgments

The authors would like to thank the anonymous referee who provided constructive comments and valuable suggestions that led to the improvement of the quality of this paper. We would also like to thank Brian Hopkins for proofreading the first draft of this paper.

References

[1] P. Filipponi and H. T. Freitag, The Zeckendorf decomposition of certain classes of integers, in G. E. Bergum, A. N. Philippou, and A. F. Horadam, eds., *Applications of Fibonacci Numbers, Vol. 6*, Springer, 2012, pp. 123–135.

[2] A. Gottschlich, On positive integers n dividing the nth term of an elliptic divisibility sequence, *New York J. Math.* **18** (2012), 409–420.

[3] T. Lengyel, The order of the Fibonacci and Lucas numbers, *Fibonacci Quart.* **33** (1995), 234–239.

[4] Y. Matijasevich, Enumerable sets are diophantine, *Dokl. Math.* **11** (1970), 354–358.

[5] K. Onphaeng and P. Pongsriiam, Exact divisibility by powers of the integers in the Lucas sequence of the first kind, *AIMS Math.* **5** (2020), 6739–6748.

[6] C. Panraksa and A. Tangboonduangjit, On some arithmetic properties of a sequence related to the quotient of Fibonacci numbers, *Fibonacci Quart.* **55** (2017), 21–28.

[7] C. Panraksa and A. Tangboonduangjit, p-Adic valuation of Lucas iteration sequences, *Fibonacci Quart.* **56** (2018), 348–353.

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

[9] C. Sanna, The p-adic valuation of Lucas sequences, *Fibonacci Quart.* **54** (2016), 118–124.

[10] J. H. Silverman and K. Stange, Terms in elliptic divisibility sequences divisible by their indices, *Acta Arith.* **146** (2011), 355–378.

[11] J. H. Silverman and J. T. Tate, *Rational Points on Elliptic Curves*, Springer, 2015.

[12] N. J. A. Sloane et al., The On-Line Encyclopedia of Integer Sequences, 2022. Available at https://oeis.org.

[13] K. E. Stange, The Tate pairing via elliptic nets, in *International Conference on Pairing-Based Cryptography*, Springer, 2007, pp. 329–348.

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

[15] M. Verzobio, A recurrence relation for elliptic divisibility sequences, preprint, 2021. Available at https://arxiv.org/abs/2102.07573.

2020 *Mathematics Subject Classification*: Primary 11B39; Secondary 11B83.
Keywords: Fibonacci number, Lucas number, elliptic divisibility sequence, strong divisibility sequence, almost strong divisibility sequence, Matijasevich, Hilbert's tenth problem.

(Concerned with sequences A000045, A000225, A006769, and A088545.)

Received May 16 2022; revised versions received July 31 2022; August 7 2022. Published in *Journal of Integer Sequences*, October 28 2022.

Return to Journal of Integer Sequences home page.