Investigating divisibility properties of quotient sequences derived from Lucas and elliptic divisibility sequences

Aram Tangboonduangjit

Mahidol University International College,
Mahidol University,
Nakhon Pathom, Thailand

Journées Arithmétiques 2023
July 3, 2023

Table of Contents

Lucas Sequences

Definition 1 (Lucas Sequence)

Let P and Q be relatively prime integers. The Lucas sequence is defined by

- $U_0 = 0$, $U_1 = 1$, and
- $U_n = P \cdot U_{n-1} - Q \cdot U_{n-2}$ for $n \geq 2$.

Definition 1 (Lucas Sequence)

Let P and Q be relatively prime integers. The Lucas sequence is defined by

- $U_0 = 0$, $U_1 = 1$, and
- $U_n = P \cdot U_{n-1} - Q \cdot U_{n-2}$ for $n \geq 2$.

- $P = 1$, $Q = -1 \implies$ the sequence of the Fibonacci numbers $(F_n)_{n\geq 0}$:

$$0, \quad 1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad \ldots$$

Definition 1 (Lucas Sequence)

Let P and Q be relatively prime integers. The Lucas sequence is defined by

- $U_0 = 0$, $U_1 = 1$, and
- $U_n = P \cdot U_{n-1} - Q \cdot U_{n-2}$ for $n \geq 2$.

- $P = 1$, $Q = -1 \implies$ the sequence of the Fibonacci numbers $(F_n)_{n\geq 0}$:

$$0, \quad 1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad \ldots$$

- $P = 3$, $Q = 2 \implies$ the sequence of the Mersenne numbers $(M_n)_{n\geq 0}$:

$$0, \quad 1, \quad 3, \quad 7, \quad 15, \quad 31, \quad 63, \quad 127, \quad \ldots$$

Definition 1 (Lucas Sequence)

Let P and Q be relatively prime integers. The Lucas sequence is defined by

- $U_0 = 0,\ U_1 = 1$, and
- $U_n = P \cdot U_{n-1} - Q \cdot U_{n-2}$ for $n \geq 2$.

- $P = 1,\ Q = -1 \implies$ the sequence of the Fibonacci numbers $(F_n)_{n\geq 0}$:

$$0, \quad 1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad \ldots$$

- $P = 3,\ Q = 2 \implies$ the sequence of the Mersenne numbers $(M_n)_{n\geq 0}$:

$$0, \quad 1, \quad 3, \quad 7, \quad 15, \quad 31, \quad 63, \quad 127, \quad \ldots$$

- In general,

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

where α and β are the zeroes of the characteristic polynomial $p(x) = x^2 - Px + Q$.

Elliptic Divisibility Sequences - Recurrence Definition

Definition 2 (Elliptic Divisibility Sequence (EDS))

A sequence $(h_n)_{n\geq 0}$ is said to be an elliptic divisibility sequence if

- $h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$ for all $m \geq n \geq 0$, and
- $m \mid n \implies h_m \mid h_n$.

Definition 2 (Elliptic Divisibility Sequence (EDS))

A sequence $(h_n)_{n\geq 0}$ is said to be an elliptic divisibility sequence if

- $h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$ for all $m \geq n \geq 0$, and
- $m \mid n \implies h_m \mid h_n$.

For example,

- The sequence $(n)_{n\geq 0}$ of nonnegative integers:

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6, \quad 7, \quad 8, \quad 9, \quad \ldots$$

Definition 2 (Elliptic Divisibility Sequence (EDS))

A sequence $(h_n)_{n\geq 0}$ is said to be an elliptic divisibility sequence if

- $h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$ for all $m \geq n \geq 0$, and
- $m \mid n \implies h_m \mid h_n$.

For example,

- The sequence $(n)_{n\geq 0}$ of nonnegative integers:

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6, \quad 7, \quad 8, \quad 9, \quad \ldots$$

- The sequence $\left((-1)^{(n-1)(n-2)/2}F_n\right)$ where F_n is the nth Fibonacci number:

$$0, \quad 1, \quad 1, \quad -2, \quad -3, \quad 5, \quad 8, \quad -13, \quad -21, \quad 34, \quad \ldots$$

Definition 2 (Elliptic Divisibility Sequence (EDS))

A sequence $(h_n)_{n\geq 0}$ is said to be an elliptic divisibility sequence if

- $h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$ for all $m \geq n \geq 0$, and
- $m \mid n \implies h_m \mid h_n$.

For example,

- The sequence $(n)_{n\geq 0}$ of nonnegative integers:

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6, \quad 7, \quad 8, \quad 9, \quad \ldots$$

- The sequence $\left((-1)^{(n-1)(n-2)/2}F_n\right)$ where F_n is the nth Fibonacci number:

$$0, \quad 1, \quad 1, \quad -2, \quad -3, \quad 5, \quad 8, \quad -13, \quad -21, \quad 34, \quad \ldots$$

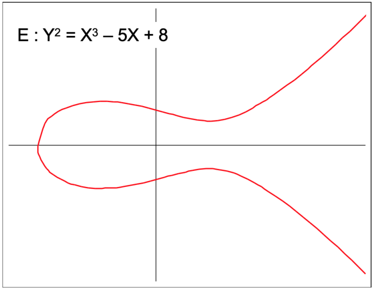
(F_n) satisfies the following identity:

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

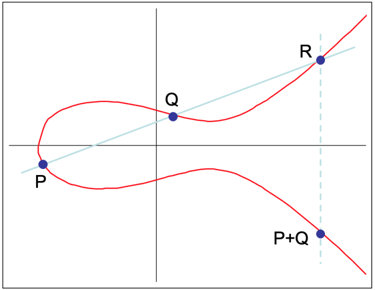
Elliptic Divisibility Sequences - Elliptic Curve Based Definition

- Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with integer coefficients.

- Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with integer coefficients.
- Rational points on this curves form a group $E(\mathbb{Q})$.

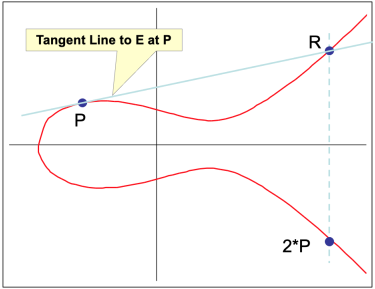


credit: J. Silverman, K. Stange

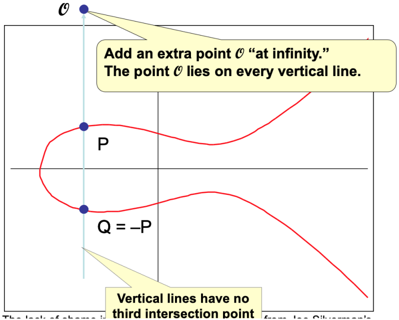


credit: J. Silverman, K. Stange

Adding Points on Elliptic Curves (cont.)



credit: J. Silverman, K. Stange



credit: J. Silverman, K. Stange

- Let P be a non-identity point in $E(\mathbb{Q})$ and n a positive integer. Consider $P + P + \cdots + P = nP$.

- Let P be a non-identity point in $E(\mathbb{Q})$ and n a positive integer. Consider $P + P + \cdots + P = nP$.
- The 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 are in lowest terms.

- Let P be a non-identity point in $E(\mathbb{Q})$ and n a positive integer. Consider $P + P + \cdots + P = nP$.
- The 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 are in lowest terms.

- The sequence $(B_{nP})_{n\geq 1}$ so obtained is called an elliptic divisibility sequence.

- Let P be a non-identity point in $E(\mathbb{Q})$ and n a positive integer. Consider $P + P + \cdots + P = nP$.
- The 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 are in lowest terms.

- The sequence $(B_{nP})_{n\geq 1}$ so obtained is called an elliptic divisibility sequence.
- For example, with the curve $y^2 + y = x^3 + x^2 - 2x$ and $P = (0, 0)$ we obtain $P = (\frac{0}{1}, \frac{0}{1})$, $2P = (\frac{3}{1}, \frac{5}{1})$, $3P = (-\frac{11}{9}, \frac{28}{27})$, $4P = (\frac{114}{121}, -\frac{267}{1331})$, $5P = (-\frac{2739}{1444}, -\frac{77033}{54872})$, $6P = (\frac{89566}{62001}, -\frac{31944320}{15438249})$, so that

- Let P be a non-identity point in $E(\mathbb{Q})$ and n a positive integer. Consider $P + P + \cdots + P = nP$.
- The 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 are in lowest terms.

- The sequence $(B_{nP})_{n\geq 1}$ so obtained is called an elliptic divisibility sequence.
- For example, with the curve $y^2 + y = x^3 + x^2 - 2x$ and $P = (0, 0)$ we obtain $P = (\frac{0}{1}, \frac{0}{1})$, $2P = (\frac{3}{1}, \frac{5}{1})$, $3P = (-\frac{11}{9}, \frac{28}{27})$, $4P = (\frac{114}{121}, -\frac{267}{1331})$, $5P = (-\frac{2739}{1444}, -\frac{77033}{54872})$, $6P = (\frac{89566}{62001}, -\frac{31944320}{15438249})$, so that

$$B_1 = 1,$$

- Let P be a non-identity point in $E(\mathbb{Q})$ and n a positive integer. Consider $P + P + \cdots + P = nP$.
- The 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 are in lowest terms.

- The sequence $(B_{nP})_{n\geq 1}$ so obtained is called an elliptic divisibility sequence.
- For example, with the curve $y^2 + y = x^3 + x^2 - 2x$ and $P = (0, 0)$ we obtain $P = (\frac{0}{1}, \frac{0}{1})$, $2P = (\frac{3}{1}, \frac{5}{1})$, $3P = (-\frac{11}{9}, \frac{28}{27})$, $4P = (\frac{114}{121}, -\frac{267}{1331})$, $5P = (-\frac{2739}{1444}, -\frac{77033}{54872})$, $6P = (\frac{89566}{62001}, -\frac{31944320}{15438249})$, so that

$$B_1 = 1, \quad B_2 = 1,$$

- Let P be a non-identity point in $E(\mathbb{Q})$ and n a positive integer. Consider $P + P + \cdots + P = nP$.
- The 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 are in lowest terms.

- The sequence $(B_{nP})_{n\geq 1}$ so obtained is called an elliptic divisibility sequence.
- For example, with the curve $y^2 + y = x^3 + x^2 - 2x$ and $P = (0,0)$ we obtain $P = (\frac{0}{1}, \frac{0}{1})$, $2P = (\frac{3}{1}, \frac{5}{1})$, $3P = (-\frac{11}{9}, \frac{28}{27})$, $4P = (\frac{114}{121}, -\frac{267}{1331})$, $5P = (-\frac{2739}{1444}, -\frac{77033}{54872})$, $6P = (\frac{89566}{62001}, -\frac{31944320}{15438249})$, so that

$$B_1 = 1, \quad B_2 = 1, \quad B_3 = 3,$$

- Let P be a non-identity point in $E(\mathbb{Q})$ and n a positive integer. Consider $P + P + \cdots + P = nP$.
- The 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 are in lowest terms.

- The sequence $(B_{nP})_{n\geq 1}$ so obtained is called an elliptic divisibility sequence.
- For example, with the curve $y^2 + y = x^3 + x^2 - 2x$ and $P = (0, 0)$ we obtain $P = (\frac{0}{1}, \frac{0}{1})$, $2P = (\frac{3}{1}, \frac{5}{1})$, $3P = (-\frac{11}{9}, \frac{28}{27})$, $4P = (\frac{114}{121}, -\frac{267}{1331})$, $5P = (-\frac{2739}{1444}, -\frac{77033}{54872})$, $6P = (\frac{89566}{62001}, -\frac{31944320}{15438249})$, so that

$$B_1 = 1, \quad B_2 = 1, \quad B_3 = 3, \quad B_4 = 11,$$

- Let P be a non-identity point in $E(\mathbb{Q})$ and n a positive integer. Consider $P + P + \cdots + P = nP$.
- The 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 are in lowest terms.

- The sequence $(B_{nP})_{n\geq 1}$ so obtained is called an elliptic divisibility sequence.
- For example, with the curve $y^2 + y = x^3 + x^2 - 2x$ and $P = (0, 0)$ we obtain $P = (\frac{0}{1}, \frac{0}{1})$, $2P = (\frac{3}{1}, \frac{5}{1})$, $3P = (-\frac{11}{9}, \frac{28}{27})$, $4P = (\frac{114}{121}, -\frac{267}{1331})$, $5P = (-\frac{2739}{1444}, -\frac{77033}{54872})$, $6P = (\frac{89566}{62001}, -\frac{31944320}{15438249})$, so that

$$B_1 = 1, \quad B_2 = 1, \quad B_3 = 3, \quad B_4 = 11, \quad B_5 = 38,$$

- Let P be a non-identity point in $E(\mathbb{Q})$ and n a positive integer. Consider $P + P + \cdots + P = nP$.
- The 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 are in lowest terms.

- The sequence $(B_{nP})_{n\geq 1}$ so obtained is called an elliptic divisibility sequence.
- For example, with the curve $y^2 + y = x^3 + x^2 - 2x$ and $P = (0, 0)$ we obtain $P = (\frac{0}{1}, \frac{0}{1})$, $2P = (\frac{3}{1}, \frac{5}{1})$, $3P = (-\frac{11}{9}, \frac{28}{27})$, $4P = (\frac{114}{121}, -\frac{267}{1331})$, $5P = (-\frac{2739}{1444}, -\frac{77033}{54872})$, $6P = (\frac{89566}{62001}, -\frac{31944320}{15438249})$, so that

$$B_1 = 1, \quad B_2 = 1, \quad B_3 = 3, \quad B_4 = 11, \quad B_5 = 38, \quad B_6 = 249,$$

- Let P be a non-identity point in $E(\mathbb{Q})$ and n a positive integer. Consider $P + P + \cdots + P = nP$.
- The 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 are in lowest terms.

- The sequence $(B_{nP})_{n\geq 1}$ so obtained is called an elliptic divisibility sequence.
- For example, with the curve $y^2 + y = x^3 + x^2 - 2x$ and $P = (0, 0)$ we obtain $P = (\frac{0}{1}, \frac{0}{1})$, $2P = (\frac{3}{1}, \frac{5}{1})$, $3P = (-\frac{11}{9}, \frac{28}{27})$, $4P = (\frac{114}{121}, -\frac{267}{1331})$, $5P = (-\frac{2739}{1444}, -\frac{77033}{54872})$, $6P = (\frac{89566}{62001}, -\frac{31944320}{15438249})$, so that

$$B_1 = 1, \quad B_2 = 1, \quad B_3 = 3, \quad B_4 = 11, \quad B_5 = 38, \quad B_6 = 249, \quad \ldots$$

Table of Contents

Lemma 3 (Sanna)

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

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

where $\tau(p) =$ least positive integer such that $p \mid U_{\tau(p)}$.

Lemma 4 (Panraksa, T)

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

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

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

Lemma 4 (Panraksa, T)

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

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

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

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

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

where $D = P^2 - 4Q$*, the discriminant of the characteristic polynomial of the sequence* (U_n)*.*

Table of Contents

Lemma 5

Let $(B_n)_{n\geq 1}$ be an elliptic divisibility sequence corresponding to an elliptic curve E with the Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and a non-torsion point P in $E(\mathbb{Q})$.

Lemma 5

Let $(B_n)_{n\geq 1}$ be an elliptic divisibility sequence corresponding to an elliptic curve E with the Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and a non-torsion point P in $E(\mathbb{Q})$.

- *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, $p \mid B_n$ iff $n_0 \mid n$.*

Lemma 5

Let $(B_n)_{n\geq 1}$ be an elliptic divisibility sequence corresponding to an elliptic curve E with the Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and a non-torsion point P in $E(\mathbb{Q})$.

- *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, $p \mid B_n$ iff $n_0 \mid n$.*
- *Let p be an odd prime. For every pair of positive integers m, n, if $\nu_p(B_n) > 0$ then $\nu_p(B_{mn}) = \nu_p(B_n) + \nu_p(m)$.*

Lemma 5

Let $(B_n)_{n\geq 1}$ be an elliptic divisibility sequence corresponding to an elliptic curve E with the Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and a non-torsion point P in $E(\mathbb{Q})$.

- *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, $p \mid B_n$ iff $n_0 \mid n$.*
- *Let p be an odd prime. For every pair of positive integers m, n, if $\nu_p(B_n) > 0$ then $\nu_p(B_{mn}) = \nu_p(B_n) + \nu_p(m)$.*
- *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 $|\nu_2(B_{mn}) - (\nu_2(B_n) + \nu_2(m))| \leq \epsilon$ otherwise, where the constant ϵ depends only on E and P.*

Lemma 5

Let $(B_n)_{n\geq 1}$ be an elliptic divisibility sequence corresponding to an elliptic curve E with the Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and a non-torsion point P in $E(\mathbb{Q})$.

- *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, $p \mid B_n$ iff $n_0 \mid n$.*
- *Let p be an odd prime. For every pair of positive integers m, n, if $\nu_p(B_n) > 0$ then $\nu_p(B_{mn}) = \nu_p(B_n) + \nu_p(m)$.*
- *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 $|\nu_2(B_{mn}) - (\nu_2(B_n) + \nu_2(m))| \leq \epsilon$ otherwise, where the constant ϵ depends only on E and P.*
- *For all positive integers m, n,*

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

  i.e., EDS is a strong divisibility sequence.

Table of Contents

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.
For example, for the sequence $U(4, -7)$, we have $\Delta = 12$ and the first five terms of the sequence (T_n) are

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.
For example, for the sequence $U(4, -7)$, we have $\Delta = 12$ and the first five terms of the sequence (T_n) are

$$1,$$

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.
For example, for the sequence $U(4, -7)$, we have $\Delta = 12$ and the first five terms of the sequence (T_n) are

$$1, \quad \frac{76751}{2},$$

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.
For example, for the sequence $U(4, -7)$, we have $\Delta = 12$ and the first five terms of the sequence (T_n) are

$$1, \quad \frac{76751}{2}, \quad \frac{3240525601}{3},$$

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.
For example, for the sequence $U(4, -7)$, we have $\Delta = 12$ and the first five terms of the sequence (T_n) are

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

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.
For example, for the sequence $U(4,-7)$, we have $\Delta = 12$ and the first five terms of the sequence (T_n) are

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

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.
For example, for the sequence $U(4,-7)$, we have $\Delta = 12$ and the first five terms of the sequence (T_n) are

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

For the Fibonacci sequence $F_n = U(1,-1)$, we have $\Delta = 5$ and the first five terms of the sequence (T_n) are

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.
For example, for the sequence $U(4,-7)$, we have $\Delta = 12$ and the first five terms of the sequence (T_n) are

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

For the Fibonacci sequence $F_n = U(1,-1)$, we have $\Delta = 5$ and the first five terms of the sequence (T_n) are

$$1,$$

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.
For example, for the sequence $U(4, -7)$, we have $\Delta = 12$ and the first five terms of the sequence (T_n) are

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

For the Fibonacci sequence $F_n = U(1, -1)$, we have $\Delta = 5$ and the first five terms of the sequence (T_n) are

$$1, \quad 11,$$

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.
For example, for the sequence $U(4, -7)$, we have $\Delta = 12$ and the first five terms of the sequence (T_n) are

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

For the Fibonacci sequence $F_n = U(1, -1)$, we have $\Delta = 5$ and the first five terms of the sequence (T_n) are

$$1, \quad 11, \quad 61,$$

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.
For example, for the sequence $U(4, -7)$, we have $\Delta = 12$ and the first five terms of the sequence (T_n) are

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

For the Fibonacci sequence $F_n = U(1, -1)$, we have $\Delta = 5$ and the first five terms of the sequence (T_n) are

$$1, \quad 11, \quad 61, \quad 451,$$

Let the sequence $(T_n)_{n\geq 1}$ be defined by

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

where $\Delta = |D|$ and D is the discriminant of the characteristic polynomial $x^2 - Px + Q$ associated with the Lucas sequence $(U_n)_{n\geq 0}$.
For example, for the sequence $U(4,-7)$, we have $\Delta = 12$ and the first five terms of the sequence (T_n) are

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

For the Fibonacci sequence $F_n = U(1,-1)$, we have $\Delta = 5$ and the first five terms of the sequence (T_n) are

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

Definition 6

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 $\gcd(mn, N) = 1$.

Theorem 7 (Panraksa, T)

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

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

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

$$T_n,$$

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

$$T_n, \quad T_{nT_n},$$

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

$$T_n, \quad T_{nT_n}, \quad T_{nT_{nT_n}},$$

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

$$T_n, \quad T_{nT_n}, \quad T_{nT_{nT_n}}, \quad T_{nT_{nT_{nT_n}}}.$$

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

$$T_n, \quad T_{nT_n}, \quad T_{nT_{nT_n}}, \quad T_{nT_{nT_{nT_n}}}.$$

Theorem 8 (Panraksa, T)

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

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

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: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and a non-torsion point P. Define the sequence $(K_n)_{n\geq 1}$ by

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

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: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and a non-torsion point P. Define the sequence $(K_n)_{n\geq 1}$ by

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

Theorem 9 (Panraksa, T)

If the coefficient a_1 is even and $\tau \mid B_\tau$, then the sequence $(K_n)_{n\geq 1}$ is a τ-almost strong divisibility sequence. That is, for all positive integers m,n, if $\gcd(mn, \tau) = 1$, then

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

For example, the elliptic divisibility sequence $(B_n)_{n\geq 1}$ corresponding to the elliptic curve $E:\ y^2+y=x^3-x$ and the point $P=(0,0)$ is

$$1,\quad 1,\quad 1,\quad 1,\quad 2,\quad 1,\quad 3,\quad 5,\quad 7,\quad 4,\quad 23,\quad 29,\quad 59,\quad 129,\quad 314,\quad 65,\quad 1529,\quad \ldots$$

For example, the elliptic divisibility sequence $(B_n)_{n\geq 1}$ corresponding to the elliptic curve $E: \; y^2 + y = x^3 - x$ and the point $P = (0,0)$ is

$$1, \quad 1, \quad 1, \quad 1, \quad 2, \quad 1, \quad 3, \quad 5, \quad 7, \quad 4, \quad 23, \quad 29, \quad 59, \quad 129, \quad 314, \quad 65, \quad 1529, \quad \ldots$$

One can check that $40 \mid B_{40}$. Then 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 $\gcd(mn, 40) = 1$.

Theorem 10 (Panraksa, T)

Let $(B_n)_{n\geq 1}$ be an elliptic divisibility sequence corresponding to an elliptic curve whose Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ has 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 $G_k(n) = B(nG_{k-1}(n))$ for $k \geq 2$. Then, if $B_n \neq 1$, we have

$$B_n^k \,||\, G_k(n)$$

for all positive integers k.

Lemma 11 (Matijasevich)

For $n > 2$, we have

$$F_n^2 \mid F_m \quad \text{if and only if} \quad nF_n \mid m.$$

Lemma 11 (Matijasevich)

For $n > 2$, we have

$$F_n^2 \mid F_m \quad \textit{if and only if} \quad nF_n \mid m.$$

Hilbert's 10th Problem

Is there a general algorithm to determine whether a given Diophantine equation (a polynomial equation with integer coefficients and a finite number of unknowns) has a solution in integers?

Lemma 11 (Matijasevich)

For $n > 2$, we have

$$F_n^2 \mid F_m \quad \textit{if and only if} \quad nF_n \mid m.$$

Hilbert's 10th Problem

Is there a general algorithm to determine whether a given Diophantine equation (a polynomial equation with integer coefficients and a finite number of unknowns) has a solution in integers? For example, the equation $x^2 + y^2 = z^2$ has infinitely many solutions in nonzero integers, while $x^n + y^n = z^n$ has no solutions in nonzero integers, for $n \geq 3$.

Lemma 11 (Matijasevich)

For $n > 2$, we have

$$F_n^2 \mid F_m \quad \textit{if and only if} \quad nF_n \mid m.$$

Hilbert's 10th Problem

Is there a general algorithm to determine whether a given Diophantine equation (a polynomial equation with integer coefficients and a finite number of unknowns) has a solution in integers? For example, the equation $x^2 + y^2 = z^2$ has infinitely many solutions in nonzero integers, while $x^n + y^n = z^n$ has no solutions in nonzero integers, for $n \geq 3$.

Theorem 12 (Panraksa, T)

Let $(B_n)_{n\geq 1}$ be an elliptic divisibility sequence corresponding to an elliptic curve whose Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ has 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

$$B_n^k \mid B_r \quad \textit{if and only if} \quad nB_n^{k-1} \mid r.$$

Table of Contents

Thank You!

References I

[Mat70] Yuri Matijasevich. "Enumerable sets are Diophantine, Dokl". In: *Dokl. Math.* 11 (1970), pp. 354–358.

[PT17] Chatchawan Panraksa and Aram Tangboonduangjit. "On some arithmetic properties of a sequence related to the quotient of Fibonacci numbers". In: *Fibonacci Quart* 55.1 (2017), pp. 21–28.

[PT18] Chatchawan Panraksa and Aram Tangboonduangjit. "p-Adic valuation of Lucas iteration sequences". In: *Fibonacci Quart* 56.4 (2018), pp. 348–353.

[PT22] Chatchawan Panraksa and Aram Tangboonduangjit. "Some divisibility properties concerning Lucas and elliptic divisibility sequences". In: *Journal of Integer Sequences* 25.2 (2022), pp. 1–15.

[San16] Carlo Sanna. "The p-adic valuation of Lucas sequences". In: *Fibonacci Quart* 54.2 (2016), pp. 118–124.