Divisibility Sequences

Aditya Bisain

Euler Circle

July 2025

A Brief History of Divisibility Sequences

- **19th century:** Édouard Lucas studies linear recurrence sequences like Fibonacci and Lucas numbers.

A Brief History of Divisibility Sequences

- **19th century:** Édouard Lucas studies linear recurrence sequences like Fibonacci and Lucas numbers.
- **1948:** Morgan Ward defines **elliptic divisibility sequences (EDS)** in the context of division polynomials on elliptic curves.

A Brief History of Divisibility Sequences

- **19th century:** Édouard Lucas studies linear recurrence sequences like Fibonacci and Lucas numbers.
- **1948:** Morgan Ward defines **elliptic divisibility sequences (EDS)** in the context of division polynomials on elliptic curves.
- **2000s:** Rachel Shipsey explores EDS modulo prime powers.

What is a Divisibility Sequence?

Definition

A sequence of integers (a_n) is a **divisibility sequence** if

$$m \mid n \implies a_m \mid a_n.$$

What is a Divisibility Sequence?

Definition

A sequence of integers (a_n) is a **divisibility sequence** if

$$m \mid n \implies a_m \mid a_n.$$

The most basic examples of divisibility sequences are constant sequences and the sequence $a_n = n$.

Examples

Example

Fibonacci Sequence:

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2}.$$

Examples

Example

Fibonacci Sequence:

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2}.$$

For example, $F_{10} = 55$ and $F_{20} = 6765$. Indeed, $6765 = 55 \cdot 123$.

Examples

Example

Fibonacci Sequence:

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2}.$$

For example, $F_{10} = 55$ and $F_{20} = 6765$. Indeed, $6765 = 55 \cdot 123$.

Example

Mersenne Numbers:

$$M_n = 2^n - 1.$$

Examples

Example

Fibonacci Sequence:

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2}.$$

For example, $F_{10} = 55$ and $F_{20} = 6765$. Indeed, $6765 = 55 \cdot 123$.

Example

Mersenne Numbers:

$$M_n = 2^n - 1.$$

For example, $M_7 = 127$ and $M_{21} = 2097151$. Indeed, one can check that $2097151 = 127 \cdot 16513$.

Both satisfy $m \mid n \implies a_m \mid a_n$.

Linear Divisibility Sequences (LDS)

Definition

A sequence (a_n) is a **linear divisibility sequence (LDS)** if:

1. It satisfies a linear recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

   where $c_1, c_2, \ldots c_k$ are non-negative integers.

2. It satisfies the divisibility property

$$m \mid n \implies a_m \mid a_n.$$

Theorem: Characterization of LDS

Theorem

Any order-2 LDS with $a_0 = 0$ *can be written as*

$$a_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

where α, β *are roots of a quadratic with integer coefficients.*

Theorem: Characterization of LDS

Theorem

Any order-2 LDS with $a_0 = 0$ can be written as

$$a_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

where α, β are roots of a quadratic with integer coefficients.

Example

The Fibonacci sequence:

$$F_n = \frac{\varphi^n - (1 - \varphi)^n}{\sqrt{5}}$$

where $\varphi = \frac{1+\sqrt{5}}{2}$.

Elliptic Sequences

Definition

A sequence (h_n) of integers satisfies

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

for all $m, n \in \mathbb{N}$ and is called an **elliptic sequence**. An elliptic sequence (h_n) is an **EDS** if it also satisfies the divisibility property

$$m \mid n \implies h_m \mid h_n.$$

Proof: $h_n = n$ is an EDS

Theorem

The sequence $h_n = n$ satisfies the elliptic recurrence and is thus an EDS.

Proof: $h_n = n$ is an EDS

Theorem

The sequence $h_n = n$ satisfies the elliptic recurrence and is thus an EDS.

Proof.

$$h_{m+n}h_{m-n} = (m+n)(m-n) = m^2 - n^2.$$

Proof: $h_n = n$ is an EDS

Theorem

The sequence $h_n = n$ satisfies the elliptic recurrence and is thus an EDS.

Proof.

$$h_{m+n}h_{m-n} = (m+n)(m-n) = m^2 - n^2.$$

$$\begin{aligned} &h_{m+1}h_{m-1}h_n^2 - (h_{n+1}h_{n-1})h_m^2 \\ &= (m+1)(m-1)n^2 - (n+1)(n-1)m^2 \\ &= (m^2-1)n^2 - (n^2-1)m^2 = m^2 - n^2. \end{aligned}$$

Both sides are equal, so $h_n = n$ satisfies the recurrence. □

Proof: $G_n = F_{2n}$ is an EDS

Theorem

The sequence $G_n = F_{2n}$ satisfies the elliptic recurrence:

$$G_{m+n}G_{m-n} = G_{m+1}G_{m-1}G_n^2 - G_{n+1}G_{n-1}G_m^2$$

and is thus an EDS.

Proof: $G_n = F_{2n}$ is an EDS

Theorem

The sequence $G_n = F_{2n}$ satisfies the elliptic recurrence:

$$G_{m+n}G_{m-n} = G_{m+1}G_{m-1}G_n^2 - G_{n+1}G_{n-1}G_m^2$$

and is thus an EDS.

- Divisibility is immediate since F_n is a divisibility sequence.

Proof: $G_n = F_{2n}$ is an EDS

Theorem

The sequence $G_n = F_{2n}$ satisfies the elliptic recurrence:

$$G_{m+n}G_{m-n} = G_{m+1}G_{m-1}G_n^2 - G_{n+1}G_{n-1}G_m^2$$

and is thus an EDS.

- Divisibility is immediate since F_n is a divisibility sequence.
- It remains to check the elliptic recurrence.

Proof: $G_n = F_{2n}$ is an EDS

Theorem

The sequence $G_n = F_{2n}$ satisfies the elliptic recurrence:

$$G_{m+n}G_{m-n} = G_{m+1}G_{m-1}G_n^2 - G_{n+1}G_{n-1}G_m^2$$

and is thus an EDS.

- Divisibility is immediate since F_n is a divisibility sequence.
- It remains to check the elliptic recurrence.

Sketch of Proof for G_n

We use the following identities for G_n:

$$G_{m+1} = 3G_m - G_{m-1}$$
$$G_{m+n} = G_m G_{n+1} - G_{m-1} G_n$$
$$G_{m-n} = G_{m-1} G_n - G_m G_{n-1}$$

Sketch of Proof for G_n

We use the following identities for G_n:

$$G_{m+1} = 3G_m - G_{m-1}$$
$$G_{m+n} = G_m G_{n+1} - G_{m-1} G_n$$
$$G_{m-n} = G_{m-1} G_n - G_m G_{n-1}$$

Substitute G_{m+n} and G_{m-n} into the recurrence:

$$G_{m+n} G_{m-n} = (G_m G_{n+1} - G_{m-1} G_n)(G_{m-1} G_n - G_m G_{n-1}).$$

Sketch of Proof for G_n

We use the following identities for G_n:

$$G_{m+1} = 3G_m - G_{m-1}$$
$$G_{m+n} = G_m G_{n+1} - G_{m-1} G_n$$
$$G_{m-n} = G_{m-1} G_n - G_m G_{n-1}$$

Substitute G_{m+n} and G_{m-n} into the recurrence:

$$G_{m+n} G_{m-n} = (G_m G_{n+1} - G_{m-1} G_n)(G_{m-1} G_n - G_m G_{n-1}).$$

Expand and simplify to get:

$$3G_m G_{m-1} G_n^2 - G_{m-1}^2 G_n^2 - G_m^2 G_{n+1} G_{n-1}.$$

Sketch of Proof for G_n

We use the following identities for G_n:

$$G_{m+1} = 3G_m - G_{m-1}$$
$$G_{m+n} = G_m G_{n+1} - G_{m-1} G_n$$
$$G_{m-n} = G_{m-1} G_n - G_m G_{n-1}$$

Substitute G_{m+n} and G_{m-n} into the recurrence:

$$G_{m+n} G_{m-n} = (G_m G_{n+1} - G_{m-1} G_n)(G_{m-1} G_n - G_m G_{n-1}).$$

Expand and simplify to get:

$$3 G_m G_{m-1} G_n^2 - G_{m-1}^2 G_n^2 - G_m^2 G_{n+1} G_{n-1}.$$

If we factor $G_{m-1} G_n^2$ from the first two terms and then plug in $G_{m+1} = 3G_m - G_{m-1}$, we get

$$G_{m+1} G_{m-1} G_n^2 - G_{n+1} G_{n-1} G_m^2.$$

Thus G_n satisfies the elliptic recurrence.

Elliptic Divisibility Sequences (EDS)

Theorem

Every EDS is a strong divisibility sequence:

$$\gcd(h_m, h_n) = h_{\gcd(m,n)}$$

if h_3, h_4 are coprime.

Elliptic Divisibility Sequences (EDS)

Theorem

Every EDS is a strong divisibility sequence:

$$\gcd(h_m, h_n) = h_{\gcd(m,n)}$$

if h_3, h_4 are coprime.

Example

$$\gcd(G_4, G_6) = \gcd(21, 144) = 3$$

$$G_{\gcd(4,6)} = G_2 = F_4 = 3$$

Thus,

$$\boxed{\gcd(G_4, G_6) = G_{\gcd(4,6)}}$$

Theorem

Let (h_n) *be an elliptic sequence, and* h_k *any nonzero term. Define*

$$\ell_n = \frac{h_{nk}}{h_k}.$$

Then (ℓ_n) *is also an elliptic sequence. If* (h_n) *is an EDS, so is* (ℓ_n)*.*

Let's look at an example with (G_n).

Example

Choose $k = 3$ and let $h_n = G_n$. Define

$$\ell_n = \frac{h_{nk}}{h_k} = \frac{h_{3n}}{8} = \frac{F_{6n}}{8}.$$

The first terms of (ℓ_n) are

$$\ell_1 = 1, \quad \ell_2 = 18, \quad \ell_3 = 323, \quad \ell_4 = 5796, \ldots$$

By the previous theorem, (ℓ_n), or $\frac{F_{6n}}{8}$ is also an EDS.

Rank of Apparition: Definition

Definition

The **rank of apparition** of an integer m in a sequence (h_n) is the smallest positive integer n such that
$$m \mid h_n.$$

Rank of Apparition: Definition

Definition

The **rank of apparition** of an integer m in a sequence (h_n) is the smallest positive integer n such that

$$m \mid h_n.$$

- We consider $m = p^k$, where p is a prime and $k \geq 1$.
- Intuitively, the rank of apparition is the first index where p divides the term.

Rank of Apparition: Theorem

Theorem

Let (h_n) *be an elliptic divisibility sequence (EDS), and fix a prime integer* p*. Denote the rank of apparition of* p^k *to be* ρ_k*. Then*

$$p^k \mid h_r \iff \rho_k \mid r.$$

That is, divisibility by powers of p *occurs exactly at multiples of* ρ_k*.*

Example

Consider G_n as our EDS. The first few terms are:

Example

Consider G_n as our EDS. The first few terms are:

$$G_1 = 1, \quad G_2 = 3, \quad G_3 = 8, \quad G_4 = 21, \quad G_5 = 55, \quad G_6 = 144.$$

Example

Consider G_n as our EDS. The first few terms are:

$$G_1 = 1, \quad G_2 = 3, \quad G_3 = 8, \quad G_4 = 21, \quad G_5 = 55, \quad G_6 = 144.$$

For prime $p = 3$:

$$3 \mid G_2 = 3, \quad 9 = 3^2 \mid G_6 = 144,$$

Example

Consider G_n as our EDS. The first few terms are:

$$G_1 = 1, \quad G_2 = 3, \quad G_3 = 8, \quad G_4 = 21, \quad G_5 = 55, \quad G_6 = 144.$$

For prime $p = 3$:

$$3 \mid G_2 = 3, \quad 9 = 3^2 \mid G_6 = 144,$$

so

$$\rho_1 = 2, \quad \rho_2 = 6.$$

Example

Consider G_n as our EDS. The first few terms are:

$$G_1 = 1, \quad G_2 = 3, \quad G_3 = 8, \quad G_4 = 21, \quad G_5 = 55, \quad G_6 = 144.$$

For prime $p = 3$:

$$3 \mid G_2 = 3, \quad 9 = 3^2 \mid G_6 = 144,$$

so

$$\rho_1 = 2, \quad \rho_2 = 6.$$

Divisibility by 3 happens at multiples of $2(G_8 = 987)$, and divisibility by 9 happens at multiples of $6(G_{12} = 46,368)$.