Divisibility Sequences

Aditya Bisain

June 2025

1 Abstract

This paper explores the theory of divisibility sequences. We briefly cover some definitions and linear divisibility sequences (LDS). Then, we take a deep dive into the theory of elliptic divisibility sequences (EDS). We present classical results for LDS such as those for Fibonacci and Lucas numbers, and build a deeper theory for EDS: including recurrence relations, doubling/stepping formulas, structure theorems, and classification of vanishing terms. We end with a number-theoretic discussion of periodicity modulo primes and ranks of apparition.

2 Introduction

Definition 2.1. *A sequence (a_n) is called a* ***divisibility sequence*** *when it has the property: if $m \mid n$, then $a_m \mid a_n$.*

Definition 2.2. *A sequence (a_n) is called a* ***strong divisibility sequence*** *when $\gcd(a_m, a_n) = a_{\gcd(m,n)}$.*

To get used to these definitions, we will cover some common examples of divisibility sequences.

Theorem 2.1. *The sequence of Mersenne numbers (numbers of the form $2^n - 1$) forms a divisibility sequence.*

Proof. Let $M_n = 2^n - 1$. If $m \mid n$, write $n = mk$ for some integer k. Then:

$$M_n = 2^{mk} - 1 = (2^m)^k - 1 = (2^m - 1)\sum_{i=0}^{k-1}(2^m)^i.$$

Since $M_m = 2^m - 1$ divides this, the claim follows. □

Theorem 2.2. *The Fibonacci sequence is a divisibility sequence.*

Proof. The proof requires using induction twice. First, we show a powerful result which states that $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$ Our base cases will be $n = 1$ and $n = 2$. For $n = 1$, we have

$$F_m = F_{m-1}F_1 + F_mF_2 = F_{m-1} + F_m$$

, which is the definition of the recurrence. For $n = 2$, we have

$$F_{m+1} = F_{m-1}F_2 + F_mF_3 = F_{m-1} + 2F_m = F_{m-1} + F_m + F_m = F_{m+1} + F_m.$$

This also satisfies the definition.

Now, assume that this holds for $n = k$ and $n = k + 1$. We will show that this holds for $n = k + 2$ as well.

For $n = k$, we have $F_{m+k} = F_{m-1}F_k + F_mF_{k+1}$. For $n = k + 1$, we have $F_{m+k+1} = F_{m-1}F_{k+1} + F_mF_{k+2}$.

Adding the two equations and using the definition of the Fibonacci recurrence yields

$$F_{m+k+2} = F_{m-1}(F_k + F_{k+1}) + F_m(F_{k+1} + F_{k+2}) = F_{m-1}F_{k+2} + F_m(F_{k+3}).$$

This completes the induction.

To show that F is a divisibility sequence, consider the index n, and let m be a divisor of n. Then, we can write $n = mk$. To prove this, we use induction again. Our base case is $k = 1$. In this case, $m = n$, which means $F_m = F_n$, so we have that $F_m \mid F_n$, completing the base case. Now, assume this holds for $k = r$. We show that it also holds for $k = r + 1$. In order to do this, we must show that F_m divides $F_{m(r+1)}$. To do this, we plug in $k = r$ into the equation from earlier. This yields

$$F_{m+mr} = F_{m(r+1)} = F_{m-1}F_{mr} + F_mF_{mr+1}.$$

Now, notice that F_m clearly divides F_mF_{mr+1}. For $F_{m-1}F_{mr}$, our inductive hypothesis assumes that $F_m \mid F_{mr}$, which means $F_m \mid F_{m-1}F_{mr}$. Thus, $F_m \mid F_{m(r+1)}$, so F is a divisibility sequence. □

As mentioned earlier, the main focus of this paper is on two deep families of divisibility sequences: linear divisibility sequences (LDS) and elliptic divisibility sequences (EDS). We cover their structure, construction, and key theorems — especially those highlighting number-theoretic aspects such as divisibility and periodicity mod p.

3 Linear Divisibility Sequences

Linear divisibility sequences (LDSs) are a classical object of study in number theory, tracing their roots to 19th-century investigations of integer sequences such as the Fibonacci and Lucas numbers. These sequences are defined by linear recurrence relations and exhibit the divisibility property that if one index divides another, then the corresponding term in the sequence divides the other term.

One of the earliest and most famous examples is the Fibonacci sequence F_n, defined by the recurrence $F_{n+2} = F_{n+1} + F_n$ with initial values $F_0 = 0$ and $F_1 = 1$. It satisfies the property that $F_m \mid F_n$ whenever $m \mid n$, a characteristic feature of LDSs. The study of such sequences became formalized in the early 20th century with the work of mathematicians like D. H. Lehmer and Édouard Lucas.

A sequence $(a_n)_{n\geq 0}$ of integers is called a *linear divisibility sequence* if:

1. It satisfies a linear recurrence relation:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}, \quad \text{for all } n \geq k,$$

   where the c_i are fixed integers, and

2. It satisfies the *divisibility property*:

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

- **Fibonacci sequence**: $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$.
- **Lucas sequence**: $L_0 = 2, L_1 = 1, L_{n+2} = L_{n+1} + L_n$.
- More generally, sequences of the form:

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

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

4 Brief Introduction to Elliptic Sequences

Before we talk about elliptic divisibility sequences, we must cover some important fundamentals about elliptic sequences that will help us study elliptic divisibility sequences and their behavior modulo p.

Definition 4.1. *(h_n) is an **elliptic sequence** if it is a sequence of rational numbers satisfying*

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \quad \textit{for all } m, n \in \mathbb{Z}.$$

This recursive sequence comes from the polynomial of division of an elliptic curve.

Notice that we have defined m and n to belong to $\mathbb{Z}$. $\mathbb{Z}$ includes negative integers. This means that the indices can be negative. To get used to this, we will prove the following theorem.

Theorem 4.1. *Let (h_n) be an elliptic sequence. Then, the sequence satisfies $h_0 = 0$, $h_1 = \pm 1$, and*

$$h_{-n} = -h_n \quad \textit{for all } n \in \mathbb{Z}.$$

Proof. Let $m = 0$ and $n = 0$. Plugging these values into our recurrence relation yields

$${h_0}^2 = h_1h_{-1}{h_0}^2 - h_1h_{-1}h_0^2.$$

Thus, we have $h_0 = 0$. If we assume that $h_0 \neq 0$, we can divide both sides by ${h_0}^2$, which would yield $1 = 0$, which is not true. Thus, we must have $h_0 = 0$.

Next, if we plug in $n = 0$, we have

$${h_m}^2 = -h_1h_{-1}{h_n}^2.$$

So, we have $h_1h_{-1} = -1$.

Now, set $m = 0$. Plugging this into our relation gives $h_nh_{-n} = h_1h_{-1}{h_n}^2$. We can plug in $h_1h_{-1} = -1$ gives $-{h_n}^2 = h_nh_{-n}$, so $-h_n = h_{-n}$, which implies that $h_1 = h_{-1}$. Combining this with $h_1h_{-1} = -1$, we find that $h_1 = \pm 1$

□

Now we talk about some powerful theorems which allow us to compute terms of an elliptic sequence.

Theorem 4.2. *A rational sequence (h_n) with $h_0 = 0$, $h_1 = 1$, $h_2 = 0$ and $h_3 \neq 0$ is an elliptic sequence if and only if*

$$h_n = \begin{cases} 0 & \text{if } n = 2k, \\ (-1)^{\frac{1}{2}k(k-1)} h_3^{\frac{1}{2}k(k+1)} & \text{if } n = 2k+1. \end{cases}$$

Note that an elliptic sequence with $h_2 = 0$ must have $h_4 = 0$.

Proof. Suppose $h_2 = 0$ and $h_3 \neq 0$. Using the recurrence relation, it follows that all even-indexed terms must vanish. Indeed, since $h_2 = 0$, setting $m = 2$ in the recurrence yields:

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 - h_3h_1h_n^2.$$

The term $h_2^2 = 0$, so the right-hand side simplifies to $-h_3h_1h_n^2$. For n even, $h_n = 0$ by induction, implying $h_{n+2}h_{n-2} = 0$. Since $h_{n-2} \neq 0$ for some odd $n-2$, we get $h_{n+2} = 0$.

Thus all even-indexed terms $h_{2k} = 0$ for $k \geq 1$.

For odd indices $n = 2k+1$, define $h_1 = 1$, $h_3 = a \neq 0$. Using the recurrence and induction, we find:

$$h_{2k+3} = -a\frac{h_{2k+1}^2}{h_{2k-1}}.$$

Unfolding this relation yields

$$h_{2k+1} = (-1)^{\frac{1}{2}k(k-1)} a^{\frac{1}{2}k(k+1)}.$$

□

Theorem 4.3. *A rational sequence (h_n) with $h_0 = 0$, $h_1 = 1$, $h_2 \neq 0$ and $h_3 = 0$ is an elliptic sequence if and only if*

$$h_n = \begin{cases} 0 & \text{if } n = 3k, \\ (-h_2)^{\frac{1}{2}k(k-1)} h_4^{\frac{1}{2}k(k+1)} & \text{if } n = 3k+1, \\ -(-h_2)^{\frac{1}{2}(k+1)(k+2)} h_4^{\frac{1}{2}k(k+1)} & \text{if } n = 3k+2. \end{cases}$$

Proof. suppose $h_2 \neq 0$ and $h_3 = 0$. Here, every third term vanishes. Since $h_3 = 0$, setting $m = 3$ gives:

$$h_{n+3}h_{n-3} = -h_4 h_2 h_n^2.$$

Thus

$$h_{n+3} = -\frac{h_4 h_2 h_n^2}{h_{n-3}}.$$

This recurrence shows that every third term $h_{3k} = 0$ by induction, starting with $h_3 = 0$.

The remaining terms h_{3k+1} and h_{3k+2} can be computed explicitly by iterating the recurrence. One finds

$$h_{3k+1} = (-h_2)^{\frac{1}{2}k(k-1)} h_4^{\frac{1}{2}k(k+1)},$$

$$h_{3k+2} = -(-h_2)^{\frac{1}{2}(k+1)(k+2)} h_4^{\frac{1}{2}k(k+1)}.$$

These formulas follow directly from induction on k, using the recurrence relation and the initial conditions. □

Finally, we have the "doubling formula" and "stepping formula", respectively:

Theorem 4.4 (Doubling)**.** *Let (h_n) be an elliptic sequence. Then for all $n \geq 2$:*

$$h_{2n+1} = h_{n+2}h_n^3 - h_{n-1}h_{n+1}^3, \tag{1}$$

$$h_{2n}h_2 = h_n(h_{n+2}h_{n-1}^2 - h_{n-2}h_{n+1}^2). \tag{2}$$

Proof. Use the elliptic recurrence:

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

Set $m = n + 1$ and $n = n$, so:

$$h_{2n+1}h_1 = h_{n+2}h_n h_n^2 - h_{n+1}h_{n-1}h_{n+1}^2.$$

Simplifying:

$$h_{2n+1} = h_{n+2}h_n^3 - h_{n-1}h_{n+1}^3.$$

For the second, set $m = n + 1$ and $n = n - 1$:

$$h_{2n}h_2 = h_{n+2}h_n h_{n-1}^2 - h_{n-2}h_n h_{n+1}^2 = h_n(h_{n+2}h_{n-1}^2 - h_{n-2}h_{n+1}^2).$$

□

Theorem 4.5 (Stepping)**.**

$$h_{m+2} = \frac{h_{m+1}h_{m-1}h_2^2 - h_3h_1h_m^2}{h_{m-2}} \quad \textit{for all } m \in \mathbb{Z}.$$

5 Elliptic Divisibility Sequences

Now that we have talked a bit about elliptic sequences, we will cover elliptic divisibility sequences(EDS). An EDS is an elliptic sequence that satisfies **Definition 2.2**.

We will go over some examples of elliptic divisibility sequences.

Theorem 5.1. *The sequence $h_n = n$ is an elliptic divisibility sequence.*

Proof. It is easy to check that $h_n = n$ satisfies the divisibility property. Now we must check that it is an elliptic sequence.

We are given the recurrence relation:

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

and we wish to verify that the sequence $h_n = n$ satisfies this identity for all integers m, n.

The left hand side evaluates to

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

The right hand side evaluates to

$$h_{m+1}h_{m-1}h_n^2 = (m+1)(m-1)n^2 = (m^2-1)n^2,$$

$$h_{n+1}h_{n-1}h_m^2 = (n+1)(n-1)m^2 = (n^2-1)m^2.$$

Therefore,

$$\text{RHS} = (m^2-1)n^2 - (n^2-1)m^2 = m^2n^2 - n^2 - n^2m^2 + m^2 = m^2 - n^2.$$

Thus, $h_n = n$ is an elliptic divisibility sequence.

□

Theorem 5.2. *The sequence $G_n = F_{2n}$ is an elliptic divisibility sequence, where (F_n) is the Fibonacci Sequence.*

Proof. In order to prove that G_n is an EDS, we must prove the following identities. Luckily, these can be proven pretty easily by just using the Fibonacci sequence.

(i) $G_{m+1} = 3G_m - G_{m-1}$

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

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

We begin by substituting G_{m+n} and G_{m-n} into the left hand side of the elliptic recurrence:

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

Then, we expand and simplify to get:

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

Now we see the use for identity (i). If we factor $G_{m-1} G_n^2$ from the first two terms, we get $G_{m-1} G_n^2 (3G_m - Gm - 1)$. So, we can plug in $G_{m+1} = 3G_m - G_{m-1}$. We get

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

This is the exact form of the elliptic recurrence. The divisibility follows directly from the fact that F_n is a divisibility sequence. Thus, we are done. □

Now, we'll go over a nice theorem that allows us to generate different elliptic divisibility sequences or elliptic sequences.

Theorem 5.3. *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).

Proof. We are given an elliptic sequence (h_n) satisfying

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

and we define

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

where $h_k \neq 0$. We wish to show that (ℓ_n) satisfies the same recurrence.

Observe that

$$\ell_{m+n}\ell_{m-n} = \frac{h_{(m+n)k}}{h_k} \cdot \frac{h_{(m-n)k}}{h_k} = \frac{h_{(m+n)k}h_{(m-n)k}}{h_k^2}.$$

By the recurrence for (h_n), we have

$$h_{(m+n)k}h_{(m-n)k} = h_{(m+1)k}h_{(m-1)k}h_{nk}^2 - h_{(n+1)k}h_{(n-1)k}h_{mk}^2.$$

Substituting this into the expression for $\ell_{m+n}\ell_{m-n}$, we get

$$\ell_{m+n}\ell_{m-n} = \frac{h_{(m+1)k}h_{(m-1)k}h_{nk}^2 - h_{(n+1)k}h_{(n-1)k}h_{mk}^2}{h_k^2}.$$

Each term in the numerator can be expressed in terms of (ℓ_n). Since $h_{pk} = \ell_p h_k$ for any p, we have

$$h_{(m+1)k}h_{(m-1)k}h_{nk}^2 = (\ell_{m+1}h_k)(\ell_{m-1}h_k)(\ell_n h_k)^2.$$

Expanding this gives

$$\ell_{m+1}\ell_{m-1}\ell_n^2 h_k^4.$$

Similarly,

$$h_{(n+1)k}h_{(n-1)k}h_{mk}^2 = \ell_{n+1}\ell_{n-1}\ell_m^2 h_k^4.$$

Thus, the numerator becomes

$$h_k^4\big(\ell_{m+1}\ell_{m-1}\ell_n^2 - \ell_{n+1}\ell_{n-1}\ell_m^2\big).$$

Substituting this back, we obtain

$$\ell_{m+n}\ell_{m-n} = \frac{h_k^4}{h_k^2}\big(\ell_{m+1}\ell_{m-1}\ell_n^2 - \ell_{n+1}\ell_{n-1}\ell_m^2\big).$$

This simplifies to

$$\ell_{m+n}\ell_{m-n} = h_k^2\big(\ell_{m+1}\ell_{m-1}\ell_n^2 - \ell_{n+1}\ell_{n-1}\ell_m^2\big).$$

Here, the extra factor h_k^2 is independent of m and n. Since the elliptic sequence recurrence is homogeneous of degree four, dividing all terms of (ℓ_n) by h_k would absorb this constant factor and result in a sequence that satisfies the recurrence exactly. In other words, the scaled sequence

$$\tilde{\ell}_n = \frac{\ell_n}{h_k} = \frac{h_{nk}}{h_k^2}$$

obeys the original recurrence without any extra scaling.

The presence of this constant factor does not alter the divisibility or structural properties of the sequence because elliptic sequences are defined projectively; multiplying all terms by a fixed nonzero constant does not affect their essential behavior.

Therefore, (ℓ_n) is an elliptic sequence. If (h_n) is an elliptic divisibility sequence, then so is (ℓ_n) because divisibility is preserved under taking subsequences of the form h_{nk} and scaling by a fixed term h_k. □

Theorem 5.4. *Let (h_n) be an elliptic sequence with initial values $h_0 = 0$, $h_1 = 1$, and such that h_2, h_3 are not both zero. If two consecutive terms of (h_n) vanish, then all subsequent terms vanish as well.*

Proof. Assume there exist indices r and $r+1$ such that $h_r = h_{r+1} = 0$, and suppose r is minimal with this property. We first note that for all $0 < k < r$, $h_k \neq 0$, by minimality.

To show that all h_n for $n > r+1$ vanish, consider applying the recurrence relations.

Case 1: $n < r/2$. Set $2n = r$, so $h_{2n} = 0$. (2) yields

$$0 = h_n(h_{n+2}h_{n-1}^2 - h_{n-2}h_{n+1}^2).$$

Since $h_n \neq 0$ (by minimality of r), the factor in parentheses must vanish. This leads recursively to further zeros.

Case 2: $n = r/2$ (when r even). Substitution into the recurrence also yields a relation showing h_{n+2} depends on h_n and h_{n-1}, forcing vanishing of later terms.

Case 3: $n > r/2$. Choose n such that $2n - r < r$. (1) gives

$$h_{2n-r}h_r = h_n(h_{n+2}h_{n-1}^2 - h_{n-2}h_{n+1}^2).$$

Since $h_r = 0$, this again implies further vanishing terms.

Hence, by induction, all h_n beyond $r+1$ vanish. □

Theorem 5.5. *Let (h_n) be a proper elliptic sequence with $h_0 = 0$, $h_1 = 1$, and $h_2, h_3, h_4 \in \mathbb{Z}$. Then (h_n) is an elliptic divisibility sequence (EDS) if and only if $h_2 \mid h_4$. Furthermore, (h_n) is uniquely determined by h_2, h_3, h_4.*

Proof. Necessity is clear: in an EDS all h_n are integers and divisibility $h_2 \mid h_4$ is immediate from the recursions.

For sufficiency, assume $h_2, h_3, h_4 \in \mathbb{Z}$ and $h_2 \mid h_4$. We prove, by induction on n, that:

(i) All $h_n \in \mathbb{Z}$ and $h_2 \mid h_{2n}$.

(ii) (h_n) is uniquely determined by h_2, h_3, h_4.

Base case: The claim holds for $n \leq 4$ by assumption.

Induction step: Suppose the claim holds for all $k < n$. Using (1) or (2), h_n is expressed in terms of earlier h_k. Since those are integers by hypothesis, $h_n \in \mathbb{Z}$.

To see $h_2 \mid h_{2n}$, let $n = ab$ for $a, b \geq 2$. By induction,

$$h_{ab}h_2 = h_{a+1}h_{a-1}h_b^2 - h_{b+1}h_{b-1}h_a^2.$$

Each term on the RHS is divisible by h_2, so $h_{ab}h_2$ is divisible by h_2, implying $h_2 \mid h_{ab}$.

Finally, uniqueness follows since any sequence with the same h_2, h_3, h_4 must satisfy the same recursions and hence coincide for all n. □

We conclude this section with one very important theorem relating to strong divisibility sequences that allow us to tell whether an EDS is a strong divisibility sequence or not.

Theorem 5.6. *If (h_n) is an elliptic divisibility sequence in which the initial values h_3 and h_4 are coprime, then*

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

for all indices m, n.

This is the exact definition of a strong divisibility sequence that we introduced as Definition 2.2! We now have the following result.

Theorem 5.7. *The sequence formed by every other Fibonacci term(G_n) forms a strong divisibility sequences.*

Proof. We simply apply the previous theorem. We know that (G) is an elliptic divisibility sequence from before. Since $G_3 = 8$ and $G_4 = 21$, we have $\gcd(8, 21) = 1$, meaning they are coprime. By the previous theorem, (G) is a strong divisibility sequence □

6 Ranks of Apparition and Modulo Behavior

Definition 6.1. *Let (h_n) be a sequence of integers. A positive integer m is called a* divisor *of the sequence if $m \mid h_r$ for some $r > 1$. The smallest such r is called the* ***rank of apparition*** *of m in (h_n), often denoted $\rho(m)$ or just ρ.*

Theorem 6.1. *Let (h_n) be a divisibility sequence. The following are equivalent:*

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

(ii) For every prime p and every $k \geq 1$, we have:

$$p^k \mid h_r \quad \iff \quad \rho_k \mid r,$$

where ρ_k is the smallest index such that $p^k \mid h_{\rho_k}$.

Proof. As a note before the proof, the notation $p^k \| h_r$ states that k is the highest power of p that divides h_r.

(i) ⇒ (ii)

Assume (i) holds. Let p be a prime dividing some h_n, and let k be a positive integer such that p^k divides h_r. Define p_k to be the smallest positive index such that $p^k \mid h_{p_k}$.

Now, assume $r \equiv 0 \pmod{p_k}$. Then $p_k \mid r$, so $h_r = h_{\gcd(r,p_k)} = \gcd(h_r, h_{p_k})$. From (i), it follows that:

$$(h_r, h_{p_k}) = h_{\gcd(r,p_k)} = h_{p_k},$$

and thus $p^k \mid h_r$ as $p^k \mid h_{p_k}$. Hence, $h_r \equiv 0 \pmod{p^k}$.

Conversely, suppose $h_r \equiv 0 \pmod{p^k}$. Then $p^k \mid h_r$. Let us show that $r \equiv 0 \pmod{p_k}$. Note that (h_r, h_{p_k}) is divisible by p^k (since $p^k \mid h_r$ and $p^k \mid h_{p_k}$), and so:

$$h_{\gcd(r,p_k)} = (h_r, h_{p_k}) \equiv 0 \pmod{p^k}.$$

By the minimality of p_k, this implies $\gcd(r, p_k) \geq p_k$, hence $\gcd(r, p_k) = p_k$, so $p_k \mid r$, i.e., $r \equiv 0 \pmod{p_k}$.

(ii) ⇒ (i)

Assume (ii) holds. Let m and n be arbitrary positive integers. We want to show that $(h_m, h_n) = h_{\gcd(m,n)}$.

First, observe that since (h_n) is a divisibility sequence, we know $h_{\gcd(m,n)}$ divides both h_m and h_n, so $h_{\gcd(m,n)} \mid (h_m, h_n)$.

Let p be any common prime divisor of h_m and h_n. Write:

$$p^a \| h_m, \quad p^b \| h_n, \quad \text{with } a, b \geq 1,$$

and define $c = \min(a, b)$. Then $p^c \mid (h_m, h_n)$.

We must show that $p^c \mid h_{\gcd(m,n)}$. Since $p^a \mid h_m$, it follows by (ii) that $m \equiv 0 \pmod{p_a}$, and similarly $n \equiv 0 \pmod{p_b}$, where p_a and p_b are the smallest indices such that $p^a \mid h_{p_a}$ and $p^b \mid h_{p_b}$. Since m and n are divisible by p_a and p_b respectively, their gcd is divisible by $\operatorname{lcm}(p_a, p_b)$. Let $p_c = \operatorname{lcm}(p_a, p_b)$.

Then, since $\gcd(m, n) \equiv 0 \pmod{p_c}$, it follows that $p^c \mid h_{\gcd(m,n)}$ by (ii). Hence, every prime power dividing (h_m, h_n) also divides $h_{\gcd(m,n)}$, and so:

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

Combined with the earlier divisibility, we conclude:

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

□

By Theorem 5.8, we know that G_n is a strong divisibility sequence. Thus, we can look at this as an example for Theorem 6.1.

Prime $p = 3$:

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

Thus, we find:

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

where ρ_k denotes the smallest index such that $3^k \mid G_{\rho_k}$. We observe:

$$3 \mid G_2, G_4, G_6, G_8, \ldots \quad (\text{indices } \equiv 0 \bmod 2),$$

$$9 \mid G_6, G_{12}, \ldots \quad \text{(indices } \equiv 0 \bmod 6).$$

Prime $p = 5$:

$$5 \mid G_5 = 55, \quad 25 = 5^2 \mid G_{15} = F_{30} = 832040.$$

So we have:

$$\rho_1 = 5, \quad \rho_2 = 15.$$

And similarly:

$$5 \mid G_5, G_{10}, G_{15}, \ldots \quad \text{(indices } \equiv 0 \bmod 5),$$

$$25 \mid G_{15}, G_{30}, \ldots \quad \text{(indices } \equiv 0 \bmod 15).$$

Prime $p = 2$:

$$2 \mid G_3 = 8, \quad 4 = 2^2 \mid G_6 = 144, \quad 8 = 2^3 \mid G_9 = 2584.$$

Thus:

$$\rho_1 = 3, \quad \rho_2 = 6, \quad \rho_3 = 9.$$

So divisibility by 2^k occurs at indices divisible by $3k$, for $k = 1, 2, 3$ respectively.

7 Acknowledgments

I would like to thank Simon for this opportunity and Justin Wu(TA) for all of the help and support he has provided throughout this project.

References

[dL10] Rutger I. de Looij. Elliptic Divisibility Sequences. Master's thesis, Universiteit Utrecht, Utrecht, Netherlands, May 2010. Supervised by G. Cornelissen.

[EvdPSW05] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. Recurrence Sequences. *Bulletin of the London Mathematical Society*, 37(4):401–435, 2005. cited via CiteSeerX.

[Mor37] Louis J. Mordell. On $\gcd(a^m - b^m, a^n - b^n)$. *Transactions of the American Mathematical Society*, 41(2):389–436, 1937.

[dL10] [Mor37] [EvdPSW05]