# ON THE PRODUCT DISTRIBUTION OF ADDITION CHAINS

THEOPHILUS AGAMA

Abstract. In this note, we study the distribution of the product of consecutive terms in an addition chain of a given length. If $1, 2, \ldots, s_{\delta(n)-1}, s_{\delta(n)} = n$ is an addition chain producing $n$ and of length $\delta(n)$, with associated sequence of generators

$1 + 1, s_2 = a_2 + r_2, \ldots, s_{\delta(n)-1} = a_{\delta(n)-1} + r_{\delta(n)-1}, s_{\delta(n)} = a_{\delta(n)} + r_{\delta(n)} = n$

then

$$\sum_{l=1}^{\delta(n)} \log s_l = \delta(n) \log n - O(\delta(n)).$$

It follows in particular that

$$\prod_{l=1}^{\delta(n)} s_l \sim n^{\delta(n)}.$$

## 1. Introduction

The notion of an addition chain producing $n \geq 3$, introduced by Arnold Scholz, is a sequence of numbers of the form

$$1, 2, \ldots, s_{k-1}, s_k = n$$

where each term in the sequence is generated by adding two earlier terms and with repetition allowed. Formally each term in the addition chain is of the form $s_k = s_i + s_j$ $(s_k > 1)$ with $i \leq j < k$, and the number of terms in the sequence (excluding 1) is the length of the chain. The length of the smallest such chain producing $n$ is the shortest length of the addition chain. It is a well-known problem to determine the length of the shortest addition chain producing numbers $2^n - 1$ of special forms. A well-known conjecture on the subject, due to Arnold Scholz, purports:

**Conjecture 1.1.** Let $\iota(n)$ for $n \geq 3$ denote the length of the shortest addition chain producing $n$, then the inequality

$$\iota(2^n - 1) \leq n - 1 + \iota(n)$$

holds for all $n \geq 2$.

The conjecture was studied fairly soon after it was published by Alfred Brauer when, who obtained some weaker bounds [1]. There had also been amazing computational work to verify the conjecture [2].

Addition chain is a classic concept in number theory that plays a crucial role in various areas of computational mathematics, including algorithmic number theory,

*Date*: January 9, 2025.

2010 *Mathematics Subject Classification.* Primary 11P81; Secondary 11P82.

*Key words and phrases.* additive chain; determiners; regulators; length; generators; partition.

cryptography, and combinatorics. The study of addition chains has deep implications in the efficiency of algorithms that require repeated summations or the representation of numbers through elementary operations, such as those encountered in the computation of exponentiations or the efficient generation of large prime numbers.

Despite their fundamental nature, addition chains are known for their complexity and subtlety, particularly in their asymptotic properties. The length of an addition chain, denoted by $\delta(n)$, has been extensively studied, with researchers trying to understand both upper and lower bounds for $\delta(n)$ and to determine the most efficient chains for large $n$. However, much less attention has been given to a detailed exploration of the distribution of the terms within an addition chain, particularly the product of the terms and the interdependencies of their logarithmic growth. This gap in the literature forms the main motivation for the current study.

In this work, we introduce a refined approach to the study of addition chains, focusing on the interplay between the generators of the chain and their associated *determiners* and *regulators*. The sequence of generators is defined as the sum of two preceding terms in the chain, and each generator is further decomposed into a determiner and a regulator. The determiner is the earlier term in the chain, while the regulator represents the additional term needed to complete the sum. These notions of determiners and regulators allow us to break down the structure of the addition chain into more manageable components and gain a deeper understanding of its internal dynamics.

We proceed by deriving an asymptotic formula for the sum of the logarithms of the terms in an addition chain. Specifically, we demonstrate that for an addition chain that produces $n$, the sum of logarithms of the chain terms grows asymptotically as $\delta(n)\log n - O(\delta(n)$, where $\delta(n)$ denotes the length of the chain. This result gives a precise characterization of the logarithmic growth of the chain terms as $n$ increases without bound, providing new information on the asymptotic behavior of addition chains.

Moreover, by extending this result, we derive an asymptotic expression for the product of the terms in the addition chain. We show that the product of the terms in the chain behaves asymptotically as $n^{\delta(n)}$, where $\delta(n)$ is the length of the chain. This result not only deepens our understanding of the distribution of terms in an addition chain but also highlights the profound relationship between the length of the chain and the growth of the product of its terms.

The implications of these findings are far-reaching. The asymptotic results presented here provide a clearer picture of the efficiency and structure of addition chains, which is of particular interest in areas such as computational number theory, where addition chains are used in the efficient computation of large powers, as well as in cryptographic algorithms that rely on the representation of integers via sums of smaller terms. Furthermore, the insights gained from the analysis of determiners and regulators open up new avenues for exploring the optimality of addition chains and could potentially inform the development of more efficient algorithms for constructing such chains.

This work contributes to a more detailed understanding of addition chains, advancing both the theoretical study of these objects and their practical applications

in number-theoretic computations. Furthermore, it paves the way for further research on the structure of addition chains, exploring the possibility of tighter bounds and the identification of more efficient constructions for specific values $n$.

## 2. The regulators and determiners of an addition chain

In this section, we recall the notion of an addition chain and introduce the notion of the generators of the chain and their accompanying *determiners* and *regulators*.

**Definition 2.1.** Let $n \geq 3$, then by an addition chain of length $k-1$ producing $n$, we mean the sequence

$$1, 2, \ldots, s_{k-1}, s_k$$

where each term $s_j$ $(j \geq 3)$ in the sequence is the sum of two earlier terms, with the corresponding sequence of partition

$$2 = 1 + 1, \ldots, s_{k-1} = a_{k-1} + r_{k-1}, s_k = a_k + r_k = n$$

where $a_{i+1} = a_i + r_i$ and $a_{i+1} = s_i$ for $2 \leq i \leq k$. We call the partition $a_i + r_i$ the $i^{th}$ **generator** of the chain for $2 \leq i \leq k$. We call $a_i$ the **determiner** and $r_i$ the **regulator** of the $i^{th}$ generator of the chain. We call the sequence $(r_i)$ the regulators of the addition chain and $(a_i)$ the determiners of the chain for $2 \leq i \leq k$. We call the subsequence $(s_{j_m})$ for $2 \leq j \leq k$ and $1 \leq m \leq t \leq k$ a truncated addition chain producing $n$.

At any rate, we do not expect the regulators to be a part of the chain, although the determiners must be the terms in the chain.

**Lemma 2.2.** *Let $1, 2, \ldots, s_{k-1}, s_k$ be an addition chain producing $n \geq 3$ with associated generators*

$$2 = 1 + 1, \ldots, s_{k-1} = a_{k-1} + r_{k-1}, s_k = a_k + r_k = n.$$

*Then the following relation for the regulators*

$$\sum_{j=2}^{k} r_j = n - 1$$

*hold.*

*Proof.* We notice that $r_k = n - a_k$. It follows that

$$\begin{aligned} r_k + r_{k-1} &= n - a_k + r_{k-1} \\ &= n - (a_{k-1} + r_{k-1}) + r_{k-1} \\ &= n - a_{k-1}. \end{aligned}$$

Again we obtain from the following iteration

$$\begin{aligned} r_k + r_{k-1} + r_{k-2} &= n - a_{k-1} + r_{k-2} \\ &= n - (a_{k-2} + r_{k-2}) + r_{k-2} \\ &= n - a_{k-2}. \end{aligned}$$

By iterating downwards in this manner the relation follows. □

## 3. Main result

We derive an *asymptotic* formula for the *logarithmic* partial sums of terms in an addition chain. Consequently, we deduce an asymptotic for the product of consecutive terms in the chain.

**Theorem 3.1.** *Let $n \geq 2$ be fixed positive integer and let $1, 2, \ldots, s_{\delta(n)-1}, s_{\delta(n)} = n$ be an addition chain producing $n$ and of length $\delta(n)$, with associated sequence of generators*

$$1+1, s_2 = a_2 + r_2, \ldots, s_{\delta(n)-1} = a_{\delta(n)-1} + r_{\delta(n)-1}, s_{\delta(n)} = a_{\delta(n)} + r_{\delta(n)} = n$$

*then*

$$\sum_{l=1}^{\delta(n)} \log s_l = \delta(n)\log n - O(\delta(n)).$$

*It follows in particular that*

$$\prod_{l=1}^{\delta(n)} s_l \sim n^{\delta(n)}.$$

*Proof.* Let $n \geq 2$ be a fixed positive integer and consider an addition chain $1, 2, \ldots, s_{\delta(n)-1}, s_{\delta(n)} = n$ producing $n$ and of length $\delta(n)$, with associated sequence of generators

$$1+1, s_2 = a_2 + r_2, \ldots, s_{\delta(n)-1} = a_{\delta(n)-1} + r_{\delta(n)-1}, s_{\delta(n)} = a_{\delta(n)} + r_{\delta(n)} = n$$

and put $(a_j)$ and $(r_j)$ to be the sequence of determiners and regulators, respectively, in the chain. We make the following observations: $s_{\delta(n)-1} = a_{\delta(n)} = a_{\delta(n)-1} + r_{\delta(n)-1} = s_{\delta(n)-2} + r_{\delta(n)-1} = a_{\delta(n)-2} + r_{\delta(n)-2} + r_{\delta(n)-1} = \cdots = 1 + \sum\limits_{j=1}^{\delta(n)-1} r_j = n + 1 - r_{\delta(n)}$, where we have used Lemma 2.2. Similarly, we can write $a_{\delta(n)-1} = 1 + \sum\limits_{j=1}^{\delta(n)-2} = n+1-r_{\delta(n)}-r_{\delta(n)-1}$. Thus by induction, we can write $a_l = n+1-\sum\limits_{j=l}^{\delta(n)} r_j$ for each $3 \leq l \leq \delta(n)$. We observe that

$$\sum_{l=1}^{\delta(n)} \log s_l = \log 2 + \sum_{l=3}^{\delta(n)} \log a_l + \log n.$$

We now analyze the latter sum of the right-hand side involving the *determiners* of the addition chain. We can write

$$\sum_{l=3}^{\delta(n)} \log a_l = \sum_{l=3}^{\delta(n)} \log((n+1) - \sum_{i=l}^{\delta(n)} r_i)$$

which can be recast as

$$\sum_{l=3}^{\delta(n)} \log a_l = \sum_{l=3}^{\delta(n)} \log(n+1) - \sum_{l=3}^{\delta(n)} \sum_{v=1}^{\infty} \frac{1}{v(n+1)^v} \bigg( \sum_{i=l}^{\delta(n)} r_i \bigg)^v$$

with $\sum\limits_{i=l}^{\delta(n)} r_i < n-1$ for each $3 \leq l \leq \delta(n)$ by Lemma 2.2. It is clear that

$$\sum_{v=1}^{\infty} \frac{1}{v(n+1)^v} \bigg( \sum_{i=l}^{\delta(n)} r_i \bigg)^v \ll 1$$

for each $3 \leq l \leq \delta(n)$ since $\sum_{i=l}^{\delta(n)} r_i < n-1$ for each $3 \leq l \leq \delta(n)$ by Lemma 2.2. It follows that

$$\sum_{l=1}^{\delta(n)} \log s_l = \log 2 + (\delta(n)-2)\log(n+1) + \log n - O(\delta(n)).$$

This completes the proof of the claimed formula. □

## 4. **Further remarks**

In this study, we have investigated the structure and growth properties of addition chains, focusing on the asymptotic behavior of the logarithmic sums and the products of their terms. Through a detailed analysis, we derived an asymptotic formula for the sum of the logarithms of the terms in an addition chain, demonstrating that it grows as $\delta(n)\log n$ where $\delta(n)$ denotes the length of the chain. We also established that the product of the terms in the addition chain behaves asymptotically as $n^{\delta(n)}$, revealing a deep connection between the length of the chain and the magnitude of its terms. These results contribute to a more nuanced understanding of the efficiency and structure of addition chains and open new avenues for future research in number theory and related fields.

One of the key insights from this work is the role of determiners and regulators in shaping the growth of chain terms. By decomposing the generators into these two components, we were able to unravel the internal dynamics of the addition chain, leading to a clearer picture of how the terms evolve as $n$ increases. However, many questions remain unanswered, and several conjectures arise naturally from our results, which could serve as fruitful directions for further study.

(1) **Conjecture on the partial sums of higher powers** Let

$$S_k(n) = \sum_{l=1}^{\delta(n)} s_l^k$$

where $s_l$ are the terms of the addition chain. For $k \geq 2$, we conjecture that

$$S_k(n) \sim \delta(n) \cdot n^k - O(\delta(n))$$

which suggests the partial sums of higher powers grow similarly to the logarithmic sum, but with a higher-order dependence on $n$.

(2) **Conjecture on the growth rate of partial sums for** $k = 2$ For $k = 2$, we hypothesize that the partial sums

$$S_2(n) = \sum_{l=1}^{\delta(n)} s_l^2$$

grow quadratically with $n$, i.e.,

$$S_2(n) \sim \delta(n) \cdot n^2 - O(\delta(n)).$$

This conjecture implies that the growth of the sum of squares of the terms in the addition chain is asymptotically dominated by the quadratic term.

(3) **Conjecture on the asymptotic of $S_k(n)$ for arbitrary powers** For any fixed integer $k$, we conjecture that the asymptotic behavior of the partial sums of higher powers satisfies:

$$S_k(n) = \sum_{l=1}^{\delta(n)} s_l^k \sim C_k \cdot \delta(n) \cdot n^k + O(\delta(n))$$

where $C_k$ is a constant that depends on the power $k$, and the error term is dominated by $O(\delta(n))$.

(4) **Conjecture on the distribution of powers in an addition chain** We conjecture that for any integer $k$ the terms $s_l^k$ exhibit a distribution where the higher powers tend to be concentrated among larger terms in the chain. Specifically, we propose that the ratio of the sum of higher powers to the sum of the original terms behaves as:

$$\frac{S_k(n)}{\sum_{l=1}^{\delta(n)} s_l} \longrightarrow \text{constant} \quad \text{as} \quad n \to \infty$$

(5) **Conjecture on the relation between powers of terms and the length of the Chain:**
For higher powers of the terms, we hypothesize that the growth of $\delta(n)$ influences the sum of powers in a non-linear manner. Specifically, we conjecture that for $k > 1$, the sum of the $k$-th powers of the terms in the chain grows faster than linearly with $\delta(n)$ and exhibits an asymptotic dependency of the form:

$$S_k(n) \sim \delta(n)^k \cdot n^k.$$

These conjectures point to exciting avenues for future research, from improving the understanding of the asymptotics of addition chains to exploring their connections to other well-known sequences and their applications in algorithmic number theory. Our results lay the foundation for a deeper exploration of the structure and optimality of addition chains, opening new possibilities for both theoretical and applied research in number theory and its computational aspects.

In conclusion, this work has advanced our understanding of addition chains by deriving key asymptotic results and uncovering the intricate relationships between the terms, the generators, and logarithmic growth. The conjectures presented here, grounded in the findings of this study, provide a roadmap for future investigations that will continue to enrich the field of number theory and its applications.
[1].

## References

1. A. Brauer, *On addition chains*, Bulletin of the American mathematical Society, vol. 45:10, 1939, 736–739.
2. M. Clift, *Calculating optimal addition chains*, Computing, vol. 91:3, Springer, 1965, pp 265–284.

Department of Mathematics, African Institute for Mathematical science, Ghana
*E-mail address*: theophilus@aims.edu.gh/emperordagama@yahoo.com

[1] .