A NOTE ON PRIMES IN AN ADDITION CHAIN

T. AGAMA

Abstract. Let $E(n)$ denote an addition chain leading to $n \in [2^m, 2^{m+1})$ of the form

$$E(n) : s_o = 1, s_1 = 2, \ldots, s_{l(n)} = n$$

with $l(n) := \beta(m)$. Using ideas in [1], we show that

$$\#\{p \in E(n) \ : \ p \text{ is prime}\} \ll (\log m)\log(\beta(m) - m)$$

for $\beta(m) > m$ as $m \longrightarrow \infty$.

1. Preliminaries and Setup

Let $l(n)$ be the length of an addition chain leading to n, denoted $E(n)$, of the form

$$E(n) : s_o = 1, s_1 = 2, \ldots, s_{l(n)} = n$$

with $2^m \leq n < 2^{m+1}$ such that $l(n) := \beta(m)$. By adapting the ideas of the paper [1], we partition the steps in an addition chain into the following classes of steps

$$\mathcal{A} := \{i \ : \ s_i = 2s_{i-1}\} \quad (\textbf{doubling steps})$$

$$\mathcal{B} := \{i \ : \ \gamma s_{i-1} \leq s_i < 2s_{i-1}\} \quad (\textbf{large steps})$$

where $\gamma := \frac{1+\sqrt{5}}{2}$ is the *golden* ratio

$$\mathcal{C} := \{i \ : \ (1+\delta)s_{i-1} \leq s_i < \gamma s_{i-1}\} \quad (\textbf{medium} - \textbf{sized steps})$$

where $\delta := \delta(m) \longrightarrow 0$ as $m \longrightarrow \infty$. In particular

$$\delta := \delta(m) = \frac{1}{\log m}$$

$$\mathcal{D} := \{i \ : \ s_i < (1+\delta)s_{i-1}\} \quad (\textbf{small steps}).$$

We denote the cardinality of the sets to be

$$\#\mathcal{A} := A, \quad \#\mathcal{B} = B, \quad \#\mathcal{C} = C, \quad \#\mathcal{D} = D.$$

Date: June 18, 2025.

Key words and phrases. prime.

We call steps in $\mathcal{B}, \mathcal{C}, \mathcal{D}$ as *non-doubling steps*. We have therefore the relation

$$A + B + C + D = \beta(m).$$

Because each non-doubling step in an addition chain cannot grow faster than a corresponding step in a Fibonacci sequence, we have (by induction) the inequality

$$2^m \leq n \leq 2^A \gamma^{B+C+D} = 2^{\beta(m)} \left(\frac{\gamma}{2}\right)^{B+C+D}$$

and we deduce from this relation an upper control for the total number of non-doubling steps in an addition chain of length $\beta(m)$ to be

Lemma 1.1. *Put*

$$E(n) : s_o = 1, s_1 = 2, \ldots, s_{l(n)} = n$$

be an addition chain with $l(n) := \beta(m)$. Let $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ be steps in an addition chain of length $\beta(m)$ with cardinality A, B, C, D, respectively. Then we have

$$B + C + D \leq \frac{\beta(m) - m}{1 - \log_2 \gamma}.$$

It turns out that the non-doubling steps in an addition chain have certain structural pattern.

Lemma 1.2. *If $j \in \mathcal{B}$, then $j - 1 \in \mathcal{C} \cup \mathcal{D}$. In particular, each large step in an addition chain must be preceded by either a small step or a medium-sized step.*

Proof. Let $j \in \mathcal{B}$ (large step) then we have by definition

$$\gamma s_{j-1} \leq s_j < 2s_{j-1}$$

where $\gamma := \frac{1+\sqrt{5}}{2}$ is the *golden ratio*. Write $s_j = s_k + s_l$ with $k \geq l$. The inequality $s_j = s_k + s_l \leq s_{j-1} + s_l$ with $s_j < 2s_{j-1}$ implies that

$$\gamma s_{j-1} \leq s_j \leq s_{j-1} + s_{j-2}$$

which further implies

$$(\gamma - 1)s_{j-1} < s_{j-2} \iff s_{j-1} < \gamma s_{j-2}$$

since $\gamma = \frac{1}{\gamma - 1}$. This proves $j - 1 \in \mathcal{C} \cup \mathcal{D}$. □

In counting the number of primes that could possibly exist in an addition chain, it suffices to scout among the non-doubling steps because doubling steps are necessarily composite by construction. We obtain

the following crude upper bound for the number of primes in an addition chain leading to a target.

Write

$$E(n) : s_o = 1 < s_1 = 2 < \cdots < s_{\beta(m)} = n$$

with $\beta(m) \geq m$ and $2^m \leq n < 2^{m+1}$. Denote by $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ the four step types as in the setup, with $\#\mathcal{A} = A, \#\mathcal{B} = B, \#\mathcal{C} = C, \#\mathcal{D} = D$. No prime can appear at a doubling step, since if $j \in \mathcal{A}$, then $s_j = 2s_{j-1}$ must be composite. The only possible steps for which primes could appear are for those $j \in \mathcal{B} \cup \mathcal{C} \cup \mathcal{D}$. Lemma 1.1 gives

$$B + C + D \leq \frac{\beta(m) - m}{1 - \log_2 \gamma}.$$

The crude upper bound

$$\#\{p \in E(n) \ : \ p \text{ is prime}\} \ll \frac{\beta(m) - m}{\log n}$$

as $m \longrightarrow \infty$ follows immediately from the prime number theorem. This naive bound can be significantly improved by using the notion of a **run** and **run** length, which will be developed in the next section.

2. The run and run length of step types in an addition chain

We begin this section with the following definition.

Definition 2.1. Let $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ be steps in an addition chain as in the setup. We call a **maximal** consecutive sequence of steps of a given type

$$j_1 < j_2 < \cdots < j_d$$

such that $j_1 - 1, j_d + 1$ cannot be a step of the given type a **run** of the step type. We call the number of terms in the *run* the **run length**.

Lemma 1.2 hints at the core idea that a **run** of step type $\mathcal{C} \cup \mathcal{B}$ or $\mathcal{D} \cup \mathcal{B}$ will always appear among the non-doubling steps in any addition chain, whether or not optimal. More likely it is for chains that are not optimal to have many **run** of types $\mathcal{C} \cup \mathcal{B}$. We now prove a lower bound for the minimal length of a **run** of step type $\mathcal{D}$.

Lemma 2.2. *Let*

$$E(n) : s_o = 1 < s_1 = 2 < \cdots < s_{\beta(m)} = n$$

be an addition chain leading to n with $\beta(m) \geq m$ and $2^m \leq n < 2^{m+1}$. Denote by $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ the four step types as in the setup, with $\#\mathcal{A} = A, \#\mathcal{B} = B, \#\mathcal{C} = C, \#\mathcal{D} = D$. Furthermore, let

$$j_1 < j_2 < \cdots < j_d$$

*be a **run** of a step of type $\mathcal{D}$ such that there is no **run** of type $\mathcal{C} \cup \mathcal{B}$ preceding this **run**, then*

$$d \gg \log m.$$

Proof. Suppose

$$E(n) : s_o = 1 < s_1 = 2 < \cdots < s_{\beta(m)} = n$$

is an addition chain leading to n with $\beta(m) \geq m$ and $2^m \leq n < 2^{m+1}$. Further assume

$$j_1 < j_2 < \cdots < j_d$$

is a **run** of a step of type $\mathcal{D}$. Then $s_{j_d} < (1+\delta)s_{j_d-1}$ so that by induction, we have

$$3 \leq s_{j_d} < (1+\delta)^d s_o = (1+\delta)^d.$$

It follows that

$$d\delta \geq \log(1+\delta) \geq \log 3.$$

The lower bound for the **run** length follows with $\delta := \delta(m) = \frac{1}{\log m}$. $\square$

Lemma 2.3. *Let*

$$E(n) : s_o = 1 < s_1 = 2 < \cdots < s_{\beta(m)} = n$$

be an addition chain leading to n with $\beta(m) \geq m$ and $2^m \leq n < 2^{m+1}$. Denote by $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ the four step types as in the setup, with $\#\mathcal{A} = A, \#\mathcal{B} = B, \#\mathcal{C} = C, \#\mathcal{D} = D$. Furthermore, let

$$j_1 < j_2 < \cdots < j_d$$

*be a **run** of a step of type $\mathcal{C} \cup \mathcal{B}$. Then*

$$d \ll m \log m.$$

Proof. Suppose

$$E(n) : s_o = 1 < s_1 = 2 < \cdots < s_{\beta(m)} = n$$

is an addition chain leading to n with $\beta(m) \geq m$ and $2^m \leq n < 2^{m+1}$. Further assume

$$j_1 < j_2 < \cdots < j_d$$

is a **run** of a step of type $\mathcal{C} \cup \mathcal{B}$. Then we have

$$2^{m+1} > s_{j_d} \geq (1+\delta)^d s_{j_1-1} \geq (1+\delta)^d.$$

It follows that

$$(m+1)\log 2 \geq d\frac{\delta}{2}$$

and the asserted upper bound follows by using $\delta := \delta(m) = \frac{1}{\log m}$. □

Lemma 2.4. *Let*

$$E(n) : s_o = 1 < s_1 = 2 < \cdots < s_{\beta(m)} = n$$

be an addition chain leading to n with $\beta(m) \geq m$ and $2^m \leq n < 2^{m+1}$. Denote by $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ the four step types as in the setup, with $\#\mathcal{A} = A, \#\mathcal{B} = B, \#\mathcal{C} = C, \#\mathcal{D} = D$. Furthermore, let

$$j_1 < j_2 < \cdots < j_d$$

*be a **run** of a step of type $\mathcal{D} \cup \mathcal{B}$ such that there is no **ran** of type $\mathcal{C}$ preceding this **run**. Then*

$$d \gg 1.$$

Proof. Suppose

$$E(n) : s_o = 1 < s_1 = 2 < \cdots < s_{\beta(m)} = n$$

is an addition chain leading to n with $\beta(m) \geq m$ and $2^m \leq n < 2^{m+1}$. Further assume

$$j_1 < j_2 < \cdots < j_d$$

is a **run** of a step of type $\mathcal{D} \cup \mathcal{B}$. Then we have by induction the inequality

$$3 < s_{j_d} \leq (1+\delta)^{d_1} 2^{d_2} \leq (2(1+\delta))^d$$

where $d_1 + d_2 = d$. We deduce

$$d \geq \frac{\log 3}{\log 2 + \delta}$$

with $\delta := \delta(m) = \frac{1}{\log m}$. □

Lemma 2.5. *Let*

$$E(n) : s_o = 1 < s_1 = 2 < \cdots < s_{\beta(m)} = n$$

be an addition chain leading to n with $\beta(m) \geq m$ and $2^m \leq n < 2^{m+1}$. Denote by $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ the four step types as in the setup, with $\#\mathcal{A} = A, \#\mathcal{B} = B, \#\mathcal{C} = C, \#\mathcal{D} = D$. Furthermore, let

$$j_1 < j_2 < \cdots < j_d$$

*be a **run** of a step of type $\mathcal{C}$. Then*

$$d \ll m \log m.$$

Proof. Suppose

$$E(n) : s_o = 1 < s_1 = 2 < \cdots < s_{\beta(m)} = n$$

is an addition chain leading to n with $\beta(m) \geq m$ and $2^m \leq n < 2^{m+1}$. Further assume

$$j_1 < j_2 < \cdots < j_d$$

is a **run** of a step of type $\mathcal{C}$. We have by induction

$$2^{m+1} > s_{j_d} \geq (1+\delta)^d s_{j_1-1} \geq (1+\delta)^d$$

which implies

$$(m+1)\log 2 \geq d\frac{\delta}{2}.$$

The upper bound for the length of the **run** is immediate. □

Lemma 2.6. *Let*

$$E(n) : s_o = 1 < s_1 = 2 < \cdots < s_{\beta(m)} = n$$

be an addition chain leading to n with $\beta(m) \geq m$ and $2^m \leq n < 2^{m+1}$. Denote by $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ the four step types as in the setup, with $\#\mathcal{A} = A, \#\mathcal{B} = B, \#\mathcal{C} = C, \#\mathcal{D} = D$. Furthermore, let

$$j_1 < j_2 < \cdots < j_d$$

*be a **run** of a step of type $\mathcal{D} \cup \mathcal{B}$ and denote by d_2 the number of steps of type $\mathcal{B}$ in this run. Then we have*

$$d_2 \ll m.$$

Proof. Suppose

$$E(n) : s_o = 1 < s_1 = 2 < \cdots < s_{\beta(m)} = n$$

is an addition chain leading to n with $\beta(m) \geq m$ and $2^m \leq n < 2^{m+1}$. Further assume

$$j_1 < j_2 < \cdots < j_d$$

is a **run** of a step of type $\mathcal{D} \cup \mathcal{B}$. By induction, we deduce

$$2^{m+1} > s_{j_d} \geq \gamma^{d_2}$$

which implies

$$(m+1)\log 2 > d_2 \log \gamma$$

□

3. An improved upper bound

We now prove a tighter upper bound for the number of primes that could possibly be built in an addition chain. This result could be viewed as a quantitative version of our earlier qualitative result, which purports that there cannot be many primes in an addition chain.

Theorem 3.1. *Let $E(n)$ denote an addition chain leading to $n \in [2^m, 2^{m+1})$ of the form*

$$E(n) : s_o = 1, s_1 = 2, \ldots, s_{l(n)} = n$$

with $l(n) := \beta(m)$. Then

$$\#\{p \in E(n) \ : \ p \text{ is prime}\} \ll (\log m) \log(\beta(m) - m)$$

for $\beta(m) > m$ as $m \longrightarrow \infty$.

Proof. We write

$$E(n) : s_o = 1 < s_1 < \ldots < s_{l(n)} = n$$

with $l(n) := \beta(m)$. Let $\mathcal{B}, \mathcal{C}, \mathcal{D}$ denote as before the four-step classes introduced in the setup. We exclude steps of type $\mathcal{A}$ from this analysis since each $s_j \in E(n)$ for $j \in \mathcal{A}$ is necessarily composite. Now let $\mathbb{P}$ denote the set of all primes and define

$$\mathbf{1}_{\mathbf{prime}}(s_j) :\leq \begin{cases} 0 & \text{if} \quad s_j \notin \mathbb{P} \\ \frac{1}{\log s_j} & \text{if} \quad s_j \in \mathbb{P}. \end{cases}$$

Then

$$\#\{p \in E(n) \ : \ p \text{ is prime}\} = \sum_{j \in \mathcal{B} \cup \mathcal{C} \cup \mathcal{D}} \mathbf{1}_{\mathbf{prime}}(s_j) \leq \sum_{j \in \mathcal{B} \cup \mathcal{C} \cup \mathcal{D}} \frac{1}{\log s_j}.$$

Put

$$T := \#(\mathcal{B} \cup \mathcal{C} \cup \mathcal{D})$$

and set $\delta := \delta(m) = \frac{1}{\log m}$. It remains to bound the latter sum on the right-hand side to furnish an upper bound. Now, we split the consecutive steps in the addition chain

$$E(n) : s_o = 1 < s_1 < \ldots < s_{l(n)} = n$$

into **run** of types $\mathcal{B} \cup \mathcal{C}$, $\mathcal{B} \cup \mathcal{D}$, $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{C} \cup \mathcal{D}$. For a **run** of types $\mathcal{C} \cup \mathcal{B}$ of the form

$$j_1 < j_2 < \cdots < j_r$$

for $r \leq T$, we have $s_{j_r} > (1 + \delta)^r$ and it follows that

$$\log s_j > r \log(1 + \delta) \geq r \frac{\delta}{2}.$$

We obtain the contribution

$$\sum_{j_r\in\mathcal{C}\cup\mathcal{B}}\frac{1}{\log s_{j_r}}\leq\sum_{r=1}^{T}\frac{2}{r\delta}=2\log m\sum_{r=1}^{T}\frac{1}{r}\ll(\log m)(\log T).$$

Similarly, for a **run** of type $\mathcal{D}\cup\mathcal{B}$ of the form

$$j_1<j_2<\cdots<j_r$$

for $r\leq T$, we have

$$s_{j_r}\geq\gamma^{d_2}$$

where $d_2\leq T$ is the number of steps of type $\mathcal{B}$ in the run of type $\mathcal{D}\cup\mathcal{B}$. We deduce

$$\sum_{j_r\in\mathcal{D}\cup\mathcal{B}}\frac{1}{\log s_{j_r}}\leq\sum_{d_2=1}^{T}\frac{1}{d_2\log\gamma}\ll\log T.$$

Similarly for **runs** of type $\mathcal{C}$ of the form

$$j_1<j_2<\cdots<j_r$$

with $r\leq T$, we have

$$s_{j_r}\geq(1+\delta)^r\iff\log s_{j_r}\geq r\log(1+\delta)\geq r\frac{\delta}{2}$$

and it follows that

$$\sum_{j_r\in\mathcal{C}}\frac{1}{\log s_{j_r}}\leq\sum_{r=1}^{T}\frac{2}{r\delta}=2\log m\sum_{r=1}^{T}\frac{1}{r}\ll(\log m)(\log T).$$

We have also for the **run** of type $\mathcal{D}$ of the forms

$$j_1<j_2<\cdots<j_r$$

with $r\leq T$ the contribution

$$\sum_{j_r\in\mathcal{D}}\frac{1}{\log s_{j_r}}\leq\sum_{j_r\in\mathcal{D}\cup\mathcal{B}}\frac{1}{\log s_{j_r}}\ll\log T.$$

Finally, for **run** of type $\mathcal{C}\cup\mathcal{D}$ of the forms

$$j_1<j_2<\cdots<j_r$$

with $r\leq T$, we have

$$\sum_{j_r\in\mathcal{C}\cup\mathcal{D}}\frac{1}{\log s_{j_r}}\leq\sum_{j_r\in\mathcal{C}}\frac{1}{\log s_{j_r}}+\sum_{j_r\in\mathcal{D}}\frac{1}{\log s_{j_r}}\ll(\log m)(\log T).$$

Putting the contribution over all the runs, we deduce

$$\#\{p\in E(n)\ :\ p\text{ is prime}\}\leq\sum_{j_r\in\mathcal{B}\cup\mathcal{C}\cup\mathcal{D}}\frac{1}{\log s_{j_r}}\ll(\log m)(\log T).$$

Using the bound

$$B + C + D = T \ll \beta(m) - m$$

in Lemma 1.1 gives the claimed upper bound. □

References

1. J.M. De Koninck, N. Doyon and W. Verreault *On the minimal length of addition chains*, arXiv preprint arXiv:2504.07332, 2025.