SMALL COMPOSITE NUMBERS IN ORBITS OF LINEAR MAPS

ALEJANDRO REYES

Abstract. Generalized Cunningham chains are sets of the form $\{f^n(z)\}_{n\geq 0}$ where all its elements are prime numbers and f is a linear polynomial with integer coefficients. Its size is called its length $\ell(z)$. We generalize this definition further to include starting terms that are not prime, and we obtain the expected bound of $\ell(z) < z$ if z is big enough, which is a new result that is not dependent on the prime factorization of z.

Contents

1. Introduction and basic definitions

Given an integer polynomial P, consider the set $P(\mathbb{Z}) = \{P(z) : z \in \mathbb{Z}\}$. Which elements of it are prime numbers? Are there even any prime numbers in it at all?

The Bouniakowsky conjecture encapsulates all these questions, as explained in [Peg25]: given a polynomial P of degree greater than 1, positive leading coefficient and with

$$\gcd(P(1), P(2), \dots, P(z), \dots) = 1,$$

it conjectures that there are infinitely many primes of the form $P(z)$ for $z \in \mathbb{Z}^+$.

No polynomial is known that makes the conjecture true. For example, it is famously not known whether there are infinitely many primes of the form $z^2 + 1$ with $z \in \mathbb{Z}^+$.

The issue becomes worse if we consider orbits of P, that is, sets of the form $\mathcal{O}_P(z) = \{P^i(z) : i \geq 1\}$ where

$$P^i(z) = \underbrace{P(P(\dots(P}_{i \text{ times}}(z))\dots))$$

with $P \in \mathbb{Z}[x]$ and $z \in \mathbb{Z}$. Consider the specific case $P(z) = z^2 - 2z + 2$ and an initial value of $z = 3$. $\mathcal{O}_P(3)$ is the set of Fermat numbers, which have a long history of study. Despite this, we do not know if there are an infinite number of Fermat primes, and more importantly, we do not even know if there are an infinite

Date: May 14, 2025.

number of composite Fermat numbers (see [Kel25] for a list of known factorizations of Fermat numbers), which is more surprising given the intuitive abundance of composite numbers in comparison to prime numbers.

In this paper we will focus on the simple case of linear polynomials. A specific case that is of significant interest is the polynomial $P(z) = 2z + 1$. Prime numbers p such that $2p + 1$ is also prime are called *Sophie Germain primes*, and lists

$$\{p, 2p + 1, 2(2p + 1) + 1, \ldots, 2^n(p + 1) - 1\}$$

of orbits using $2z + 1$ starting at a prime number such that all terms of the list are prime are called *Cunningham chains*. Löh conducted an exhaustive search for Cunningham chains with starting term less than 2^{50} in [Lö89, Section 2. Computations]. A small example of a Cunningham chain is $\{41, 83, 167\}$.

A *generalized Cunningham chain* is a list

$$\{p, f(p), f^2(p), \ldots, f^{\ell-1}(p)\}$$

where all its elements are prime and $f(z) = az + b$ with a, b relatively prime (note that this is necessary in order for $f(p)$ to be prime).

A *complete generalized Cunningham chain* (using the same f) is a list

$$\{p, f(p), f^2(p), \ldots, f^{\ell(p)-1}(p)\}$$

that is a generalized Cunningham chain, has $f^{\ell(p)}(p)$ composite and has $f^{-1}(p)$ composite or not an integer (so it cannot be extended forwards or backwards). We say this Cunningham chain has *length* $\ell(p)$.

For $f(z) = 2z + 1$, one can prove that $\ell(p) \leq p - 1$ with Fermat's little theorem and Kanado gives a better bound of $\ell(p) < \dfrac{p}{2}$ in page 2 of [Kan22].

In this paper, we will generalize these proofs to all linear f.

We will be using a slightly modified definition for Cunningham chains in order to cover a wider breadth of cases.

Definition 1. Given integers z, a, b with a, b relatively prime, a *rooted Cunningham chain* is a list

$$\{f(z), f^2(z), \ldots, f^{\ell(z)}(z)\}$$

such that all its elements are prime and $f^{\ell(z)+1}(z)$ is composite (here, $f(z) = az+b$). We say $\ell(z)$ is its length and that it has root z.

Notably, in this definition z is excluded from the list itself, so it is not necessary for it to be prime. Definition 1 generalizes all non-generalized complete Cunningham chains (that is, complete Cunningham chains that use $f(z) = 2z + 1$) except $\{2, 5, 11, 23, 47\}$ because they are rooted Cunningham chains with root $\dfrac{p-1}{2}$, even if $\dfrac{p-1}{2}$ is not prime. It is also important to mention that this definition of length is one less than if you include a prime n into the list, which was our previous definition of length.

The goal of this paper is to prove the following two elementary bounds on the length of a rooted Cunningham chain that generalize the bounds for Cunningham chains.

THEOREM 2. *For coprime positive integers a, b with $a > 1$, define $f\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ as $f(z) = az + b$. For all $z \in \mathbb{Z}_{>1}$ coprime with a, the rooted Cunningham chain*

$$\{f(z), f^2(z), \ldots, f^{\ell(z)}(z)\}$$

has length $\ell(z) < z$.

THEOREM 3. *For coprime positive integers a, b with $a > 1$, define $f\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ as $f(z) = az + b$. There exists $M \in \mathbb{Z}^+$ such that for all $z \in \mathbb{Z}^+$ with $z > M$, the rooted Cunningham chain*

$$\{f(z), f^2(z), \ldots, f^{\ell(z)}(z)\}$$

has length $\ell(z) < z$.

The case $a = 1$ transforms the Cunningham chain into an arithmetic progression. Results on the distribution of primes in an arithmetic progressions are covered elsewhere in greater detail, such as with Dirichlet's theorem on arithmetic progressions or Green and Tao's paper [GT08] which directly addresses lengths.

Theorems 2 and 3 give the same bound with different conditions on z. Theorem 2 is easier to prove and is analogous to the result on non-generalized Cunningham chains. However, it requires z to be relatively prime to a, so there is an infinite subset of $\mathbb{Z}^+$ that is not addressed by Theorem 2. Theorem 3 requires additional machinery but uses the same essential ideas as Theorem 2, and it provides the desired bound for all but finite $z \in \mathbb{Z}^+$. In both cases we have restricted the linear maps to a, b positive. In the case of Theorem 2, this gets rid of some pesky cases such as the one where z remains fixed by f, but the condition on the coefficients being positive can be relaxed and Theorem 2 remains true. For Theorem 3, setting a, b to be positive avoids the same issues, but if we relax similar conditions the bound becomes $\ell(z) < z + C$ for some constant $C > 0$ dependent on a and b, so we omit this case.

In Section 2, we will provide a proof of Theorem 2 using Fermat's little theorem and some casework, and in Section 3 we will provide a proof of Theorem 3 using two additional lemmas.

2. Proof of Theorem 2

Firstly, note that $f(z) = az + b > z + b > z$ so $f(z) > z$ always. We can also calculate $f^n(z)$ explicitly:

$$\begin{aligned} f^n(z) &= a^n z + b + ab + a^2 b + \cdots + a^{n-1} b \\ &= a^n z + b \cdot \frac{a^n - 1}{a - 1} \end{aligned}$$

Proof of Theorem 2: If z and b share a common factor $d > 1$, then d divides both $a^n z$ and $b \cdot \dfrac{a^n - 1}{a - 1}$ while being smaller than their sum, so $f^n(z)$ is composite for all n. We may then assume that z and b are coprime for the rest of the proof.

Since $z > 1$, we may take a prime divisor p of z. Because z is coprime with a, p does not divide a. We proceed with two cases, considering whether p divides $a - 1$ or not.

Case 1: p divides $a - 1$.

$$\begin{aligned} f^p(z) &= a^p z + b + ab + a^2 b + \cdots + a^{p-1} b \\ &\equiv a^p \cdot 0 + b + 1b + 1^2 b + \cdots + 1^{p-1} b \pmod{p} \\ &\equiv pb \pmod{p} \\ &\equiv 0 \pmod{p} \end{aligned}$$

Therefore, p divides $f^p(z)$. Because p is a divisor of z and $f(z) > z$, $p \leq z < f^p(z)$, so $f^p(z)$ is composite and the length $\ell(z)$ obeys $\ell(z) < p \leq z$, as desired.

Case 2: p does not divide $a - 1$.

Using Fermat's little theorem, $a^{p-1} - 1$ is divisible by p. Because $a - 1$ and p are coprime and both divide $a^{p-1} - 1$, their product divides $a^{p-1} - 1$ as well, which is equivalent to $\dfrac{a^{p-1} - 1}{a - 1}$ being divisible by p. Then

$$\begin{aligned} f^{p-1}(z) &= a^{p-1} z + b \cdot \frac{a^{p-1} - 1}{a - 1} \\ &\equiv a^{p-1} \cdot 0 + b \cdot 0 \pmod{p} \\ &\equiv 0 \pmod{p} \end{aligned}$$

Therefore, p divides $f^{p-1}(z)$. Because p is a divisor of z and $f(z) > z$, $p \leq z < f^{p-1}(z)$, so $f^{p-1}(z)$ is composite and the length $\ell(z)$ obeys $\ell(z) < p - 1 < z$, as desired. □

The main idea of this proof of Theorem 2 is that the simplest way to obtain that the expression

$$f^n(z) = a^n z + b \cdot \frac{a^n - 1}{a - 1}$$

is composite is to find a common factor of $a^n z$ and $b \cdot \dfrac{a^n - 1}{a - 1}$.

The set of z's that share all their prime factors with a is always infinite: pick any prime factor q of a and $\{q, q^2, \ldots, q^n, \ldots\}$ is an infinite subset of z's that have this property. So the boundedness of z's that do not obey Theorem 3 is not an easy consequence of Theorem 2.

One way of exploiting Theorem 2 to eliminate the condition of z being coprime with a is to consider $f(z)$ instead of z directly. $f(z) = az + b$ is always coprime with a, so if we instead consider the rooted Cunningham chain $\{f^2(z), f^3(z), \ldots, f^{\ell(f(z))}(z)\}$ with root $f(z)$, we can apply Theorem 2. This will tell us $\ell(f(z)) < f(z)$, which in turn tells us $\ell(z) \leq \ell(f(z))+1 < f(z)+1 = az+b+1$ by appending $f(z)$ to the beginning of the list $\{f^2(z), f^3(z), \ldots, f^{\ell(f(z))}(z)\}$. We conclude that $\ell(z) < az + b + 1$ in all cases, which is already a linear bound, but this is not as satisfying as a general bound as it depends on the size of a, b.

Let us look at an example of how this proof of Theorem 2 and subsequent discussion works. Take $f(z) = 2z + 3$ and consider the rooted Cunningham chain $\{5, 13, 29, 61\}$ with root 1. Because Theorem 2 requires the root of the Cunningham chain to have at least one prime factor, we cannot apply it directly. However, as we discussed in the previous paragraph, if we consider $f(1) = 5$ we'll be able to leverage this prime factor to get a composite number further down the line, and because 5 is coprime with $a - 1 = 1$, we know that this will be maximally at the term $f^4(5)$. Indeed, $f^4(5) = f(61) = 125 = 5^3$.

How can we prove Theorem 3 if we require our prime factors to divide z? It is not immediately clear that we'll be able to leverage the bijective nature of linear maps modulo some prime p as we have been implicitly doing by using Fermat's little theorem to prove that some small enough term further along the Cunningham chain is composite. But it turns out that we will be able to do it by considering a specific sequence, as we will explain in the next section.

3. Proof of Theorem 3

Our answer lies in the sequence $(s_n)_{n\geq 1}$ defined explicitly as

$$\begin{aligned} s_1 &= z - b \\ s_2 &= z - b - ab \\ &\vdots \\ s_n &= z - b - ab - \cdots - a^{n-1}b \\ &= z - b \cdot \frac{a^n - 1}{a - 1} \\ &\vdots \end{aligned}$$

or defined inductively as $s_1 = z - b$, $s_{n+1} = s_n - a^n b$.

Consider a prime divisor p of $s_n = z - b - ab - \cdots - a^{n-1}b$. We have

$$\begin{aligned} f^m(z) &= a^m z + b + ab + \cdots + a^{m-1}b \\ &\equiv a^m \cdot (b + ab + \cdots + a^{n-1}b) + b + ab + \cdots + a^{m-1}b \pmod{p} \\ &\equiv b \cdot (1 + a + a^2 + \cdots + a^{m-1} + a^m + \cdots + a^{m+n-1}) \pmod{p} \\ &\equiv b \cdot \left(\frac{a^{m+n} - 1}{a - 1}\right) \pmod{p} \end{aligned}$$

This is an eerily similar expression to what we had before in the proof of Theorem 2. In fact, it is exactly the same as what we had when $p \mid z$, with the exponent on a changed from m to $n+m$. This is no coincidence: a nice feature of linear maps is that they have an explicit inverse that is also a linear map, explicitly,

$$f^{-1}(z) = \frac{z-b}{a}.$$

We have

$$f^{-n}(z) = \frac{z - b - ab - \cdots - a^{n-1}b}{a^n} = \frac{s_n}{a^n},$$

so we may suspect that we should somehow be able to include the numerator of this expression in our previous framework in order to obtain other composite numbers, and our suspicions would be correct.

Before proving Theorem 3, we will examine the prime factorizations for elements of the sequence $(s_n)_{n\geq 1}$ closely with two crucial lemmas.

LEMMA 4. *Let a have k distinct prime factors. If $z > b + ab + a^2b + \cdots a^{k+1}b$, then there exists a prime p that divides s_i for some index i with $1 \leq i \leq k+1$ but does not divide a.*

In order to prove Lemma 4, we need a better description of the prime factorizations of the elements of the sequence $(s_n)_{n\geq 1}$. We will get this description from Lemma 5. Let $\nu_p(x)$ be the p-adic valuation of x.

LEMMA 5. *If p is a prime factor of a, then for each $n \in \mathbb{Z}^+$ we will have two possibilities:*

$$\begin{cases} \nu_p(s_{n+1}) = n\nu_p(a) & \text{if } \nu_p(s_n) > n\nu_p(a) \\ \nu_p(s_{n+1}) \geq \nu_p(s_n) & \text{otherwise} \end{cases}$$

Additionally, if $\nu_p(s_{n+1}) = n\nu_p(a)$, then for every $n_1 > n$ we will have

$$\nu_p(s_{n_1}) = n\nu_p(a)$$

Proof of Lemma 5: If $\nu_p(s_n) > n\nu_p(a)$, then

$$\begin{aligned} \nu_p(s_{n+1}) &= \nu_p(s_n - a^n b) \\ &= \min\{\nu_p(s_n), \nu_p(a^n b)\} \\ &= \min\{\nu_p(s_n), n\nu_p(a)\} \\ &= n\nu_p(a) \end{aligned}$$

and we may prove by induction the claim that for every $n_1 > n$ we will have $\nu_p(s_{n_1}) = n\nu_p(a)$. The above is the base case $n_1 = n+1$. For the inductive step, if $\nu_p(s_{n_1}) = n\nu_p(a)$ for $n_1 > n$, then

$$\begin{aligned}\nu_p(s_{n_1+1}) &= \nu_p(s_{n_1} - a^{n_1}b) \\ &= \min\{\nu_p(s_{n_1}), \nu_p(a^{n_1}b)\} \\ &= \min\{n\nu_p(a), n_1\nu_p(a)\} \\ &= n\nu_p(a)\end{aligned}$$

as desired.

Otherwise, we'll have $\nu_p(s_n) \leq n\nu_p(a)$, so $p^{\nu_p(s_n)}$ divides both s_n and $a^n b$. Therefore, it divides their difference, s_{n+1}, which yields $\nu_p(s_{n+1}) \geq \nu_p(s_n)$. □

Lemma 5 gives us a characterization of indices n for which the p-adic valuation of s_n breaks out of a weakly ascending pattern, in relation to a specific prime p. In order to formalize this, consider the following definition.

Definition 6. For a prime p that divides a, we'll say that it is *n-stable* if $\nu_p(s_{n+1}) = n\nu_p(a)$.

Each prime that divides a may only be n-stable for at most one n, because of the last sentence of Lemma 5. Lemma 5 gives us all the necessary tools to prove Lemma 4.

Proof of Lemma 4: Assume the contrary. Then each s_i is divisible only by the k primes that divide a.

By Lemma 5 and the fact that each prime is n-stable for at most one n, there is at least one $1 \leq i \leq k+1$ such that none of the k distinct primes that divide a are i-stable. For this specific i, we'll have that $\nu_p(s_{i+1}) \geq \nu_p(s_i)$ for all p that divide a.

By our initial assumption, these are actually all the primes that are in the prime factorizations of s_i and s_{i+1}, so this actually yields that s_i divides s_{i+1}. Therefore,

$$\begin{aligned}&s_i \mid s_{i+1} - s_i = a^i b \\ \Rightarrow\ &z - b - ab - \cdots - a^{i-1}b \mid a^i b \\ \Rightarrow\ &z - b - ab - \cdots - a^{i-1}b \leq a^i b \\ \Rightarrow\ &z \leq b + ab + \cdots + a^i b \leq b + ab + \cdots a^{k+1}b\end{aligned}$$

which is a contradiction with our assumption on the size of z. □

From Lemma 4 we can essentially repeat the same proof we had for Theorem 2 to prove Theorem 3, but with a prime divisor of this s_i that does not divide a instead of a prime divisor of z.

Proof of Theorem 3: If z and b share a common factor $f(z)$ is composite, so assume that $\gcd(z, b) = 1$. If $z > b + ab + \cdots + a^{k+1}b = M$, then by Lemma 4 there exists a prime p that divides s_i (from the sequence $(s_n)_{n\geq 1}$) for some index i with $1 \leq i \leq k+1$ but does not divide a.

Because $z \equiv b + ab + \cdots + a^{i-1}b \pmod{p}$, we'll have

$$\begin{aligned} f^n(z) &= a^n z + b + ab + \cdots + a^{n-1}b \\ &\equiv a^n(b + ab + \cdots + a^{i-1}b) + b + ab + \cdots + a^{n-1}b \pmod{p} \\ &\equiv b \cdot (1 + a + a^2 + \cdots + a^{n+i-1}) \pmod{p} \\ &\equiv b \cdot \left(\frac{a^{n+i} - 1}{a - 1} \right) \pmod{p} \end{aligned}$$

We again proceed with two cases, considering whether p divides $a - 1$ or not.

Case 1: p divides $a - 1$.

Let $r \in \{1, 2, \ldots, p\}$ be the residue of $-i \pmod{p}$. We'll have

$$\begin{aligned} f^r(z) &\equiv b \cdot (1 + a + a^2 + \cdots + a^{r+i-1}) \pmod{p} \\ &\equiv b \cdot (1^0 + 1^1 + 1^2 + \cdots + 1^{r+i-1}) \pmod{p} \\ &\equiv b \cdot (r + i) \pmod{p} \\ &\equiv 0 \pmod{p} \end{aligned}$$

So p divides $f^r(z)$. Because it is a divisor of s_i and $f(z) > z$, $p \leq s_i < z < f^p(z)$, so $f^r(z)$ is composite and the length $\ell(z)$ obeys $\ell(z) < r \leq p < z$ as desired.

Case 2: p does not divide $a - 1$.

Using Fermat's little theorem, $a^{(p-1)m} - 1$ is divisible by p for all $k \in \mathbb{Z}^+$. Because $a - 1$ and p are coprime and both divide $a^{(p-1)m} - 1$, their product divides $a^{(p-1)m} - 1$ as well, which is equivalent to $\dfrac{a^{(p-1)m} - 1}{a - 1}$ being divisible by p.

Let $r \in \{1, 2, \ldots, p - 1\}$ be the residue of $-i \pmod{p - 1}$. Then

$$\begin{aligned} f^r(z) &\equiv b \cdot \frac{a^{r+i} - 1}{a - 1} \\ &\equiv b \cdot 0 \pmod{p} \\ &\equiv 0 \pmod{p} \end{aligned}$$

since $r + i$ is a multiple of $p - 1$.

So p divides $f^r(z)$. Because p is a divisor of s_i and $f(z) > z$, $p \leq s_i < z < f^r(z)$, so f^r is composite and the length $\ell(z)$ obeys $\ell(z) < r \leq p - 1 < z$ as desired. $\square$

References

[GT08] Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. *Ann. of Math. (2)*, 167(2):481–547, 2008.

[Kan22] Yuya Kanado. The relation between a generalized fibonacci sequence and the length of cunningham chains, 2022.

[Kel25] Wilfrid Keller. Summary of factoring status for fermat numbers f_m as of january 14, 2025, 2025. [Online; accessed 30-April-2025].

[Lŏ9] Günter Löh. Long chains of nearly doubled primes. *Math. Comp.*, 53(188):751–759, 1989.

[Peg25] Ed Jr. Pegg. Bouniakowsky conjecture, 2025. From MathWorld–A Wolfram Web Resource, created by Eric W. Weisstein [Online; accessed 30-April-2025].

Massachusetts Institute of Technology
Email address: aleu@mit.edu