A Study of Cunningham Bounds Through Rogue Primes

A. Bhardwaj, L. Degen, R. Petkov, and S. Stanbury

Abstract - A sequence of prime numbers $\{p, 2p+1, 4p+3, ..., 2^{n-1}(p+1)-1\}$ is called a Cunningham chain. These are finite sequences of prime numbers, for which each element is a Sophie Germain prime. It is conjectured that there are arbitrarily large such Cunningham chains, and these chains form an essential part of the study of Sophie Germain primes. In this paper, we aim to significantly improve existing bounds for the length of Cunningham chains by considering their behaviour in the framework of what we will define as *rogueness*.

Keywords : Cunningham chains; Sophie Germain primes; rogue primes

Mathematics Subject Classification (2020) **:** 11A41; 11B50; 11N13; 11P32

Introduction

If p is prime, a sequence of prime numbers $\{p, 2p+1, 4p+3, ..., 2^{n-1}(p+1)-1\}$ (resp. $\{p, 2p-1, 4p-3, ..., 2^{n-1}(p-1)+1\}$) is called a Cunningham chain of the first (resp. second) kind. The congruence class of the base prime modulo n, where n is prime, directly impacts the length of the subsequent Cunningham chain. This is particularly important when considering a potential strategy for finding arbitrarily long chains. Suppose $n = 5$, and we wish to generate a Cunningham chain of the first kind $\{a_n\}$. Then if $a_1 \equiv 1 \mod 5$, we have

$$a_2 \equiv 3 \mod 5 \implies a_3 \equiv 2 \mod 5 \implies a_4 \equiv 0 \mod 5,$$

where $\implies$ denotes 'implies that', which forces the chain to terminate at a_3. In fact, this demonstrates that any chain with length higher than 3 must have $a_1 \equiv 4 \mod 5$. It follows similarly that any Cunningham chain of the second kind of length higher than 3 must have $a_1 \equiv 1 \mod 5$. The ability to place such a unique restriction allows us to bound chains for most initial elements. In addition, if we were able to find similar restrictions for other values of n, we could apply the Chinese Remainder Theorem on the base prime to significantly reduce the possibilities for chains of arbitrarily long length. Moreover, for all n, a Cunningham chain of the first kind will never reach 0 modulo n if $a_1 \equiv n-1 \mod n \equiv -1 \mod n$. This follows as $a_2 \equiv 2 \times -1 + 1 \equiv -1 \mod n$, with $a_k = -1 \mod n$ by induction. A similar result holds for a Cunningham chain of the second kind when $a_1 \equiv 1 \mod n$.

In the spirit of the $p = 5$ case, for a given prime p, we want to determine congruence classes in $\mathbb{Z}/p\mathbb{Z}$ for which a starting element from such a congruence class would generate a chain (now thought of as being canonically embedded in $\mathbb{Z}/p\mathbb{Z}$) that would eventually hit $0 \mod p$. As before, for a chain of the first (resp. second) kind, we ignore the equivalence class -1 (resp. 1), and aim for every other equivalence class to fit our desired restriction. However, we observe that this is not possible for $n = 7$ by noting

$$a_1 \equiv 2 \mod 7 \implies a_2 \equiv 5 \mod 7 \implies a_3 \equiv 4 \mod 7 \implies a_4 \equiv 2 \equiv a_1 \mod 7,$$

leading to a repetition that will always be non-zero. This undesired loop for $n = 7$ does not allow us to enforce a unique restriction on a general starting element due to the behaviour when $a_1 \in \{2, 4, 5\} \mod 7$. This leads us to label 7 as a *rogue* prime.

In this paper, we will devote the first two sections to the construction of the idea of rogueness. The next sections apply these ideas to improve bounds on the length of a Cunningham chain. The final two sections give further investigation into *rogue loops*, and their relation to Cunningham chains. We also conjecture a logarithmic bound for these chains, for which we give numerical evidence. Finally, we conjecture a result concerning divisors of the extensions of Cunningham chains, which is closely related to our logarithmic bound. Although this conjecture is simple to state, we find it far from obvious how to approach it.

1 Basic Definitions

Throughout we let $\mathbb{P}$ denote the set of odd prime numbers. In this paper, we will focus on sequences of prime numbers. The basic pattern of the sequences we will study is motivated by the notion of a Sophie Germain prime.

Definition 1.1 (Sophie Germain prime) *A **Sophie Germain prime** is a prime number p, such that $2p + 1$ is also prime.*

We remark that if for some odd prime $q < p$ we have $p \equiv \frac{q-1}{2} \mod q$, then p is not a Sophie Germain prime.

If p is a Sophie Germain prime, it is natural to wonder whether $2p+1$ is also a Sophie Germain prime, and if we can continue this process to get more primes. Whilst we keep hitting Sophie Germain primes, we can continue this process, and in doing so we construct sequences of prime numbers, which are called Cunningham chains.

Definition 1.2 (Cunningham chain) *Let $p \in \mathbb{P}$. We define the **Cunningham chain** of the first (resp. second) kind generated by p to be the finite sequence*

$$a_n^+ = 2^{n-1}(p + 1) - 1, \quad \text{for } n : 1 \leqslant n \leqslant k^+$$

where $k^+ = \min\{m \in \mathbb{Z}_{\geq 1} : a_{m+1}^+ \notin \mathbb{P}\}$, and resp.

$$a_n^- = 2^{n-1}(p - 1) + 1, \quad \text{for } n : 1 \leqslant n \leqslant k^-$$

where $k^- = \min\{m \in \mathbb{Z}_{\geq 1} : a^-_{m+1} \notin \mathbb{P}\}$. *Here,* k^+ *(resp.* k^-*) depends on* p *and* $+$ *(resp.* $-$*) and the sequence is characterised by the recursion*

$$a^+_{n+1} = 2a^+_n + 1 \qquad \textit{resp.} \qquad a^-_{n+1} = 2a^-_n - 1$$

We use this notation for k^+ *(resp.* k^-*) throughout. The prime* p *is sometimes referred to as the* ***base*** *prime.*

For example, taking $p = 2$, the set of elements in the Cunningham chain of the first (resp. second) kind would be $\{2, 5, 11, 23, 47\}$ (resp. $\{2, 3, 5\}$). It is believed that there exist infinitely many Cunningham chains, with the Bateman-Horn conjecture producing an asymptotic density estimate ([3]). In fact, this would additionally imply that there exist arbitrarily long chains, but as of August 2020, the longest known Cunningham chain is of length 19, discovered by Raanan Chermoni and Jaroslaw Wroblewski. A **bi-twin chain** is generated from a pair of twin primes $(n-1, n+1)$, as opposed to a single base prime. It takes the form $(n-1, n+1, 2n-1, 2n+1, ...)$ consisting of solely prime elements and can be considered as the intertwining of a Cunningham chain of the first kind with base prime $n-1$ and a Cunningham chain of the second kind with base prime $n+1$.

It is useful to refer to the set of elements that form these Cunningham chains.

Definition 1.3 (Cunningham set) *Let* $p \in \mathbb{P}$. *Given the sequence* a^+_n *(resp.* a^-_n*) we define the* ***Cunningham set*** *of the first (resp. second) kind to be the set of elements in the respective Cunningham sequence and we denote these sets by* $C^+[p]$ *(resp.* $C^-[p]$*). That is,*

$$C^+[p] = \left\{a^+_n \mid 1 \leq n \leq k^+\right\} \quad \textit{resp. } C^-[p] = \left\{a^-_n \mid 1 \leq n \leq k^-\right\}$$

It is a simple consequence from group theory that if $p \in \mathbb{P}$, then the set $C^{\pm}[p]$ has size at most $p - 1 > 1$. Moreover, from [2] we can extract a better bound, namely for $p \geqslant 7$

$$|C^{\pm}[p]| \leqslant \frac{p-3}{2}, \tag{1}$$

for $p \in \mathbb{P}$. In what follows, we will consider a new approach for finding bounds for Cunningham chains, by considering their reductions modulo primes.

2 Rogue Primes

We now proceed to formalise the ideas mentioned in our introduction.

Definition 2.1 (Rogue set, rogue sequence) *Let* p *be a prime. We define the* ***rogue set*** *of the first (resp. second) kind by*

$$A^+_p = (\mathbb{Z}/p\mathbb{Z})^\times \setminus \{-1 \mod p\}, \quad \textit{resp. } A^-_p = (\mathbb{Z}/p\mathbb{Z})^\times \setminus \{1 \mod p\}$$

Let $g^+ \in A^+_p, g^- \in A^-_p$. *Define the sequences*

$$u^+_n = \begin{cases} g^+, & n = 1 \\ 2u^+_{n-1} + 1, & n > 1 \end{cases} \quad \textit{and} \quad u^-_n = \begin{cases} g^-, & n = 1 \\ 2u^-_{n-1} - 1, & n > 1 \end{cases}$$

and set $g_k^{\pm} = \min\{n \in \mathbb{N} \mid u_n^{\pm} = 0\} \cup \infty$. *We define the* ***rogue sequence*** *of* g^+ *(resp.* g^-*) to be the sequence*

$$\langle g^+ \rangle_p^+ = \left\{ u_n^+ \mid 1 \leq n < g_k^+ \right\}, \quad \text{resp. } \langle g^- \rangle_p^- = \left\{ u_n^- \mid 1 \leq n < g_k^- \right\}$$

We use this notation for g_k^+ *(resp.* g_k^-*) throughout. Note that if* g_k^+ *(resp.* g_k^-*) is finite, then* $u_{g_k^+}^+$ *(resp.* $u_{g_k^-}^-$*) is not in the rogue sequence of* g^+ *(resp.* g^-*).*

To avoid having too much notation, when it will be clear, we will often denote the elements of a rogue sequence by u_n^+ or u_n^- (depending on the appropriate case), and we will simply write $u_n^{\pm}$ when considering elements that can be of a rogue sequence of either kind. We give a few examples of rogue sets and sequences to illustrate the above definition.

Example 2.2 For $p \in \mathbb{P}$, the rogue sets of the first and second kind are the sets (where here we make the abuse of notation by writing x for $x \mod p$)

$$A_p^+ = \{1, 2, 3, ..., p-2\}, \quad A_p^- = \{2, 3, ..., p-2, p-1\}.$$

Furthermore, for $p = 5$ we have

$$\langle 1 \rangle_5^+ = \{1, 3, 2\}$$

whilst for $p = 7$

$$\langle 2 \rangle_7^+ = \{2, 5, 4, 2, ...\}, \quad \langle 2 \rangle_7^- = \{2, 3, 5, 2, ...\}.$$

We thus have examples of both finite and infinite rogue sequences.

We now give a formal definition for the primes that lack restriction on our Cunningham chains. To do so, we will first need to introduce terminology for these *loops*, whose structure will generalise that of the rogue sequences $\langle 2 \rangle_7^+$ and $\langle 2 \rangle_7^-$, seen in Example 2.2.

Definition 2.3 (Rogue loop, rogue prime of the first and second kind) *Let* p *be an odd prime. We call a periodic rogue sequence a* ***rogue loop****. We define* p *to be* ***rogue*** *of the first (resp. second) kind if* A_p^+ *(resp.* A_p^-*) contains a rogue loop. A prime which is not rogue is said to be a* ***non-rogue prime****.*

Remark 2.4 It is worth noting that in the case of a rogue loops of the first (resp. second) kind, we have that g_k^+ (resp. g_k^-) $= \infty$.

It follows immediately by applying Fermat's little theorem on the closed form expressions of the sequences $\langle 1 \rangle_p^+$ and $\langle -1 \rangle_p^-$ that these always terminate, and hence are not rogue loops. Remark that for $p \in \mathbb{P}$, if we were to allow -1 to be in A_p^+ (resp. 1 to be in A_p^-), we would then have as rogue sequences:

$$\langle -1 \rangle_p^+ = \{-1, -1, -1, ...\}, \quad \text{resp.} \langle 1 \rangle_p^- = \{1, 1, 1, ...\}$$

and hence we would always have a rogue loop, and all primes would be rogue. This motivates our choice of the sets A_p^+ and A_p^-, which are more suitable for this study.

Going back to Example 2.2, we see that $\langle 1\rangle_5^+$ does not form a rogue loop in A_5^+, whilst $\langle 2\rangle_7^+$ and $\langle 2\rangle_7^-$ do form rogue loops in A_7^+ and A_7^- respectively. It follows that 7 is a rogue prime of both the first and second kind, whilst for $p = 5$ we have

$$\langle 1\rangle_5^+ = \{1, 3, 2\}, \langle 2\rangle_5^+ = \{2\}, \langle 3\rangle_5^+ = \{3, 2\}, \tag{2}$$

and hence 5 is non-rogue of the first kind.

Remark 2.5 Definition 2.3 is closely related to our motivational examples. If p is non-rogue of the first (resp. second) kind, then the only criteria on a Cunningham generator a_1, of the first (resp. second) kind is

$$a_1 \equiv -1 \mod p, \quad \text{resp.} \quad a_1 \equiv 1 \mod p.$$

In what follows, we will want to refer to the sets of rogue primes of the two kinds.

Definition 2.6 (Set of rogue primes of first and second kind) *We define the* ***set of rogue primes*** *of the first (resp. second) kind to be*

$$\begin{aligned} Rog(\mathbb{P})_+ &= \{p \in \mathbb{P} \mid p \text{ is rogue of the first kind}\}, \\ \text{resp. } Rog(\mathbb{P})_- &= \{p \in \mathbb{P} \mid p \text{ is rogue of the second kind}\} \end{aligned}$$

If we consider the rogue sets A_5^+ and A_5^-, we have

$$\langle 1\rangle_5^+ = \{1, 3, 2\} \quad \langle -1\rangle_5^- = \{4, 2, 3\},$$

and hence every element of A_5^+ is contained in the sequence $\langle 1\rangle_5^+$, and every element of A_5^- is contained in $\langle -1\rangle_5^-$. This leads to the idea of a rogue sequence being able to generate a rogue set.

Definition 2.7 (Generated rogue set, p^{th} rogue generator) *Let $p \in \mathbb{N}$ be odd. We say A_p^+ (resp. A_p^-) is a* ***generated*** *rogue set of the first (resp. second) kind if $\exists g^+ \in A_p^+$ (resp. $g^- \in A_p^-$) such that*

$$A_p^+ = \left\{u_n^+ \in \langle g^+\rangle_p^+\right\}, \qquad \text{resp. } A_p^- = \left\{u_n^- \in \langle g^-\rangle_p^-\right\}$$

Note that here we ignore the ordering of the sequence, and it only matters that the elements of A_p^+ (resp. A_p^-) are the same as those in $\langle g^+\rangle_p^+$ (resp. $\langle g^-\rangle_p^-$). We call g^+ (resp. g^-) a p^{th} ***rogue generator*** *of the first (resp. second) kind.*

To facilitate notation, we introduce the following convention.

Notation 2.8 For $\alpha \in \{+, -\}$, we write $\alpha = +$ (resp. $\alpha = -$) to mean that we denote by α the symbol $+$ (resp. $-$). We denote by $\alpha 1$

$$\alpha 1 := \begin{cases} 1, & \alpha = + \\ -1, & \alpha = - \end{cases}$$

and continue to abuse notation by thinking of elements of $\mathbb{Z}$ in the groups $\mathbb{Z}/p\mathbb{Z}$.

In (2), we found that the rogue sequence $\langle 1\rangle_5^+$ is an extension of the rogue sequence $\langle 3\rangle_5^+$, which itself was an extension of $\langle 2\rangle_5^+$. It is trivial that for any terminating rogue sequence of $\langle g^+\rangle_p^+$ (resp. $\langle g^-\rangle_p^-$), the last element must be of the form

$$u_{g_k^+-1} \equiv \frac{p-1}{2} \mod p \qquad \text{resp. } u_{g_k^--1} \equiv \frac{p+1}{2} \mod p \tag{3}$$

where it is useful to recall that if g_k^+ (resp. g_k^-) is finite, then $u_{g_k^+}^+$ (resp. $u_{g_k^-}^-$) is not in the rogue sequence of g^+ (resp. g^-). We can thus ask ourselves how far back this sequence may be extended? In other words, which elements in A_p^+ (resp. A_p^-) can only ever be the first element of a rogue sequence? Clearly, for $p \in \mathbb{P}$ and $\alpha \in \{+,-\}$, we have

$$\bigcup_{g\in A_p^\alpha} \langle g\rangle_p^\alpha = A_p^\alpha.$$

We can further ask ourselves, what is the smallest subset $G^\alpha \subset A_p^\alpha$ such that

$$\bigsqcup_{g\in G^\alpha} \langle g\rangle_p^\alpha = A_p^\alpha, \tag{4}$$

and if any such proper subsets of A_p^α exist? Going back to Example 2.2, in A_7^+ and A_7^- we have

$$\langle 2\rangle_7^+ = \{2,5,4,2,...\}, \quad \langle 1\rangle_7^+ = \{1,3\}, \qquad \langle 2\rangle_7^- = \{2,3,5,2,...\}, \quad \langle 6\rangle_7^- = \{6,4\},$$

and hence

$$A_7^+ = \bigsqcup_{g\in\{1,2\}} \langle g\rangle_7^+, \quad A_7^- = \bigsqcup_{g\in\{2,6\}} \langle g\rangle_7^-.$$

For now, we first consider this with (3), and the following result becomes very immediate.

Lemma 2.9 *Let $p \in \mathbb{P}$ and let $\alpha \in \{+,-\}$. Then*

$$A_p^\alpha \text{ is generated} \iff \text{the } p^{th} \text{ rogue generator is given by } g_\alpha \equiv \alpha 1 \mod p.$$

Proof. ($\Longrightarrow$) Suppose A_p^α is generated. Then $\exists\, g \in A_p^\alpha$ such that $\langle g\rangle_p^\alpha = A_p^\alpha$. Consider A_p^+ and suppose that $g \neq 1$. Then $1 \in \langle g\rangle_p^+ \setminus \{g\}$, and thus $\exists\, q \in \mathbb{N}$ such that

$$2q+1 \equiv 1 \mod p.$$

Thus

$$2q \equiv 0 \mod p \implies q \equiv 0 \mod p.$$

This is a contradiction since $0 \notin A_p^+$. The proof is analogous for A_p^-. The converse follows by the definition of a rogue generator. □

Let $p \in \mathbb{P}$ and suppose that $p \notin \mathrm{Rog}(\mathbb{P})_+$ (resp. $p \notin \mathrm{Rog}(\mathbb{P})_-$). It then follows that there are no rogue loops in A_p^+ (resp. A_p^-), and hence we can find a terminating sequence. In

the same way as our motivation for Lemma 2.9, we can extend such a sequence to get a generating sequence, and hence this raises the question as to which elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ can be expressed as powers of 2? This leads to the following remarkable result (below by $\iff$ we mean if and only if).

Theorem 2.10 *Let $p \in \mathbb{P}$ and let $\alpha \in \{+,-\}$. Then*

$$p \in \mathit{Rog}(\mathbb{P})_\alpha \iff 2 \text{ is not a primitive root modulo } p.$$

Proof. ($\Longrightarrow$) Suppose $p \in \mathrm{Rog}(\mathbb{P})_+$. Then there exists a rogue loop $\langle g \rangle_p^+$, given by

$$\langle g \rangle_p^+ = \left\{ 2^{n-1}(g+1) - 1 \mid n \in \mathbb{N} \right\}.$$

By definition, $\forall n \in \mathbb{N}$ we have

$$2^{n-1}(g+1) \not\equiv 1 \mod p,$$

and hence 2 cannot be a primitive root modulo p. A similar process gives the same result for $p \in \mathrm{Rog}(\mathbb{P})_-$.

($\Longleftarrow$) Suppose $p \notin \mathrm{Rog}(\mathbb{P})_+$. Then $\forall g \in A_p^+$, the rogue sequence $\langle g \rangle_p^+$ is finite. Hence, for such g there exists a $K_g \in \mathbb{N}$ such that

$$2^{K_g - 1}(g+1) - 1 \equiv 0 \mod p,$$

giving

$$2^{K_g - 1} \equiv (g+1)^{-1} \mod p.$$

Since g was arbitrary, writing $\langle 2 \rangle := \{2^k \mod p \mid k \in \mathbb{N}\}$ we get

$$\langle 2 \rangle \supseteq \left\{ (g+1)^{-1} \mid g \in A_p^+ \right\} = \left\{ g^{-1} \mid g \in (\mathbb{Z}/p\mathbb{Z})^\times \setminus \{1\} \right\} = (\mathbb{Z}/p\mathbb{Z})^\times \setminus \{1\}$$

and it follows that 2 is a primitive root modulo p. The proof is analogous for the $\mathrm{Rog}(\mathbb{P})_-$ case. □

This leads to the following satisfying result, which will allow us to talk more freely about rogue primes.

Corollary 2.11 *Let $p \in \mathbb{P}$. Then p is a rogue prime of the first kind if and only if p is a rogue prime of the second kind.*

Proof. This follows immediately from Theorem 2.10, since the right hand side is independent of α. □

Definition 2.12 (Rogue prime, set of rogue primes) *Let $p \in \mathbb{P}$. Then p is said to be a **rogue prime** if p is a rogue prime of the first and/or second kind. We define the **set of rogue primes** to be*

$$\mathit{Rog}(\mathbb{P}) = \{ p \in \mathbb{P} \mid p \text{ is rogue} \}.$$

In other words, the rogue primes are simply the primes which do not have 2 as a primitive root. Here is a list of the first 15 of these:

$$\mathrm{Rog}(\mathbb{P}) = \{7, 17, 23, 31, 41, 43, 47, 71, 73, 79, 89, 97, 103, 109, 113, ...\}.$$

Let $\alpha \in \{+, -\}$ and suppose that A_P^α is generated. Then any rogue sequence fits in as a subsequence of $\langle \alpha 1 \rangle_p^\alpha$, and hence cannot be a rogue loop. However, if $p \notin \mathrm{Rog}(\mathbb{P})$, then every rogue sequence must terminate. The question remains: by how much can we extend these terminating sequences? We answer this with the following result.

Lemma 2.13 *Let $p \in \mathbb{P}$ and let $\alpha \in \{+, -\}$. Then*

1. *A_p^α is generated $\iff$ $p \notin$ Rog($\mathbb{P}$),*
2. *A_p^+ is generated $\iff$ A_p^- is generated.*

Proof.

1. ($\Longrightarrow$) Let $p \in \mathrm{Rog}(\mathbb{P})$ and $\alpha \in \{+, -\}$. Suppose A_p^α is generated. Let $k_\alpha \in A_p^\alpha$. Then $\exists\, n_\alpha \in \mathbb{N}$ such that

   $$k_\alpha = \alpha 1 \cdot (2^{n_\alpha} - 1) \implies 2^{n_\alpha} = \alpha 1 \cdot k_\alpha + 1 = \alpha 1 \cdot (k_\alpha + \alpha 1).$$

   where the above equalities hold in the group $\mathbb{Z}/p\mathbb{Z}$. Furthermore, since $p \in \mathrm{Rog}(\mathbb{P})$, it follows by Lemma 2.10 that 2 is not a primitive root modulo p, and hence 2 has order at most $\frac{p-1}{2}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. In other words,

   $$|\{2^n \mod p \mid n \in \mathbb{N}\}| \leqslant \frac{p-1}{2}.$$

   Since 2 is a primitive root modulo 3, we can assume $p > 3$. However

   $$\left|\left\{k + \alpha 1 \mid k \in A_p^\alpha\right\}\right| = |(\mathbb{Z}/p\mathbb{Z})^\times \setminus \{\alpha 1\}| = p - 2 > \frac{p-1}{2},$$

   and we have a contradiction.

   ($\Longleftarrow$) Suppose $p \notin \mathrm{Rog}(\mathbb{P})$. Consider the rogue sequence

   $$\langle 1 \rangle_p^+ = \{2^n - 1 \mod p \mid n \in \mathbb{N}\}.$$

   Then, if $k \in A_p^+$, it follows that $k + 1 \in (\mathbb{Z}/p\mathbb{Z})^\times$, and thus $\exists\, N \in \mathbb{N}$ such that

   $$2^N = k + 1 \implies k = 2^N - 1,$$

   from which it follows that A_p^+ is generated. An analogous argument using the rogue sequence $\langle -1 \rangle_p^-$ shows that A_p^- must also be generated.

2. Follows from (1) immediately.

□

Remark 2.14 We can thus partially answer the question raised in (4). When $p \notin \text{Rog}(\mathbb{P})$, we have that both A_p^+ and A_p^- are generated, and by Lemma 2.9, the generator is given by 1 and -1 respectively. Hence, in this case, it follows that for $\alpha \in \{+, -\}$, we can take G^α to be the sets $G^\alpha = \{\alpha 1\}$, and we are done. The case for when $p \in \text{Rog}(\mathbb{P})$ is more complex.

Having now worked through several results concerning rogue primes, rogue sets, and rogue sequences, we have built an intuition for the subject. We finish this section by noting that from Theorem 2.10, it follows that Artin's Conjecture ([4]) for $n = 2$ implies the existence of infinitely many rogue primes. This motivates further investigation of this notion of *rogueness*.

3 Cunningham Bounds

In this section, we will apply the ideas developed in the previous section to study bounds for Cunningham chains; the main result of the section is Theorem 3.6 which gives a new look at bounds for Cunningham chains, and (7) which gives a fast method of finding a bound for Cunningham chains. To do so, we will need a few more definitions, and to introduce terminology on the order of an element in a rogue sequence.

Definition 3.1 *Let $n \in \mathbb{N}$ and let $\alpha \in \{+, -\}$. We define Q_n^α to be the set*

$$Q_n^\alpha = \{p \in \mathbb{P} \setminus \mathit{Rog}(\mathbb{P}) \mid p < n, n \not\equiv -\alpha 1 \mod p\}$$

In other words, Q_n^α is the set of non-rogue primes p less than n, such that $n \in A_p^\alpha$.

We can express the elements of a generated rogue set by a rogue sequence. In the context of groups, the order of an element vaguely corresponds to how far away that element is from the identity, in a multiplicative sense. We use this notion to give an analogous definition of order in such a generated rogue sense. This will essentially be the number of steps that element is from being divisible by the prime, upon which the rogue set is defined.

Definition 3.2 (Order of an element in a generated rogue set) *Let p be a non-rogue prime and let $\alpha \in \{+, -\}$. Let $q_\alpha \in A_p^\alpha$. Since $\langle \alpha 1 \rangle_p^\alpha = A_p^\alpha$, there exists $k_{q_\alpha} \leqslant p - 2$ such that*

$$q_\alpha = u_{k_{q_\alpha}}$$

*We define the **order** of q_α in A_p^α to be*

$$ord_{A_p^\alpha}(q_\alpha) = p - 1 - k_{q_\alpha} \tag{5}$$

Remark 3.3 It is worth noting that in the above definition, k_{q_α} is the discrete logarithm base 2 of $1 + \alpha 1 \cdot q_\alpha$. This is strongly related to the result in Theorem 2.10.

We give some examples to illustrate how the order of elements in generated rogue sets is calculated.

Example 3.4 In A_{11}^+ and A_{11}^- we have

$$\langle 1\rangle_{11}^+ = \{1,3,7,4,9,8,6,2,5\}, \quad \langle 10\rangle_{11}^- = \{10,8,4,7,2,3,5,9,6\}.$$

We thus have

$$\mathrm{ord}_{A_{11}^+}(7) = 7, \quad ,\mathrm{ord}_{A_{11}^+}(4) = 6, \quad \mathrm{ord}_{A_{11}^-}(7) = 6, \quad \mathrm{ord}_{A_{11}^-}(4) = 7.$$

Remark 3.5 In Example 3.4, we found that

$$\mathrm{ord}_{A_{11}^+}(7) = \mathrm{ord}_{A_{11}^-}(4) = \mathrm{ord}_{A_{11}^-}(-7).$$

In fact there is nothing special about the fact that we are in $A_{11}^{\pm}$, and it follows for $p \notin \mathrm{Rog}(\mathbb{P})$, for all $k \in A_p^+ \setminus \{1\}$ (resp. $k \in A_p^- \setminus \{-1\}$) we have from Definition 2.1, and Lemma 2.9

$$\mathrm{ord}_{A_p^+}(k) = \mathrm{ord}_{A_p^-}(-k).$$

We can now state and prove our main result of this section that will give us an improved bound for Cunningham chains.

Theorem 3.6 (Rogue bound for Cunningham chains) *Let $p \in \mathbb{P}$ and $\alpha \in \{+,-\}$. If Q_p^α is non-empty, we have*

$$|C^\alpha[p]| \leqslant \min\left\{ ord_{A_q^\alpha}(p) \mid q \in Q_p^\alpha \right\}. \tag{6}$$

Moreover, in this case we have

$$\min\left\{ ord_{A_q^\alpha}(p) \mid q \in Q_p^\alpha \right\} < p-1.$$

Remark 3.7 The question of when Q_p^α is non-empty is difficult. In Section 5, we will develop terminology which will explain how Conjecture 5.6 allows us to bypass this difficulty. Furthermore, note that the conclusion of the above theorem is false when $p = 2$.

Proof. Fix $\alpha \in \{+,-\}$. If $q \in Q_p^\alpha$, then we have $q \notin \mathrm{Rog}(\mathbb{P})$, and hence A_q^α is generated. Furthermore, q being in Q_p^α implies that $p \in A_q^\alpha$, and hence $\mathrm{ord}_{A_q^\alpha}(p)$ is well defined. Thus $p \in \langle \alpha 1\rangle_q^\alpha$, and it follows that $p = u_{k_\alpha}^\alpha$ for some $k_\alpha \leqslant q-2$. Furthermore, we have that $k_\alpha = q - 1 - \mathrm{ord}_{A_q^\alpha}(p)$. Write (a_n^α) for the sequence of elements in $C^\alpha[p]$. Then, we have that the terms of the sequence (a_n^α) considered in A_q^α are exactly $\langle u_{k_\alpha}^\alpha\rangle_q^\alpha$. This is an equality of sequences. Since $u_{g_k^\alpha}^\alpha \equiv 0 \mod q$, it follows

$$a^\alpha_{\mathrm{ord}_{A_q^\alpha}(p)} \equiv 0 \mod q,$$

and thus $a^\alpha_{\mathrm{ord}_{A_q^\alpha}(p)}$ cannot be prime. Now, since A_q^α is generated, it follows $\forall k \in A_q^\alpha$

$$\mathrm{ord}_{A_q^\alpha}(k) \leqslant q-1 < p-1.$$

Hence

$$|C^\alpha[p]| \leqslant \min\left\{\mathrm{ord}_{A_q^\alpha}(p) \mid q \in Q_p^\alpha\right\} < p-1,$$

and the result follows. □

Example 3.8 Take $p = 89$, then

$$C^+[89] = \{89, 179, 359, 719, 1439, 2879\},$$

and hence $|C^+[89]| = 6$. Using the previously known Cunningham bound presented in (1), the best estimate we could have had was

$$|C^+[89]| \leqslant 43.$$

We now consider our improved Cunningham bound with

$$Q_{89}^+ = \{11, 13, 19, 29, 37, 53, 59, 61, 67, 83\},$$

Computing, we find that

$$\begin{gathered}
\operatorname{ord}_{A_{11}^+}(89) = 9, \quad \operatorname{ord}_{A_{13}^+}(89) = 6, \quad \operatorname{ord}_{A_{19}^+}(89) = 11, \quad \operatorname{ord}_{A_{29}^+}(89) = 23, \\
\operatorname{ord}_{A_{37}^+}(89) = 32, \quad \operatorname{ord}_{A_{53}^+}(89) = 22, \quad \operatorname{ord}_{A_{59}^+}(89) = 9, \quad \operatorname{ord}_{A_{61}^+}(89) = 25, \\
\operatorname{ord}_{A_{67}^+}(89) = 38 \quad \operatorname{ord}_{A_{83}^+}(89) = 74,
\end{gathered}$$

and hence by the improved Cunningham bound it follows that

$$|C^+[89]| \leqslant 6.$$

In fact, in this case $|C^+[89]| = 6$, and hence our bound holds with equality. We will come back to this later.

Remark 3.9 The bound given in Theorem 3.6, is quite a complicated one to conceptualise. However, since it is a minimum of a set, using the same notation from the statement of the theorem, we have that $\forall q \in Q_p^\alpha$

$$|C^\alpha[p]| \leqslant \operatorname{ord}_{A_q^\alpha}(p).$$

Hence, a more tangible upper bound would be

$$|C^\alpha[p]| \leqslant \operatorname{ord}_{A_{\beta_\alpha}^\alpha}(p), \tag{7}$$

where $\beta_\alpha = \min\left\{q \in Q_p^\alpha\right\}$. We thus only need to find the smallest non-rogue prime β_α such that p is not congruent to $-\alpha 1$ modulo β_α, in order to find an upper bound for $C^\alpha[p]$, that is better than $p-1$. For example, if $p \in \mathbb{P}$ such that $p > 5$, and $p \not\equiv 4 \mod 5$, then $5 \in Q_p^+$, and hence $|C^1[p]| \leqslant 4$. Similarly, if $p \not\equiv 1 \mod 5$, then $5 \in Q_p^-$, and hence $|C^-[p]| \leqslant 4$. Moreover, we can even consider extreme cases, and find that this process is extremely fast: if we take $p = 1122659$, then it follows that $|C^+[p]| = 7$,

$$\min\left\{q \in Q_p^+\right\} = 11,$$

and $\operatorname{ord}_{A_{11}^+}(p) = 7$. We give a plot in Figures 1 and 2, illustrating the accuracy of this more accessible bound. We refer the reader to A.1 and A.2 respectively, for the Python code of these figures.

Remark that the function $\log_2(x+1)+1$ is a bound for the error of both f_1 and f_2, and hence we have

$$0 \leqslant \mathrm{ord}_{A^{\alpha}_{\beta_\alpha}}(x) - |C^{\alpha}[x]| < \log_2(x+1)+1,$$

giving the lower bound

$$|C^{\alpha}[x]| > \mathrm{ord}_{A^{\alpha}_{\beta_\alpha}}(x) - \log_2(x+1) - 1.$$

This bound however is only motivated from numerical calculations, and is more of an interesting observation for now.

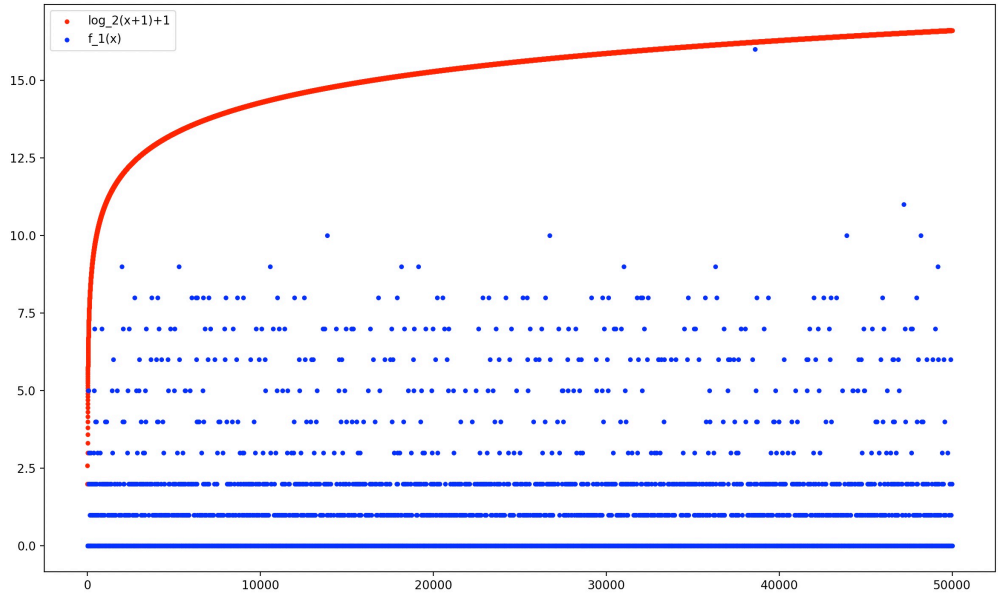

Figure 1: $f_1(x) = \mathrm{ord}_{A^{+}_{\beta_+}}(x) - |C^{+}[x]|$

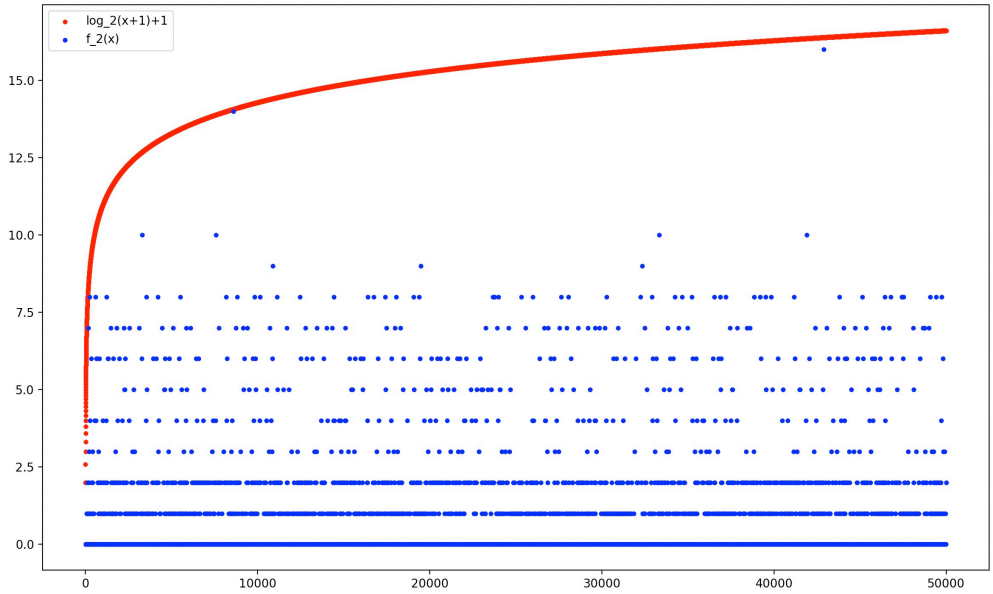

Figure 2: $f_2(x) = \mathrm{ord}_{A^-_{\beta_-}}(x) - |C^-[x]|$

4 Rogue Loops

In (4), we discussed the partition of $A_p^{\pm}$ into disjoint rogue sequences. Whereas for $p \notin \mathrm{Rog}(\mathbb{P})$, we found that the partition is a single rogue sequence. The case for $p \in \mathrm{Rog}(\mathbb{P})$ is more complicated, due to these rogue loops. We can thus ask ourselves; what length can these loops have, and how many distinct loops can there be? We begin to tackle these questions with a useful equivalence relation.

Proposition 4.1 *Let $p \in \mathbb{P}$ and let $\alpha \in \{+,-\}$. The relation*

$$R_p^\alpha = \left\{(a,b) \in A_p^\alpha \times A_p^\alpha \mid a \in \langle b\rangle_p^\alpha \text{ or } b \in \langle a\rangle_p^\alpha\right\},$$

defines an equivalence relation on A_p^α.

Proof. Fix $\alpha \in \{+,-\}$. Clearly R_p^α is both symmetric and reflexive. It remains to prove transitivity. Let $a,b,c \in A_p^\alpha$, such that $(a,b),(b,c) \in R_p^\alpha$. Suppose $p \notin \mathrm{Rog}(\mathbb{P})$. Since

$$\left\{y \in \langle 1\rangle_p^+\right\} = A_p^+, \quad \text{and} \quad \left\{y \in \langle -1\rangle_p^-\right\} = A_p^-$$

there must exist $k,l,m \in \mathbb{N}$ satisfying

$$a = u_k^\alpha, \quad b = u_l^\alpha, \quad c = u_m^\alpha.$$

Without loss of generality, suppose $b \in \langle a\rangle_p^\alpha$, and $c \in \langle b\rangle_p^\alpha$. Then, since

$$\langle a\rangle_p^\alpha = \{u_n^\alpha \mid n \geqslant k\}, \quad \langle b\rangle_p^\alpha = \{u_n^\alpha \mid n \geqslant l\},$$

it follows that $m \geq l \geq k$, and hence $c \in \langle a \rangle_p^\alpha$, giving $(a, c) \in R_p^\alpha$. Suppose now that $p \in \text{Rog}(\mathbb{P})$. Note that by Definition 2.3, if $\langle g \rangle_p^\alpha$ is a rogue loop in A_p^α, then $\forall k \in \langle g \rangle_p^\alpha$, the sequence $\langle k \rangle_p^\alpha$ is a shift of $\langle g \rangle_p^\alpha$. Thus, if $(a, b) \in R_p^\alpha$, and either one of $\langle a \rangle_p^\alpha$ or $\langle b \rangle_p^\alpha$ is a rogue loop, it follows that both rogue sequences are rogue loops. Hence if $(a, b) \in R_p^\alpha$, then either both $\langle a \rangle_p^\alpha$ and $\langle b \rangle_p^\alpha$ are rogue loops, or both are terminating rogue sequences. Using the same reasoning for $(b, c) \in R_p^\alpha$, we have that $\langle a \rangle_p^\alpha$ and $\langle c \rangle_p^\alpha$ are either both rogue loops or both terminating rogue sequences. If the former holds, then by our above reasoning, it follows that $(a, c) \in R_p^\alpha$. If the latter holds, then we can say without loss of generality that $a \in \langle b \rangle_p^\alpha$, and $c \in \langle b \rangle_p^\alpha$. It then follows $\exists\, m, k \in \mathbb{N}$ such that

$$a = v_m^\alpha, \quad c = v_k^\alpha,$$

where $\langle b \rangle_p^\alpha = (v_n^\alpha)$. Suppose $k > m$,, then

$$\langle a \rangle_p^\alpha = \{v_n^\alpha \mid n \geqslant m\} \ni c$$

and hence $(a, c) \in R_p^\alpha$. The other cases follow analogously. □

Remark 4.2 We can thus partition $A_p^\pm$ into equivalence classes. It follows that the rogue loops are precisely the equivalence classes, except for the equivalence class of 1 in A_p^+ and -1 in A_p^-. Thus, for $\alpha \in \{+, -\}$, it follows that A_p^α can be written as the disjoint union of the rogue loops together with the elements of $\langle \alpha \rangle_p^\alpha$ (see (8) and (9) for examples that illustrate this partition). Of course, by Lemma 2.9, we knew this for $p \notin \text{Rog}(\mathbb{P})$, but we have now covered all cases of $p \in \mathbb{P}$.

We now study these rogue loops to get a better understanding of this partition.

Lemma 4.3 *Let $p \in Rog(\mathbb{P})$, and let $\alpha \in \{+, -\}$. If $g \in A_p^\alpha$, then*

$$\langle g \rangle_p^\alpha \textit{ is a rogue loop} \iff g \notin \langle \alpha 1 \rangle_p^\alpha.$$

Proof. Fix $\alpha \in \{+, -\}$. ($\Longrightarrow$) Consider the rogue sequence

$$\langle \alpha 1 \rangle_p^\alpha = \{u_k^\alpha \mid k \in \mathbb{N}, k < g_k^\alpha\},$$

and suppose $g \in \langle \alpha 1 \rangle_p^\alpha$. Then, $\exists\, K \in \mathbb{N}$ such that $g = u_K^\alpha$, and hence

$$\langle g \rangle_p^\alpha = \{u_n^\alpha \mid K \leq n < g_k^\alpha\}.$$

It follows that $\langle g \rangle_p^\alpha$ can not be periodic, and hence $\langle g \rangle_p^\alpha$ is not a rogue loop.

($\Longleftarrow$) Suppose $\langle g \rangle_p^\alpha$ is not a rogue loop. If $g = \alpha 1$, the result is obvious. Suppose $g \neq \alpha 1$. Then, if

$$\langle g \rangle_p^\alpha = \{v_k^\alpha \mid k < g_k^\alpha\},$$

where $g_k^\alpha = \min\{n \in \mathbb{N} \mid v_n^\alpha \equiv 0 \mod p\}$, it follows by (3) that

$$v_{g_k^\alpha - 1}^\alpha = \frac{p - \alpha 1}{2},$$

and hence $(g, \frac{p-\alpha 1}{2}) \in R_p^\alpha$, where R_p^α is the equivalence relation on A_p^α defined in Proposition 4.1. By a similar reasoning, $(\frac{p-\alpha 1}{2}, \alpha 1) \in R_p^\alpha$, and since R_p^α is an equivalence relation, it follows that $(g, \alpha 1) \in R_p^\alpha$. Hence, $g \in \langle \alpha 1 \rangle_p^\alpha$ or $\alpha 1 \in \langle g \rangle_p^\alpha$. Suppose the latter holds, then $\exists\, N \in \mathbb{N}$, such that $N < g_k^\alpha$ and

$$2v_N^\alpha + \alpha 1 \equiv \alpha 1 \mod p \implies v_N^\alpha \equiv 0 \mod p,$$

contradicting the minimality of g_k^α. Hence, $g \in \langle \alpha 1 \rangle_p^\alpha$, and the result follows. □

Remark 4.4 It follows from this result that any terminating rogue sequence in A_p^+ (resp. A_p^-) is a subsequence of the rogue sequence $\langle 1 \rangle_p^+$ (resp. $\langle -1 \rangle_p^-$). Of course, by Lemma 2.9, we knew this for $p \notin \mathrm{Rog}(\mathbb{P})$, and we can now use Lemma 4.3, to generalise this for $p \in \mathrm{Rog}(\mathbb{P})$.

We further study rogue loops. Let $\alpha \in \{+, -\}$. For a rogue prime p, and a rogue loop $\langle g \rangle_p^\alpha$ in A_p^α, by the **length** of $\langle g \rangle_p^\alpha$, we will mean the size of its underlying set. We will denote the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$ by $O_p(2)$. Take $p = 7$, we have

$$A_7^+ = \langle 2 \rangle_7^+ \sqcup \langle 1 \rangle_7^+, \quad |\langle 2 \rangle_7^+| = 3, \quad |\langle 1 \rangle_7^+| = 2 \tag{8}$$

In this simple example, we notice that rogue loops have size one more than $\langle 1 \rangle_7^+$. Furthermore, if $p = 31$, we have

$$A_{31}^+ = \langle 2 \rangle_{31}^+ \sqcup \langle 4 \rangle_{31}^+ \sqcup \langle 10 \rangle_{31}^+ \sqcup \langle 27 \rangle_{31}^+ \sqcup \langle 29 \rangle_{31}^+ \sqcup \langle 1 \rangle_{31}^+, \tag{9}$$

and a simple calculation gives that every rogue loop has size 5, and that $|\langle 1 \rangle_{31}^+| = 4$. Note that 2 has order 3 in $(\mathbb{Z}/7\,\mathbb{Z})^\times$, and has order 5 in $(\mathbb{Z}/31\mathbb{Z})^\times$. With this in mind, we provide the following powerful result.

Theorem 4.5 *Let $p \in Rog(\mathbb{P})$ and $\alpha \in \{+, -\}$. Then*

$$|\langle \alpha 1 \rangle_p^\alpha| = O_p(2) - 1 \leqslant \frac{p-3}{2}.$$

Furthermore, if $\langle g \rangle_p^\alpha$ is a rogue loop in A_p^α, then

$$|\langle g \rangle_p^\alpha| = O_p(2), \tag{10}$$

and hence the maximum length of a rogue loop is $\frac{p-1}{2}$. Finally, the number of disjoint rogue loops in A_p^α is given by

$$\frac{p-1}{O_p(2)} - 1. \tag{11}$$

Remark 4.6 It is interesting to see that when $p \notin \mathrm{Rog}(\mathbb{P})$, we have $O_p(2) = p - 1$, and there are no rogue loops. Hence (11) holds for all $p \in \mathbb{P}$, and furthermore, for $p \notin \mathrm{Rog}(\mathbb{P})$, it follows by Lemma 2.9, that

$$|\langle \alpha 1 \rangle_p^\alpha| = p - 2 = O_p(2) - 1,$$

and hence the right equation in (10) also holds for all $p \in \mathbb{P}$.

Proof. Fix $\alpha \in \{+,-\}$. Since $p \in \mathrm{Rog}(\mathbb{P})$, by Theorem 2.10, 2 is not a primitive root modulo p, and hence

$$O_p(2) \leqslant \frac{p-1}{2}. \tag{12}$$

Now let $\langle g \rangle_p^\alpha$ be a rogue loop in A_p^α, then

$$\langle g \rangle_p^\alpha = \left\{ 2^{n-1}(g+\alpha 1) - \alpha 1 \mod p \mid n \in \mathbb{N} \right\}.$$

Suppose $k, \ell \in \mathbb{N}$ satisfy

$$2^{k-1}(g+\alpha 1) - \alpha 1 \equiv 2^{\ell-1}(g+\alpha 1) - \alpha 1 \mod p.$$

It then follows

$$2^k \equiv 2^\ell \mod p \implies k \equiv \ell \mod O_p(2).$$

Hence the set $\{2^{n-1}(g+\alpha 1) - \alpha 1 \mod p \mid n \in \mathbb{N}\}$, contains $O_p(2)$ distinct values, and it follows that

$$|\langle g \rangle_p^\alpha| = O_p(2).$$

Furthermore, we have

$$\langle \alpha 1 \rangle_p^\alpha = \{ 2^n \alpha 1 - \alpha 1 \mod p \mid n \in \mathbb{N}, n < g_k^\alpha \},$$

and since

$$g_k^\alpha = \min \{ n \in \mathbb{N} \mid 2^n \cdot \alpha 1 - \alpha 1 \equiv 0 \mod p \} = O_p(2),$$

it follows that $|\langle \alpha 1 \rangle_p^\alpha| = O_p(2) - 1$. Combining this with (12), we get

$$|\langle \alpha 1 \rangle_p^\alpha| \leqslant \frac{p-1}{2} - 1 = \frac{p-3}{2}.$$

Finally by Proposition 4.1, we have

$$A_p^\alpha = \bigsqcup_{[g]_{R_p^\alpha}} \left\{ y \in \langle g \rangle_p^\alpha \right\} \implies p - 2 = |A_p^\alpha| = \sum_{[g]_{R_p^\alpha}} |\langle g \rangle_p^\alpha|.$$

If we let

$$X = \left\{ [g]_{R_p^\alpha} \mid \langle g \rangle_p^\alpha \text{ is a rogue loop} \right\},$$

it then follows that

$$p - 2 = \sum_{[g]_{R_p^\alpha}} |\langle g \rangle_p^\alpha| = |\langle \alpha 1 \rangle_p^\alpha| + \sum_{[g]_{R_p^\alpha} \in X} |\langle g \rangle_p^\alpha| = O_p(2) - 1 + O_p(2)|X|,$$

and solving for $|X|$ gives the result. □

Remark 4.7 Let $p \in \mathbb{P}$, and consider $C^{\alpha}[p]$. It follows from the above result that if we can find a $q \in \mathrm{Rog}(\mathbb{P})$ such that $q < p$, and $p \in \langle \alpha 1 \rangle_q^{\alpha}$, then

$$|C^{\alpha}[p]| \leqslant |\langle \alpha 1 \rangle_q^{\alpha}| \leqslant \frac{q-3}{2} < \frac{p-3}{2}. \tag{13}$$

Hence, it would follow that the bound (1) is strict. In other words, if we can find a $q \in \mathrm{Rog}(\mathbb{P})$ such that $q < p$, and the congruence relation

$$2^n \equiv \alpha 1 \cdot p + 1 \mod q, \tag{14}$$

has a solution, then (13) holds.

We write this formally as a conjecture, which is numerically supported for the first 100000 rogue primes up to $N = 2157537$. We refer the reader to A.5 for the Python code of this computation.

Conjecture 4.8 Let $N \in \mathbb{N}$, let $\alpha \in \{+, -\}$. Then, $\exists\, q \in \mathrm{Rog}(\mathbb{P})$ such that $N \in \langle \alpha 1 \rangle_q^{\alpha}$. Hence (14) always has solutions.

5 Further Investigation and Open Questions

We begin this section by studying (6). We have seen in Example 3.8 that this equation can hold with equality, and it is natural to ask ourselves whether this is always the case. If $p \in \mathbb{P}$, then one reason for (6) to not hold with equality is if there exists a prime $q \in \mathrm{Rog}(\mathbb{P})$ such that $q < p, (p, \alpha 1) \in R_q^{\alpha}$, and

$$\mathrm{ord}_{A_q^{\alpha}}(p) = |C^{\alpha}[p]|.$$

Hence, $2 \cdot \max\{C^{\alpha}[p]\} + \alpha 1$ could have q as its only factor smaller than p, and thus (6), would not hold with equality. This raises a further question: does $2\max\{C^{\alpha}[p]\} + \alpha 1$ have divisors smaller than p? We tackle the first of these potential issues with an improved version of Q_p^{α}.

Definition 5.1 (Corogueness) *Let $n \in \mathbb{N}$ and $\alpha \in \{+, -\}$. A prime $q \in \mathbb{P}$ is said to be* ***corogue*** *to n in A_p^{α} if $(n, \alpha 1) \in R_q^{\alpha}$. The set of primes corogue to n in A_p^{α} is denoted by*

$$Rog_{\alpha}(n) = \left\{ p \in \mathbb{P} \mid p < n, \text{ and } (n, \alpha 1) \in R_p^{\alpha} \right\}. \tag{15}$$

Remark 5.2 Clearly, $Q_n^{\alpha} \subseteq \mathrm{Rog}_{\alpha}(n)$. In fact, $\mathrm{Rog}_{\alpha}(n)$ is simply the set Q_n^{α} together with an appropriate set of rogue primes, depending on n.

We give an example to illustrate that this inclusion can be proper.

Example 5.3

$$Q_{17}^{+} = \{5, 11, 13\}, \quad \mathrm{Rog}_{+}(17) = \{5, 7, 11, 13\}.$$

The set $\mathrm{Rog}_\alpha(n)$ is precisely the set we need in order to obtain an extended notion of order, which coincides with our original definition. The idea here is to use the results from Theorem 4.5: we can rewrite (5) as

$$\mathrm{ord}_{A_p^\alpha}(q) = |\langle \alpha 1 \rangle_p^\alpha| - k_{q_\alpha} = O_p(2) - 1 - k_{q_\alpha}.$$

This motivates the following definition.

Definition 5.4 (Order of an element in a corogue set) *Let $n \in \mathbb{N}$ and $\alpha \in \{+,-\}$. For a prime $p \in Rog_\alpha(n)$ we define the **order** of n in A_p^α to be*

$$ord_{A_p^\alpha}(n) = O_p(2) - 1 - k_{p_\alpha},$$

where

$$u_{k_{p_\alpha}} = n,$$

in the rogue sequence $\langle \alpha 1 \rangle_p^\alpha$.

The only difference between Definition 5.4 and Definition 3.2, is that for $n \in \mathbb{N}$, the number $\mathrm{ord}_{A_p^\alpha}(n)$ is now defined for $p \in \mathrm{Rog}_\alpha(n)$, whereas previously, it was only defined for $p \in Q_n^\alpha$. We can thus give an improved version of Theorem 3.6, which is more likely to give equality.

Theorem 5.5 *Let $p \in \mathbb{P}$ and let $\alpha \in \{+,-\}$. Suppose that $Rog_\alpha(p)$ is non-empty, then*

$$|C^\alpha[p]| \leqslant \min\left\{ ord_{A_q^\alpha}(p) \mid q \in Rog_\alpha(p) \right\}. \tag{16}$$

Proof. Repeat the argument of Theorem 3.6, using the extended terminology. □

To address the second issue we raised concerning equality of (6), we conjecture the existence of divisors of the first composite element of a rogue sequence, that are smaller then the base prime.

Conjecture 5.6 Let $p \in \mathbb{P}$, such that $p > 3$ and let $\alpha \in \{+,-\}$. Denote $\gamma_\alpha = 2\max\{C^\alpha[p]\} + \alpha 1$. Then

$$\min\{q \in \mathbb{P} : q \mid \gamma_\alpha\} < p.$$

Hence, (16) holds with equality.

The following note illustrates how Conjecture 5.6 justifies the choice of introducing rogue sets and rogue sequences to study Cunningham chains.

Remark 5.7 In Note 3.7 we discussed that the non-emptiness of Q_p^α is difficult to study. The formulation of Theorem 5.5 translates this issue to the non-emptiness of $\mathrm{Rog}_\alpha(p)$. Conjecture 5.6 says that this is never the case. Hence, if Conjecture 5.6 holds true, in addition to saying that (16) holds with equality, we can also remove the non-emptiness assumption on $\mathrm{Rog}_\alpha(p)$.

Another interesting consequence of Conjecture 5.6 is the following.

Remark 5.8 If Conjecture 5.6 holds, then given $p \in \mathbb{P}, \exists\, a_\alpha \in \mathbb{P}$ such that $a_\alpha < p$, and

$$2^{|C^\alpha[p]|}(p + \alpha 1) - \alpha 1 = a_\alpha \cdot b_\alpha,$$

for some $b_\alpha \in \mathbb{N}$. It then follows that

$$b_\alpha = \frac{2^{|C^\alpha[p]|}(p + \alpha 1) - \alpha 1}{a_\alpha} \geqslant \frac{2^{|C^\alpha[p]|}(p + \alpha 1) - \alpha 1}{p + \alpha 1}$$

and thus, since b is a positive integer, we must have $b_\alpha \geq 2^{|C^\alpha[p]|}$. We thus have

$$|C^\alpha[p]| \leq \log_2(b_\alpha),$$

giving some kind of logarithmic bound.

With this remark, we give a simple logarithmic bound for a specific type of prime, namely the Mersenne Primes[1].

Lemma 5.9 *Let $p \in \mathbb{P}$ and let $\alpha \in \{+, -\}$. If $p = 2^n - 1$, for some $n \in \mathbb{N}$, then*

$$|C^\alpha[p]| < \log_2(p + 1).$$

Proof. Suppose $p = 2^n - 1$, for some $n \in \mathbb{N}$, it follows that $\log_2(p + 1) \in \mathbb{N}$, and

$$2^{\log_2(p+1)}(p + 1) - 1 = (p + 1)^2 - 1 = p(p + 2),$$

which is composite. Similarly, we have

$$2^{\log_2(p+1)}(p - 1) + 1 = p^2,$$

which is also composite. □

It is conjectured that there are infinitely many such Mersenne primes, and hence we can imagine that this logarithmic bound could hold for infinitely many primes.

Conjecture 5.10 Let $p \in \mathbb{P}$, such that $p > 5$ and let $\alpha \in \{+, -\}$. Then

$$|C^\alpha[p]| < \log_2(p + 1). \tag{17}$$

We give graphs in Figures 3 and 4, which illustrate this bound, and refer the reader to A.3 and A.4 respectively for the Python code of these figures.

[1] See [1, page 25]

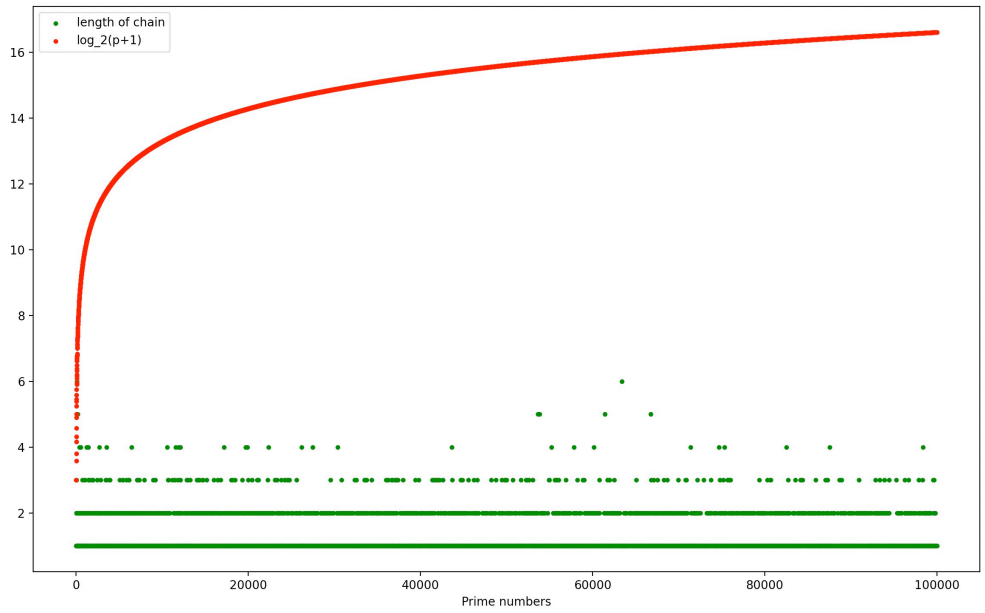

Figure 3: Chains of the first kind

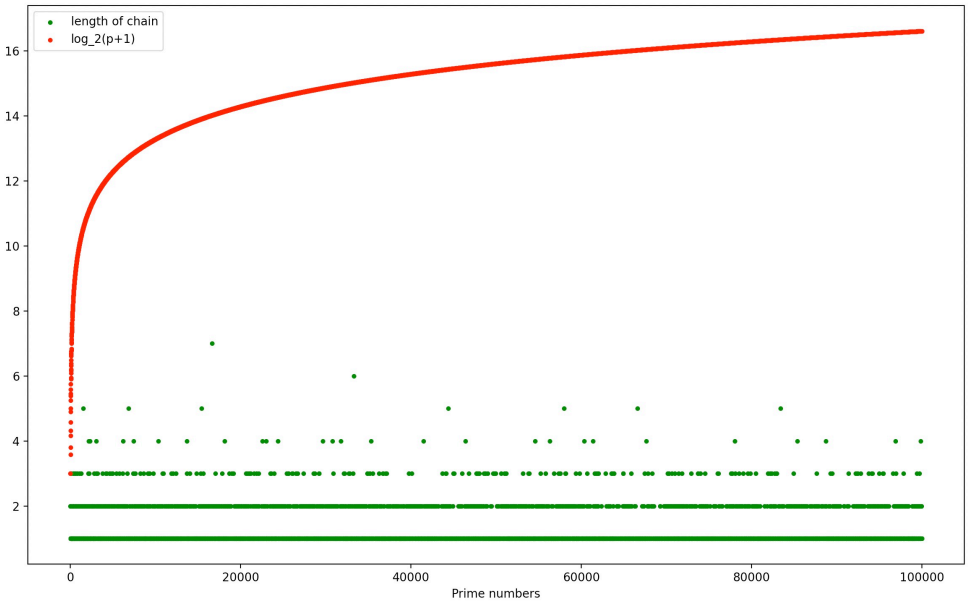

Figure 4: Chains of the second kind

Theorem 5.11 *Conjecture 5.10 implies Conjecture 5.6.*

Proof. We fix $\alpha \in \{+,-\}$, and show that by induction on the length of $|C^\alpha[p]|$, by assuming Conjecture 5.10, we have Conjecture 5.6. Suppose $p \in \mathbb{P}$ such that $|C^\alpha[p]| = 1$. Then $p \neq 3$, and it follows that

$$p^2 - (2p+1) > 0, \quad p^2 - (2p-1) > 0.$$

Hence there exists a divisor of $2p+\alpha 1$ which is smaller than p. Assume the result holds for some $n \geq 1$ and suppose $p \in \mathbb{P}$ such that $|C^\alpha[p]| = n+1$. It follows that $|C^\alpha[2p+\alpha 1]| = n$, and hence there exists a prime divisor q of

$$\gamma_\alpha = 2\max\{C^\alpha[p]\} + \alpha 1$$

such that $q < 2p + \alpha 1$. Suppose for a contradiction, that $q \geqslant p$. Then we have

$$\gamma_\alpha \geqslant p^2 \implies 2^{|C^\alpha[p]|}(p+\alpha 1) - \alpha 1 \geqslant p^2 \implies |C^\alpha[p]| \geqslant \log_2\left(\frac{p^2+\alpha 1}{p+\alpha 1}\right) \tag{18}$$

If $\alpha = -$, we conclude that $|C^-[p]| \geq \log_2(p+1)$, contradicting (17). For $\alpha = +$, we first note that from (18) we obtain $|C^+[p]| \geq \log_2(p+1-\frac{2p}{p+1})$. Now, if $p+1 = 2^n$ for some n, then by Lemma 5.9, it follows that $\log_2(p+1-\frac{2p}{p+1}) \leq |C^+[p]| < \log_2(p+1)$, which is a contradiction, since $|C^+[p]|$ is an integer. Hence, we assume that $p+1$ is not equal to a power of 2. But then since $|C^+[p]|$ is an integer, it follows that $|C^+[p]| \geq \log_2(p+1)$ which again contradicts (17). □

We now give a result which establishes a relationship between logarithmic bounds on the size of chains to quadratic bounds on the size of the elements on the chain.

Proposition 5.12 *Let $p \in \mathbb{P}$. Then*

1. *For chains of the first kind*

$$|C^+[p]| < \log_2(p+1) \iff 2\max\left\{C^+[p]\right\} + 1 < (p+1)^2 \tag{19}$$

2. *For chains of the second kind*

   (i) If $|C^-[p]| < \log_2(p-2)$, then $2\max\{C^-[p]\} - 1 < (p-1)^2$

   (ii) If $2\max\{C^-[p]\} - 1 < (p-1)^2$, then $|C^-[p]| < \log_2(p-1)$

Remark 5.13 In the above proposition, we can say more for chains of the first kind than for chains of the second kind. This is a consequence of Lemma 5.9. Note that adapting the proof of Lemma 5.9 to primes of the form $p = 2^n + 1$ fails to produce bounds on the size of chains of both the first and second kind.

Proof.

1. ($\Longrightarrow$) If the LHS of (19) holds, then

$$2\max\{C^+[p]\}+1 = 2^{|C^+[p]|}(p+1)-1 < 2^{\log_2(p+1)}(p+1)-1 < (p+1)^2$$

giving the RHS of (19).

($\Longleftarrow$) Suppose that the RHS of (19) holds, and assume for a contradiction that $|C^+[p]| \geq \log_2(p+2)$. Then

$$2\max\{C^+[p]\}+1 = 2^{|C^+[p]|}(p+1)-1 \geq 2^{\log_2(p+2)}(p+1)-1 = (p+1)^2+p > (p+1)^2$$

which is a contradiction. Hence, $|C^+[p]| \leqslant \log_2(p+2)$. If $p+1 = 2^n$, for some $n \in \mathbb{N}$, it follows by Lemma 5.9 that $|C^+[p]| < \log_2(p+1)$. If $p+1 \neq 2^n$ for any $n \in \mathbb{N}$, it then follows that

$$\lfloor \log_2(p+2) \rfloor = \lfloor \log_2(p+1) \rfloor < \log_2(p+1)$$

and hence $|C^+[p]| < \log_2(p+1)$. In either case, we obtain the LHS of (19).

2. (i) If $|C^-[p]| < \log_2(p-2)$ holds, then

$$\begin{aligned} 2\max\{C^-[p]\}-1 &= 2^{|C^-[p]|}(p-1)+1 < 2^{\log_2(p-2)}(p-1)+1 \\ &= (p-1)^2+2-p < (p-1)^2 \end{aligned}$$

giving (i).

(ii) Suppose that $2\max\{C^-[p]\}-1 < (p-1)^2$, and assume for a contradiction that $|C^-[p]| \geq \log_2(p-1)$. Then

$$2\max\{C^-[p]\}-1 = 2^{|C^-[p]|}(p-1)+1 \geq 2^{\log_2(p-1)}(p-1)+1 > (p-1)^2$$

which contradicts our assumption, and (ii) follows.

□

We finish by remarking that Problem 5.1 in [2], implies that

$$|C^1[p]| < \log_2(p)-1 < \log_2(p+1),$$

giving Conjecture 5.10. This last conjecture is heavily supported by numerical evidence, and hence gives further reason to investigate (17). By Theorem 5.11, this would prove the very deep result that is Conjecture 5.6, and give equality to (16), giving an exact formula for the length of the Cunningham chains.

A Python Codes

A.1 Python Code for $\mathbf{f_1(x)}$:

```
import matplotlib.pyplot as plt
import numpy as np
import math

def prime(n):
    for i in range(2, int(n / 2) + 1):
        if (n % i == 0):
            return 0
    return 1

def getSophieGermainPrime(startLimit, endLimit):
    l1 = []
    p, r = startLimit, endLimit
    if p == 1:
        p = 2
    for a in range(p, r + 1):
        k = 0
        for i in range(2, int(a / 2) + 1):
            if (a % i == 0):
                k = k + 1
                break
        if (k <= 0):
            x = prime(2 * a + 1)
            if (x == 1):
                l1.append(a)
    return (l1)

def print_C_len(p0):
    i = 0;
    list = []
    while (True):
        flag = 1;
        x = pow(2, i);
        p1 = x * p0 + (x - 1);

        for k in range(2, p1):
            if (p1 % k == 0):
                flag = 0;
                break;
```

```
        if (flag == 0):
            break;
        list.append(p1)
        i += 1;
    return (len(list))

def print_C_list(p0):
    i = 0;
    list = []
    while (True):
        flag = 1;
        x = pow(2, i);
        p1 = x * p0 + (x - 1);

        for k in range(2, p1):
            if (p1 % k == 0):
                flag = 0;
                break;

        if (flag == 0):
            break;
        list.append(p1)
        i += 1;
    return (list)

List_Primes=[]

for i in range(6,50000):
    if prime(i)==True:
        List_Primes.append(i)

Non_rogue_list = [set of Non rogue prime numers]
p = 0
SG_primes = getSophieGermainPrime(6, 50000)
Chain_length = []

x1 = [i for i in List_Primes]
for j in x1:
    p = print_C_len(j)
    Chain_length.append(p)

Q = []
List_of_k = []
```

```
for i in List_Primes:
    for j in Non_rogue_list:
        if j < i:
            Q.append(j)
        for m in Q:
            if (i + 1) % m == 0:
                Q.remove(m)
        if Q:
            k_i = min(Q)
            List_of_k.append(k_i)
            Q = []
            break
Order_list=[]
Chain_list=[]

index=0
for i in range(len(List_Primes)):
    new_k=List_of_k[i]
    remainder=List_Primes[i]%new_k
    while remainder !=0:
        remainder=remainder*2+1
        remainder=remainder%new_k
        index=index+1
    Order_list.append(index)
    index=0

array1 = np.array(Order_list)
array2 = np.array(Chain_length)
subtracted_array = np.subtract(array1, array2)
subtracted = list(subtracted_array)
index2=0

x=range(1,50000)
y=[]
for i in x:
    y.append(math.log(i+1,2)+1)
plt.scatter(x, y, marker='.', label="log_2{x+1}+1",c='r')
plt.scatter(List_Primes, subtracted, marker='.', label="f_1(x)",c='b')

plt.legend()
plt.show()
```

A.2 Python Code for $\mathbf{f_2(x)}$:

```
import matplotlib.pyplot as plt
import numpy as np
import math

def prime(n):
    for i in range(2, int(n / 2) + 1):
        if (n % i == 0):
            return 0
    return 1

def getSophieGermainPrime(startLimit, endLimit):
    l1 = []
    p, r = startLimit, endLimit
    if p == 1:
        p = 2
    for a in range(p, r + 1):
        k = 0
        for i in range(2, int(a / 2) + 1):
            if (a % i == 0):
                k = k + 1
                break
        if (k <= 0):
            x = prime(2 * a - 1)
            if (x == 1):
                l1.append(a)
    return (l1)

def print_C_len(p0):
    i = 0;
    list = []
    while (True):
        flag = 1;
        x = pow(2, i);
        p1 = x * p0 - (x - 1);

        for k in range(2, p1):
            if (p1 % k == 0):
                flag = 0;
                break;

        if (flag == 0):
```

```
            break;
        list.append(p1)
        i += 1;
    return (len(list))

def print_C_list(p0):
    i = 0;
    list = []
    while (True):
        flag = 1;
        x = pow(2, i);
        p1 = x * p0 - (x - 1);

        for k in range(2, p1):
            if (p1 % k == 0):
                flag = 0;
                break;

        if (flag == 0):
            break;
        list.append(p1)
        i += 1;
    return (list)

List_Primes=[]

for i in range(6,50000):
    if prime(i)==True:
        List_Primes.append(i)

Non_rogue_list = [set of Non rogue prime numers]
p = 0
SG_primes = getSophieGermainPrime(6, 50000)
Chain_length = []

x1 = [i for i in List_Primes]
for j in x1:
    p = print_C_len(j)
    Chain_length.append(p)

Q = []
List_of_k = []
for i in List_Primes:
```

```
    for j in Non_rogue_list:
        if j < i:
            Q.append(j)
        for m in Q:
            if (i - 1) % m == 0:
                Q.remove(m)
        if Q:
            k_i = min(Q)
            List_of_k.append(k_i)
            Q = []
            break
Order_list=[]
Chain_list=[]

index=0
for i in range(len(List_Primes)):
    new_k=List_of_k[i]
    remainder=List_Primes[i]%new_k
    while remainder !=0:
        remainder=remainder*2-1
        remainder=remainder%new_k
        index=index+1
    Order_list.append(index)
    index=0

array1 = np.array(Order_list)
array2 = np.array(Chain_length)
subtracted_array = np.subtract(array1, array2)
subtracted = list(subtracted_array)
index2=0

x=range(1,50000)
y=[]
for i in x:
    y.append(math.log(i+1,2)+1)
plt.scatter(x, y, marker='.', label="log_2{x+1}+1",c='r')
plt.scatter(List_Primes, subtracted, marker='.', label="f_2(x)",c='b')

plt.legend()
plt.show()
```

A.3 Python Code for $g_1(x)$:

```
import matplotlib.pyplot as plt
import math
def prime(n):
    for i in range(2,int(n/2)+1):
        if(n%i==0):
            return 0
    return 1
def getSophieGermainPrime(startLimit,endLimit):
    l1=[]
    p,r=startLimit,endLimit
    if p==1:
        p=2
    for a in range(p,r+1):
        k=0
        for i in range(2,int(a/2)+1):
            if(a%i==0):
                k=k+1
                break
        if(k<=0):
            x=prime(2*a+1)
            if(x==1):
                l1.append(a)
    return(l1)

def print_C(p0):
    i = 0;
    list=[]
    while (True):
        flag = 1;
        x = pow(2, i);
        p1 = x * p0 + (x - 1);

        for k in range(2, p1):
            if (p1 % k == 0):
                flag = 0;
                break;

        if (flag == 0):
            break;
        list.append(p1)
        i += 1;
```

```
    return(len(list))
p = 0
SG_primes = getSophieGermainPrime(1,1000)

List_Primes=[]
for i in range(6,100000):
    if prime(i)==True:
        List_Primes.append(i)
y1=[]
x1 = [i for i in List_Primes]
for j in x1:
    p = print_C(j)
    y1.append(p)

y=[]
for i in List_Primes:
    y.append(math.log(i+1,2))

plt.scatter(x1, y1, marker='.', label="length of chain",c='g')
plt.scatter(List_Primes, y, marker='.', label="log_2(p+1)",c='r')
plt.xlabel('Prime numbers')
plt.legend()
plt.show()
```

A.4 Python Code for $\mathbf{g_2(x)}$:

```
import matplotlib.pyplot as plt
import math
def prime(n):
    for i in range(2,int(n/2)+1):
        if(n%i==0):
            return 0
    return 1
def getSophieGermainPrime(startLimit,endLimit):
    l1=[]
    p,r=startLimit,endLimit
    if p==1:
        p=2
    for a in range(p,r+1):
        k=0
        for i in range(2,int(a/2)+1):
            if(a%i==0):
```

```
                k=k+1
                break
        if(k<=0):
            x=prime(2*a-1)
            if(x==1):
                l1.append(a)
    return(l1)

def print_C(p0):
    i = 0;
    list=[]
    while (True):
        flag = 1;
        x = pow(2, i);
        p1 = x * p0 - (x - 1);

        for k in range(2, p1):
            if (p1 % k == 0):
                flag = 0;
                break;

        if (flag == 0):
            break;
        list.append(p1)
        i += 1;
    return(len(list))
p = 0
SG_primes = getSophieGermainPrime(1,1000)

List_Primes=[]
for i in range(6,100000):
    if prime(i)==True:
        List_Primes.append(i)
y1=[]
x1 = [i for i in List_Primes]
for j in x1:
    p = print_C(j)
    y1.append(p)

y=[]
for i in List_Primes:
    y.append(math.log(i+1,2))
```

```
plt.scatter(x1, y1, marker='.', label="length of chain",c='g')
plt.scatter(List_Primes, y, marker='.', label="log_2(p+1)",c='r')
plt.xlabel('Prime numbers')
plt.legend()
plt.show()
```

A.5 Python Code for Conjecture 4.8

```
from itertools import islice
from sympy import nextprime, is_primitive_root

def generator():
    p = 2
    while(p:=nextprime(p)):
        if not(is_primitive_root(2, p)):
            yield p

roguePrimes = list(islice(generator(), 100000)) #OEIS A001122 Chai Wah Wu

c = max(roguePrimes)
#print(c)
valid = set() #numbers which are generated by plus (minus) 1


for prime in roguePrimes:
    generated = []
    a = 1
    while True:
        generated.append(a)
        a = (2*a + 1)%prime
        if a == 0:
            break
    valid.update(generated)

m = list(valid)

for i in range(1, c+1): #largest number+1 for which we can guarantee q
    if m[i-1] != i:
        print(i)
        break
```

Acknowledgments

We are extremely thankful to Dr Keenan Kidwell for his incredible support and insightful feedback that has culminated in the paper as it stands. We would like to thank Melissa Ozturk for her contributions and insights during our group project in the final term of the 2021/22 academic year, which led to the writing of this paper, and the referee for their suggestions on improving the notation. We are deeply thankful to Elliot Cocks for his calculations which helped us get these ideas started.

References

[1] R.M. Hill, *Introduction to Number Theory*, World Scientific Europe, 2018.

[2] Y. Kanado, The relation between a generalized Fibonacci sequence and the length of Cunningham chains, available online at the URL: `https://arxiv.org/abs/2205.07650`

[3] G. Löh, Long chains of nearly doubled primes, *Math. Comp.*, **53** (1989), 751–759.

[4] M.R. Murty, Artin's conjecture for primitive roots, *Math. Intelligencer*, **10** (1988), 59–67.

Anand Bhardwaj
University College London
25 Gordon St, WC1H 0AY
London, United Kingdom
E-mail: `anand.bhardwaj.20@ucl.ac.uk`

Luisa Degen
University College London
25 Gordon St, WC1H 0AY
London, United Kingdom
E-mail: `luisa.degen.20@ucl.ac.uk`

Radostin Petkov
University College London
25 Gordon St, WC1H 0AY
London, United Kingdom
E-mail: `radostin.petkov.20@ucl.ac.uk`

Sidney Stanbury
University College London
25 Gordon St, WC1H 0AY
London, United Kingdom
E-mail: `sidney.stanbury.20@ucl.ac.uk`

Received: September 5, 2023 **Accepted**: April 15, 2024
Communicated by Mike Krebs