Periods of Linear Recurrence Relations and Orders of Polynomial Roots in Finite Fields

J. Fraser

November 11, 2018

Abstract

In this paper we give conditions for the existence of a root to a polynomial in a finite field of given order. We then use these conditions to show that, for a fixed polynomial $f(x)$, meeting certain requirements, there are only finitely many numbers n such that there is no finite field containing a root of $f(x)$ of multiplicative order n. Further, for polynomials $f(x)$ with some additional requirements we give an algorithm for determining this set of orders n which roots of $f(x)$ can never have. Further, we use these conditions to investigate the behaviour of periods of linear recurrence relations. In particular, we show for each k-Fibonacci sequence, and each even number n, with finitely many exceptions, there exists at least one prime p such that the period of the k-Fibonacci sequence modulo p is n. Finally, we give necessary and sufficient conditions for a particular prime p to be a Wall-Sun-Sun prime.

1 Introduction

In this paper we aim to prove the following theorem

Theorem 1. *If $f(x) \in \mathbb{Z}[x]$ is irreducible, $x \nmid f(x)$ and $\Phi_n(x) \nmid f(x)$ for all $n \in \mathbb{N}$, then for all but finitely many values $k \in \mathbb{N}$ there exists at least one prime p such that $f(x)$ has a root of multiplicative order k in a finite field of characteristic p.*

Further, for specific choices of the polynomial $f(x)$ we shall show how to compute the set of k for which no root exists. In pursuing this problem we shall see that it is very closely related to the periods of linear recurrence relations modulo primes. As a result, we shall show that for any $k \in \mathbb{Z}$, we have

Theorem 2. *For a k-Fibonacci sequence f_n, given by $f_0 = 0, f_1 = 1$ and $f_{n+1} = kf_n + f_{n-1}$, there are only finitely many even numbers k such that there is no prime p such that the period of f_n modulo p is n.*

Further, we shall compute this set for specific k-Fibonacci sequences, including the Fibonacci sequence itself.

The proof of the first results follows the method used first in [1] and later simplified in [5]. These works concern proving that all but finitely many Fibonacci numbers have a *primitive prime divisor*. That is, a prime divisor which is not a prime divisor of any smaller Fibonacci number.

To address our questions, we introduce the sequences A_n and a_n, known as the *Pierce numbers*, first studied in [4]. These sequences play analagous roles to the Fibonacci sequence f_n and its divisor sequence q_n as in Carmichael's work. Once these are introduced, we show the following:

(i) the existence of a root of $f(x)$ of multiplicative order k is equivalent to the existence of a primitive prime divisor of a_k;

(ii) there is a polynomial function in n bounding the size of each a_n with no primitive prime divisor;

(iii) the sequence a_n increases exponentially.

This paper will logically be divided into sections showing these three properties, and into a final section applying our work to finding prime moduli for given periods of the Fibonacci sequence and Fibonacci like sequences.

Throughout this paper, we make use of the following notation:

- for a polynomial $f(x)$ we denote by $\rho(f)$ the multiset of roots of f including repetitions;
- by $\Phi_n(x)$ we denote the n^{th} cyclotomic polynomial;
- if $f(x) \in \mathbb{Z}[x]$ then by Δ_f we shall denote the discriminant of f;

Further, we shall abuse notation by ignoring signs of expressions when using equalities, given that we are only concerned with divisibility properties and signs are not relevant to our purposes.

2 Conditions for Existence, Pierce Numbers

We begin by considering the problem of, for a fixed polynomial $f(x) \in \mathbb{Z}[x]$, and a fixed number $n \in \mathbb{N}$, trying to find a prime p such that there is a root α of $f(x)$ in some extension field of $\mathbb{Z}_p$ with multiplicative order n. We begin with the following lemma.

Lemma 1. *For arbitrary polynomials $f, g \in \mathbb{Z}[x]$ and prime number p, f and g share a root in some extension field of $\mathbb{Z}_p$ if, and only if, $p \mid \text{Res}(f, g)$ where $\text{Res}(f, g)$ is the resultant of f and g.*

Proof. Considering the resultant of f and g over the integers, we have that $\text{Res}(f, g)$ satisfies the following formulae

$$\text{Res}(f, g) = \prod_{\substack{\alpha \in \rho(f) \\ \beta \in \rho(g)}} (\alpha - \beta) = \prod_{\alpha \in \rho(f)} g(\alpha) = \prod_{\beta \in \rho(g)} f(\beta).$$

Considering the expression $\prod(\alpha - \beta)$, we see that $\text{Res}(f, g) = 0$ if, and only if, f and g share a root in common. Equally, considering this expression in a suitable extension field $\mathbb{F}$ of $\mathbb{Z}_p$ shows that $\prod(\alpha - \beta) = 0$ in $\mathbb{F}$ if, and only if, f and g share a common root. Finally, the theory of symmetric functions applied to the expressions $\prod g(\alpha)$ or $\prod f(\beta)$ shows that $\text{Res}(f, g) \in \mathbb{Z}$, and hence $\text{Res}(f, g) = 0$ in $\mathbb{F}$ if, and only if, $p \mid \text{Res}(f, g)$. □

Remark. *Originally the author first encountered expressions of the form $\prod_{\alpha \in \rho(f)} g(\alpha)$ in the context of algebraic norms. For irreducible $f(x) \in \mathbb{Z}[x]$ and $\alpha \in \rho(f)$, the algebraic norm of the element $g(\alpha)$ in the field $K = \mathbb{Q}(\alpha)$ is given by $N = \prod_{\alpha \in \rho(f)} g(\alpha)$. It is clear that if some $p \mid N$ then the ideal $J = \langle p \rangle$ is maximal in the ring of integers $\mathcal{O}_K$ of K, and the quotient ring $\mathcal{O}_k / J$ is a finite field of order p^k in which f and g share a root. Whilst it was clear this condition was sufficient, it was not evident it was necessary. However, from the above work it follows easily that this is a necessary condition.*

From this lemma, we gain the following useful corollary which we will make extensive use of.

Corollary 1. *For a polynomial $f(x) \in \mathbb{Z}[x]$ and prime p, the polynomial $f(x)$ contains a root of multiplicative order k where $p \nmid k$ in a finite field of characteristic p if, and only if, $p \mid \text{Res}(f, \Phi_k)$, where Φ_n is the n^{th} cyclotomic polynomial.*

Proof. We note only that an element α of a finite field $\mathbb{F}$ of characteristic p has multiplicative order k, where $p \nmid k$, if and only if α is a root of Φ_k. This follows from the construction of the cyclotomic polynomials. The rest immediately follows. □

Hence, in the problem of locating roots of given multiplicative order in arbitrary finite fields for a given polynomial $f(x) \in \mathbb{Z}[x]$, we now turn our attention to the series a_n and A_n defined by

$$a_n = \text{Res}(f, \Phi_n) = \prod_{\alpha \in \rho(f)} \Phi_n(\alpha) = \prod_{\xi \in \Xi_n} f(\xi) \quad \text{and} \quad A_n = \prod_{d \mid n} a_d = \text{Res}(f, x^n - 1) = \prod_{\alpha \in \rho(f)} (\alpha^n - 1).$$

These series were first studied by Pierce in [4] and subsequently by Lehmer in [3]. The study by Pierce follows closely the work [1] of Carhmichael in which the analogous series $(\alpha^n - \beta^n)/(\alpha - \beta)$ and $\alpha^n + \beta^n$ are studied.

We now make the definition that a prime divisor p of a_n is a *primitive* prime divisor of a_n if $p \mid a_n$ but $p \nmid n$. We note that there is a finite field $\mathbb{F}$ in which the polynomial $f(x)$ contains a root of order k if, and only if, a_k has a primitive prime divisor.

Remark. *It may appear that the definitions of primitive prime divisor here and the usual definition of primitive prime divisor in the Fibonacci sequence are incompatible. However, if a prime $p \neq 5$ is a primitive prime divisor of the Fibonacci number f_n, then $p \nmid n$. The prime 5 is exceptional as it divides the discriminant of the characteristic polynomial of the Fibonacci sequence, and apart from this exception our definitions of primitive prime divisor are compatible.*

We now note some basic properties of the sequences a_n and A_n.

Lemma 2. *If $p \mid a_{pn}$ then $p \mid a_n$.*

Proof. If $p \nmid n$, then we have the identity $\Phi_{pn}(x)\Phi_n(x) = \Phi_n(x^p)$. Therefore, in $\mathrm{GF}(p^k)$ we have

$$a_n = \prod_{\alpha \in \rho(f)} \Phi_n(\alpha) = \prod_{\alpha \in \rho(f)} \Phi_n(\alpha^p) = \prod_{\alpha \in \rho(f)} \Phi_{pn}(\alpha)\Phi_n(\alpha) = a_{pn}a_n.$$

Hence, if $p \mid a_{pn}$ then $a_n = a_{pn}a_n = 0$ in $\mathrm{GF}(p^k)$, and so $p \mid a_n$.

If $p \mid n$, then we have the identity $\Phi_{pn}(x) = \Phi_n(x^p)$. Therefore, in $\mathrm{GF}(p^k)$ we have

$$a_n = \prod_{\alpha \in \rho(f)} \Phi_n(\alpha) = \prod_{\alpha \in \rho(f)} \Phi_n(\alpha^p) = \prod_{\alpha \in \rho(f)} \Phi_{pn}(\alpha) = a_{pn}.$$

Hence, if $p \mid a_{pn}$ then $a_n = a_{pn} = 0$ in $\mathrm{GF}(p^k)$, and so $p \mid a_n$. □

Lemma 3. *If C is the companion matrix of the polynomial $f(x)$, then $A_n = |C^n - I|$.*

Proof. The companion matrix of $f(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0$, C, is similar to the diagonal matrix D, where C and D are given by

$$C = \begin{pmatrix} 0 & 0 & 0 & \dots & a_0 \\ 1 & 0 & 0 & \dots & a_1 \\ 0 & 1 & 0 & \dots & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_{n-1} \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} \alpha_1 & 0 & 0 & \dots & 0 \\ 0 & \alpha_2 & 0 & \dots & 0 \\ 0 & 0 & \alpha_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \alpha_n \end{pmatrix},$$

where $\alpha_1 \dots \alpha_n$ are the roots of $f(x)$, and guaranteed to be distinct as f is irreducible in $\mathbb{Z}$. Hence, there exists some matrix Q such that $C = Q^{-1}DQ$, and so

$$|C^n - I| = |(Q^{-1}DQ)^n - I| = |Q^{-1}(D^n - I)Q| = |Q^{-1}||D^n - I||Q| = |D^n - I|.$$

Finally, $D^n - I$ is given by the expression

$$\begin{pmatrix} \alpha_1^n - 1 & 0 & 0 & \dots & 0 \\ 0 & \alpha_2^n - 1 & 0 & \dots & 0 \\ 0 & 0 & \alpha_3^n - 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \alpha_n^n - 1 \end{pmatrix},$$

and so satisfies $|D^n - I| = \prod \alpha^n - 1 = A_n$. □

Corollary 2. *With the notation above, $a_n = |\Phi_n(C)|$.*

Remark. *Both of the above points are special instances of a more general observation that, if $f, g \in \mathbb{Z}[x]$ and C, D are companion matrices of f and g respectively, then* $\mathrm{Res}(f, g) = |f(D)| = |g(C)|$.

3 Bounding From Above, Carmichael's Lemma

In this section we show that any a_n containing no primitive divisors is bounded by a polynomial function in n. This follows the logic of Carmichael's proof that all Fibonacci numbers contain a primitive prime divisor with some calculable exceptional cases. In this proof, Carmichael has a lemma that if p^k is the highest power of k dividing f_n, then p^{k+1} is the highest power of k dividing f_{pn}. This lemma is of fundamental importance as it tells us that the highest power of p dividing q_{pn} is p, for all n, thus giving a bound on the size of any q_n containing no primitive divisors. Despite the apparent fundamental importance of this lemma, and the fact it carries over to our case with some modification, the methods of proof used are somewhat ad-hoc and do not reflect the fundamental nature of this insight.

Unfortunately, we are unable to give a constructive proof of what the bounding function is in the general case. However, we will give a constructive proof in the case of primes not dividing the discriminant of f, and further show that this requirement is required in general. Subsequently, we will give a non-constructive proof that such a function exists in general.

Hence, in this section, taking $f(x) \in \mathbb{Z}[x]$ to be an irreducible polynomial, δ to be the degree of f, and Δ_f to be the discriminant of f, we aim to show the following result.

Proposition 1 (Carmichael's Lemma)**.** *If $p \nmid \Delta_f, p \mid a_n$ and $p \mid n$, then $p^{\delta+1} \nmid a_n$.*

In other words, if $p \nmid \Delta_f$ and p is a non-primitive prime divisor of a_n then p^δ is the largest power of p that can divide a_n, and so if a_n contains no primitive prime divisors $a_n \leq n^\delta$.

For the sake of clarity, we will first prove this result in a simple special case and then show that we can generalise this method of proof to cover all cases. Hence, we begin by considering some irreducible $f(x) \in \mathbb{Z}[x]$ and $p \nmid \Delta_f$ such that f splits in $\mathbb{Z}/p\mathbb{Z}$. First, we reproduce some standard results.

Lemma 4 (Hensel's Lemma)**.** *If α is a root of f in $\mathbb{Z}/p^k\mathbb{Z}$, then there is a unique root $\hat{\alpha} \in \mathbb{Z}/p^{k+1}\mathbb{Z}$ such that $\alpha \equiv \hat{\alpha} \pmod{p^k}$.*

Proof. By considering the Taylor expansion of $f(x)$ in $\mathbb{Z}$ we have the formal equality

$$f(x+nh) = f(x) + nhf'(x) + (nh)^2 f''(x) + \dots$$

Hence, if $n = p^k$ and we consider this expression mod p^{k+1}, we have the formal equality

$$f(x+p^k h) \equiv f(x) + p^k h f'(x) \pmod{p^{k+1}}.$$

Now, suppose α is a root of $f(x)$ modulo p^k. We therefore have $f(\alpha) = ap^k \pmod{p^{k+1}}$ for some a. As $p \nmid \Delta_f$, $f(x)$ does not have repeated roots modulo p, and so $f'(\alpha) \neq 0 \pmod{p}$. Hence, $f(\alpha + p^k h) \equiv 0 \pmod{p^{k+1}}$ if, and only if, h is the solution of $a \equiv f'(\alpha)h \pmod{p}$. This shows that there is a unique root $\hat{\alpha}$ of $f(x) \bmod p^{k+1}$ such that $\hat{\alpha} \equiv \alpha \pmod{p^k}$. □

Due to Hensel's Lemma, we may identify each root α of f modulo p with all of its lifts. First, we will consider the sequence of roots $\alpha_1, \alpha_2, \dots$ such that each α_i is a root of f in $\mathbb{Z}/p^i\mathbb{Z}$. Trivially, as $\alpha_1 \in \mathbb{Z}/p\mathbb{Z}$ we have that $\operatorname{ord}(\alpha_1) \mid p-1$. Letting $b = \operatorname{ord}(\alpha_1)$ we now prove the following lemma.

Lemma 5. *There exists some number k such that $\operatorname{ord}(\alpha_1) = \dots = \operatorname{ord}(\alpha_k) = b$ and $\operatorname{ord}(\alpha_{k+i}) = p^i b$.*

Proof. In the following we note by $\delta, \delta', \dots$ arbitrary constants, and by $\varepsilon, \varepsilon', \dots$ arbitrary constants with the property $\varepsilon \not\equiv 0 \pmod{p}$. First, we show that if $\operatorname{ord}(\alpha_i) = b$ in $\mathbb{Z}/p^i\mathbb{Z}$, then $\operatorname{ord}(\alpha_{i+1})$ is b or pb in $\mathbb{Z}/p^{i+1}\mathbb{Z}$. We have

$$\alpha_{i+1}^{pb} \equiv ((\alpha_i + p^i\delta)^b)^p \equiv (\alpha_i^b + p^i b\delta')^p \equiv ((1 + p^i\delta'') + p^i b\delta'))^p \equiv (1 + p^i\delta''')^p \equiv 1 \pmod{p^{i+1}}.$$

Hence we see that $\operatorname{ord}(\alpha_{i+1}) \mid pb$, and as $\alpha_{i+1} \equiv \alpha_i \pmod{p^i}$ we know that $b \mid \operatorname{ord}(\alpha_{i+1})$, and so $\operatorname{ord}(\alpha_{i+1})$ is either b or pb.

Now we suppose that there is no k such that $\operatorname{ord}(\alpha_{k+1}) = pb$. If this is the case, then for all i we have

$$A_b \equiv \prod_{\alpha \in \rho(f)} (\alpha^b - 1) \equiv (\alpha_i^b - 1) \prod_{\beta \in \rho(f) \setminus \{\alpha_i\}} (\beta^b - 1) \equiv 0 \pmod{p^i}.$$

As $A_b \in \mathbb{Z}$, this is only possible if $A_b = 0$. However, the restriction that no $\Phi_n(x) \mid f(x)$ in $\mathbb{Z}[x]$ ensures that f has no roots α satisfying $\alpha^n = 1$ in $\mathbb{Z}$, and so this cannot happen. Hence, we know there exists a minimal k such that $\operatorname{ord}(\alpha_1) = \cdots = \operatorname{ord}(\alpha_k) = b$ and $\operatorname{ord}(\alpha_{k+1}) = pb$.

Now we show by induction that $\operatorname{ord}(\alpha_{k+i}) = p^i b$, with our base case $i = 1$ as above. Given the hypothesis for $\operatorname{ord}(\alpha_{k+i})$, we have

$$\begin{aligned}\alpha_{k+i+1}^{p^i b} &\equiv ((\alpha_{k+1} + p^{k+1}\delta)^b)^{p^i} \equiv (\alpha_{k+1}^b + p^{k+1}\delta')^{p^i} \equiv ((1 + p^k\varepsilon) + p^{k+1}\delta')^{p^i} \\ &\equiv (1 + p^k\varepsilon')^{p^i} \equiv 1 + p^{k+i}\varepsilon' \not\equiv 1 \pmod{p^{k+i+1}}.\end{aligned}$$

Hence $\operatorname{ord}(\alpha_{k+i+1}) \neq p^i b$, but as $\alpha_{k+i+1} \equiv \alpha_{k+i} \pmod{p^i}$ we have $p^i b \mid \operatorname{ord}(\alpha_{k+i+1})$. Now, considering $\alpha_{k+i+1}^{p^{i+1}b}$ we have

$$\alpha_{k+i+1}^{p^{i+1}b} \equiv ((\alpha_k + p^k\delta)^b)^{p^{i+1}} \equiv (\alpha_k^b + p^k\delta')^{p^{i+1}} \equiv ((1+p^k\delta'') + p^k\delta')^{p^{i+1}} \equiv (1+p^k\delta''')^{p^{i+1}} \equiv 1 \pmod{p^{k+i+1}}.$$

Hence $\operatorname{ord}(\alpha_{k+i+1}) \mid p^{i+1}b$. Finally, as $p^i b \mid \operatorname{ord}(\alpha_{k+i+1}) \mid p^{i+1}b$ and $\operatorname{ord}(\alpha_{k+i+1}) \neq p^i b$ we must have $\operatorname{ord}(\alpha_{k+i+1}) = p^{i+1}b$. □

For a given sequence of roots we shall refer to the number b as the *base order* and the number k as the *base order multiplicity*. For each root α of f we now introduce a pair of sequences in related to A_n and a_n. Denote by $\Lambda(\alpha)_n$ the sequences given by

$$\Lambda(\alpha)_n = \begin{cases} 0, & \text{if } \alpha^n \not\equiv 1 \pmod{p}, \\ i, & \text{for the largest } i \text{ such that } \alpha^n \equiv 1 \pmod{p^i}, \end{cases} \quad \text{and} \quad \lambda(\alpha)_n = \begin{cases} k, & \text{if } n = b, \\ 1, & \text{if } n = p^i b \text{ for } i \geq 1, \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 6. $\Lambda(\alpha)_n = \sum_{d|n} \lambda(\alpha)_d$.

Proof. We consider two cases. For $b \nmid n$, we have that $\Lambda(\alpha)_n = 0$, and for each $d \mid n$ we have $\lambda(\alpha)_d = 0$. Hence in this case $\Lambda(\alpha)_n = \sum_{d|n} \lambda(\alpha)_d$.

If $b \mid n$, then n is of the form $p^i bm$ for some m with $p \nmid m$. In this case, $\operatorname{ord}(\alpha_{k+i}) = p^i b \mid n$, but $\operatorname{ord}(\alpha_{k+i+1}) = p^{i+1}b \nmid n$. Hence, p^{k+i} is the highest power of p such that $\alpha^n \equiv 1 \pmod{p^{k+i}}$, and so $\Lambda(\alpha)_n = k + i$. For our other expression, we have

$$\sum_{d|n} \lambda(\alpha)_d = \sum_{d|p^i b} \lambda(\alpha)_d = \lambda(\alpha)_b + \sum_{j=1}^{i} \lambda(\alpha)_{p^j b} = k + i.$$

Hence, in all cases we have $\Lambda(\alpha)_n = \sum_{d|n} \lambda(\alpha)_d$. □

We now make the definitions $\Lambda_n = \sum_{\alpha \in \rho(f)} \Lambda(\alpha)_n$ and $\lambda_n = \sum_{\alpha \in \rho(f)} \lambda(\alpha)_n$. These sequences are of fundamental interest because of the following property.

Lemma 7. *The highest power of p dividing A_n is Λ_n.*

Proof. Considering the each root α of f separately, we have that $\alpha^n - 1 \equiv p^i\varepsilon \pmod{p^j}$ where $i = \Lambda(\alpha)_n, \varepsilon \not\equiv 0 \pmod{p}$ and j can be taken to be arbitrarily large. Hence, denoting by $\alpha, \beta, \ldots, \omega$ the roots of f; by $i_\alpha, i_\beta, \ldots, i_\omega$ the values $\Lambda(\alpha)_n, \Lambda(\beta)_n, \ldots, \Lambda(\omega)_n$ we have

$$A_n \equiv (\alpha^n - 1)(\beta^n - 1)\ldots(\omega^n - 1) \equiv p^{i_\alpha}\varepsilon_\alpha p^{i_\beta}\varepsilon_\beta \ldots p^{i_\omega}\varepsilon_\omega \equiv p^{\Lambda_n}\varepsilon \pmod{p^j},$$

where each ε_ι and ε satisfy $\varepsilon \not\equiv 0 \pmod{p}$, and j can be taken to be arbitrarily large. □

Corollary 3. *The highest power of p dividing a_n is λ_n.*

Proof. The relations $A_n = \prod_{d|n} a_d$ and $\Lambda_n = \sum_{d|n} \lambda_d$ uniquely define the sequences a_n and λ_n. The sequence μ_n of highest powers of p dividing a_n is uniquely defined and satisfies $\sum_{d|n} \mu_d = \Lambda_n$ due to the previous lemma, and hence $\lambda_n = \mu_n$. □

Corollary 4. *If p is a not a primitive prime divisor of a_n, then the highest power of p that can divide a_n is p^δ.*

Proof. If p is not a primitive prime divisor of a_n, then $p \mid n$, and therefore $\lambda(\alpha)_n \leq 1$ for all $\alpha \in \rho(f)$. Hence, the highest power of p dividing a_n is given by $\lambda_n = \sum \lambda(\alpha)_n \leq \delta$, where the sum is over all roots of f and δ is the degree of f. □

Altogether this gives us a version of Carmichael's lemma for the case where f splits into linear factors over $\mathbb{Z}/p\mathbb{Z}$. Now we may generalise this result to cover all cases where $p \nmid \Delta_f$, the discriminant of f. To do so, we introduce the notion of a *Galois ring*. First, we will need some technical results.

Let $f, g \in \mathbb{Z}[x]$ such that f and g are irreducible in $\mathbb{Z}/p\mathbb{Z}$ and $\deg(g) = e$ and $\deg(f) \mid e$. We define the ring R_k by $R_k = (\mathbb{Z}/p^k\mathbb{Z})[x]/\langle g(x)\rangle$. We note that $R_1 \cong \mathrm{GF}(p^e)$, and so f splits in R_1. Let α be an arbitrary root of f in R_1.

Lemma 8 (Hensel's Lemma)**.** *There is a unique sequence of roots $\alpha_1 = \alpha, \alpha_2, \alpha_3, \ldots$ in $R_1, R_2, \ldots$ such that each α_i is a root of f and $\alpha_{i+1} \equiv \alpha_i \pmod{i}$.*

Proof. Suppose $\alpha_1, \ldots, \alpha_k$ are the first k elements of such a unique sequence. Again using a Taylor expansion of f we have

$$f(x + p^k h) \equiv f(x) + p^k h f'(x) \quad \text{in } R_{k+1}.$$

As α_k is a root of f in R_k, we have

$$f(\alpha_k + p^k h) = f(\alpha_k) + p^k h f'(\alpha_k) = p^k(\delta + h f'(\alpha_k)) \quad \text{in } R_{k+1}.$$

Considering the expression $\delta + h f'(\alpha_k) \pmod{p}$, i.e. in $R_1 \cong \mathrm{GF}(p^e)$, we have that $f'(\alpha_k) \neq 0$ in $\mathrm{GF}(p^e)$, as f is irreducible, hence there is a unique choice of h in $\mathrm{GF}(p^e)$ such that $\delta + h f'(\alpha_k) = 0$ in $\mathrm{GF}(p^e)$. Any two such choices of h in R_{k+1}, say h and h', satisfy $\alpha_k + p^k h = \alpha_k + p^k h'$ in R_{k+1}. As all roots of f in R_{k+1} with $\beta \equiv \alpha_k \pmod{p^k}$ can be written as $\alpha_k + p^k h$ for some $h \in R_{k+1}$, this shows that there is a unique root α_{k+1} of f in R_{k+1} such that $\alpha_{k+1} \equiv \alpha_k$ in R_k. □

We now state and prove an important technical result. Let $h(x) \in \mathbb{Z}[x]$ such that h is irreducible in $\mathbb{Z}/p\mathbb{Z}$ and $\deg(h) = \deg(g)$. Define S_k by $S_k = (\mathbb{Z}/p^k\mathbb{Z})[x]/\langle h(x)\rangle$.

Lemma 9. *For all $k \geq 1$, $R_k \cong S_k$.*

Proof. First fix an arbitrary root α of $g(x)$ in R_1 and let $\alpha_1, \alpha_2, \ldots$ be its sequence of lifts. We may think of R_k as an algebraic extension of $\mathbb{Z}/p^k\mathbb{Z}$ by adjoining an element α_k which is a root of $g(x)$. Basic Galois theory tells us such an extension is unique to isomorphism. Trivially we have $R_1 \cong \mathrm{GF}(p^e) \cong S_1$. Hence, let β be the image of α in a fixed isomorphism from R_1 to S_1. We have that β is a root of g in S_1, and hence from the previous lemma we may let $\beta_1, \beta_2, \ldots$ be its sequence of lifts. Finally, as S_k contains a root β_k of g, we may consider S_k as an algebraic extension of $\mathbb{Z}/p^k\mathbb{Z}$ by adjoining a root of g, and therefore isomorphic to R_k. □

We are now in the position to define a *Galois ring*. For $k, e \geq 1$, and a prime p, let $g(x) \in \mathbb{Z}[x]$ be a polynomial such that g is irreducible in $\mathbb{Z}/p\mathbb{Z}$ and $\deg(g) = e$. The Galois ring $\mathrm{GR}(p, k, e)$ is the quotient ring $(\mathbb{Z}/p^k\mathbb{Z})[x]/\langle g(x)\rangle$. We note that the previous lemma shows that $\mathrm{GR}(p, k, e)$ is unique to isomorphism, and thus well defined. We shall call e the *extension degree* and k the *characteristic power*. We note the special cases $\mathrm{GR}(p, 1, e) \cong \mathrm{GF}(p^e)$ and $\mathrm{GR}(p, k, 1) \cong \mathbb{Z}/p^k\mathbb{Z}$.

We now note that our previous argument concerning the powers of a prime p dividing the numbers A_n and a_n was based on lifts of roots from the rings $\mathbb{Z}/p^k\mathbb{Z}$ to $\mathbb{Z}/p^{k+1}\mathbb{Z}$. With our new notation, this becomes lifts of roots from $\mathrm{GR}(p, k, 1)$ to $\mathrm{GR}(p, k+1, 1)$. We can now recreate the previous argument but considering lifts from $\mathrm{GR}(p, k, e)$ to $\mathrm{GR}(p, k+1, e)$, in the case where the fixed polynomial f only splits in some extension $\mathrm{GF}(p^e)$ of $\mathrm{GF}(p)$. As the argument is entirely analagous to that previously given, we omit it here. This completes the proof of Proposition 1.

Unfortunately, this leaves open the case of when $p \mid \Delta_f$. We first provide an example to show that if $p \mid \Delta_f$ it is possible that $p^{\delta+1} \mid a_{pn}$ for some n.

Proposition 2. *For $f(x) = x^2 - x + 10$, we have $3^4 \mid a_6$.*

Proof. The discriminant of f is $-39 = -1 \times 3 \times 13$, hence $3 \mid \Delta_f$. We can use Lemma 3 to compute a_6 as $\det(\Phi_6(C)) = 3^4$. □

Remark. *This example was found as* $f(x) = x^2 - x + 10 = \Phi_6(x) + 9$. *Hence* f *is congruent to* Φ_6 *in* $\mathbb{Z}/3^2\mathbb{Z}$, *and so in the expression* $a_6 = \prod_{\alpha \in \rho(f)} \Phi_6(\alpha)$ *it is clear that, modulo* 3^2, *roots of* f *are also roots of* Φ_6, *and so each term* $\Phi_6(\alpha) \equiv 0 \pmod{3^2}$. *Though the lifting argument which we used is not applicable to the case* $p \mid \Delta_f$, *if it were each root* α *of* f *would contribute a factor of* 3^2 *to* a_6, *and so the fact* $3^4 \mid a_6$ *is not surprising (note that we used explicit computation to show* $3^4 \mid a_6$ *in this example). We could also choose an example like* $f(x) = \Phi_6(x) + 81$, *and it would be immediately clear* $a_6 \equiv 0 \pmod{3^4}$, *again showing that the assumption* $p \nmid \Delta_f$ *is necessary in the preceding argument.*

In that case, we can only offer a non-constructive bound on the power of p dividing a_n when p is not a primitive prime divisor of a_n.

Proposition 3. *For each prime* p *with* $p \mid \Delta_f$ *there is some number* k *such that* $p^k \nmid a_{p^r n}$ *for all* $r \geq 1$.

Proof. TODO: e-mail Will.
We consider the expression $\mathrm{Res}(f, \Phi_n)$ where $n = p^r b$. We have

$$\mathrm{Res}(f, \Phi_n) = \prod_{\xi \in \Xi_n} f(\xi) = \prod_{\substack{\xi_a \in \Xi_{p^r} \\ \xi_b \in \Xi_b}} f(\xi_a \xi_b)$$

and so

$$\mathrm{v}_p(\mathrm{Res}(f, \Phi_n)) = \sum \mathrm{v}_p(f(\xi_a \xi_b)),$$

where v_p is the p-adic valuation function. □

As we concern ourselves with computing sets of impossible orders explicitly we give an algorithm for computing a polynomial bound on a_n with no primitive prime divisors in the special case where the determinant of f and the constant coefficient of f are coprime. In the following, let C be the companion matrix of f and p be a prime dividing Δ_f.

Lemma 10. *If* $p \parallel n$ *and* $p \mid a_n$, *then for each* k *there exists a finite computable number* r *such that* $a_{p^i n} \not\equiv 0 \pmod{p^k}$ *for any* i *if, and only if,* $a_{p^i n} \not\equiv 0 \pmod{p^k}$ *for all* $0 \leq i \leq r$.

Proof. Letting $p \parallel n$, from the identity of cyclotomic polynomials $\Phi_{p^r n}(x) = \Phi_n(x^{p^r})$ and the fact $a_m = \det(\Phi_m(C))$, we have $a_{p^r n} = \det(\Phi_n(A^{p^r}))$. By assumption p is not a divisor of the constant coefficient of f, which is given by $\det(C)$, hence C is not a zero-divisor in any matrix ring over $\mathbb{Z}/p^k\mathbb{Z}$, and has multiplicative order bp^c for some b with $p \nmid b$. In we have $A^n \equiv A^m \pmod{p^k}$ where bp^c is the multiplicative order of A over $\mathbb{Z}/p^k\mathbb{Z}$ and $m \equiv n \pmod{bp^c}$. Hence, let k be a high enough power of p such that $p \nmid a_{p^r n}$ for any r, which we know to exist by the previous proposition, and let bp^c be the multiplicative order of C over $\mathbb{Z}/p^k\mathbb{Z}$. By the Chinese remainder theorem, the sequence $p^r \pmod{bp^c}$ is determined uniquely by the sequences $p^r \pmod{b}$ and $p^r \pmod{p^c}$. For $r \geq c$, the sequence $p^r \equiv 0 \pmod{p^c}$, and the sequence $p^r \pmod{b}$ repeats with period the order of $p \pmod{b}$. Letting m be the order of $p \pmod{b}$, we see that for $r \geq c$, if $0 \leq r' < m$ and $r \equiv c + r' \pmod{m}$, then $a_{p^r n} \equiv a_{p^{c+r'} n} \pmod{p^k}$. Therefore, if $a_{p^r n} \not\equiv 0 \pmod{p^k}$ for all $r \leq m + c$, then $a_{p^r n} \not\equiv 0 \pmod{p^k}$ for all r. □

To clarify the situation, we give an example.

Proposition 4. *For* $f(x) = x^2 - x - 1$, *if* $p \mid n$ *then* $a_n \not\equiv 0 \pmod{p^3}$.

Proof. We have $\Delta_f = 5$, hence for all primes other than 5 we have the result immediately from Proposition 1. For $p = 5$, we follow the previous lemma. The companion matrix of f, C, is given by

$$C = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

We consider C modulo 5^3, where C has order $500 = 4 \times 5^3$. For n such that $p \nmid n$, $a_n \equiv 0 \pmod{5}$ if and only if $f(x)$ has a root of order n in an extension of $\mathbb{Z}/5\mathbb{Z}$. As $f(x) \equiv (x-3)^2 \pmod{5}$ we have that $a_n \equiv 0$

(mod 5) for $p \nmid n$ if and only if $n = 4$. We have that the multiplicative order of 5 modulo 4 is 1. Therefore, for $r \geq 3$ we have

$$a_{20\times 5^r} \equiv \det(\Phi_{20\times 5^r}(C)) \equiv \det(\Phi_{20}(C^{5^r})) \equiv \det(\Phi_{20}(C^{5^3})) \equiv a_{2500} \pmod{125}.$$

Hence we calculate $a_{20\times 5^r} \pmod{125}$ for $0 \leq r \leq 3$. We have $a_{20} \equiv 25, a_{20\times 5} \equiv 25, a_{20\times 5^2} \equiv 25$, and $a_{20\times 5^3} \equiv 25 \pmod{125}$. The result immediately follows. □

Of course, this has the immediate corollary that if a_n contains no primitive prime divisor then $a_n \leq n^2$. Although this test requires that the discriminant and constant coefficient are coprime, and has the appearance of possibly requiring large calculations, in practice it converges quickly and is useful in most cases to gain a constructive upper bound.

4 Boudning From Below, Baker's Theorem

In this section we show that the sequence a_n increases exponentially. In the case where $f(x)$ has no roots of absolute value 1 this is achieved by simple analysis, hence we will only focus on the case where f has at least one root of absolute value 1. The argument given is not the author's and was found in an exchange on Mathoverflow [2]. First we quote a key corollary Baker's theorem.

Lemma 11. *If α is an algebraic number other than a root of unity, then there exists a constant k depending only on α such that $|\alpha^n - 1| > n^{-k}$.*

We now prove the main result on the growth of a_n.

Proposition 5. *There are constants C and N such that $|a_n| > e^{C\sqrt{n}}$ for all $n > N$.*

Proof. We begin by finding upper and lower bounds on the terms $\log(|A_n|)$. For each root α of f we give upper and lower bounds of $|\alpha^n - 1|$ for the cases $|\alpha| < 1, |\alpha| = 1$ and $|\alpha| > 1$.

	$\lvert\alpha\rvert < 1$	$\lvert\alpha\rvert = 1$	$\lvert\alpha\rvert > 1$
Upper bound	2	2	$\lvert\alpha^n\rvert + 1$
Lower bound	$1 - \lvert\alpha\rvert$	n^{-k_α}	$\lvert\alpha^n\rvert - 1$

Hence, for an upper bound we have

$$\log(|A_n|) = \sum_{\alpha\in\rho(f)} \log(|\alpha^n - 1|) \leq \sum_{\substack{\alpha\in\rho(f)\\ |\alpha|\leq 1}} \log(2) + \sum_{\substack{\alpha\in\rho(f)\\ |\alpha|>1}} \log(|\alpha^n| + 1) \leq n\log(\mathrm{M}(\alpha)) + A,$$

and for a lower bound we have

$$\begin{aligned}\log(|A_n|) = \sum_{\alpha\in\rho(f)} \log(|\alpha^n - 1|) &\geq \sum_{\substack{\alpha\in\rho(f)\\ |\alpha|<1}} \log(1 - |\alpha|) + \sum_{\substack{\alpha\in\rho(f)\\ |\alpha|=1}} \log(n^{-k_\alpha}) + \sum_{\substack{\alpha\in\rho(f)\\ |\alpha|>1}} \log(|\alpha^n| - 1)\\ &\geq n\log(\mathrm{M}(\alpha)) - A - B\log(n),\end{aligned}$$

for some appropriate constants A and B. Using these bounds, we now find a lower bound for $\log(|a_n|)$. We have $\sum_{d|n} \log(|a_n|) = \log(|A_n|)$, and therefore $\log(|a_n|) = \sum_{d|n} \log(|A_d|)\mu(n/d)$. This gives

$$\begin{aligned}\log(|a_n|) = \sum_{d|n} \log(|A_d|)\mu(n/d) &= \sum_{\substack{d|n\\ \mu(n/d)=1}} \log(|A_d|)\mu(n/d) + \sum_{\substack{d|n\\ \mu(n/d)=-1}} \log(|A_d|)\mu(n/d)\\ &\geq \sum_{\substack{d|n\\ \mu(n/d)=1}} \big(d\log(\mathrm{M}(\alpha)) - A - B\log(d)\big)\mu(n/d) + \sum_{\substack{d|n\\ \mu(n/d)=-1}} (d\log(\mathrm{M}(\alpha)) + A)\mu(n/d)\\ &= \log(\mathrm{M}(\alpha))\sum_{d|n} d\mu(n/d) - \sum_{d|n} A - \sum_{\substack{d|n\\ \mu(n/d)=1}} B\log(d)\\ &\geq \varphi(n)\log(\mathrm{M}(\alpha)) - \mathrm{d}(n)(A + B\log(n)).\end{aligned}$$

Hence, as $\varphi(n)$ grows faster than $n^{1-\varepsilon}$ for all $\varepsilon > 0$, and $\mathrm{d}(n)$ grows slower than n^{ε} for all $\varepsilon > 0$, the result follows. □

Unlike the proof in the previous section, the constants in this bound are all effectively computable. Unfortunately, however, in practice computing values for real examples is still likely to be prohibitively difficult in most cases. The main difficulty arises due to the necessity to use Baker's Theorem to bound the contribution made to the series by roots of $f(x)$ with absolute value 1. Hence, we give a bound for the case where $f(x)$ has no roots of absolute value 1. To do this, we first give a lower bound of $\Phi_n(z)$ for $z \in \mathbb{C}$ such that $|z| < 1$.

Lemma 12. *For all $|z| < 1$ we have $|1 - z| \geq 1 - |z|$.*

Proof. Immediate as $|1 - z|$ is the distance between 1 and z in $\mathbb{C}$, and $1 - |z|$ is the distance between 1 and $|z|$ in $\mathbb{C}$. □

Lemma 13. *For all $|z| < 1$ we have $|1/(1 - z)| \geq 1 - |z|$.*

Proof. The term $|1/(1 - z)|$ is the inverse of the distance between 1 and z. We have $|1 - z| \leq 1 + |z|$, hence $|1/(1 - z)| \geq 1/(1 + |z|)$. As we have

$$\frac{1}{1+|z|} \geq 1 - |z| \quad \Leftrightarrow \quad \frac{1}{1+|z|} - (1 - |z|) \geq 0 \quad \Leftrightarrow \quad \frac{|z|^2}{1+|z|} \geq 0,$$

we have $|1/(1 - z)| \geq 1/(1 + |z|) \geq 1 - |z|$. □

We now modify slightly the inequality used in [5].

Proposition 6. *For all $z \in \mathbb{C}$ such that $|z| < 1$, we have $|\Phi_n(z)| \geq \exp(-(1 - |z|)^{3/2})$.*

Proof. We start with the identity

$$\Phi_n(z) = \prod_{d|n} (1 - z^d)^{\mu(n/d)}.$$

First, we note

$$|\Phi_n(z)| = \prod_{d|n} |1 - z^d|^{\mu(n/d)} \geq \prod_{d|n} 1 - |z|^d \geq \prod_{n=1}^{\infty} 1 - |z|^n,$$

by combining Lemma 12, Lemma 13 and the fact $1 \geq 1 - |z|^n > 0$. We now note the inequality,

$$\log(1 - x) \geq \frac{-x}{\sqrt{1 - x}},$$

for all $0 \leq x < 1$. Letting $\alpha = |z|$, we have

$$\log\left(\prod (1 - \alpha^n)\right) = \sum \log(1 - \alpha^n) \geq -\sum \frac{\alpha^n}{\sqrt{1 - \alpha^n}}.$$

From $0 \leq \alpha < 1$ we have $\sqrt{1 - \alpha^n} \geq \sqrt{1 - \alpha}$, $1/\sqrt{1 - \alpha^n} \leq 1/\sqrt{1 - \alpha}$ and therefore $-1/\sqrt{1 - \alpha^n} \geq -1/\sqrt{1 - \alpha}$, allowing us to take out the power of n in each factor $-1/\sqrt{1 - \alpha^n}$. Continuing, we have

$$-\sum \frac{\alpha^n}{\sqrt{1 - \alpha^n}} \geq -\frac{1}{\sqrt{1 - \alpha}} \sum \alpha^n = -(1 - \alpha)^{3/2}.$$

Altogether, this gives

$$\log |\Phi_n(z)| \geq -(1 - |z|)^{3/2} \quad \Leftrightarrow \quad |\Phi_n(z)| \geq \exp(-(1 - |z|)^{3/2}).$$ □

This bound allows us to give an easily computable lower bound on the series a_n for a polynomial f with no roots of absolute value 1.

Proposition 7. *If f is a polynomial with no roots of absolute value 1, then the series a_n satisfies $a_n \geq C\,\mathrm{M}(f)^{\sqrt{n/2}}$ where $\mathrm{M}(f)$ is the Mahler measure of f and C is an easily computable constant.*

Proof. Our series a_n satisfies

$$a_n = \prod_{\alpha \in \rho(f)} \Phi_n(\alpha).$$

By assumption, f has no roots of absolute value 1. Hence, we split the product as follows

$$\prod_{\alpha \in \rho(f)} \Phi_n(\alpha) = \prod_{\substack{\alpha \in \rho(f) \\ |\alpha|>1}} \Phi_n(\alpha) \prod_{\substack{\alpha \in \rho(f) \\ |\alpha|<1}} \Phi_n(\alpha) = \prod_{\substack{\alpha \in \rho(f) \\ |\alpha|>1}} \alpha^{\varphi(n)} \Phi_n(\alpha^{-1}) \prod_{\substack{\alpha \in \rho(f) \\ |\alpha|<1}} \Phi_n(\alpha).$$

We note that in this factorisation, we only evaluate Φ_n at points inside the unit disk, and hence may apply Proposition 6. We now define C as follows

$$C = \prod_{\substack{\alpha \in \rho(f) \\ |\alpha|>1}} \exp(-(1-|\alpha|^{-1})^{3/2}) \prod_{\substack{\alpha \in \rho(f) \\ |\alpha|<1}} \exp(-(1-|\alpha|)^{3/2}) \leq \left| \prod_{\substack{\alpha \in \rho(f) \\ |\alpha|>1}} \Phi_n(\alpha^{-1}) \prod_{\substack{\alpha \in \rho(f) \\ |\alpha|<1}} \Phi_n(\alpha) \right|.$$

Finally, we note

$$\prod_{\substack{\alpha \in \rho(f) \\ |\alpha|>1}} \alpha^{\varphi(n)} = \mathrm{M}(f)^{\varphi(n)} \geq \mathrm{M}(f)^{\sqrt{n/2}},$$

from $\varphi(n) \geq \sqrt{n/2}$. The result immediately follows. □

5 Main Result

6 Application to k-Fibonacci Sequences

We now apply our results to determining for which numbers n there do not exist prime moduli p such that the Fibonacci sequence has period n modulo p. We shall call any such n an *impossible period* of the Fibonacci sequence. As we shall later generalise our results to the k-Fibonacci sequence, we first define k-Fibonacci sequences, and will prove lemmas to be used in our generalised results on k-Fibonacci sequences.

The k-Fibonacci sequence f_n is defined by $f_0 = 0, f_1 = 1$ and $f_{n+1} = kf_n + f_{n-1}$. Equivalently, letting $f(x) = x^2 - kx - 1 = (x-\alpha)(x-\beta)$, we have $f_n = (\alpha^n - \beta^n)/(\alpha - \beta)$. The polynomial $f(x)$ is called the *characteristic polynomial* of the k-Fibonacci sequence. We note that as in our previous work we require $x \nmid f(x)$ and $\Phi_n(x) \nmid f(x)$ for all n. This means that $k \neq 0$, but any other integer value of k is allowed. We note that for the value $k = 1$ the k-Fibonacci sequence is the usual Fibonacci sequence. We begin with the following lemma.

Lemma 14. *The period of the k-Fibonacci sequence modulo p is equal to the order of the element x in $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$.*

Proof. By induction, using the relation $x^2 \equiv kx + 1 \pmod{p}$, we may show that $x^n \equiv f_n x + f_{n-1}$. Hence, $x^n \equiv 1 \pmod{p}$ if, and only if, $f_n \equiv 0 \pmod{p}$ and $f_{n-1} \equiv 1 \pmod{p}$. Therefore, n is the order of x if, and only if, n is the smallest n such that $f_n \equiv 0 \pmod{p}$ and $f_{n+1} \equiv 1 \pmod{p}$, which is equivalent to n is the period of the k-Fibonacci sequence modulo p. □

In the following let $\mathrm{GF}(p^e)$ be the splitting field of $f(x)$, and α, β be the roots of $f(x)$ in $\mathrm{GF}(p^e)$.

Lemma 15. *For $p \nmid \Delta_f$, the period of the k-Fibonacci sequence modulo p is equal to the least common multiple of $\mathrm{ord}(\alpha)$ and $\mathrm{ord}(\beta)$.*

Proof. In the case where $f(x)$ is irreducible in $\mathbb{Z}/p\mathbb{Z}$ we have that $\mathrm{GF}(p^e) = \mathrm{GF}(p^2) \cong (\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$, and the roots α and β are both isomorphic to x in $(\mathbb{Z}/p\mathbb{Z})/\langle f(x)\rangle$, so $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta) = \mathrm{ord}(x)$.

In the case where $f(x)$ is reducible in $\mathbb{Z}/p\mathbb{Z}$, the Chinese remainder theorem gives

$$(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle \cong (\mathbb{Z}/p\mathbb{Z})[x]/\langle x-\alpha\rangle \oplus (\mathbb{Z}/p\mathbb{Z})[x]/\langle x-\beta\rangle \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z},$$

with an isomorphism ϕ such that $\phi(x) = (x, x) = (\alpha, \beta)$. Clearly the order of the element (α, β) is the least common multiple of $\mathrm{ord}(\alpha)$ and $\mathrm{ord}(\beta)$. This gives the result. □

Corollary 5. *For $p \nmid \Delta_f$, the period of the k-Fibonacci sequence modulo p is equal to the least common multiple of the order of the roots of f modulo p.*

Remark. *We note that this is only a special case of a more general result for linear recurrences of more than two terms.*

Lemma 16. *For $p \nmid \Delta_f$ and $p \neq 2$, one of the following two cases occur:*

Case (i) there is a unique even number n such that p is a primitive divisor of a_n;

Case (ii) there is a unique odd number n such that p is a primitive divisor of a_n and a_{2n}.

Proof. We will consider α and β in the field $\mathrm{GF}(p^e)$ in which $f(x)$ splits. We note that we have $\beta = -\alpha^{-1}$, and so $\mathrm{ord}(\beta) \mid 2\,\mathrm{ord}(\alpha)$, and $\mathrm{ord}(\alpha) \mid 2\,\mathrm{ord}(\beta)$ by symmetry. Without loss of generality we may choose $\mathrm{ord}(\alpha) \geq \mathrm{ord}(\beta)$, combining with $\mathrm{ord}(\alpha) \mid 2\,\mathrm{ord}(\beta)$ gives $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$ or $\mathrm{ord}(\alpha) = 2\,\mathrm{ord}(\beta)$. If $n = \mathrm{ord}(\beta)$ is odd, then $\beta^n = (-\alpha^{-1})^n = -1$, and we must have $\mathrm{ord}(\beta) = 2\,\mathrm{ord}(\alpha)$. If $n = \mathrm{ord}(\beta)$ is even, then $\beta^n = (-\alpha^{-1})^n = 1$, and we must have $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$. Finally, we complete the proof noting that p is a primitive divisor of a_n if, and only if, one of α or β is order n. □

Corollary 6. *If $p \nmid \Delta_f, p \neq 2$ is a primitive prime divisor of a_n, and n is even, then the period of the k-Fibonacci sequence modulo p is n.*

We have now reduced the problem of showing that for an even number n there exists a prime such that the k-Fibonacci sequence has period n modulo p to the problem of showing that a_n has a primitive prime divisor. We now give a bound on the terms $|a_n|$ with no primitive prime divisor, independent of k.

Lemma 17. *The value $|a_n|$ is smallest in the 1-Fibonacci sequence for any $n > 2$.*

Proof. Noting that $\alpha + \beta = k$ and $\alpha\beta = -1$, we have

$$\begin{aligned}
|a_n| = |\Phi_n(\alpha)\Phi_n(\beta)| &= \prod_{\xi,\xi^{-1}\in\rho(\Phi_n)} \big((\alpha-\xi)(\beta-\xi^{-1})\big)\big((\alpha-\xi^{-1})(\beta-\xi)\big) \\
&= \prod_{\xi,\xi^{-1}\in\rho(\Phi_n)} (\alpha\beta - \alpha\xi^{-1} - \beta\xi + 1)(\alpha\beta - \alpha\xi - \beta\xi^{-1} + 1) \\
&= \prod_{\xi,\xi^{-1}\in\rho(\Phi_n)} (\alpha\xi^{-1} + \beta\xi)(\alpha\xi + \beta\xi^{-1}) = \prod_{\xi,\xi^{-1}\in\rho(\Phi_n)} (\alpha^2 + \beta^2 + \alpha\beta(\xi^2 + \xi^{-2})) \\
&= \prod_{\xi,\xi^{-1}\in\rho(\Phi_n)} (k^2 + 2 - (\xi^2 + \xi^{-2})).
\end{aligned}$$

As $|k| \geq 1$ and $2 - (\xi^2 + \xi^{-2}) \geq 0$ each term in the product is at least 1 and strictly increasing with k. Therefore $|a_n|$ takes a minimum value in the 1-Fibonacci sequence. □

7 Application to Specific Polynomials

In this section we demonstrate our results on specific example polynomials. We will choose the examples $f(x) = x^6 + 2x^5 + 2x^4 + 3x^3 + 2x^2 + 2x + 1$ and $g(x) = 3x^2 + 2x + 3$. The polynomial f demonstrates the difficulty of lower bounding the associated sequence a_n when the polynomial has roots of absolute value 1. Polynomial g shows that only very little adjustment needs to be made to deal with the case of a non-monic polynomial.

References

[1] R. D. Carmichael. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Annals of Mathematics*, pages 30–48, 1913.

[2] Will Sawin (https://mathoverflow.net/users/18060/will sawin). The resultant of an arbitrary polynomial and a cyclotomic polynomial. MathOverflow. URL:https://mathoverflow.net/q/98149 (version: 2017-04-13).

[3] D. H. Lehmer. Factorization of certain cyclotomic functions. *Annals of Mathematics*, pages 461–479, 1933.

[4] Tracy A. Pierce. The numerical factors of the arithmetic forms $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$. *Annals of Mathematics*, pages 53–64, 1916.

[5] Minoru Yabuta. A simple proof of carmichael's theorem on primitive divisors. *The Fibonacci Quarterly*, pages 439–443, 2001.