# IRREDUCIBILITY AND POSTCRITICALLY FINITE UNICRITICAL POLYNOMIALS

XAVIER BUFF, ADAM L. EPSTEIN, AND SARAH KOCH

ABSTRACT. Fix $D \geq 2$ and consider the unicritical polynomial $f_a : \mathbb{C} \to \mathbb{C}$ defined by $f_a(z) = az^D + 1$. We say that 0 is (pre)periodic under iteration of $f_a$ if $f_a^{\circ(k+n)}(0) = f_a^{\circ k}(0)$ for some integers $k \geq 0$ and $n \geq 1$. If $k$ and $n$ are minimal, then $k$ is the preperiod and $n$ is the period. Recently, Goksel proved that if $D$ is prime, then two parameters $a_1 \in \mathbb{C}$ and $a_2 \in \mathbb{C}$ for which 0 is preperiodic with period 1 and with the same preperiod $k \geq 2$ are Galois conjugate; he also proved that when $D = 2$, the result extends to the case of period 2. We give a new proof of this result and extend it to the case of periods 1 and 2 for arbitrary prime power degrees, i.e., $D = p^e$ for some prime $p$. We also extend the result to the case of period 3 in degree $D = 2$.

## INTRODUCTION

Consider the polynomials $f_a : \mathbb{C} \to \mathbb{C}$ defined by

$$f_a(z) = az^D + 1, \quad a \in \mathbb{C}.$$

The polynomial $f_a$ is unicritical: it has a unique critical point at $z = 0$. We are interested in parameters $a$ such that $f_a$ is postcritically finite; that is, values of $a$ for which the orbit of the critical point is finite under iteration of $f_a$. If $f_a$ is postcritically finite, then there exist integers $k \geq 0$ and $n \geq 1$ such that $f_a^{\circ(k+n)}(0) = f_a^{\circ k}(0)$. If $k$ and $n$ are minimal with this property, then $k$ is the preperiod and $n$ the period. Note that either $k = 0$ or $k \geq 2$.

For $n \geq 1$, let $F_n \in \mathbb{Z}[a]$ be the polynomial

$$F_n(a) := f_a^{\circ n}(0).$$

Gleason observed that the discriminant of $F_n$ is 1 (mod $D$), and thus $F_n$ has simple roots. It follows that

$$F_n = \prod_{m|n} G_m \quad \text{with} \quad G_n := \prod_{m|n} F_m^{\mu(n/m)} \in \mathbb{Z}[a],$$

where $\mu$ is the Möbius function defined by $\mu(i) = (-1)^j$ if $i$ is the product of $j$ distinct primes with $j \geq 0$ and $\mu(i) = 0$ otherwise. For example,

$$G_1 = F_1 = 1, \quad G_2 = F_2 = a + 1 \quad \text{and} \quad G_3 = F_3 = a(a+1)^D + 1.$$

It is conjectured that when $D = 2$, the polynomials $G_n$ are irreducible over $\mathbb{Q}$ for all $k \geq 2$. The following result shows that this is not true when $D \equiv 1$ (mod 6).

The research of the first author was supported in part by the ANR grant Lambda ANR-13-BS01-0002.

The research of the third author was supported in part by the NSF.

**Proposition 1** ([B]). *The polynomial $G_3$ is irreducible over $\mathbb{Q}$ if and only if $D$ is not congruent to 1 modulo 6. When $D \equiv 1 \pmod 6$, the polynomial $G_3$ has exactly two irreducible factors over $\mathbb{Q}$, one of which is $a^2 + a + 1$.*

Assume now that 0 is preperiodic for $f_a$ with preperiod $k \geq 2$ and period $n \geq 1$. Then,

$$f_a^{\circ(k+n-1)}(0) = \omega f_a^{\circ(k-1)}(0) \quad \text{with} \quad \omega^D = 1 \quad \text{and} \quad \omega \neq 1. \tag{1}$$

In fact, Equation (1) is satisfied if and only if either 0 is periodic for $f_a$ with period dividing $\gcd(n, k-1)$, or 0 is preperiodic for $f_a$ with preperiod $k$ and period dividing $n$.

For $k \geq 2$, $n \geq 1$ and $d \geq 2$ dividing $D$, we therefore consider the monic polynomial $G_{k,n,d}$ whose roots are the parameters $a \in \mathbb{C}$ such that

- 0 is preperiodic for $f_a$ with preperiod $k$ and period $n$, and
- Equation (1) is satisfied for some primitive $d$-th root of unity $\omega$.

We claim that $G_{k,n,d} \in \mathbb{Z}[a]$. Indeed, let $\Phi_d \in \mathbb{Z}[X, Y]$ be the (homogenized) $d$-th cyclotomic polynomial: if $\Omega_d$ is the set of primitive $d$-th roots of unity, then

$$\Phi_d := \prod_{\omega \in \Omega_d} (X - \omega Y).$$

Let $F_{k,n,d} \in \mathbb{Z}[a]$ be the polynomial defined by

$$F_{k,n,d} := \Phi_d(F_{k+n-1}, F_{k-1}) = \prod_{\omega \in \Omega_d} (F_{k+n-1} - \omega F_{k-1}).$$

The polynomial $F_{k+n-1} - \omega F_{k-1}$ has simple roots (see [B] for example). In addition, the common roots of $F_{k+n-1}$ and $F_{k-1}$ are the roots of $F_{\gcd(n,k-1)}$. It follows that the multiple roots of $F_{k,n,d}$ are the roots of $F_{\gcd(n,k-1)}$ with multiplicities $\varphi(d) = \deg(\Phi_d)$, where $\varphi$ is the Euler totient function. As a consequence,

$$F_{k,n,d} = F_{\gcd(n,k-1)}^{\varphi(d)} \cdot \prod_{m|n} G_{k,m,d} \tag{2}$$

and according to the Möbius Inversion Formula,

$$G_{k,n,d} = \prod_{m|n} \left( \frac{F_{k,m,d}}{F_{\gcd(m,k-1)}^{\varphi(d)}} \right)^{\mu(n/m)} \in \mathbb{Z}[a].$$

We shall also consider the polynomials $F_{k,n} \in \mathbb{Z}[a]$ and $G_{k,n} \in \mathbb{Z}[a]$ defined by

$$F_{k,n} := \prod_{\substack{d|D \\ d \neq 1}} F_{k,n,d} = \frac{F_{k+n-1}^D - F_{k-1}^D}{F_{k+n-1} - F_{k-1}} = \sum_{i+j=D-1} F_{k+n-1}^i \cdot F_{k-1}^j.$$

and

$$G_{k,n} := \prod_{\substack{d|D \\ d \neq 1}} G_{k,n,d} \in \mathbb{Z}[a] \quad \text{so that} \quad F_{k,n} = F_{\gcd(n,k-1)}^{D-1} \cdot \prod_{m|n} G_{k,m}. \tag{3}$$

We shall study the following conjecture of Milnor [M] (compare with [HT]).

**Conjecture.** *For all $k \geq 2$, $n \geq 1$, and $d \geq 2$ that divide $D \geq 2$, the polynomial $G_{k,n,d}$ is irreducible over $\mathbb{Q}$.*

There are few cases where the expression of $G_{k,n,d}$ is sufficiently simple so that existing results in the literature directly apply (see Appendix A). In this article, our study is inspired by the following fundamental result of Goksel.

**Theorem 2** ([G])**.** *If $D$ is a prime number, then $G_{k,1}(c^{D-1}) \in \mathbb{Z}[c]$ is irreducible for all $k \geq 2$. If $D = 2$, then $G_{k,2}$ is irreducible for all $k \geq 2$.*

Our main result is the following. In the whole article, $p$ is a prime number.

**Theorem 3.** *Assume $D = p^e$ is a prime power. Then $G_{k,1,d}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$, and for all $d \geq 2$ that divide $D$. More generally, if $n \geq 2$ and the polynomial $G_n \pmod p$ is irreducible over $\mathbb{F}_p$, then $G_{k,n,d}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$, and for all $d \geq 2$ that divide $D$.*

**Corollary 4.** *Assume $D = p^e$ is a prime power. Then $G_{k,2,d}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$, and for all $d \geq 2$ that divide $D$.*

*Proof.* The reduction of $G_2 = a + 1$ modulo $p$ is irreducible over $\mathbb{F}_p$. □

**Corollary 5.** *If $D = 2$ then $G_{k,3}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$.*

*Proof.* If $D = 2$, then $G_3 = a(a+1)^2 + 1 \equiv 1 + a + a^3 \pmod 2$ and $G_3 \pmod 2$ is irreducible over $\mathbb{F}_2$. □

**Corollary 6.** *If $D = 8$, then $G_{k,3,2}$, $G_{k,3,4}$ and $G_{k,3,8}$ are irreducible over $\mathbb{Q}$ for all $k \geq 2$.*

*Proof.* If $D = 8$, then $G_3 = a(a+1)^8 + 1 \equiv 1 + a + a^9 \pmod 2$ and $G_3 \pmod 2$ is irreducible over $\mathbb{F}_2$. □

**Remark.** The only values of $D = p^e$ and $n \geq 2$ for which the polynomial $G_n \pmod p$ is irreducible over $\mathbb{F}_p$ are the one listed previously: $n = 2$ for any prime power degree $D$, and $n = 3$ for both $D = 2$ and $D = 8$ (see Appendix B).

Our proof of Theorem 3 relies on the following two results (see §3).

**Lemma 7.** *Assume $d \geq 2$ divides $D \geq 2$. Assume $k \geq 2$, $n \geq 1$ and $m \geq 1$. Then,*

$$\operatorname{resultant}(G_{k,m,d}, G_n) = \begin{cases} \pm p^{\deg(G_n)} & \text{if } n = m \text{ and } d = p^e \text{ is a prime power} \\ \pm 1 & \text{otherwise.} \end{cases}$$

**Lemma 8.** *Assume $D = p^e$ is a prime power and $d \geq 2$ is a divisor of $D$. Then for all $k \geq 2$, the polynomials $G_{k,1,d} \pmod p$ are powers of $a \in \mathbb{F}_p[a]$; and for all $k \geq 2$ and all $n \geq 2$, the polynomials $G_{k,n,d} \pmod p$ are powers of $G_n \pmod p$.*

**Remark.** Lemma 7 shows a connection between the polynomials $G_{k,n,d}$ and the polynomials $G_n$, valid for all degrees $D \geq 2$. Lemma 8 shows a stronger connection between these polynomials, but only valid for prime power degrees $D = p^e$. We think that it is worth investigating what this relation becomes when $D$ is no longer a prime power.

## 1. The critical orbit

We shall first study some properties of the polynomials $F_k \in \mathbb{Z}[a]$. Recall that by definition, for all $k \geq 1$,

$$F_k(a) := f_a^{\circ k}(0).$$

For $k \geq 0$, set

$$N_k := \frac{D^k - 1}{D - 1} \quad \text{so that} \quad 1 + DN_k = \frac{D - 1 + D^{k+1} - D}{D - 1} = N_{k+1}.$$

**Lemma 9.** *For all $k \geq 1$, the polynomial $F_k$ has constant coefficient 1 and is monic of degree $N_{k-1}$.*

*Proof.* First, note that $F_1 = 1$ and for all $k \geq 1$, $F_{k+1} = aF_k^D + 1$. It follows that the constant coefficient of $F_{k+1}$ is 1. Second, let us prove by induction on $k \geq 1$ that $F_k$ is monic of degree $N_{k-1}$. The property holds for $k = 1$: indeed, $F_1 = 1$ and $N_0 = 0$. Now, if the result holds for some integer $k \geq 1$, then $F_{k+1} = aF_k^D + 1$ is monic of degree $1 + DN_{k-1} = N_k$. □

**Lemma 10.** *Assume $D = p^e$ is a prime power. For all $k \geq 1$,*

$$F_{k+1} - F_k \equiv a^{N_k} \pmod{p}.$$

*Proof.* We prove the result by induction on $k \geq 1$. For $k = 1$,

$$F_2 - F_1 = a + 1 - 1 = a = a^{N_1}.$$

Now, assume the property holds for some $k \geq 1$. Since $D = p^e$,

$$\begin{aligned} F_{k+2} - F_{k+1} &= (aF_{k+1}^D + 1) - (aF_k^D + 1) \\ &= a \cdot (F_{k+1}^D - F_k^D) \equiv a \cdot (F_{k+1} - F_k)^D \pmod{p}. \end{aligned}$$

Thus,

$$F_{k+2} - F_{k+1} \equiv a^{1+DN_k} \pmod{p} \equiv a^{N_{k+1}} \pmod{p}. \qquad \square$$

We conclude this section by the following observation due to Poonen.

**Lemma 11** (Poonen)**.** *For $m \neq n$, we have that* resultant$(G_m, G_n) = \pm 1$.

*Proof.* Assume $n > m$. It is not hard to see by induction on $k \geq 1$, that

$$F_{m+k} \equiv F_k \pmod{F_m^D}.$$

Indeed, $F_{m+1} = aF_m^D + 1 = F_1 + aF_m^D$ and if $F_{m+k} \equiv F_k \pmod{F_m^D}$, then

$$F_{m+k+1} = aF_{m+k}^D + 1 \equiv aF_k^D + 1 \pmod{F_m^D} \equiv F_k \pmod{F_m^D}.$$

This implies that, $F_{mn} \equiv F_m \pmod{F_m^D}$. Since $m < n$, $F_m G_n$ divides $F_{mn}$. So, there are polynomials $A \in \mathbb{Z}[a]$ and $B \in \mathbb{Z}[a]$ such that

$$AF_m G_n = F_{mn} = F_m + BF_m^D.$$

Dividing by $F_m$ yields $AG_n - BF_m^{D-1} = 1$. It follows that $G_m$ and $G_n$ are relatively prime in $\mathbb{Z}[a]$ and resultant$(G_m, G_n) = \pm 1$. □

## 2. When the critical point is preperiodic to a fixed point

As a warm up, let us first prove the following proposition that is due to Goksel. Our proof differs significantly from the one given in [G].

**Proposition 12.** *If $D$ is prime, then $G_{k,1}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$.*

*Proof.* Our proof relies on the following two lemmas.

**Lemma 13.** *For $k \geq 2$ and $n \geq 1$, the polynomial $F_{k,n}$ has constant coefficient $D$ and is monic of degree $(D-1)N_{k+n-2}$.*

*Proof.* According to Lemma 9, if $i+j=D-1$, the polynomial $F_{k+n-1}^i \cdot F_{k-1}^j$ has constant coefficient 1 and is monic of degree

$$i \cdot N_{k+n-2} + j \cdot N_{k-2} \leq (D-1)N_{k+n-2}$$

with equality if and only if $i=D-1$ and $j=0$. There are $D$ pairs $(i,j) \in \mathbb{N}^2$ such that $i+j=D-1$. Only one pair contributes to the leading term. Thus the polynomial is monic. Every pair contributes to the constant coefficient, which therefore is equal to $D$. □

**Lemma 14.** *If $D$ is prime, then for all $k \geq 1$,*

$$G_{k,1} = F_{k,1} \equiv a^{(D-1)N_{k-1}} \pmod{D}.$$

*Proof.* Assume $D$ is prime. On the one hand, according to Lemma 10:

$$F_k^D - F_{k-1}^D \equiv (F_k - F_{k-1})^D \pmod{D} \equiv a^{DN_{k-1}} \pmod{D}. \tag{4}$$

On the other hand, by definition of $F_{k,1}$:

$$F_k^D - F_{k-1}^D = (F_k - F_{k-1}) \cdot F_{k,1} \equiv a^{N_{k-1}} F_{k,1} \pmod{D}.$$

As a consequence,

$$a^{N_{k-1}} F_{k,1} \equiv a^{DN_{k-1}} \pmod{D} \quad \text{so that} \quad F_{k,1} \equiv a^{(D-1)N_{k-1}} \pmod{D}. \qquad \square$$

The proposition now follows from the Eisenstein criterion: $G_{k,1}$ is monic, $D$ divides all the coefficients except the one of the leading term, and $D^2$ does not divide the constant coefficient. □

## 3. The general case

This section is devoted to the proof of Theorem 3. We first prove Lemmas 7 and 8.

*Proof of Lemma 7.* Assume $d \geq 2$ divides $D \geq 2$, $k \geq 2$, $n \geq 1$ and $m \geq 1$. We need to show that

$$\text{resultant}(G_{k,m,d}, G_n) = \begin{cases} \pm p^{\deg(G_n)} & \text{if } n=m \text{ and } d=p^e \text{ is a prime power} \\ \pm 1 & \text{otherwise.} \end{cases}$$

The proof splits in several cases.

**Case 1: $n$ does not divide $m$.** Assume $\alpha$ is a root of $G_n$. Then, $F_{j_1}(\alpha) = F_{j_2}(\alpha)$ if and only if $j_1 \equiv j_2 \pmod{n}$. Since $n$ does not divide $m$, for all $k \geq 2$,

$$F_{k+m-1}(\alpha) - F_{k-1}(\alpha) \neq 0 \quad \text{and} \quad \alpha F_{k,m}(\alpha) = \frac{F_{k+m}(\alpha) - F_k(\alpha)}{F_{k+m-1}(\alpha) - F_{k-1}(\alpha)},$$

so that

$$\alpha^n \prod_{j=0}^{n-1} F_{k+j,m}(\alpha) = 1.$$

The polynomial $G_n$ is monic with constant coefficient 1. So, $\alpha$ is an algebraic unit. Thus,

$$\prod_{j=0}^{n-1} \text{resultant}(F_{k+j,m}, G_n) = \prod_{j=0}^{n-1} \prod_{\alpha \in G_n^{-1}(0)} F_{k+j,m}(\alpha) = \prod_{j=0}^{n-1} \prod_{\alpha \in G_n^{-1}(0)} \frac{1}{\alpha^n} = \pm 1.$$

Since $G_{k,m,d}$ divides $F_{k,m}$, it follows that

$$\text{resultant}(G_{k,m}, G_n) = \pm 1.$$

**Case 2: $n$ divides $m$.** Set

$$\nu := \Phi_d(1,1) = \begin{cases} p & \text{if } d = p^e \text{ is a prime power} \\ 1 & \text{otherwise.} \end{cases}$$

It is enough to prove that

$$\prod_{\ell | m} \text{resultant}(G_{k,\ell,d}, G_n) = \pm \nu^{\deg(G_n)}. \tag{5}$$

Indeed, assume Equation (5) holds. We have seen that $\text{resultant}(G_{k,\ell,d}, G_n) = \pm 1$ when $n$ does not divide $\ell$. So, for $m = n$,

$$\begin{aligned} \pm \nu^{\deg(G_n)} &= \text{resultant}(G_{k,n,d}, G_n) \cdot \prod_{\substack{\ell | n \\ \ell \neq n}} \text{resultant}(G_{k,\ell,d}, G_n) \\ &= \pm \text{resultant}(G_{k,n,d}, G_n). \end{aligned}$$

Now, if $n$ divides $m \neq n$, the polynomial $G_{k,n,d} \cdot G_{k,m,d}$ divides $F_{k,m,d}$; and

$$\text{resultant}(G_{k,n,d} \cdot G_{k,m,d}, G_n) = \pm \nu^{\deg(G_n)} \cdot \text{resultant}(G_{k,m,d}, G_n)$$

divides

$$\text{resultant}(F_{k,m,d}, G_n) = \pm \nu^{\deg(G_n)}.$$

This forces

$$\text{resultant}(G_{k,m,d}, G_n) = \pm 1.$$

So, it is enough to prove that Equation (5) holds.

**Case 2.a: $n$ does not divide $k-1$.** Assume $\alpha$ is a root of $G_n$. Since $n$ divides $m$, we have that $F_{k+m-1}(\alpha) = F_{m-1}(\alpha)$ and

$$F_{k,m,d}(\alpha) = \Phi_d\big(F_{k+m-1}(\alpha), F_{k-1}(\alpha)\big) = F_{k-1}^{\varphi(d)}(\alpha) \cdot \Phi_d(1,1) = \nu F_{k-1}^{\varphi(d)}(\alpha).$$

It follows that

$$\begin{aligned} \text{resultant}(F_{k,m,d}, G_n) &= \prod_{\alpha \in G_n^{-1}(0)} F_{k,m,d}(\alpha) \\ &= \nu^{\deg(G_n)} \cdot \prod_{\alpha \in G_n^{-1}(0)} F_{k-1}^{\varphi(d)}(\alpha) = \nu^{\deg(G_n)} \cdot \text{resultant}(F_{k-1}^{\varphi(d)}, G_n). \end{aligned}$$

Since $n$ does not divide $k-1$, Lemma 11 yields $\text{resultant}(G_\ell, G_n) = \pm 1$ for any divisor $\ell$ of $k-1$. Thus,

$$\begin{aligned} \text{resultant}(F_{k,m,d}, G_n) &= \nu^{\deg(G_n)} \cdot \text{resultant}(F_{k-1}^{\varphi(d)}, G_n) \\ &= \nu^{\deg(G_n)} \cdot \prod_{\ell | k-1} \big(\text{resultant}(G_\ell, G_n)\big)^{\varphi(d)} = \pm \nu^{\deg(G_n)}. \end{aligned}$$

Equation (5) now follows from Equation (2).

**Case 2.b: $n$ divides $k-1$.** As in the proof of Lemma 11, if $n$ divides $\ell$, then

$$F_\ell = F_n \pmod{F_n^D} = F_n \cdot (1 + H_\ell)$$

with $H_\ell \in \mathbb{Z}[a]$ divisible by $F_n$. It follows that

$$F_{k,m,d} = \Phi_d\big(F_{k+m-1}, F_{k-1}\big) = F_n^{\varphi(d)} \cdot (\nu + H_{k,m,d})$$

with $H_{k,m,d} \in \mathbb{Z}[a]$ divisible by $F_n$. Since $n$ divides $\gcd(m, k-1)$, Equation (2) yields

$$\left( \prod_{\substack{\ell \mid \gcd(m,k-1) \\ \ell \text{ does not divide } n}} G_\ell^{\varphi(d)} \right) \cdot \left( \prod_{\ell \mid m} G_{k,\ell,d} \right) = \nu + H_{k,m,d} F_n^{D-1}$$

and since $\text{resultant}(G_\ell, G_n) = \pm 1$ for $\ell \neq n$, we deduce that

$$\begin{aligned} \prod_{\ell \mid m} \text{resultant}(G_{k,\ell,d}, G_n) &= \text{resultant}(\nu + H_{k,m,d} F_n^{D-1}, G_n) \\ &= \text{resultant}(\nu, G_n) = \pm \nu^{\deg(G_n)}. \end{aligned}$$

This is Equation (5).

The proof of Lemma 7 is completed □

*Proof of Lemma 8.* Assume $D = p^e$ is a prime power and $d \geq 2$ is a divisor of $D$. We need to show that for all $k \geq 2$, the polynomials $G_{k,1,d} \pmod p$ are powers of $a \in \mathbb{F}_p[a]$; and for all $k \geq 2$ and $n \geq 2$, the polynomials $G_{k,n,d} \pmod p$ are powers of $G_n \pmod p$. Since $G_{k,n,d}$ divides $G_{k,n}$ for all $n \geq 1$, it is enough to prove that for all $k \geq 2$, the polynomials $G_{k,1} \pmod p$ are powers of $a \in \mathbb{F}_p[a]$; and for all $k \geq 2$ and $n \geq 2$, the polynomials $G_{k,n} \pmod p$ are powers of $G_n \pmod p$.

For $k \geq 2$, set $M_{k,1} := (D-1)N_{k-1}$ and for $n \geq 2$, set

$$M_{k,n} := \begin{cases} (D-1)(D^{k-1}-1) & \text{if } n \text{ divides } k-1 \\ (D-1)D^{k-1} & \text{if } n \text{ does not divide } k-1. \end{cases}$$

We shall prove that for $k \geq 2$ and $n \geq 2$,

$$G_{k,1} \equiv a^{M_{k,1}} \pmod p \quad \text{and} \quad G_{k,n} \equiv G_n^{M_{k,n}} \pmod p. \tag{6}$$

Note that $N_{i+j} - N_i = D^i N_j$ for all integers $i \geq 0$ and $j \geq 0$. So, according to Lemma 10, if $k \geq 2$ and $n \geq 1$,

$$\begin{aligned} F_{k+n-1} - F_{k-1} &\equiv a^{N_{k-1}} + a^{N_k} + \cdots + a^{N_{k+n-2}} \pmod p \\ &\equiv a^{N_{k-1}} \cdot \left( a^{D^{k-1}N_0} + a^{D^{k-1}N_1} + \cdots + a^{D^{k-1}N_{n-1}} \right) \pmod p \\ &\equiv a^{N_{k-1}} \cdot \left( a^{N_0} + a^{N_1} + \cdots + a^{N_{n-1}} \right)^{D^{k-1}} \pmod p \\ &\equiv a^{N_{k-1}} F_n^{D^{k-1}} \pmod p. \end{aligned}$$

As a consequence,

$$F_{k+n-1}^D - F_{k-1}^D \equiv a^{DN_{k-1}} F_n^{D^k} \pmod p$$

and

$$F_{k,n} \equiv a^{(D-1)N_{k-1}} F_n^{D^k - D^{k-1}} \pmod p \equiv a^{M_{k,1}} F_n^{(D-1)D^{k-1}} \pmod p.$$

In particular, for $n = 1$, this yields

$$G_{k,1} = F_{k,1} \equiv a^{M_{k,1}} \pmod p.$$

According to Equation (3),

$$\left( \prod_{m \mid \gcd(n,k-1)} G_m^{D-1} \right) \cdot \left( \prod_{m \mid n} G_{k,m} \right) = F_{k,n} \equiv a^{M_{k,1}} \cdot \prod_{m \mid n} G_m^{(D-1)D^{k-1}} \pmod p$$

and since $G_1 = 1$ and $G_{k,1} \equiv a^{M_{k,1}} \pmod{p}$,

$$\prod_{\substack{m|n \\ m\neq 1}} G_{k,m} = \prod_{\substack{m|n \\ m\neq 1}} G_m^{M_{k,m}} \pmod{p}.$$

Equation (6) now follows from the Möbius inversion formula, completing the proof of Lemma 8. □

To complete the proof of Theorem 3, we shall use the following generalization of the Eisenstein criterion.

**Lemma 15.** *Assume $A \in \mathbb{Z}[a]$ and $B \in \mathbb{Z}[a]$ are monic polynomials and $p$ is a prime number such that*

- *$A = B^N \pmod{p}$ for some integer $N \geq 1$;*
- *the polynomial $B \pmod{p}$ is irreducible over $\mathbb{F}_p$;*
- *$p^{2\deg(B)}$ does not divide $\operatorname{resultant}(A, B)$.*

*Then, $A$ is irreducible over $\mathbb{Q}$.*

*Proof.* Assume by contradiction that $A$ is reducible over $\mathbb{Q}$, so that $A = A_1A_2$ with $A_1 \in \mathbb{Z}[a]$ and $A_2 \in \mathbb{Z}[a]$ non constant. Let $\overline{A}_1$, $\overline{A}_2$ and $\overline{B}$ be the reductions of the polynomials modulo $p$. Then, $\overline{A}_1\overline{A}_2 = \overline{B}^N$ and since $\overline{B}$ is irreducible over $\mathbb{F}_p$, we have that $\overline{A}_1 = \overline{B}^{N_1}$ and $\overline{A}_2 = \overline{B}^{N_2}$ for some positive integers $N_1 \geq 1$ and $N_2 \geq 1$. In other words, $A_1 = B^{N_1} + pC_1$ and $A_2 = B^{N_2} + pC_2$ for some polynomials $C_1 \in \mathbb{Z}[a]$ and $C_2 \in \mathbb{Z}[a]$. In that case,

$$\begin{aligned}\operatorname{resultant}(A, B) = \operatorname{resultant}(A_1A_2, B) &= \operatorname{resultant}(A_1, B) \cdot \operatorname{resultant}(A_2, B) \\ &= \operatorname{resultant}(pC_1, B) \cdot \operatorname{resultant}(pC_2, B) \\ &= p^{2\deg(B)}\operatorname{resultant}(C_1C_2, B).\end{aligned}$$

This contradicts the assumption that $p^{2\deg(B)}$ does not divide $\operatorname{resultant}(A, B)$. □

We may now complete the proof of Theorem 3. Assume $D = p^e$ is a prime power and $d \geq 2$ is a divisor of $D$. Then $d$ is a power of $p$.

According to Lemma 8, the polynomial $G_{k,1,d} \pmod{p}$ is a power of $a \in \mathbb{F}_p[a]$, which is irreducible over $\mathbb{F}_p$; and according to Lemma 7, $p^{2\deg(G_n)}$ does not divide $\operatorname{resultant}(G_{k,1,d}, G_1) = \pm p^{\deg(G_n)}$. It follows from Lemma 15 that $G_{1,k,d}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$.

Similary, according to Lemma 8, if $n \geq 2$, the polynomial $G_{k,n,d} \pmod{p}$ is a power of $G_n \pmod{p}$; and according to Lemma 7, $p^{2\deg(G_n)}$ does not divide $\operatorname{resultant}(G_{k,n,d}, G_n) = \pm p^{\deg(G_n)}$. It follows from Lemma 15 that when $G_n \pmod{p}$ is irreducible over $\mathbb{F}_p$, the polynomial $G_{k,n,d}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$.

This completes the proof of Theorem 3.

## Appendix A. Particular cases

For small values of $k$ and $n$, the expression of $G_{k,n,d}$ is quite simple and we may obtain irreducibility as follows.

**Proposition 16.** *For all $D \geq 2$ and all $d$ that divide $D$, the polynomial $G_{2,1,d}$ is irreducible over $\mathbb{Q}$.*

*Proof.* We have that

$$G_{2,1,d} = \Phi_d(a+1,1).$$

Since cyclotomic polynomials are irreducible over $\mathbb{Q}$, so is $G_{2,1,d}$. □

**Proposition 17.** *For all $D \geq 2$ even, the polynomial $G_{3,1,2}$ is irreducible over $\mathbb{Q}$.*

*Proof.* Setting $b := a+1$, we have that

$$G_{3,1,2} = \Phi_2(F_3, F_2) = F_3 + F_2 = a(a+1)^D + 1 + (a+1) = b^{2d+1} - b^{2d} + b + 1.$$

By [FJ, Theorem 2], this quadrinomial is irreducible for all $d \geq 1$. □

**Proposition 18.** *For all $D \geq 2$ even, the polynomial $G_{2,2,2}$ is irreducible over $\mathbb{Q}$.*

*Proof.* Assume $D = 2d$ is even. Then setting $b = a+1$ as previously,

$$\begin{aligned} G_{2,2,2} = \frac{\Phi_2(F_3,F_1)}{\Phi_2(F_2,F_1)} &= \frac{F_3+F_1}{F_2+F_1} \\ &= \frac{a(a+1)^D+2}{a+2} \\ &= \frac{b^{2d+1}-b^{2d}+2}{b+1} = b^{2d} - 2b^{2d-1} + 2b^{2d-2} \ - \cdots - 2b + 2. \end{aligned}$$

According to the Eisenstein criterion, this polynomial is irreducible over $\mathbb{Q}$. □

## Appendix B. Irreducibility over $\mathbb{F}_p$

Here, $D = p^e$ is a prime power. In this appendix, we shall work over the field $\mathbb{F}_p$ or its algebraic closure $\overline{\mathbb{F}}_p$. With an abuse of notation, we shall keep the notation $F_n$ and $G_n$ for their reductions modulo $p$. In other words, $F_n \in \mathbb{F}_p[a]$ and $G_n \in \mathbb{F}_p[a]$ are defined by

$$F_n := \sum_{k=0}^{n-1} a^{N_k} \quad \text{with} \quad N_k := \frac{D^k - 1}{D-1} \quad \text{and} \quad G_n := \prod_{m|n} F_m^{\mu(n/m)}.$$

We study the irreducibility of $G_n$ over $\mathbb{F}_p$. Note that

$$G_1 = 1 \quad \text{and} \quad G_2 = a+1.$$

So, we shall restrict our study to the case $n \geq 3$.

**Proposition 19.** *Assume $D = p^e$ is a prime power and $n \geq 3$. Then, the polynomial $G_n \in \mathbb{F}_p[a]$ is irreducible over $\mathbb{F}_p$ if and only if either $n = 3$ and $D = 2$, or $n = 3$ and $D = 8$.*

*Proof.* Let $f : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ be the Frobenius automorphism $x \mapsto x^p$.

**Lemma 20.** *If $\alpha \in \overline{\mathbb{F}}_p$ is a root of $G_n$, then $\alpha$ is a periodic point of $f$ of period dividing $n \cdot e$.*

*Proof.* Assume $\alpha$ is a root of $G_n$. Then, $F_n(\alpha) = 0$, so that

$$\begin{aligned} 1 = 1 + \alpha F_n^D(\alpha) &= 1 + \alpha F_n(\alpha^D) \\ &= 1 + \sum_{k=0}^{n-1} \alpha^{1+DN_k} \\ &= 1 + \sum_{k=0}^{n-1} \alpha^{N_{k+1}} = F_n(\alpha) + \alpha^{N_n} = \alpha^{N_n}. \end{aligned}$$

It follows that

$$f^{\circ(n\cdot e)}(\alpha) = \alpha^{D^n} = \alpha^{1+(D-1)N_n} = \alpha \cdot \left(\alpha^{N_n}\right)^{D-1} = \alpha. \qquad \square$$

As a consequence, if $G_n$ is irreducible over $\mathbb{F}_p$, then the degree of $G_n$ divides $n \cdot e$. The degree of $G_n$ is

$$\deg(G_n) = \sum_{m|n} \mu\left(\frac{n}{m}\right) \deg(F_m) = \sum_{m|n} \mu\left(\frac{n}{m}\right) N_{m-1} \geq D^{n-2}.$$

So, if $G_n$ is irreducible over $\mathbb{F}_p$, then $p^{(n-2)e} \leq n \cdot e$.

Set $\kappa := (n-2)\log(p) > 0$. The function $(0, +\infty) \ni x \mapsto \exp(\kappa x)/x \in (0, +\infty)$ reaches a minimum at $x = 1/\kappa$ with value $\kappa \cdot \exp(1)$. It follows that for $n \geq 3$,

$$\frac{p^{(n-2)e}}{n \cdot e} \geq \left(1 - \frac{2}{n}\right) \log(p) \exp(1).$$

If $n \geq 3$ and $p \geq 5$, or if $n \geq 4$ and $p = 3$, or if $n \geq 5$ and $p = 2$, this is greater than 1. So, it is enough to study the following cases.

**Case $n = 3$ and $p = 2$.** In that case, for $e \geq 1$,

$$\deg(G_n) = 1 + D = 2^e + 1 \quad \text{and} \quad n \cdot e = 3e.$$

The function $(0, +\infty) \ni x \mapsto (2^x + 1)/(3x) \in (0, +\infty)$ is increasing on $[2, +\infty)$ and takes the values 1 at $x = 1$, $5/6$ at $x = 2$ and 1 at $x = 3$. It follows that $\deg(G_n)$ divides $n \cdot e$ if and only if $e = 1$ or $e = 3$, i.e. $D = 2$ or $D = 8$; in those two cases, $G_3$ is irreducible.

**Case $n = 3$ and $p = 3$.** In that case, for $e \geq 1$,

$$\deg(G_n) = 1 + D = 3^e + 1 > 3e = n \cdot e = 3e.$$

So, $G_n$ cannot be irreducible in that case.

**Case $n = 4$ and $p = 2$.** In that case, for $e \geq 1$,

$$\deg(G_n) = 1 + D + D^2 = 1 + 3^e + 3^{2e} > 4e = n \cdot e.$$

So, $G_n$ cannot be irreducible in that case. $\square$

## References


[B] X. Buff *On Postcritically Finite Unicritical Polynomials*, Preprint, `https://www.math.univ-toulouse.fr/~buff/Preprints/Gleason/Gleason.pdf`.

[E] A. L. Epstein *Integrality and rigidity for postcritically finite polynomials*, Bull. London Math. Soc. 44 (2012), 39–46.

[FJ] C. Finch & L. Jones *On the irreducibility of $\{-1, 0, 1\}$-quadrinomials*, Integers 6 (2006).

[G] V. Goksel *On the orbit of a post-critically finite polynomial of the form $x^d + c$*, Preprint, `https://arxiv.org/abs/1806.01208`.

[HT] B. Hutz & A. Towsley *Misiurewicz points for polynomial maps and transversality*, New York J. Math. 21 (2015) 297–319.

[M] J. Milnor *Arithmetic of unicritical polynomial maps*, Frontiers in Complex Dynamics: In Celebration of John Milnor's 80th Birthday (2012) 15–23.



*E-mail address*: `xavier.buff@math.univ-toulouse.fr`

Institut de Mathématiques de Toulouse, Université Paul Sabatier, 118, route de Narbonne, 31062 Toulouse Cedex, France

*E-mail address*: `adame@maths.warwick.ac.uk`

Mathematics institute, University of Warwick, Coventry CV4 7AL, United Kingdom

*E-mail address*: kochsc@umich.edu

Department of Mathematics, 530 Church Street, East Hall, University of Michigan, Ann Arbor MI 48109, United States