Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Vefa GOKSEL

A note on Misiurewicz polynomials

Tome 32, nº 2 (2020), p. 373-385.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2020__32_2_373_0>

Journal de Théorie des Nombres
de Bordeaux **32** (2020), 373–385

A note on Misiurewicz polynomials

par Vefa GOKSEL

Résumé. Soit $f_{c,d}(x) = x^d + c \in \mathbb{C}[x]$. On appelle point de Misiurewicz une valeur c_0 pour laquelle $f_{c_0,d}$ a une orbite critique finie et strictement prépériodique. Tout point de Misiurewicz appartient à $\overline{\mathbb{Q}}$. Supposons que les points $c_0, c_1 \in \overline{\mathbb{Q}}$ sont tels que les orbites de $f_{c_0,d}$ et de $f_{c_1,d}$ sont du même type. Une question classique est de savoir si c_0 et c_1 sont nécessairement conjugués sur $\mathbb{Q}$. Récemment, certains progrès ont été réalisés par plusieurs auteurs pour répondre à cette question. Dans cette note, nous démontrons de nouveaux résultats dans le cas où d est un nombre premier. Tous les résultats connus jusqu'à présent portent sur des cas où la période est au plus 3. En particulier, notre travail est le premier à fournir des informations dans le cas de période plus grande que 3.

Abstract. Let $f_{c,d}(x) = x^d + c \in \mathbb{C}[x]$. The c_0 values for which $f_{c_0,d}$ has a strictly pre-periodic finite critical orbit are called Misiurewicz points. Any Misiurewicz point lies in $\overline{\mathbb{Q}}$. Suppose that the Misiurewicz points $c_0, c_1 \in \overline{\mathbb{Q}}$ are such that the polynomials $f_{c_0,d}$ and $f_{c_1,d}$ have the same orbit type. One classical question is whether c_0 and c_1 need to be Galois conjugates or not. Recently there has been partial progress on this question by several authors. In this note, we prove some new results when d is a prime. All the results known so far were in the cases of period at most 3. In particular, our work is the first to say something provable in the cases of period greater than 3.

1. Introduction

Let $f(x) \in \mathbb{C}[x]$ be a polynomial of degree $d \geq 2$. We denote by $f^n(x)$ the nth iterate of $f(x)$ for $n \geq 1$. We also make the convention that $f^0(x) = x$. For a given $c \in \mathbb{C}$, the orbit of c under f is defined to be the set

$$O_f(c) = \{f(c), f^2(c), \dots\}.$$

The polynomial f is called *post-critically finite* (PCF) if this orbit is finite for every critical point of f. Most polynomials are not post-critically finite, so such polynomials are rather special. In this paper, we will consider an even more special case, namely post-critically finite polynomials of the form $x^d + c \in \mathbb{C}[x]$, where $d \geq 2$. From now on, we set $f_{c,d}(x) = x^d + c$.

Manuscrit reçu le 19 août 2019, révisé le 17 juin 2020, accepté le 28 juillet 2020.
2020 *Mathematics Subject Classification.* 11R09, 37P15.
Mots-clefs. iteration, post-critically finite, Misiurewicz point.

Polynomials in this family are particularly nice, because they all have the unique critical point 0.

Now suppose $f_{c,d}$ is PCF, i.e. there exist integers $m, n \in \mathbb{Z}$ with $n \neq 0$ such that $f_{c,d}^m(0) = f_{c,d}^{m+n}(0)$. We say that $f_{c,d}$ *has exact type* (m,n) if n is the minimal positive integer such that $f_{c,d}^m(0) = f_{c,d}^{m+n}(0)$ and $f_{c,d}^k(0) \neq f_{c,d}^{k+n}(0)$ for any $k < m$. It is easy to see that if $m \neq 0$, then m has to be at least 2. A number c_0 for which $f_{c_0,d}$ has type (m,n) with $m \geq 2$ is called a *Misiurewicz point of type* (m,n). Any Misiurewicz point of type (m,n) is a root of a polynomial $G_{d,m,n}(c) \in \mathbb{Z}[c]$, which we call the *Misiurewicz polynomial of type* (m,n). So, in particular, all Misiurewicz points lie in $\overline{\mathbb{Q}}$.

It is straightforward to check that for $c_0, c_1 \in \mathbb{C}$, the polynomials $f_{c_0,d}$ and $f_{c_1,d}$ are affine conjugate to each other if and only if $c_0^{d-1} = c_1^{d-1}$. Milnor [11] asked the following question.

Question 1.1. *Suppose that $f_{c_0,d}$ and $f_{c_1,d}$ have the same exact type (m,n). Does it follow that c_0^{d-1} and c_1^{d-1} are Galois conjugates?*

In this note, we will study the following question, which is a more general version of Question 1.1. It appears in [1, Question 9.8] in a different form.

Question 1.2. *Suppose that $f_{c_0,d}$ and $f_{c_1,d}$ have the same exact type (m,n). Does it follow that c_0 and c_1 are Galois conjugates?*

Before we talk about some recent partial progress on these questions, let us first precisely define the polynomial $G_{d,m,n}(c)$.

Definition 1.3 ([12])**.** We set $G_{d,0,n}(c) = \prod_{k|n}(f_{c,d}^k(0))^{\mu(\frac{n}{k})}$. For $m \neq 0$, we define $G_{d,m,n}(c)$ as follows: We first set

$$F_{d,m,n}(c) = \prod_{k|n}\left(\frac{f_{c,d}^{m+k}(0) - f_{c,d}^m(0)}{f_{c,d}^{m-1+k}(0) - f_{c,d}^{m-1}(0)}\right)^{\mu(\frac{n}{k})}.$$

Then, for $m \geq 2$, we define

$$G_{d,m,n}(c) = \begin{cases} F_{d,m,n}(c) & \text{if } n \nmid m-1 \\ F_{d,m,n}(c)/(F_{d,1,n}(c))^{d-1} & \text{if } n \mid m-1. \end{cases}$$

See [7] for a proof that $G_{d,m,n}(c)$ is in fact a polynomial with integer coefficients.

We also need to introduce the polynomials $H_{d,m,n}(c) \in \mathbb{Z}[c]$, which are the unique polynomials that satisfy $H_{d,0,1}(c) = 1$, and $H_{d,m,n}(c^{d-1}) = G_{d,m,n}(c)$ for $(m,n) \neq (0,1)$. The polynomials $H_{d,m,n}(c)$ arise when one works with the polynomials $g_{c,d}(x) = cx^d + 1$ instead of $f_{c,d}(x)$ (see [2] and [3]). In other words, they can be defined by simply replacing $f_{c,d}$ with $g_{c,d}$ in Definition 1.3.

Question 1.1 is equivalent to asking whether the polynomial $H_{d,m,n}(c)$ is irreducible over $\mathbb{Q}$ or not, and Question 1.2 is equivalent to asking whether the polynomial $G_{d,m,n}(c)$ is irreducible over $\mathbb{Q}$ or not. From now on, whenever we say irreducible, we will mean irreducibility over $\mathbb{Q}$ (unless we state otherwise).

We note that because of the relation given above, the irreducibility questions for the polynomials $G_{d,m,n}(c)$ and $H_{d,m,n}(c)$ are not equivalent when $d > 2$, namely the irreducibility of $G_{d,m,n}(c)$ is a stronger condition than the irreducibility of $H_{d,m,n}(c)$.

We now summarize the known partial results regarding Question 1.1 and Question 1.2. Buff [2] has shown that $H_{d,0,3}(c)$ is irreducible if and only if $d \not\equiv 1 \pmod 6$. The author [5] has proven that for any $m \geq 2$, $G_{d,m,1}(c)$ is irreducible when d is a prime, and also that $G_{2,m,2}(c)$ is irreducible. Buff, Epstein and Koch [3] have proven that for any $m \geq 2$, $H_{d,m,1}(c)$ and $H_{d,m,2}(c)$ have exactly k irreducible factors when d is a prime power, where k is such that $d = p^k$ for some rational prime p. They have also proven that for any $m \geq 2$, $G_{2,m,3}(c)$ is irreducible, and $H_{8,m,3}(c)$ has exactly 3 irreducible factors. These irreducibility results they have proven were corollaries of one of their main theorems ([3, Theorem 19]), which makes a somewhat surprising connection between the polynomial $H_{d,m,n}(c) \in \mathbb{Z}[c]$ and the reduced polynomial $\overline{H_{d,0,n}}(c) \in \mathbb{F}_p[c]$ when d is a power of p. More precisely, it states that if the reduced polynomial $\overline{H_{d,m,n}}(c) \in \mathbb{F}_p[c]$ is irreducible over $\mathbb{F}_p$, then the polynomial $H_{d,m,n}(c)$ has exactly k irreducible factors over $\mathbb{Q}$, where $d = p^k$ for some prime p. They also remark that the reduced polynomial $\overline{H_{d,0,n}}(c) \in \mathbb{F}_p[c]$ is irreducible only in the cases that show up in the above corollaries: $(d, n) = (p^k, 1), (p^k, 2), (2, 3)$ or $(8, 3)$.

We now state our main result.

Theorem 1.4. *Let d be a prime. Then, for all m, the number of irreducible factors of $G_{d,m,n}(c)$ over $\mathbb{Q}$ is bounded from above by the number of irreducible factors of the reduced polynomial $\overline{G_{d,0,n}}(c) \in \mathbb{F}_d[c]$. In particular, if $\overline{G_{d,0,n}}(c) \in \mathbb{F}_d[c]$ is irreducible over $\mathbb{F}_d$, then $G_{d,m,n}(c)$ is irreducible over $\mathbb{Q}$.*

The following immediate corollary to this theorem recovers all the cases that the polynomial $G_{d,m,n}(c)$ is known to be irreducible.

Corollary 1.5. *Let d be a prime. Then, for any $m \geq 2$, $G_{d,m,1}(c)$, $G_{2,m,2}(c)$ and $G_{2,m,3}(c)$ are irreducible over $\mathbb{Q}$.*

Proof. Noting that each of $\overline{G_{d,0,1}}(c) = c \in \mathbb{F}_d[c]$, $\overline{G_{2,0,2}}(c) = c + 1 \in \mathbb{F}_2[c]$, and $\overline{G_{2,0,3}}(c) = c^3 + c + 1 \in \mathbb{F}_2[c]$ is irreducible, the corollary follows from Theorem 1.4. $\square$

We also obtain the following new irreducibility result.

Corollary 1.6. *For any $m \geq 2$, $G_{3,m,2}(c)$ is irreducible over $\mathbb{Q}$.*

Proof. We have $G_{3,0,2}(c) = c^2 + 1$, which is irreducible in $\mathbb{F}_3[c]$, hence the result again follows from Theorem 1.4. $\square$

Remark 1.7. Theorem 1.4 does not imply the irreducibility of $G_{d,m,2}(c)$ for any prime $d > 3$, because we have $G_{d,0,2}(c) = c^{d-1} + 1$, and one can easily show that $c^{d-1} + 1$ is always reducible in $\mathbb{F}_d[c]$ when $d > 3$. In fact, one can prove something much stronger; $c^{d-1} + 1$ is reducible modulo every prime when $d > 3$.

Although Theorem 1.4 does not give any analogue of Corollary 1.5 or Corollary 1.6 when $n > 3$, it provides an upper bound for the number of irreducible factors of the polynomial $G_{d,m,n}(c)$, which is independent of m. In particular, because of the way its proof proceeds, it reduces Question 1.2 to perhaps a simpler problem. We illustrate this with the following example.

Example 1.8. One of the simplest cases that $G_{d,m,n}(c)$ is not known to be irreducible is the case $d = 2, n = 4$. Since we have $\overline{G_{2,0,4}}(c) = (c^2 + c + 1)(c^4 + c + 1) \in \mathbb{F}_2[c]$, the proof of Theorem 1.4 implies that if $G_{2,m,4}(c)$ is not irreducible for some $m \geq 2$, then there must exist polynomials $f(c), g(c) \in \mathbb{Z}[c]$ such that

$$G_{2,m,4}(c) = [(c^2 + c + 1)^{M_{m,4}} + 2f(c)][(c^4 + c + 1)^{M_{m,4}} + 2g(c)],$$

where $M_{m,4} = 2^{m-1}$ if $m \not\equiv 1 \pmod 4$, and $M_{m,4} = 2^{m-1} - 1$ otherwise. MAGMA computations reveal that this does not happen for the small values of m (thus $G_{2,m,4}(c)$ is irreducible), but whether this is the case for all m or not remains open.

Using Theorem 1.4 together with a result of Buff–Epstein–Koch [3] and Dedekind's criterion [4], we also prove the following result about the number fields generated by Misiurewicz points.

Theorem 1.9. *Let d be a prime, and c_0 a root of $G_{d,m,n}(c)$. Set $K = \mathbb{Q}(c_0)$. Then we have $d \nmid [\mathcal{O}_K : \mathbb{Z}[c_0]]$.*

Theorem 1.9 has an arithmetic consequence for the critical orbit of $f_{c,d}$, see Corollary 3.5 for details.

Finally, we introduce some notation that we will be using throughout the article. Let K be a number field, and $\mathcal{O}_K$ its ring of integers. For any $a \in \mathcal{O}_K$, we denote by (a) the ideal of $\mathcal{O}_K$ generated by a. We will also denote by $N_{K/\mathbb{Q}}(a)$ the norm of a in the extension $K/\mathbb{Q}$. When the polynomial $f_{c_0,d}$ has type (m, n), we will use the set $\{a_1, \ldots, a_{m+n-1}\}$ to denote the critical orbit of $f_{c_0,d}$, where we set $a_i = f^i_{c_0,d}(0)$. Whenever we use a_i for some $i > m + n - 1$, we again obtain it by setting $a_i = f^i_{c_o,d}(0)$ and using the periodicity of $f_{c_0,d}$.

Acknowledgments. The author would like to thank Nigel Boston and Rafe Jones for helpful conversations related to this work. It is also a pleasure to thank Rafe Jones for useful feedback on an early draft of this paper. The author also thanks the anonymous referee for a careful reading of the paper, and for helpful suggestions which improved the exposition.

2. Proof of Theorem 1.4

The goal in this section is to prove Theorem 1.4. We start by recalling the main theorem of [5], as it will be crucial throughout the paper.

Theorem 2.1 ([5]). *Let $f_{c,d}(x) = x^d + c \in \overline{\mathbb{Q}}[x]$ be a PCF polynomial having exact type (m, n) with $m \neq 0$. Set $K = \mathbb{Q}(c)$, and let $O_{f_{c,d}} = \{a_1, a_2, \ldots, a_{m+n-1}\} \subset \mathcal{O}_K$ be the critical orbit of $f_{c,d}$. Then the following holds:*

(a) *If $n \nmid i$, then a_i is a unit.*
(b) *If d is a prime and $n \mid i$, then one has $(a_i)^{M_{m,n}} = (d)$, where*

$$M_{m,n} = \begin{cases} d^{m-1}(d-1) & \text{if } n \nmid m-1 \\ (d^{m-1}-1)(d-1) & \text{if } n \mid m-1. \end{cases}$$

Lemma 2.2. *Let p be a rational prime, and c_0 a root of $G_{d,m,n}(c)$, where $m \neq 0$. Set $K = \mathbb{Q}(c_0)$. Then we have $a_n = G_{d,0,n}(c_0)u$ for some unit u in $\mathcal{O}_K$.*

Proof. We know from Theorem 2.1 that a_i is a unit in $\mathcal{O}_K$ for all $1 \leq i \leq n-1$. It is also clear by the definition of $G_{d,0,n}(c)$ that $G_{d,0,n}(c_0)$ divides a_n in $\mathbb{Z}[c_0]$. Note that the sequence $\{a_i\}_{i\geq 1}$ is a rigid divisibility sequence (see [6] for a definition of a rigid divisibility sequence and the proof of this fact), from which one sees that $G_{d,0,n}(c_0)$ is the primitive part of a_n ([9, Lemma 5.4]). This implies that $\frac{a_n}{G_{d,0,n}(c_0)}$ divides $a_1 \cdots a_{n-1}$ in $\mathbb{Z}[c_0]$. But, the product $a_1 \cdots a_{n-1}$ is a unit in $\mathcal{O}_K$, hence $\frac{a_n}{G_{d,0,n}(c_0)}$ must be a unit in $\mathcal{O}_K$, which is what we wanted. □

The following lemma due to Buff–Epstein–Koch will also be crucial in the proof of Theorem 1.4.

Lemma 2.3 ([3]). *Let d be a rational prime, and define $M_{m,n}$ as in Theorem 2.1. Then we have $G_{d,m,n} \equiv G_{d,0,n}^{M_{m,n}} \pmod{d}$ for all $n \geq 1$.*

We now recall the following standard result, which we state without proof.

Lemma 2.4. *Let K be a number field, p a rational prime, and $\alpha \in \mathcal{O}_K$. Then the ideal (p, α) is the unit ideal if and only if $N_{K/\mathbb{Q}}(\alpha)$ is relatively prime to p.*

Lemma 2.5. *Let K be a number field, and p a rational prime. Choose $\alpha \in \mathcal{O}_K$ so that $K = \mathbb{Q}(\alpha)$. Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. Suppose $\bar{f}(x) \in \mathbb{F}_p[x]$ factors as*

$$\bar{f}(x) = g_1(x)^{e_1} \cdots g_k(x)^{e_k},$$

where $g_1(x), \ldots, g_k(x) \in \mathbb{F}_p[x]$ are distinct and irreducible. Then, for any monic polynomial $h(x) \in \mathbb{Z}[x]$, $(p, h(\alpha))$ is not the unit ideal in $\mathcal{O}_K$ if and only if $g_i(x)|\bar{h}(x)$ in $\mathbb{F}_p[x]$ for some $1 \le i \le k$.

Proof. First suppose that $(p, h(\alpha))$ is not the unit ideal in $\mathcal{O}_K$. Then by Lemma 2.4, $N_{K/\mathbb{Q}}(h(\alpha)) \equiv 0 \pmod{p}$. Recall that $N_{K/\mathbb{Q}}(h(\alpha)) = \operatorname{Res}(f, h)$. Hence, we get $\operatorname{Res}(f, h) \equiv 0 \pmod{p}$, which forces $\bar{f}$ and $\bar{h}$ to have a common factor in $\mathbb{F}_p[x]$, which proves this part of the statement. For the other direction, assume $g_i(x)|\bar{h}(x)$ for some $1 \le i \le k$. Since this means that $\bar{f}$ and $\bar{h}$ have a common factor in $\mathbb{F}_p[x]$, this again implies that $N_{K/\mathbb{Q}}(h(\alpha)) = \operatorname{Res}(f, h) \equiv 0 \pmod{p}$, which, by Lemma 2.4, shows that $(p, h(\alpha))$ is not the unit ideal in $\mathcal{O}_K$, as desired. □

The next proposition combined with the remark following it will provide us an explicit factorization of the ideal (d) in the number field generated by a root of the Misiurewicz polynomial $G_{d,m,n}(c)$, which will be heavily used in the proof of Theorem 1.4.

Proposition 2.6. *Let d be a prime. Suppose $\overline{G_{d,0,n}}(c)$ factors as*

$$\overline{G_{d,0,n}}(c) = f_1(c) \cdots f_k(c),$$

where $f_1(c), \ldots, f_k(c) \in \mathbb{F}_p[c]$ are distinct irreducible polynomials. Then, if $\widetilde{f_1}(c), \ldots, \widetilde{f_k}(c) \in \mathbb{Z}[c]$ are any lifts of these polynomials, and c_0 is a root of $G_{d,m,n}$, we have

$$(a_n) = (d, \widetilde{f_1}(c_0)) \cdots (d, \widetilde{f_k}(c_0)). \tag{2.1}$$

Proof. First note that from Lemma 2.2, we have $a_n = G_{d,0,n}(c_0)u$ for some unit $u \in \mathbb{Z}[c_0]$. This gives that

$$a_n = \widetilde{f_1}(c_0) \cdots \widetilde{f_k}(c_0)u + d\alpha(c_0) \tag{2.2}$$

for some $\alpha(c) \in \mathbb{Z}[c]$. We will now prove the proposition by showing that each side of (2.1) is contained in the other side:

We first show that the right-hand side is contained in the left-hand side. All the generators of the product ideal involving d already belong to (a_n), because from Theorem 2.1 we have $d \in (a_n)$. So, it suffices to show that $\widetilde{f_1}(c_0) \cdots \widetilde{f_k}(c_0) \in (a_n)$. We have $d \in (a_n)$, which gives $a_n - d\alpha(c_0) = \widetilde{f_1}(c_0) \cdots \widetilde{f_k}(c_0)u \in (a_n)$, which gives what we want, since u is a unit.

For the other direction, first note that if $k \le M_{m,n}$, then since $a_n \in (d, \widetilde{f_i}(c_0))$ for all i (by (2.2)), we get that d lies in the right-hand side of (2.1), because from Theorem 2.1 we have $d \in (a_n)^k$, and a_n^k lies in the right-hand side. But then, if d lies in the right-hand side of (2.1), we get that $a_n = \widetilde{f_1}(c_0) \cdots \widetilde{f_k}(c_0)u + d\alpha(c_0)$ lies in the right-hand side of (2.1) as well, as desired. So, we can assume without loss of generality that $k > M_{m,n}$. By the reasoning above, to finish the proof, it suffices to prove that d lies in the right-hand side of (2.1). Write $k = M_{m,n}l + q$, $0 \le q < M_{m,n}$. Note that similar to above, we will have

$$a_n \in (d, \widetilde{f}_{iM_{m,n}+1}(c_0)) \cdots (d, \widetilde{f}_{(i+1)M_{m,n}}(c_0))$$

for $i = 0, \ldots, l-1$, and

$$a_n \in (d, \widetilde{f}_{lM_{m,n}+1}(c_0)) \cdots (d, \widetilde{f}_{lM_{m,n}+q}(c_0)).$$

This implies that a_n^{l+1} lies in the right-hand side of (2.1), which, if $l+1 \le M_{m,n}$, will again imply that d lies in the right-hand side of (2.1), which will finish the proof. If $l+1 > M_{m,n}$, we can repeat the same argument again, and it is obvious that this procedure will eventually terminate, and we will get that d lies in the right-hand side of (2.1), so we are done. □

Remark 2.7. Note that since we have $(a_n)^{M_{m,n}} = (d)$ from Theorem 2.1, Proposition 2.3 gives a factorization of the ideal (d) in $\mathcal{O}_K$. More precisely, we get

$$(d) = (d, \widetilde{f_1}(c_0))^{M_{m,n}} \cdots (d, \widetilde{f_k}(c_0))^{M_{m,n}}. \tag{2.3}$$

We are finally ready to prove Theorem 1.4.

Proof of Theorem 1.4. Recall from Lemma 2.3 that if $\overline{G_{d,0,n}}(c) \in \mathbb{F}_d[c]$ factors as

$$\overline{G_{d,0,n}}(c) = f_1(c) \cdots f_k(c),$$

then we have

$$\overline{G_{d,m,n}}(c) = (f_1(c) \cdots f_k(c))^{M_{m,n}}.$$

Let $H(c) \in \mathbb{Z}[c]$ be any irreducible factor of $G_{d,m,n}(c)$, and take c_0 to be a root of $H(c)$. If we can show that $\overline{H}(c) = (A(c))^{M_{m,n}}$ for some $A(c) \in \mathbb{F}_d[c]$, this will clearly prove the theorem. Assume for the sake of contradiction that $\overline{H}(c) = f_1(c)^{\alpha_1} \cdots f_k(c)^{\alpha_k}$, where for at least one i we have $0 < \alpha_i < M_{m,n}$. This gives $H(c) = f_1(c)^{\alpha_1} \cdots f_k(c)^{\alpha_k} + dH_1(c)$ for some $H_1(c) \in \mathbb{Z}[c]$. In particular, we have $f_1(c_0)^{\alpha_1} \cdots f_k(c_0)^{\alpha_k} = -dH_1(c_0)$. The last equality implies that the product $(d, \widetilde{f}_1(c_0))^{\alpha_1} \cdots (d, \widetilde{f}_k(c_0))^{\alpha_k}$ is contained in the ideal (d), because all the generators of the product ideal are divisible by d. This gives

$$(d) | (d, \widetilde{f}_1(c_0))^{\alpha_1} \cdots (d, \widetilde{f}_k(c_0))^{\alpha_k}. \tag{2.4}$$

Now (2.3) and (2.4) together will clearly imply that if $\alpha_i < M_{m,n}$, then $(d, \widetilde{f}_i(c_0))$ must be the unit ideal in $\mathcal{O}_K$, which contradicts Lemma 2.5.

Hence, we conclude that for all i we have $\alpha_i = 0$ or $\alpha_i = M_{m,n}$, which shows that $\overline{H}(c) = (A(c))^{M_{m,n}}$ for some $A(c) \in \mathbb{F}_d[c]$, as desired. $\square$

3. Proof of Theorem 1.9

The goal of this section is to prove Theorem 1.9. We start by recalling a basic fact from algebraic number theory:

Theorem 3.1 ([8])**.** *Let $K/\mathbb{Q}$ be an algebraic number field of degree n with ring of integers $\mathcal{O}_K$ and discriminant D_K. Let $\alpha \in \mathcal{O}_K$ with minimal polynomial $f(x)$ be such that $K = \mathbb{Q}(\alpha)$. Then*

$$\operatorname{Disc}(f(x)) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 D_K.$$

Understanding the rational primes which divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is important for the following reason: By Dedekind's Factorization Theorem, for a rational prime p not dividing the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, the factorization of the ideal (p) in $\mathcal{O}_K$ can be obtained from the factorization of the reduced polynomial $\overline{f}(x) \in \mathbb{F}_p[x]$ (See for instance [10] for a precise statement).

Next, we recall Dedekind's criterion (see for instance [4, Theorem 6.1.4]), which will be the most important tool for the proof of Theorem 1.9.

Theorem 3.2. *Let α be an algebraic integer, f its minimal polynomial, $K = \mathbb{Q}(\alpha)$, and $\mathcal{O}_K$ its ring of integers. Let p be a rational prime. Let $\overline{f} = f_1^{e_1} \cdots f_k^{e_k}$ be the decomposition of $\overline{f}$ in $\mathbb{F}_p[x]$. Let $\widetilde{f}_i \in \mathbb{Z}[x]$ be any lift of f_i, and $g \in \mathbb{Z}[x]$ such that $f = \widetilde{f_1}^{e_1} \cdots \widetilde{f_k}^{e_k} + pg$. The following are equivalent:*

(a) $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

(b) *For all i, either $e_i = 1$ or f_i does not divide $\overline{g}$ in $\mathbb{F}_p[x]$.*

We also need the following lemma, which is a special case of Lemma 23 in [3]. We give an alternative proof in this special case.

Lemma 3.3. *Let d be a prime. Then we have*

$$\operatorname{Res}(G_{d,m,n}, G_{d,0,k}) = \begin{cases} \pm d^{\deg(G_{d,0,n})} & \text{if } n = k \\ \pm 1 & \text{if } n \neq k. \end{cases}$$

Proof. Suppose $G_{d,m,n}(c) \in \mathbb{Z}[c]$ factors as

$$G_{d,m,n}(c) = H_1(c) \cdots H_l(c)$$

for some $H_1(c), \dots, H_l(c) \in \mathbb{Z}[c]$, and let $c_1, \dots, c_l$ be some roots of $H_1(c)$, $\dots, H_l(c)$, respectively. Set $K_i = \mathbb{Q}(c_i)$ for $i = 1, \dots, l$. Also define $a_s^{(i)} = f_{c_i,d}^s(0)$ for $i = 1, \dots, l$. Note that we have

$$\operatorname{Res}(G_{d,m,n}, G_{d,0,k}) = \prod_{i=1}^{l} \operatorname{Res}(H_i, G_{d,0,k}).$$

Recall as in the proof of Lemma 2.5 that $\mathrm{Res}(H_i, G_{d,0,k}) = N_{K_i/\mathbb{Q}}(G_{d,0,k}(c_i))$ for $i = 1, \dots, l$. Then, if $k = n$, we obtain

$$\mathrm{Res}(H_i, G_{d,0,k}) = \mathrm{Res}(H_i, G_{d,0,n}) = N_{K_i/\mathbb{Q}}(G_{d,0,n}(c_i)) = \pm N_{K_i/\mathbb{Q}}(a_n^{(i)}) = \pm d^{\frac{\deg(H_i)}{M_{m,n}}},$$

where the third equality follows from Lemma 2.2, and the last equality follows by using the fact that norm is multiplicative, because we have $(a_n^{(i)})^{M_{m,n}} = (d)$ in $\mathcal{O}_{K_i}$ (from Theorem 2.1). Thus, we get

$$\mathrm{Res}(G_{d,m,n}, G_{d,0,k}) = \prod_{i=1}^{l} \mathrm{Res}(H_i, G_{d,0,k}) = \pm d^{\frac{\deg(G_{d,m,n})}{M_{m,n}}} = \pm d^{\deg(G_{d,0,n})},$$

which gives us the result we want. Note that we used Lemma 2.3 for the last equality. Now assume $k \neq n$. First note that we will be done if we can show that $\mathrm{Res}(H_i, G_{d,0,k}) = \pm 1$ for $i = 1, \dots, l$. There are two cases: Either $n|k$ or $n \nmid k$. If $n|k$, since the sequence $\{a_j^{(i)}\}_{j\geq 1}$ is a rigid divisibility sequence, and $G_{d,0,k}(c_i)$ is the primitive part of $a_k^{(i)}$ for $i = 1, \dots, l$, it follows that $G_{d,0,k}(c_i)$ divides $\frac{a_k^{(i)}}{a_n^{(i)}}$ in $\mathbb{Z}[c_i]$, which, by Theorem 2.1, implies that $G_{d,0,k}(c_i)$ is a unit in $\mathcal{O}_{K_i}$, i.e. $N_{K_i/\mathbb{Q}}(G_{d,0,k}(c_i)) = \pm 1$, which gives $\mathrm{Res}(H_i, G_{d,0,k}) = \pm 1$. If $n \nmid k$, then $a_k^{(i)}$ is a unit in $\mathcal{O}_{K_i}$ for $i = 1, \dots, l$, but $G_{d,0,k}(c_i)$ divides $a_k^{(i)}$ in $\mathbb{Z}[c_i]$, hence $G_{d,0,k}(c_i)$ is a unit in $\mathcal{O}_{K_i}$, i.e. $N_{K_i/\mathbb{Q}}(G_{d,0,k}(c_i)) = \pm 1$, which again implies that $\mathrm{Res}(H_i, G_{d,0,k}) = \pm 1$, as desired. □

We are finally ready to prove Theorem 1.9.

Proof of Theorem 1.9. Using the proof of Theorem 1.4, we can write the factorization of $G_{d,m,n}(c)$ over $\mathbb{Q}$ as

$$G_{d,m,n}(c) = (A_1(c)^{M_{m,n}} + dB_1(c)) \cdots (A_l(c)^{M_{m,n}} + dB_l(c))$$

for some $A_1, \dots, A_l, B_1, \dots, B_l \in \mathbb{Z}[c]$, and note that $A_i(c) \in \mathbb{Z}[c]$ are not necessarily irreducible. By Dedekind's criterion, to prove that $d \nmid [\mathcal{O}_K : \mathbb{Z}[c_0]]$ for any root c_0 of $G_{d,m,n}(c)$, it suffices to show that $\overline{A}_i(c)$ and $\overline{B}_i(c)$ have no common factor in $\mathbb{F}_d[c]$ for $i = 1, \dots, l$. To prove this, we will do some computations with resultants.

Using Lemma 2.3, we can write

$$G_{d,0,n}(c) = A_1(c) \cdots A_l(c) + dG(c) \tag{3.1}$$

for some $G(c) \in \mathbb{Z}[c]$. First let

$$X_1 = \mathrm{Res}\Big(A_1(c)^{M_{m,n}} + dB_1(c), G_{d,0,n}(c)\Big)\mathrm{Res}(A_2(c) \cdots A_l(c), G_{d,0,n}(c)). \tag{3.2}$$

Hence, we have

$$X_1 = \mathrm{Res}\Big(A_1(c)^{M_{m,n}} A_2(c) \cdots A_l(c) + dA_2(c) \cdots A_l(c)B_1(c), G_{d,0,n}(c)\Big).$$

Using (3.1), this gives

$$X_1 = \mathrm{Res}\Big(G_{d,0,n}(c)A_1(c)^{M_{m,n}-1} + dA_2(c)\cdots A_l(c)B_1(c) - dG(c)A_1(c)^{M_{m,n}-1}, G_{d,0,n}(c)\Big). \tag{3.3}$$

Thus, by the basic properties of resultants, we get

$$\begin{aligned} X_1 &= \mathrm{Res}\Big(d\Big(A_2(c)\cdots A_l(c)B_1(c) - G(c)A_1(c)^{M_{m,n}-1}\Big), G_{d,0,n}(c)\Big) \\ &= d^{\deg(G_{d,0,n})}\,\mathrm{Res}\Big(A_2(c)\cdots A_l(c)B_1(c) - G(c)A_1(c)^{M_{m,n}-1}, G_{d,0,n}(c)\Big). \end{aligned} \tag{3.4}$$

On the other hand, using (3.1) in the second factor in (3.2), we also have

$$\begin{aligned} X_1 &= \mathrm{Res}\Big(A_1(c)^{M_{m,n}} + dB_1(c), G_{d,0,n}(c)\Big)\,\mathrm{Res}(A_2(c)\cdots A_l(c), A_1(c)\cdots A_l(c) + dG(c)) \\ &= \mathrm{Res}\Big(A_1(c)^{M_{m,n}} + dB_1(c), G_{d,0,n}(c)\Big)\,\mathrm{Res}(A_2(c)\cdots A_l(c), G(c))d^{\deg(A_2(c)\cdots A_l(c))} \end{aligned} \tag{3.5}$$

Hence, in (3.4) and (3.5), we obtained two different expressions for X_1. Doing the same thing for each $1 \leq i \leq l$, and multiplying out X_is, we will obtain two different expressions for the product $X_1 \cdots X_l$. Namely, if we write each X_i similarly to (3.4), we get

$$X_1\cdots X_l = d^{l\deg(G_{d,0,n})}\prod_{i=1}^{l}\mathrm{Res}\left(\frac{A_1(c)\cdots A_l(c)}{A_i(c)}B_i(c) - G(c)A_i(c)^{M_{m,n}-1}, G_{d,0,n}\right). \tag{3.6}$$

On the other hand, if we write each X_i similarly to (3.5), we obtain

$$\begin{aligned} X_1\dots X_l &= \mathrm{Res}\left(\prod_{i=1}^{l}(A_i(c)^{M_{m,n}} + dB_i(c)), G_{d,0,n}(c)\right)\mathrm{Res}(A_1(c)\cdots A_l(c), G(c))^{l-1}d^{(l-1)\deg(G_{d,0,n})} \\ &= \mathrm{Res}(G_{d,m,n}(c), G_{d,0,n}(c))\,\mathrm{Res}(A_1(c)\cdots A_l(c), G(c))^{l-1}d^{(l-1)\deg(G_{d,0,n})} \\ &= \pm d^{l\deg(G_{d,0,n})}\,\mathrm{Res}(A_1(c)\cdots A_l(c), G(c))^{l-1}, \end{aligned} \tag{3.7}$$

where the last equality follows from Lemma 3.3. Hence, equating (3.6) and (3.7), and simplifying, we get

$$\pm(\mathrm{Res}(A_1(c)\cdots A_l(c), G(c)))^{l-1} = \prod_{i=1}^{l}\mathrm{Res}\left(\frac{A_1(c)\cdots A_l(c)}{A_i(c)}B_i(c) - G(c)A_i(c)^{M_{m,n}-1}, G_{d,0,n}\right). \tag{3.8}$$

Recall that our goal was to show that $\overline{A}_i(c)$ and $\overline{B}_i(c)$ have no common factors in $\mathbb{F}_d[c]$. Recalling (3.1), it is clear that to prove this, it suffices to show that the right-hand side of (3.8) is not divisible by d. So, we will be done if we can show that $\mathrm{Res}(A_1(c)\cdots A_l(c), G(c))$ is not divisible by d, i.e., it is enough to show that $\mathrm{Res}(A_i(c), G(c))$ is not divisible by d for each i. We need the following lemma to achieve this.

Lemma 3.4. *Let p be a rational prime, $f(x) \in \mathbb{Z}[x]$ a monic polynomial (not necessarily irreducible) such that* $\mathrm{Disc}(f)$ *is relatively prime to p. Suppose that the reduced polynomial $\overline{f}(x) \in \mathbb{F}_p[x]$ factors as*

$$\overline{f}(x) = f_1(x)\cdots f_k(x),$$

where $f_1(x), \ldots, f_k(x) \in \mathbb{F}_p[x]$ *are irreducible. Then we can choose lifts* $\widetilde{f_1}(x), \ldots, \widetilde{f_k}(x) \in \mathbb{Z}[x]$ *of* $f_1(x), \ldots, f_k(x)$*, respectively, and write* $f(x) = \widetilde{f_1}(x) \cdots \widetilde{f_k}(x) + pF(x)$ *such that* $\mathrm{Res}(\widetilde{f_i}(x), F(x))$ *is relatively prime to* p *for all* i*.*

Proof of Lemma 3.4. Considering the factorization of $f(x) \in \mathbb{Z}[x]$, without loss of generality, we can write

$$f(x) = (\widetilde{f}_1(x) \cdots \widetilde{f}_{i_1}(x) + pF_1(x)) \cdots (\widetilde{f}_{i_{l-1}+1}(x) \cdots \widetilde{f}_{i_l}(x) + pF_l(x)).$$

Then we have $f(x) = \widetilde{f}_1(x) \cdots \widetilde{f}_k(x) + pF(x)$, where

$$F(x) = F_1(x)\widetilde{f}_{i_1+1}(x) \cdots \widetilde{f}_{i_l}(x) + \widetilde{f}_1(x)K(x) + pL(x)$$

for some $K(x), L(x) \in \mathbb{Z}[x]$. We would like to have that $f_1(x)$ and $\overline{F}(x)$ have no common factor in $\mathbb{F}_p[x]$. (This will finish the proof, because one can then do the same thing for all i.) We have

$$\overline{F}(x) = \overline{F_1}(x) f_{i_1+1}(x) \cdots f_{i_l}(x) + f_1(x)\overline{K}(x).$$

If $\overline{F}(x)$ and $f_1(x)$ had a common factor in $\mathbb{F}_p[x]$, then $\overline{F_1}(x) f_{i_1+1} \cdots f_{i_l}(x)$ and $f_1(x)$ would have a common factor in $\mathbb{F}_p[x]$. But, this would force $\overline{F_1}(x)$ and $f_1(x)$ to have a common factor in $\mathbb{F}_p[x]$, since $\mathrm{Disc}(f)$ is relatively prime to p. So, if f_1 and $\overline{F}_1(x)$ have no common factor in $\mathbb{F}_p[x]$, we are already done. If they have a common factor, replace $\widetilde{f}_1(x)$ by $\widetilde{g}_1(x) = \widetilde{f}_1(x) + p$, which, since $\widetilde{f}_1(x) \cdots \widetilde{f}_{i_1}(x) + pF_1(x)$ is a fixed polynomial in $\mathbb{Z}[x]$, will replace $F_1(x)$ by $G_1(x) = F_1(x) - \widetilde{f}_2(x) \cdots \widetilde{f}_{i_1}(x)$. Now $\overline{\widetilde{g}}_1(x) = f_1(x)$ cannot have a common factor with $\overline{G}_1(x)$ in $\mathbb{F}_p[x]$, because $f_1(x) | \overline{F}_1(x)$ (since $f_1(x)$ and $\overline{F}_1(x)$ are assumed to have a common factor, and $f_1(x) \in \mathbb{F}_p[x]$ is irreducible), and f_1 is relatively prime to f_j in $\mathbb{F}_p[x]$ for $j = 2, \ldots, i_1$ (recall that $\mathrm{Disc}(f)$ was relatively prime to p). It is easy to see that we can do the same thing for each f_i without affecting the fact that f_j and $\overline{F}_1$ have no common factor in $\mathbb{F}_p[x]$ for $j < i$, which finishes the proof. ☐

Noting that $\mathrm{Disc}(G_{d,0,n})$ is relatively prime to d (see e.g. [2, Lemma 3]), now the proof of Theorem 1.9 clearly follows from Lemma 3.4. ☐

Corollary 3.5. *Let* d *be a prime and* $m \neq 0$*. Suppose that* c_0 *is a root of* $G_{d,m,n}(c)$*. Set* $K = \mathbb{Q}(c_0)$*. Then all the elements in the critical orbit* $\{a_1, \ldots, a_{m+n-1}\}$ *of* $f_{c,d}$ *are square-free in* $\mathcal{O}_K$*.*

Proof. Note that if $n \nmid i$, then a_i is a unit in $\mathcal{O}_K$ by Theorem 2.1, so there is nothing to prove. We also know from Theorem 2.1 that $(a_n) = (a_{nk})$ in $\mathcal{O}_K$ for any $k \geq 1$, so it is enough to prove that a_n is square-free in $\mathcal{O}_K$. Recall from Proposition 2.6 that we have

$$(a_n) = (d, \widetilde{f_1}(c_0)) \cdots (d, \widetilde{f_k}(c_0)), \tag{3.9}$$

where $\widetilde{f}_1, \ldots, \widetilde{f}_k$ are some lifts of the irreducible factors $f_1, \ldots, f_k \in \mathbb{F}_d[c]$ of the reduced polynomial $\overline{G_{d,0,n}}(c) \in \mathbb{F}_d[c]$. Let $H(c) \in \mathbb{Z}[c]$ be the minimal polynomial of c_0. It is clear from the proof of Theorem 1.4 that

$$\overline{H}(c) = (f_{i_1}(c) \ldots f_{i_t}(c))^{M_{m,n}}$$

for some $i_1, \ldots, i_t \in \{1, \ldots, k\}$. Then, Lemma 2.5 implies that for any $j \in \{1, \ldots k\}$, $(d, \widetilde{f}_j(c_0))$ is not the unit ideal if and only if $j \in \{i_1, \ldots, i_t\}$. Hence, we can rewrite (3.9) as

$$(a_n) = (d, \widetilde{f}_{i_1}(c_0)) \cdots (d, \widetilde{f}_{i_t}(c_0)). \tag{3.10}$$

But, since we know from Theorem 1.9 that $d \nmid [\mathcal{O}_K : \mathbb{Z}[c_0]]$, combining (3.10) with Dedekind's Factorization Theorem will imply that $(d, \widetilde{f}_{i_1}(c_0)), \ldots,$ $(d, \widetilde{f}_{i_t}(c_0))$ are distinct prime ideals in $\mathcal{O}_K$, which proves that a_n is square-free in $\mathcal{O}_K$, as desired. $\square$

Remark 3.6. The author's interest in Corollary 3.5 comes from the questions related to the irreducibility of iterates of polynomials. For a field K, we call a polynomial $f(x) \in K[x]$ *stable* if all of its iterates are irreducible over K. In our special case, it is known that $f_{c,d}$ is stable if the critical orbit of $f_{c,d}$ does not contain $\pm d$th power ([6, Theorem 8]). Corollary 3.5 implies that non-unit elements in the orbit cannot be $\pm d$th power. This establishes stability in the case $n = 1$, because in that case there is no unit in the orbit (by Theorem 2.1). This was already proven in [5, Corollary 1.2]. In other words, Corollary 3.5 can be thought of as a mild generalization of [5, Corollary 1.2].

References

[1] R. BENEDETTO, P. INGRAM, R. JONES, M. MANES, J. H. SILVERMAN & T. J. TUCKER, "Current trends and open problems in arithmetic dynamics", *Bull. Am. Math. Soc.* **56** (2019), no. 4, p. 611-685.

[2] X. BUFF, "On postcritically finite unicritical polynomials", *New York J. Math.* **24** (2018), p. 1111-1122.

[3] X. BUFF, A. L. EPSTEIN & S. KOCH, "Rational maps with a preperiodic critical point", `https://arxiv.org/abs/1806.11221`, 2018.

[4] H. COHEN, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer, 1993.

[5] V. GOKSEL, "On the orbit of a post-critically finite polynomial of the form $x^d + c$", *Funct. Approximatio, Comment. Math.* **62** (2020), no. 1, p. 95-104.

[6] S. HAMBLEN, R. JONES & K. MADHU, "The density of primes in orbits of $z^d + c$", *Int. Math. Res. Not.* **2015** (2015), no. 7, p. 1924-1958.

[7] B. HUTZ & A. TOWSLEY, "Misiurewicz points for polynomial maps and transversality", *New York J. Math.* **21** (2015), p. 297-319.

[8] S. LANG, *Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 110, Springer, 1994.

[9] N. R. LOOPER, "Dynamical Galois groups of trinomials and Odoni's conjecture", *Bull. Lond. Math. Soc.* **51** (2019), no. 2, p. 278-292.

[10] D. A. MARCUS, *Number Fields*, Universitext, Springer, 1977.

[11] J. MILNOR, “Arithmetic of unicritical polynomial maps”, in *Frontiers in Complex Dynamics: In Celebration of John Milnor’s 80th Birthday*, Princeton University Press, 2012, p. 15-23.
[12] J. H. SILVERMAN, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241, Springer, 2007.

Vefa GOKSEL
Department of Mathematics and Statistics
Lederle Graduate Research Tower, 1623D
University of Massachusetts Amherst
710 N. Pleasant Street
Amherst, MA 01003-9305, USA
E-mail: `goksel@math.umass.edu`