Dynamical irreducibility of polynomials modulo primes

László Mérai¹ · Alina Ostafe² · Igor E. Shparlinski²

Received: 2 September 2019 / Accepted: 24 September 2020 / Published online: 4 November 2020
© Springer-Verlag GmbH Germany, part of Springer Nature 2020

Abstract
For a class of polynomials \( f \in \mathbb{Z}[X] \), which in particular includes all quadratic polynomials, and also trinomials of some special form, we show that, under some natural conditions (necessary for quadratic polynomials), the set of primes \( p \) such that all iterations of \( f \) are irreducible modulo \( p \) is of relative density zero. Furthermore, we give an explicit bound on the rate of the decay of the density of such primes in an interval \([1, Q]\) as \( Q \to \infty \). For this class of polynomials this gives a more precise version of a recent result of Ferraguti (Proc Am Math Soc 146:2773–2784, 2018), which applies to arbitrary polynomials but requires a certain assumption about their Galois group. Furthermore, under the Generalised Riemann Hypothesis we obtain a stronger bound on this density.

1 Introduction

1.1 Motivation

For a polynomial \( f \in \mathbb{K}[X] \) over a field \( \mathbb{K} \) we define the sequence of polynomials:

\[
f^{(0)}(X) = X, \quad f^{(n)}(X) = f\left(f^{(n-1)}(X)\right), \quad n = 1, 2, \ldots.
\]

The polynomial \( f^{(n)} \) is called the \( n \)-th iterate of the polynomial \( f \).

Following the established terminology, see [1,2,8,9,14,16], one says that a polynomial \( f \in \mathbb{K}[X] \) is stable if all iterates \( f^{(n)}(X) \), \( n = 1, 2, \ldots \), are irreducible over \( \mathbb{K} \). However, we prefer to use the more informative terminology introduced by Heath-Brown and Micheli [12] and instead we call such polynomials dynamically irreducible.

---

¹ Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenberger Straße 69, 4040 Linz, Austria
² School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia
For a polynomial $f \in \mathbb{Q}[X]$ and a prime $p$ we define $\tilde{f}_p \in \mathbb{F}_p[X]$ to be the reduction of $f$ modulo $p$. In this paper we consider the following question, see [3, Question 19.12].

**Open Question 1.1** Let $f \in \mathbb{Q}[X]$ be a dynamically irreducible polynomial of degree $d \geq 2$. Is it true that the set of primes

$$\{ p : \tilde{f}_p \text{ is dynamically irreducible over } \mathbb{F}_p \}$$

is a finite set?

For example, Jones [15, Conjecture 6.3] has conjectured that $x^2 + 1$ is dynamically irreducible over $\mathbb{F}_p$ if and only if $p = 3$. Ferraguti [7, Theorem 2.3] has shown that if the size of the Galois group $\text{Gal}(f^{(n)})$ of $f^{(n)}$ is asymptotically close to its largest possible value then the set of primes (1.1) has density zero. It is natural to assume that this condition on the size of $\text{Gal}(f^{(n)})$ is generically satisfied, however it may be difficult to verify it for concrete polynomials or find examples of such polynomials.

Here we consider a special class of polynomials which includes trinomials of the form $f(X) = aX^d + bX^{d-1} + c \in \mathbb{Z}[X]$ of even degree, and hence all quadratic polynomials. For these polynomials, we prove such a zero-density result for the set of primes (1.1), which holds under some mild assumptions, that are also easily verifiable from the initial data. Moreover, combining

- some effective results from Diophantine geometry [4],
- the square-sieve of Heath–Brown [11],
- a slightly refined bound of character sums over almost-primes from [18],

we obtain an explicit saving in our density estimate.

Furthermore, assuming the generalised Riemann hypothesis (GRH), we obtain a stronger bound.

We believe these techniques have never been used before in this combination and for similar purposes. Hence we expect that this approach may find several other applications.

**1.2 Main results**

Clearly, it is enough to consider the distribution of primes for which $\tilde{f}_p$ is dynamically irreducible in dyadic intervals of the form $[Q, 2Q]$. Thus, given a polynomial $f(X) \in \mathbb{Z}[X]$ we define

$$P_f(Q) = \#\{ p \in [Q, 2Q] \cap \mathcal{P} : \tilde{f}_p \text{ is dynamically irreducible over } \mathbb{F}_p \},$$

where $\mathcal{P}$ denotes the set of primes.

**Theorem 1.2** Let $f(X) \in \mathbb{Z}[X]$ be such that the derivative $f'(X)$ is of the form

$$f'(X) = g(X)^2(aX + b), \quad g(X) \in \mathbb{Z}[X], \quad a, b \in \mathbb{Z}, \quad a \neq 0.$$ 

Assume that $\gamma = -b/a$ is not a pre-periodic point of $f$. Then one has

$$P_f(Q) \leq \frac{(\log \log \log \log Q)^{2+\alpha(1)}}{\log \log Q} \cdot \frac{Q}{\log Q}, \quad \text{as } Q \to \infty.$$ 

Obviously all quadratic polynomials have their derivatives of the form required in Theorem 1.2.
We also note that for quadratic polynomials the condition of $\gamma$ not to be a pre-periodic point of $f$ in Theorem 1.2 is necessary, as otherwise using [16, Lemma 2.5] (see also [17, Lemma 2.5']) one can produce all primes in an arithmetic progression contained in the set (1.1). For example, for the polynomial $f(X) = (X - 2)^2 + 2$ with $\gamma = 2$, the reduction $\tilde{f}_p$ is dynamically irreducible for all primes $p \equiv 5 \mod 8$. This example also shows that the condition is needed for higher degree polynomials as well, for example, consider $g(X) = f^{(k)}(X)$ for some $k \geq 2$, which is a polynomial of degree $2^k$ and by the above $g$ is also dynamically irreducible for all primes $p \equiv 5 \mod 8$.

One can give similar examples for odd degrees as well. For example, it follows from [20, Theorem 3.75] that for the polynomial $f(X) = (X + 2)^3 - 2$, $\tilde{f}_p$ is dynamically irreducible if
\[ 2 \text{ is a cubic non-residue modulo } p \text{ and } p \equiv 4, 7 \mod 9. \tag{1.4} \]

The set of such primes $p$ that 2 is a cubic residue modulo $p$, or equivalently, of the form $p = x^2 + 27y^2$ with integers $x$ and $y$, by [6, Theorem 9.12], is of Dirichlet density at most $1/7(-108) < 1/3$ (see, for example, [6, Equation (2.14)]). Thus the set of primes (1.4) is of positive Dirichlet density.

We now exhibit a larger class of polynomials of higher degree to which Theorem 1.2 applies.

**Corollary 1.3** Let $f(X) = r(X - u)^d + s(X - u)^{d-1} + t \in \mathbb{Z}[X]$ with some $r, s, t, u \in \mathbb{Z}$, $r \neq 0$, be such that $d$ is even and
\[ \gamma = u - (d - 1)s \]
is not a pre-periodic point of $f$. Then
\[ P_f(Q) \leq \frac{(\log \log \log \log Q)^{2+\alpha(1)}}{\log \log Q} \cdot \frac{Q}{\log Q}, \quad \text{as } Q \to \infty. \]

We now give conditional (on the GRH) estimates.

**Theorem 1.4** Let $f(X) \in \mathbb{Z}[X]$ be such that the derivative $f'(X)$ is of the form (1.3). Assume that $\gamma = -b/a$ is not a pre-periodic point of $f$. Then, assuming the GRH, for $Q \geq 3$,
\[ P_f(Q) = O\left(\frac{Q}{\log Q \log \log Q}\right), \]
where the implied constant depends only on $f$.

Accordingly, we also have:

**Corollary 1.5** Let $f(X) = r(X - u)^d + s(X - u)^{d-1} + t \in \mathbb{Z}[X]$ with some $r, s, t, u \in \mathbb{Z}$, $r \neq 0$, be such that $d$ is even and
\[ \gamma = u - (d - 1)s \]
is not a pre-periodic point of $f$. Then, assuming the GRH, for $Q \geq 3$,
\[ P_f(Q) = O\left(\frac{Q}{\log Q \log \log Q}\right), \]
where the implied constant depends only on $f$. 
We note that \( s = 0 \) is admissible in Corollaries 1.3 and 1.5 and thus they apply to binomials of the form \( r(X - u)^d + t \), which (for \( r = 1 \) and \( u = 0 \)) are commonly studied in arithmetic dynamics. Specially, Corollary 1.3 also answers a weakened version of a conjecture of Jones [15, Conjecture 6.3].

2 Preliminaries

2.1 Notation, general conventions and definitions

Throughout the paper, \( p \) always denotes a prime number.

For a prime \( p \), \( v_p : \mathbb{Q}^* \to \mathbb{Z} \) represents the usual \( p \)-adic valuation, that is, for \( a \in \mathbb{Z} \setminus \{0\} \), we let \( v_p(a) = k \) if \( p^k \) is the highest power of \( p \) which divides \( a \), and for \( a, b \in \mathbb{Z} \setminus \{0\} \) we let \( v_p(a/b) = v_p(a) - v_p(b) \).

We define the Weil logarithmic height of \( a/b \in \mathbb{Q} \) as
\[
h(a/b) = \max \{ \log |a|, \log |b| \},
\]
with the convention \( h(0) = 0 \).

We use the Landau symbol \( O \) and the Vinogradov symbol \( \ll \). Recall that the assertions \( U = O(V) \) and \( U \ll V \) are both equivalent to the inequality \( |U| \leq cV \) with some absolute constant \( c > 0 \). To emphasize the dependence of the implied constant (or a list of parameters) \( \rho \), we write \( U = O_\rho(V) \) or \( U \ll_\rho V \).

2.2 Basic properties of resultants

Here we recall the following well known properties of resultants of polynomials, see [24], that hold over any field \( \mathbb{K} \).

Lemma 2.1 Let \( f, g \in \mathbb{K}[X] \) be polynomials of degrees \( d \geq 1 \) and \( e \geq 1 \), respectively, and let \( h \in \mathbb{K}[X] \). Denote by \( \beta_1, \ldots, \beta_e \) the roots of \( g \) in an extension field. Then we have:

(i) \( \text{Res}(f, g) = (-1)^{de} g_e^d \prod_{i=1}^e f(\beta_i) \),
(ii) \( \text{Res}(fg, h) = \text{Res}(f, h) \text{Res}(g, h) \),

where \( g_e \) is the leading coefficient of \( g \).

2.3 Dynamically irreducible polynomials

The following result gives a necessary condition that a polynomial is dynamically irreducible over a finite field of odd characteristic [9, Corollary 3.3].

Lemma 2.2 Let \( q \) be an odd prime power, and let \( f \in \mathbb{F}_q[X] \) be a dynamically irreducible polynomial of degree \( d \geq 2 \) with leading coefficient \( f_d \), nonconstant derivative \( f' \), \( \deg f' = k \leq d - 1 \). Then the following properties hold:

1. if \( d \) is even, then \( \text{Disc}(f) \) and \( f_d^k \text{Res}(f^{(n)}, f') \), \( n \geq 2 \), are nonsquares in \( \mathbb{F}_q \),
2. if \( d \) is odd, then \( \text{Disc}(f) \) and \( (-1)^{d-1} f_d^{(n-1)k+1} \text{Res}(f^{(n)}, f') \), \( n \geq 2 \), are squares in \( \mathbb{F}_q \).

We note that when \( d = 2 \), then by [16, Lemma 2.5] (see also [17, Lemma 2.5']) the condition of Lemma 2.2 is also sufficient.
2.4 Jacobi symbol

For \( n \geq 3 \), \( \left( \frac{a}{n} \right) \) denotes the Jacobi symbol, which is identical to the Legendre symbol if \( n \) is prime. We recall the following well-known properties, see [13, Section 3.5].

Lemma 2.3 For odd integers \( m, n \geq 3 \) we have

\[
\left( \frac{m}{n} \right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left( \frac{n}{m} \right) \quad \text{and} \quad \left( \frac{2}{n} \right) = (-1)^{\frac{n^2-1}{8}}.
\]

2.5 On some character sums over almost-primes

For \( \eta > 0 \), let \( \mathcal{P}(\eta, M) \) denote the set of positive integers \( m \leq M \) which do not have prime divisors \( p \leq M^{\eta} \). It is well known that for all positive \( \eta < 1 \) and \( M \geq 2 \) one has

\[
\#\mathcal{P}(\eta, M) \ll \frac{M}{\eta \log M},
\]

(2.1)

see [23, Part III, Theorem 6.4 and Equation (6.23)].

One important tool in the proof of Theorem 1.2 is the following result which is a slightly more precise form of [18, Corollary 10]. Namely, it is easy to trace the dependence of \( \eta \) in the second term of the bound of [18, Corollary 10] and see that the term \( O_\eta(M^{1-\eta}) \) can be refined as \( O(\eta^{-2}M^{1-\eta}) \). More precisely, we have:

Lemma 2.4 For any \( \varepsilon > 0 \) there exists some \( \eta_0 > 0 \) such that for any positive \( \eta < \eta_0 \), integer \( M \geq q^{1/3+\varepsilon} \), where \( q \geq 2 \) is not a perfect square, we have

\[
\left| \sum_{m \in \mathcal{P}(\eta, M)} \left( \frac{m}{q} \right) \right| \ll \eta^{-1/2} M \frac{1}{\log M} + \eta^{-2} M^{1-\eta}.
\]

Furthermore, under the GRH we have a rather strong bound for sums over primes, see [21, Equation (13.21)]

Lemma 2.5 For any positive integers \( q \) and \( M \), where \( q \geq 2 \) is not a perfect square, we have

\[
\left| \sum_{p \leq M} \left( \frac{p}{q} \right) \right| \ll M^{1/2} \log(qM).
\]

2.6 Integer solutions to hyperelliptic equations

We also need the following effective result of Bérczes et al. [4, Theorem 2.2], which bounds the height of \( S \)-integer solutions to a hyperelliptic equation. We present it in the form needed for the proof of Theorem 1.2.

Let \( S \) be a finite set of primes of cardinality \( s = \#S \) and define \( \mathbb{Z}_S \) to be the ring of \( S \)-integers, that is, the set of rational numbers \( r \) with \( v_p(r) \geq 0 \) for any \( p \notin S \). Put

\[
Q_S = \prod_{p \in S} p.
\]
**Lemma 2.6** Let \( f \in \mathbb{Z}_S[X] \) be a polynomial of degree \( d \geq 3 \) without multiple zeros, and let \( b \in \mathbb{Z}_S \) be a nonzero \( S \)-integer. If \( x, y \in \mathbb{Z}_S \) are solutions to the equation

\[
f(x) = by^2,
\]

then

\[
h(x), h(y) \leq (4ds)^{21d^3} Q_S^{20d^3} \exp(O_f(h(b))).
\]

**2.7 On the height of some iterates and resultants**

We need the following simple estimates on the height of some iterates and resultants:

**Lemma 2.7** Let \( f \in \mathbb{Q}[X] \) be a polynomial of degree \( d \geq 1 \) and let \( \gamma \in \overline{\mathbb{Q}} \). Then, there exists a constant \( C_f \) depending only on \( f \) such that for any \( n \geq 1 \) we have

\[
h\left(f^{(n)}(\gamma)\right) \geq d^n (h(\gamma) - C_f).
\]

**Proof** The proof follows inductively applying [22, Theorem 3.11], this inequality is also given in [22, Equation (3.8)].

We remark in Lemma 2.7 we do not insist that \( \gamma \) is pre-periodic. Indeed, if it is, then \( h(\gamma) \) is bounded and adjusting \( C_f \) we can make the result to be trivially correct.

**Lemma 2.8** Let \( f \in \mathbb{Q}[X] \) be a polynomial of degree \( d \geq 1 \). Then, for any \( n \geq 1 \), we have

\[
h\left(\text{Res}\left(f^{(n)}, f'\right)\right) = O_f\left(d^n\right).
\]

**Proof** Let \( f_d \) be the leading coefficient of \( f \) and \( \gamma_1, \ldots, \gamma_{d-1} \) be the roots of the derivative \( f' \). Then \( \text{Res}\left(f^{(n)}, f'\right) \) is defined by

\[
\text{Res}\left(f^{(n)}, f'\right) = (-1)^{dn(d-1)} (df_d)^{dn} \prod_{i=1}^{d-1} f^{(n)}(\gamma_i).
\]

We have

\[
h\left((df_d)^{dn}\right) \leq d^n (\log |d| + h(f_d)) \ll_f d^n. \tag{2.2}
\]

Applying [22, Theorem 3.11], we also have

\[
h\left(f^{(n)}(\gamma_i)\right) \ll_f d^n. \tag{2.3}
\]

Putting (2.2) and (2.3) together, we conclude the proof.

**3 Proof of Theorem 1.2**

**3.1 An application of the square-sieve**

We can assume that \( f \) is dynamically irreducible over \( \mathbb{Q} \) as otherwise its reduction \( \bar{f}_p \) can be dynamically irreducible for at most just finitely many primes \( p \).
Let \( d = \deg f \). We can assume that \( Q \) is large enough, thus \( f \) and \( f' \) are of degrees \( d \) and \( d - 1 \), respectively, modulo any prime \( p \in [Q, 2Q] \). From the shape (1.3) of \( f' \) we see that \( d - 1 \) is odd (and thus \( d \) is even).

Let \( \varepsilon > 0 \). All of the constants in this proof may depend on \( \varepsilon \) and \( f \).

Put

\[
\begin{align*}
N &= c_1 \log \log Q \quad \text{and} \quad t = c_2 \log \log \log Q \\
\end{align*}
\]

with some sufficiently small constants \( c_1, c_2 > 0 \) fixed later.

Write

\[
\begin{align*}
f_d \cdot \text{Res} \left( f^{(n)}(x), f'(x) \right) &= 2v_n u_n, \quad v_2(u_n) = 0, \quad n \geq 2,
\end{align*}
\]

where \( f_d \) is the leading coefficient of \( f \).

By the Dirichlet principle there is a set \( N \subseteq [N, N + t] \) of size

\[
\#N \geq \frac{1}{4} t
\]

such that for all \( r, s \in N \) we have

\[
u_r \equiv u_s \mod 4 \quad \text{and} \quad \nu_r \equiv \nu_s \mod 2.
\]

Therefore, since \( u_n, n \geq 2 \), are odd, we have

\[
u_r + \nu_s \equiv 2 \mod 4 \quad \text{and} \quad v_r + v_s \equiv 0 \mod 2.
\]

Using that for an odd \( m \) we have \( 2 \mid m - 1 \) and \( 8 \mid m^2 - 1 \), we conclude that

\[
(-1)^{\frac{v_r+v_s-2}{2} \cdot \frac{1}{2} + (v_r + v_s) \mod 2} = 1.
\]

Consider

\[
S = \sum_{p \in [Q, 2Q]} \left| \sum_{n \in N} \left( f_d \cdot \text{Res} \left( f^{(n)}(x), f'(x) \right) \right) \right|^2.
\]

If \( \tilde{f}_p \) is dynamically irreducible modulo \( p \), then by Lemma 2.2, we have

\[
\sum_{n \in N} \left( f_d \cdot \text{Res} \left( f^{(n)}(x), f'(x) \right) \right) \equiv \sum_{n \in N} \left( f_d^{d-1} \cdot \text{Res} \left( f^{(n)}(x), f'(x) \right) \right) \equiv -\#N \leq -\frac{t}{4},
\]

as \( d - 1 \) is odd, thus

\[
P_f(Q) \leq 16 \frac{S}{t^2}, \tag{3.4}
\]

where \( P_f(Q) \) is defined by (1.2).

Let \( \eta_0 \) as in Lemma 2.4 and \( \eta < \eta_0 \) be chosen later. Then we extend the summation for integers \( m \in \mathcal{P}(\eta, 2Q) \), where \( \mathcal{P}(\eta, 2Q) \) is defined in Sect. 2.5, to obtain

\[
S \leq \sum_{m \in \mathcal{P}(\eta, 2Q)} \left| \sum_{n \in N} \left( f_d \cdot \text{Res} \left( f^{(n)}(x), f'(x) \right) \right) \right|^2.
\]
By Lemma 2.3, we have
\[ S \leq \sum_{m \in \mathcal{P}(\eta, 2Q)} \left| \sum_{n \in \mathcal{N}} (-1) \frac{a_{n_1} + a_{n_2} - 2 m - 1}{2} \nu_{a} \frac{m^2 - 1}{8} \left( \frac{m}{u_n} \right)^2 \right|. \]

By opening the square and changing the order of summation, we see from (3.3) that
\[ S \leq \sum_{n_1, n_2 \in \mathcal{N}} \sum_{m \in \mathcal{P}(\eta, 2Q)} \left( \frac{m}{u_{n_1} u_{n_2}} \right). \]

Let \( Z \) be the set of pairs \((n_1, n_2) \in \mathcal{N}^2 \) such that \( u_{n_1} u_{n_2} \) is a square. For a pair \((n_1, n_2) \notin Z\), we have by Lemma 2.8, that
\[ |u_{n_1} u_{n_2}|^{1/3 + \epsilon} \leq \exp \left( (1/3 + \epsilon) \left( h \left( f_d \text{Res} \left( f^{(n_1)}, f' \right) \right) + h \left( f_d \text{Res} \left( f^{(n_2)}, f' \right) \right) \right) \right) \leq \exp \left( O_f(d^{N+t}) \right) \leq Q \]
if \( c_1 \) and \( c_2 \) are small enough. Then by Lemma 2.4, and by (2.1) we have
\[ S \ll \frac{Q}{\eta \log Q} + r^2 \left( \eta^{\epsilon/4-1} \frac{Q}{\log Q} + \eta^{-2} Q^{1-\eta} \right). \]

Recalling (3.4), we now conclude
\[ P_f(Q) \ll \frac{\#Z}{t^2} \frac{Q}{\eta \log Q} + \eta^{\epsilon/4-1} \frac{Q}{\log Q} + \eta^{-2} Q^{1-\eta}. \quad (3.5) \]

In the next section, we give a bound on \#Z.

### 3.2 Perfect squares in denominators

We show that \( Z \) does not contain nontrivial (off-diagonal) pairs and hence
\[ \#Z = \#\mathcal{N} \leq t. \quad (3.6) \]

Let \( n_1 \neq n_2 \) be a pair of integers in \( \mathcal{N} \) such that \( u_{n_1} u_{n_2} \) is a square. We can assume that \( n_2 > n_1 \). Then, since
\[ u_{n_1} u_{n_2} = 2^{-v_{n_1} - v_{n_2}} f_d^2 \text{Res} \left( f^{(n_1)}, f' \right) \text{Res} \left( f^{(n_2)}, f' \right) \]
and, by Lemma 2.1,
\[ \text{Res} \left( f^{(n_1)}, f' \right) \text{Res} \left( f^{(n_2)}, f' \right) = \text{Res} \left( f^{(n_1)} f^{(n_2)}, f' \right), \]
we obtain, recalling (3.2), that
\[ \text{Res} \left( f^{(n_1)} f^{(n_2)}, f' \right) \]
is also a square.

Now, let
\[ f'(X) = g(X)^2(aX + b), \quad g(X) \in \mathbb{Z}[X], \quad a, b \in \mathbb{Z}, \quad a \neq 0. \]
Let $\beta_1, \ldots, \beta_m$ be the roots of $g$ (taken with multiplicities, that is, $m = (d - 2)/2$).

From here, using again Lemma 2.1, we obtain that
\[
\text{Res}\left(f^{(n_1)} f^{(n_2)}, f'\right) = (-1)^{(d-1)(d^{n_1}+d^{n_2})} (df_d)^{d^{n_1}+d^{n_2}} \prod_{i=1}^m \left(f^{(n_1)}(\beta_i)\right)^2 \left(f^{(n_2)}(\beta_i)\right)^2 f^{(n_1)}(\gamma) f^{(n_2)}(\gamma),
\]
where $\gamma = -b/a \in \mathbb{Q}$.

Now, since $d$ is even we have, that
\[
f^{(n_1)}(\gamma) f^{(n_2)}(\gamma)
\]
is a square in $\mathbb{Q}$.

We let $S$ be the set of primes, which consists of the prime divisors of $d$ and $a$. We thus have the equation
\[
\alpha f^{(n_2-n_1)}(\alpha) = \beta^2,
\]
where $\alpha = f^{(n_1)}(\gamma)$ and $\beta$ are $S$-integers in $\mathbb{Q}$, and $\deg f^{(n_2-n_1)}(X) \leq d'$. Since $f$ is dynamically irreducible of degree at least two, $f^{(n_2-n_1)}$ is irreducible and $X \nmid f^{(n_2-n_1)}(X)$ is a polynomial of degree at least 3 without multiple roots in $\mathbb{C}$. We can apply now Lemma 2.6 with the polynomial $X f^{(n_2-n_1)}(X)$. As the quantities $d$, $s$ and $Q_S$ depend only on $f$, we conclude that
\[
h(\alpha) \leq \exp(O_f(d^{4t})).
\]
(3.7)
On the other hand, since $\gamma$ is not a pre-periodic point of the polynomial $f$, there exists a positive integer $n_0$ depending only on $f$ such that $h\left(f^{(n_0)}(\gamma)\right) \geq C_f + 1$, where $C_f$ is defined as in Lemma 2.7. Applying then Lemma 2.7 we have
\[
h(\alpha) = h\left(f^{(n_1-n_0)}\left(f^{(n_0)}(\gamma)\right)\right) \geq d^{n_1-n_0} \left(h\left(f^{(n_0)}(\gamma)\right) - C_f\right) \geq d^{N-n_0}.
\]
We choose now a suitable constant $c_2$ in (3.1), depending only on $f$, and $Q$ large enough to obtain a contradiction with (3.7). We thus conclude that there is no nontrivial pair $n_1, n_2 \in \mathcal{N}$ such that $u_{n_1} u_{n_2}$ is a square in $\mathbb{Q}$ which proves (3.6).

### 3.3 Final optimisation

In order to conclude the proof, observe that (3.5) and (3.6) give
\[
P_f(Q) \ll \frac{1}{t} \frac{Q}{\eta \log Q} + \eta^{\eta^{-1}/4-1} \frac{Q}{\log Q} + \eta^{-2} Q^{1-\eta}.
\]
Let us choose $\eta$ to satisfy
\[
\eta^{\eta^{-1}/4} = t^{-1}
\]
for which we derive
\[
P_f(Q) \ll \frac{1}{t} \frac{Q}{\eta \log Q} + \eta^{-2} Q^{1-\eta}.
\]
(3.8)
Since for the above choice of $\eta$ we have
\[
\eta^{-1/2} \log \left(\eta^{-1}\right) = 4 \log t
\]
we conclude that $\eta = (\log t)^{-2+o(1)}$. It is easy to check that with the choice of $t$ as in (3.1), the second term in (3.8) never dominates and the result follows.

4 Proof of Theorem 1.4

Since the proof is very similar to that of Theorem 1.2 we only sketch the main steps. We now put

$$N = c_3 \log Q \quad \text{and} \quad t = c_4 \log \log Q \quad (4.1)$$

with some sufficiently small constants $c_3, c_4 > 0$ fixed later.

We recall the inequality (3.4), however this time we do not expand the sum over primes in $S$ to the set $P(\eta, 2Q)$.

As before, let $Z$ be the set of pairs $(n_1, n_2) \in \mathcal{N}^2$ such that $u_{n_1}u_{n_2}$ is a square. For a pair $(n_1, n_2) \notin Z$, again by Lemma 2.8, with the choice (4.1), we conclude that

$$\log |u_{n_1}u_{n_2}| \ll d^{N+t} \leq Q^{1/3}$$

if $c_3$ and $c_4$ are small enough. Hence, using Lemma 2.5 instead of Lemma 2.4, we arrive to the following analogue of (3.5)

$$P_f(Q) \ll \frac{\#Z}{t^2} \frac{Q}{\log Q} + Q^{5/6}. \quad (4.2)$$

For $N$ and $t$ in (4.1) related similarly to those in (3.1) we also have the bound (3.6), which after substitution in (4.2) gives

$$P_f(Q) \ll \frac{1}{t} \frac{Q}{\log Q} + Q^{5/6},$$

and the result follows.

5 Comments

We remark that our method applies to any polynomial for which we can control the existence, or at least the frequency, of perfect squares in the products $\text{Res}(f(n_1), f')\text{Res}(f(n_2), f')$ with $N \leq n_1 < n_2 \leq N + t$. We also remark that we have a lot of flexibility in selecting the interval $[N, N + t]$ from which $n_1$ and $n_2$ are chosen. Besides, we do not have to use all values from the set $\mathcal{N}$ in the proofs of Theorems 1.2 and 1.4, but limit ourselves to certain (reasonably large) subset $\tilde{\mathcal{N}} \subseteq \mathcal{N}$ of integers with some desirable properties, and then use $\tilde{\mathcal{N}}$ in the argument.

Unfortunately, despite the above flexibility of the method, besides the shifted trinomials of Corollaries 1.3 and 1.5, we have not found any natural classes of polynomials for which this can be applied. Moreover, it is natural to try to extend Corollaries 1.3 and 1.5 to trinomials of odd degree. We note that in this case, the same approach as in Theorems 1.2 and 1.4 applies, but using Lemma 2.2 (2) instead of Lemma 2.2 (1). However the part about the square avoidance breaks down.

Our main goal has been to establish an unconditional result, at least with respect to the polynomials we consider. However we observe that under the celebrated $ABC$-conjecture one can further extend the class of polynomials to which our method applies. To sketch this
argument, for an integer \( k \neq 0 \) we define \( \rho(k) \) as the product of all distinct prime divisors of \( k \), that is,

\[
\rho(k) = \prod_{p | k} p,
\]

which is also commonly called the radical of \( k \). Next, we recall that Langevin [19] (see also [10, Theorem 5]) has shown that under \( ABC \)-conjecture, for any polynomial \( g \in \mathbb{Z}[X] \) of degree \( e \geq 2 \), under some natural conditions, and any \( m \in \mathbb{Z} \) we have

\[
\rho(g(m)) \geq |m|^{e-1+o(1)}, \quad |m| \to \infty.
\]

Hence if we write \( |g(m)| = uv^2 \) with a squarefree \( u \) and an integer \( v \geq 1 \), we see that

\[
uv \geq \rho(g(m)) \geq |m|^{e-1+o(1)}
\]

and using \( v = (|g(m)|/u)^{1/2} \ll |m|^{e/2}u^{-1/2} \), we derive

\[
u \geq |m|^{e-2+o(1)}.
\]

Suppose that all roots

\[|\gamma_1| > |\gamma_2| \geq \cdots \geq |\gamma_{d-1}|\]

of \( f' \) are integers and the largest root \( \gamma_1 \) is of multiplicity one.

Additionally, assume that the iterations \( f^{(n)}(\gamma_i) \) grow as expected, that is, doubly exponentially,

\[|f^{(n)}(\gamma_i)| = \exp\left((1+o(1))\vartheta_i^n\right), \quad i = 1, \ldots, d-1,\]

for some constants \( \vartheta_i > 1 \), and furthermore

\[\vartheta_i < \vartheta_1^{(d-3)/d}, \quad i = 2, \ldots, d-1.\]

In this case the squarefree part of \( f^{(n_1)}(\gamma_1) \) is so large, namely, it is at least

\[|f^{(n_1-1)}(\gamma_1)|^{d-3+o(1)} \geq \exp\left(|\vartheta_1^{d'}|^{d-3+o(1)}\right),\]

that the product of other terms

\[
\prod_{i=2}^{d-1} f^{(n_1)}(\gamma_i) \prod_{i=1}^{d-1} f^{(n_2)}(\gamma_i) \leq \exp\left((1+o(1))\left(\sum_{i=1}^{d-1} \vartheta_i^{d \cdot n_1} + \vartheta_1^{d \cdot n_2}\right)\right)
\]

is not large enough to complement it up to a square.

Certainly this argument can be modified in several directions to cover many other scenarios and with an appropriate generalisation of the \( ABC \)-conjecture and the argument of [10,19] to number fields, see [5, Chapter 14], it can work without the assumption of the integrality of the critical points. We do not pursue this venue here since, as we have mentioned, our goal is deriving unconditional results for various classes of polynomials.

Finally, we remark on obtaining analogues of Theorems 1.2 and 1.4 when \( f \) is an arbitrary polynomial with the property that its derivative is irreducible. In this case, following the same approach as in the proofs of Theorems 1.2 and 1.4, we get to the point when we have to discuss when \( \text{Res}(f^{(n_1)}, f') \text{Res}(f^{(n_2)}, f') \) is a square. Using the irreducibility assumption of \( f' \), we reduce this problem to analysing when

\[
N_{\mathbb{Q}(\gamma)}/\mathbb{Q} \left(f^{(n_1)}(\gamma) f^{(n_2)}(\gamma)\right) = y^2
\]
for some \( y \in \mathbb{Q} \), where \( \gamma \) is one of the roots of \( f' \) and \( N_{\mathbb{Q}(\gamma)/\mathbb{Q}} : \mathbb{Q}(\gamma) \to \mathbb{Q} \) is the usual field norm map. To finalise our argument, under some natural assumptions on the polynomial \( g \in \mathbb{Z}[X] \) (in our case \( g = f^{(n_2-n_1)} \)), we need an effective result for the height of \( S \)-integer solutions to the norm equation

\[
N_{\mathbb{Q}(\gamma)/\mathbb{Q}}(xg(x)) = y^2,
\]

similar to those in [4].

Acknowledgements The authors thank Andrea Ferraguti for feedback on an early version of the paper and pointing out an imprecision in the initial statement of Theorem 1.2 and supplying the example at the end of Sect. 1.2. The authors are also grateful to the anonymous referee for helpful comments and suggestions. During the preparation of this work, L.M. was supported by the Austrian Science Fund (FWF): Project P31762, A. O. was supported by the Australian Research Council (ARC): Grant DP180100201 and I. S. was supported by the Australian Research Council (ARC): Grant DP170100786.

References

1. Ali, N.: Stabilité des polynômes. Acta Arith. 119, 53–63 (2005)
2. Ayad, M., McQuillan, D. L.: Irreducibility of the iterates of a quadratic polynomial over a field. Acta Arith. 93, 87–97 (2000) [Corrigendum: Acta Arith., 99 (2001), 97]
3. Benedetto, R., DeMarco, L., Ingram, P., Jones, R., Manes, M., Silverman, J.H., Tucker, T.J.: Current trends and open problems in arithmetic dynamics. Bull. Am. Math. Soc. 56, 611–685 (2019)
4. Bérczes, A., Evertse, J.-H., Györy, K.: Effective results for hyper- and superelliptic equations over number fields. Publ. Math. Debr. 82, 727–756 (2013)
5. Bombieri, E., Gubler, W.: Heights in Diophantine geometry. Cambridge University Press, Cambridge (2006)
6. Cox, D.: Primes of the form \( x^2 + ny^2 \): Fermat, class field theory, and complex multiplication. Wiley, New York (1997)
7. Ferraguti, A.: The set of stable primes for polynomial sequences with large Galois group. Proc. Am. Math. Soc. 146, 2773–2784 (2018)
8. Gómez, D., Nicolás, A.P.: An estimate on the number of stable quadratic polynomials. Finite Fields Appl. 16(6), 401–405 (2010)
9. Gómez, D., Nicolás, A.P., Ostafe, A., Sadornil, D.: Stable polynomials over finite fields. Rev. Mat. Iberoam. 30, 523–535 (2014)
10. Granville, A.: ABC allows us to count squarefrees. Int. Math. Res. Not. 19, 991–1009 (1998)
11. Heath-Brown, D.R.: The square sieve and consecutive squarefree numbers. Math. Ann. 266, 251–259 (1984)
12. Heath-Brown, D.R., Micheli, G.: Irreducible polynomials over finite fields produced by composition of quadratics. Rev. Mat. Iberoam. (2020) (to appear)
13. Iwaniec, H., Kowalski, E.: Analytic number theory. American Mathematical Society, Providence, RI (2004)
14. Jones, R.: The density of prime divisors in the arithmetic dynamics of quadratic polynomials. J. Lond. Math. Soc. 78, 523–544 (2008)
15. Jones, R.: An iterative construction of irreducible polynomials reducible modulo every prime. J. Algebra 369, 114–128 (2012)
16. Jones, R., Boston, N.: Settled polynomials over finite fields. Proc. Am. Math. Soc. 140, 1849–1863 (2012)
17. Jones, R., Boston, N.: Errata to “Settled polynomials over finite fields”. Proc. Am. Math. Soc. 148, 913–914 (2020)
18. Konyagin, S., Shparlinski, I.E.: Quadratic non-residues in short intervals. Proc. Am. Math. Soc. 143, 4261–4269 (2015)
19. Langevin, M.: ’Cas dégalité pour le théorème de Mason et applications de la conjecture (abc).’, C. R. Acad. Sci. Paris Sér. I Math. 317, 441–444 (1993)
20. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge (1986)
21. Montgomery, H.L., Vaughan, R.C.: Multiplicative number theory I: Classical theory. Cambridge University Press, Cambridge (2006)
Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.