STABILITY OF CERTAIN HIGHER DEGREE POLYNOMIALS

SHANTA LAISHRAM, RITUMONI SARMA AND HIMANSHU SHARMA

Abstract. One of the interesting problems in arithmetic dynamics is to study the stability of polynomials over a field. In this paper, we study the stability of \( f(z) = z^d + \frac{1}{c} \) for \( d \geq 2, c \in \mathbb{Z} \setminus \{0\} \). We show that for infinite families of \( d \geq 3 \), whenever \( f(z) \) is irreducible, all its iterates are irreducible, that is, \( f(z) \) is stable. For \( c \equiv 1 \pmod{4} \), we show that all the iterates of \( z^2 + \frac{1}{c}z \) are irreducible. Also we show that for \( d = 3 \), if \( f(z) \) is reducible, then the number of irreducible factors of each iterate of \( f(z) \) is exactly 2 for \( |c| \leq 10^{12} \).

1. Introduction

An important question in the field of arithmetic dynamics is to study the recurrence sequences satisfying \( t_n = f(t_{n-1}) \), where \( t_0 \in \mathbb{Q} \) and \( f(z) \in \mathbb{Q}[z] \) with \( \text{deg}(f(z)) \geq 2 \). One can ask how many primes are there in the sequence \( (t_n) \) or which primes are dividing at least one element of the sequence \( (t_n) \). Many authors have investigated these questions in \([19],[15],[12],[10],[9]\). One interesting problem in this direction is about the stability and eventual stability of polynomials over a field. In fact stability and eventual stability have been recently used in proving finite index results for some arboreal representations in \([4]\) and \([5]\).

If each iterate of \( f(z) \in \mathbb{Q}[z] \) is irreducible over \( \mathbb{Q} \) then we say that \( f(z) \) is stable over \( \mathbb{Q} \). More generally if the number of irreducible factors of iterates of \( f(z) \) is bounded by a constant, that is, there exist \( n_0 \in \mathbb{N} \) such that the number of irreducible factors of \( f^n(z) \) remains constant for \( n \geq n_0 \) then we say that \( f(z) \) is eventually stable.

We consider the stability and eventual stability of \( z^d + b \) with \( b \in \mathbb{Q}, b \neq 0 \). Put \( b = \frac{a}{c} \) with \( a, c \in \mathbb{Z}, c \neq 0 \). It was shown in \([11]\) Theorem 1.6] that \( f(z) = z^d + \frac{a}{c} \) is eventually stable when \( a \neq 1 \). The stability and eventual stability of \( z^d + \frac{1}{c} \) is not known completely. Even for the quadratic polynomial \( z^2 + \frac{1}{c}z \) over \( \mathbb{Q} \), it is not completely known though some partial results are available in \([8]\). We refer to \([2]\) for a more detailed survey. In this paper, we consider the stability and eventual stability of the polynomial \( z^d + \frac{1}{c}, c \in \mathbb{Z} \setminus \{0\} \). We prove the following results.

\begin{itemize}
    \item \textit{Date: June 10, 2022.}
    \item \textit{Key words and phrases.} Stable, Eventually stable, non-Archimedean valuation.
\end{itemize}
Stability of Certain Higher Degree Polynomials

**Theorem 1.** Let $d \geq 2$ be a positive integer and $f(z) = z^d + \frac{1}{c}$ where $c \neq 0$ is an integer. We have

(a) Let $d = 2$. If $c \equiv 1 \pmod{4}$ then each iterate of $f(z)$ is irreducible over $\mathbb{Q}$.
(b) Let $d > 2$. Assume that $f(z)$ is irreducible. Then $f(z)$ is stable over $\mathbb{Q}$ when

1. $d \geq 3$ is odd.
2. $d = 2^r$ with $r \geq 2$.
3. $d = 2^r \cdot 3^s$ with $r, s \geq 1$.
4. $d = 2^r \cdot 5^s \cdot 7^t$ with $r \geq 1, s, t \geq 0$ and $d \equiv 1 \pmod{3}$
5. $d \equiv 4 \pmod{12}$.

We note that when $d = 2$ and $c = -m^2$, then $c \equiv 0, 3 \pmod{4}$ and $f(z) = z^2 + \frac{1}{c}$ is reducible. We refer to [8, Theorem 1.3] for other values of $c$ for which each iterate of $z^2 + \frac{1}{c}$ is irreducible over $\mathbb{Q}$. The case $d > 3$ odd and not divisible by 3 follows from [7, Theorem 7]. From Theorem 1 and the remarks made in [7] and , we believe that the following conjecture is true.

**Conjecture 1.** If $f(z) = z^d + \frac{1}{c}, c \in \mathbb{Z} \setminus \{0\}, d \geq 3$, is irreducible over $\mathbb{Q}$ then $f(z)$ is stable over $\mathbb{Q}$.

Though we are not able to completely prove this conjecture unconditionally, by using an explicit version of $abc$-conjecture due to Baker [1] (see Conjecture 4), we are able to show that the Conjecture 1 is true.

**Theorem 2.** The explicit $abc$–Conjecture implies Conjecture 1. That is $f(z) = z^d + \frac{1}{c}$ with $c \in \mathbb{Z} \setminus \{0\}$ and $d \geq 3$ is stable over $\mathbb{Q}$ whenever $f(z)$ is irreducible over $\mathbb{Q}$.

When $f(z) = z^d + \frac{1}{c}$ is reducible over $\mathbb{Q}$, nothing much is known about the irreducible factors of iterates of $f(z)$ for $d \geq 3$. In this paper, we prove the following result about the eventual stability of $f(z) = z^3 + \frac{1}{c}$ when it is reducible.

**Theorem 3.** Let $f(z) = z^3 + \frac{1}{c}, c \in \mathbb{Z} \setminus \{0\}$. If $f(z)$ is reducible over $\mathbb{Q}$ then $f^n(z)$ has exactly two irreducible factors over $\mathbb{Q}$ for each $n \in \mathbb{N}$ and for $c$ with $|c| \leq 10^{12}$.

We believe that above result should be true for all $c$ and we propose the following conjecture.

**Conjecture 2.** Let $f(z) = z^3 + \frac{1}{c}, c \in \mathbb{Z} \setminus \{0\}$. If $f(z)$ is reducible over $\mathbb{Q}$ then $f^n(z)$ has exactly two irreducible factors over $\mathbb{Q}$ for each $n \in \mathbb{N}$ and for all $c$.

We prove Theorems 1 and 2 in Section 4. Theorem 3 is proved in Section 3. In Section 2, we give the preliminaries.
2. Preliminaries

Let \( K \) be a number field, \( \phi(z) \in K(z) \) and let \( \alpha \in \mathbb{P}^1(K) \). Assume that \( \phi(z) = \frac{f(z)}{g(z)} \), where \( f(z) \) and \( g(z) \) are coprime in \( K[z] \). The degree of a rational function \( \phi(z) = \frac{f(z)}{g(z)} \) is defined as \( \deg \phi(z) = \max\{\deg f(z), \deg g(z)\} \). Let \( \phi^n(z) = \phi(\phi^{n-1}(z)) \), the \( n \)-th iterate of \( \phi(z) \) and put \( \phi^n(z) = \frac{f_n(z)}{g_n(z)} \), where \( f_n(z), g_n(z) \in K[z] \) are coprime polynomials.

**Definition 4.** The pair \( (\phi, \alpha) \) is said to be stable over \( K \) if \( f_n(z) - \alpha g_n(z) \) is irreducible over \( K \) for each \( n \in \mathbb{N} \).

However stability is not preserved under field extensions. A weaker condition called eventual stability behaves well with respect to finite field extensions.

**Definition 5.** If there exist a constant \( C(\phi, \alpha) \) such that the number of irreducible factors of \( f_n(z) - \alpha g_n(z) \), for all \( n \geq 1 \), is bounded by \( C(\phi, \alpha) \) then we say that \( (\phi, \alpha) \) is *eventually stable* over \( K \). If the number of irreducible factors of \( g_n(z) \) is similarly bounded then we say that \( (\phi, \infty) \) is eventually stable.

If \( (\phi, 0) \) is eventually stable then we say that \( \phi(z) \) is eventually stable. Eventual stability of a rational function over \( K \) is preserved over finite extensions of \( K \).

A map \( \nu : K \rightarrow \mathbb{Z} \cup \{\infty\} \) is called a *discrete* valuation on \( K \) if it satisfies the following properties:

1. \( \nu(x) = \infty \iff x = 0 \),
2. \( \nu(xy) = \nu(x) + \nu(y) \forall x, y \in K \) and
3. \( \nu(x+y) \geq \inf\{\nu(x), \nu(y)\} \).

Suppose \( p \) is a rational prime. Then every rational number \( x \) can be written as \( p^tx_0 \) where \( t \in \mathbb{Z} \) and \( p \) divides neither the numerator nor the denominator of \( x_0 \). Then, \( \nu_p : \mathbb{Q} \setminus \{0\} \rightarrow \mathbb{Z} \) defined by \( \nu_p(x) = t \) is a discrete valuation which is called the \( p \)-adic valuation on \( \mathbb{Q} \).

Given a discrete valuation \( \nu \) on the number field \( K \), \( R \) denote the following ring \( \{x \in K : \nu(x) \geq 0\} \). Then \( \mathfrak{p} = \{x \in K : \nu(x) > 0\} \) is the unique maximal ideal of the ring \( R \). The field \( k = R/\mathfrak{p} \) is called the residue field of \( \nu \). Denote by \( \tilde{x} \in \mathbb{P}^1(k) \) the reduction modulo \( \mathfrak{p} \) of \( x \in \mathbb{P}^1(K) \). Further we denote by \( \tilde{f}(z) \) the polynomial obtained from \( f(z) \in R[z] \) by reducing each coefficient modulo \( \mathfrak{p} \).

Let \( \phi(z) = \frac{f(z)}{g(z)} \in K(z) \) where \( f(z), g(z) \in R[z] \). Then we say that \( \frac{f(z)}{g(z)} \) is *normalized* if \( f(z), g(z) \in R[z] \) are coprime and at least one of the coefficients of \( f(z) \) or \( g(z) \) is a unit in \( R \). Define \( \tilde{\phi}(z) = \frac{\tilde{f}(z)}{\tilde{g}(z)} \). Suppose \( \phi(z) \) is non-constant. Then \( \phi(z) \in K(z) \) is
said to have good reduction at \( \nu \) if \( \deg(\tilde{\phi}(z)) = \deg(\phi(z)) \). We say that \( \phi(z) \) is bijective on residue extensions for the discrete valuation \( \nu \) on \( K \) if \( \tilde{\phi}(z) \) defines a bijection on \( \mathbb{P}^1(E) \) for every finite extension \( E \) of the residue field \( \kappa \) of \( \nu \).

**Proposition 2.1.** [13] Let \( K \) be a number field with discrete valuation \( \nu \), \( \phi(z) \in K(z) \) be such that \( \deg \phi(z) \geq 2 \) and let \( \alpha \in \mathbb{P}^1(K) \) be non-periodic with respect to \( \phi(z) \). Assume \( \phi(z) \) is bijective on residue extensions for \( \nu \) and has good reduction at \( \nu \). Assume further \( \phi^n(z) = \frac{f_n(z)}{g_n(z)} \) is normalized and \( \alpha \neq \infty \). Then the number of irreducible factors of \( f_n(z) - \alpha g_n(z) \) over \( K \) is at most

1. \( \nu(\phi(\alpha))^{-1} - \alpha^{-1} \) if \( \nu(\alpha) < 0 \),
2. \( \nu(\phi^i(\alpha) - \alpha) \) if \( \nu(\alpha) \geq 0 \) for \( i = \min\{n \geq 1 : \phi^n(\alpha) = \tilde{\alpha}\} \).

**Lemma 2.1.** [8] Suppose \( g(x) \in K[x] \) is a monic irreducible polynomial with degree \( d \geq 1 \) and \( \text{char}(K) \neq 2 \). Let \( f(x) \in K[x] \) be a monic quadratic polynomial and \( \gamma \) be such that \( f'(\gamma) = 0 \). If no element of

\[
\{(-1)^d g(f(\gamma))\} \cup \{g(f^n(\gamma)) : n \geq 2\}
\]

is a square in \( K \), then \( g(f^n(x)) \) is irreducible over \( K \) for each \( n \in \mathbb{N} \).

We will use the following result for \( d = 3 \) in the proof of Theorem 3 which deals with the irreducible factors of the iterates of \( z^3 + \frac{1}{5} \) when it is reducible.

**Lemma 2.2** (Capelli’s Lemma, [13]). Suppose \( f(x), g(x) \) are polynomials over the field \( K \) such that \( g(x) \) is irreducible. Then \( g(f(x)) \) is irreducible over \( K \) if and only if \( f(x) - \beta \) is irreducible over \( K(\beta) \) for every root \( \beta \in \overline{K} \) of \( g(x) \).

**Proposition 2.2.** [7] Let \( n \geq 3 \) be an odd integer and let \( f(x) = x^n - b \in \mathbb{Q}[x] \). For each \( m \geq 1 \), let \( S(n, m) = \{b \in \mathbb{Q} : f^m \text{ is irreducible but } f^{m+1} \text{ is reducible over } \mathbb{Q}\} \). Then \( S(n) = \bigcup_{m=1}^\infty S(n, m) \) is finite and is empty if \( 3 \nmid n \).

The above result was proved by using Lemma 2.2 and the non-existence of primitive solutions of the generalized Fermat equation. Let \( p, q, r \) be integers \( \geq 2 \) and consider the generalized Fermat equation

\[
x^p + y^q = z^r.
\]

Given a triple \( (a, b, c) \in \mathbb{Z}^3 \), we say that \( (a, b, c) \) is a solution of equation (2.1) if \( a^p + b^q = c^r \). If \( a, b, c \) are pairwise coprime then this solution is called proper. A proper solution \( (a, b, c) \) is primitive if \( abc \neq 0 \). A well-known conjecture regarding the generalized Fermat equations is due to Tijdeman and Zagier (see [16]), also known as Beal’s conjecture.

**Conjecture 3.** There are no primitive solutions of the diophantine equation

\[
x^p + y^q = z^r
\]

in \( \mathbb{Z} \) for \( p, q, r \geq 3 \).
This is open. However there are a number of partial results on this conjecture. For the proof of our theorems, we need the following result on the non-existence of primitive solutions of the following equations, see [3].

**Lemma 2.3.** There are no primitive solutions for the equation \( x^p + y^q = z^r \) when 
\[(p, q, r) \in \{(2, 3, 7), (2, 3, 10), (2, n, 4), (2, n, 6), (3, 3, 2n), (3, n, 6), (n, n, 2), (n, n, 3)\} \]
where \( n \geq 2 \) and further \( n \geq 3 \) when \((p, q, r) \in \{(3, n, 6), (n, n, 3)\}\); \( n \geq 4 \) when \((p, q, r) \in \{(2, n, 6), (n, n, 2)\}\) and \( n \geq 6 \) when \((p, q, r) = (2, n, 4)\).

The next result is a Catalan’s conjecture, now a theorem of Mihăilescu [18].

**Lemma 2.4.** The only solution of \( x^m - y^n = 1 \) in integers \( x, y, m > 1, n > 1 \) with \( xy \neq 0 \) is given \( 3^2 - 2^3 = 1 \).

We end with this section with the explicit abc-conjecture due to Baker [1]. If \( m \) is a positive integer, then its radical \( N(m) \) is the product of distinct prime divisors of \( m \) and \( \omega(m) \) denotes the number of distinct primes dividing \( m \).

**Conjecture 4.** [Explicit abc-conjecture] Let \( a, b \) and \( c \) be pairwise coprime integers satisfying \( a + b = c \). Then
\[
c < \frac{6}{5} N \left( \frac{\log N}{\omega} \right) \frac{\omega}{\omega!}
\]
where \( N = N(abc) \) and \( \omega = \omega(N) \).

An easily applicable formulation was given by Laishram and Shorey [16, Theorem 1]. The next result is contained in [16, Theorem 1].

**Proposition 2.3.** Assume Conjecture 4. Let \( a, b \) and \( c \) be pairwise coprime integers such that \( a + b = c \). Then
\[
c < N^{1 + \frac{3}{7}} \quad \text{where} \quad N = N(abc).
\]
Further for \( 0 < \epsilon \leq \frac{3}{7} \), there exist \( N_\epsilon \), depending only on \( \epsilon \), such that whenever \( N \geq N_\epsilon \), we have \( c < N^{1+\epsilon} \). In particular, for \( \epsilon = \frac{7}{12} \), \( N_\epsilon = \exp(204.75) \).

Explicit abc–Conjecture can be used to give a general result on the Conjecture 3, see [16, Theorem 3].

**Proposition 2.4.** Assume Conjecture 4. Then there are no primitive solutions of the equation \( x^p + y^q = z^r \) with \( p \geq 3, q \geq 3, r \geq 3 \) and
\[
[p, q, r] \notin \{[3, 5, \ell] : 7 \leq \ell \leq 23, \ell \text{ prime}\} \cup \{[3, 4, \ell] : \ell \text{ prime}\}
\]
where \([p, q, r]\) denote all the permutations of ordered triples \((p, q, r)\).
Stability of Certain Higher Degree Polynomials

3. PROOF OF THEOREM 3

We start this section with a lemma which is analogous to Lemma 2.1.

**Lemma 3.1.** Let $g(z)$ be a monic irreducible polynomial over a number field $K$ and let $f(z) = z^3 + \frac{1}{c} \in K[z]$. If none of $\{g(f^n(0))\}_{n \geq 1}$ is a cube in $K$ then $g(f^n(z))$ is irreducible for each $n \in \mathbb{N}$.

**Proof.** We prove it by induction on $n$. For $n = 0$, $g(z)$ is given to be irreducible. Assume now irreducibility of $g(f^{n-1}(z))$. Then by Capelli’s Lemma 2.2, $g(f^n(z))$ is irreducible over $K$ if and only if $z^3 + 1/c - \gamma$ is irreducible over $K(\gamma)$, that is, $1/c - \gamma$ is not a cube in $K(\gamma)$, for every root $\gamma$ of $g(f^{n-1}(z))$. Note that

$$N_{K(\gamma)/K}\left(\frac{1}{c} - \gamma\right) = \prod_{\alpha \text{ is root of } g(f^{n-1}(z))\left(\frac{1}{c} - \alpha\right) = g\left(f^{n-1}\left(\frac{1}{c}\right)\right) = g(f^n(0)).$$

If $N_{K(\gamma)/K}(1/c - \gamma)$ is not a cube in $K$ then $1/c - \gamma$ is not a cube in $K(\gamma)$. Thus, if $g(f^n(0))$ is not a cube in $K$ then $z^3 + 1/c - \gamma$ is irreducible over $K(\gamma)$ so that $g(f^n(z))$ is irreducible over $K$ for each $n \in \mathbb{N}$. \(\square\)

**Lemma 3.2.** Let $f(z) = z^d + \frac{1}{c}$ with $d$ an odd integer. For any prime $p$ dividing $d$, if $f^n(0)$ is not a $p$-th power in $\mathbb{Q}$ for $c > 0$ then it is also not a $p$-th power for $c < 0$ in $\mathbb{Q}$. Additionally, If $d = 3$ then similar result holds for $g(f^n(0))$ for any divisor $g(z)$ of $f(z)$.

**Proof.** Let $f_c(z) = z^d + \frac{1}{c}$ with $d$ an odd integer. By induction, we have $f^n_c(0) = -f^n_c(0)$ for all $n \geq 1$. Therefore $f^n_c(0)$ is a $p$-th power if and only if $f^n_c(0)$ is a $p$-th power in $\mathbb{Q}$. Suppose $d = 3$, $f_c(z)$ is reducible and $g(z)|f(z)$. It is also easy to observe that $g_c(f^n_c(0)) = \pm g_c(f^n_c(0))$. Hence the proposition follows. \(\square\)

Let $f(z) = z^3 + \frac{1}{c}$. We know that $f(z)$ is reducible if and only if $c = m^3$ for some $m \in \mathbb{Z}$. In that case $f(z) = (z + \frac{1}{m})(z^2 - \frac{z}{m} + \frac{1}{m^2})$. Set

$$g_1(z) = z + \frac{1}{m} \quad \text{and} \quad g_2(z) = z^2 - \frac{z}{m} + \frac{1}{m^2}.$$  

(3.1)

Since $g_1(f(z)) = z^3 + 1/m^3 + 1/m = z^3 + \frac{m^3+1}{m^3}$, $g_1(f(z))$ is reducible if and only if $m^2 + 1$ is a cube in $\mathbb{Z}$. By Lemma 2.1, $m^2 + 1$ is not a cube unless $m = 0$. Hence $g_1(f(z))$ is irreducible for all $m \neq 0$. For considering the irreducible factors of iterates of $f(z)$, we require the following lemma for which the proof is similar to that of [14] Proposition 5.4.

**Lemma 3.3.** Let $f(z) = z^3 + \frac{1}{c}$ be reducible with the irreducible factors $g_1(z)$ and $g_2(z)$ as in (3.1). Then $(g_i(f^n(0))), n \geq 1,$ is a rigid divisibility sequence for $i = 1, 2.$
3.1. **Proof of Theorem** Let \( f(z) = z^3 + \frac{1}{z} \) be reducible. Then \( c = m^3 \) for some \( 0 \neq m \in \mathbb{Z} \) and write \( f(z) = g_1(z)g_2(z) \), where \( g_1(z), g_2(z) \) are given by (3.1). Let \( w_n(m) \) be the numerator of \( g_1(f^{n-1}(0)) \), so that \( w_2(m) \) is the numerator of \( g_1(f(0)) \). We observe that \( w_2(m) = m^2 + 1 \) is not a cube in \( \mathbb{Z} \) by Lemma 3.3. By Lemma 3.3 it follows that \( (w_n(m)) \) is a rigid divisibility sequence. Hence \( w_2(m) \) is not a cube in \( \mathbb{Z} \) for each \( n \geq 1 \).

For a given \( k \in \mathbb{N} \) and \( m \not\equiv 0 \pmod{k} \), the sequence \( (g_1(f^n(0)) \pmod{k}) \) eventually becomes a repeating cycle and we search for values of \( k \) and congruence classes of \( m \) modulo \( k \) such that \( (g_1(f^n(0)) \pmod{k}) \) is not a cube for each \( n \in \mathbb{N} \). Since we have shown above that \( w_{2j} \) is not a cube in \( \mathbb{Z} \) for each \( j \geq 1 \), that is, \( g_1(f^{2j-1}(0)) \) is not a cube in \( \mathbb{Q} \), it is enough to check that \( (g_1(f^{2j}(0)) \pmod{k}) \) is not a cube for \( j \geq 1 \). In fact, with the help of SAGE we verify for each \( j \in \mathbb{N} \) that \( (g_1(f^{2j}(0))) \) is not a cube for \( m \) belonging to the congruences classes modulo \( k \in \{7, 13, 19, 31, 37, 43\} \) that are listed in Table 1.

| \( k \) | \( m \) (mod \( k \)) |
|-------|------------------|
| 7     | \( m \equiv \pm 1, \pm 3 \) |
| 13    | \( m \equiv \pm 1, \pm 2, \pm 3, \pm 6 \) |
| 19    | \( m \equiv \pm 2, \pm 4 \) |
| 31    | \( m \equiv \pm 1, \pm 3, \pm 4, \pm 6, \pm 8, \pm 9, \pm 10, \pm 11, \pm 12 \) |
| 37    | \( m \equiv \pm 3, \pm 9, \pm 17 \) |
| 43    | \( m \equiv \pm 2, \pm 5, \pm 8, \pm 10, \pm 12, \pm 13, \pm 14, \pm 15, \pm 20 \) |

**Table 1**

One can verify that the congruence classes in Table 1 cover all integers belonging to the interval \([1, 10^4]\) except for 267 of them. For each of the remaining integers, we could find a prime \( p < 150 \) such that \( g_1(f^n(0) \pmod{p}) \) is not a cube for every even integer \( n \). For example, \( p = 73 \) works for \( m = 4342 \). Hence by Lemma 3.1 \( g_1(f^n(z)) \) is irreducible for all \( n \geq 1 \) when \( 1 \leq m \leq 10^4 \).

Let \( x_n(m) \) be the numerator of \( g_2(f^{n-1}(0)) \). In particular \( x_2(m) \) is the numerator of \( g_2(f(0)) \). It again follows from Lemma 3.3 that \( (x_n(m)) \) is a rigid divisibility sequence. Since \( g_2(f(0)) = \frac{m^4 - m^2 + 1}{m^2} \), we have \( x_2(m) = m^4 - m^2 + 1 \). Now \( x_2(m) \) is a cube if and only if the elliptic curve \( y^2 - y + 1 = x^3 \) has integral point with \( y = m^2 \). It follows from the curve 243.a1 in LMFDB that \( y^2 - y + 1 = x^3 \) has only integral points \((1, 1), (7, 19), (1, 0), (7, -18)\). Since \( m \neq 0, m^4 - m^2 + 1 \) is a cube in \( \mathbb{Q} \) for \( m = \pm 1 \) only, that is, \( x_2(m) \) is not a cube in \( \mathbb{Z} \) for \( |m| \geq 2 \). Let \( m = 1 \). In this
case \( f(z) = z^3 + 1 \) and \( g_2(z) = z^2 - z + 1 \), we verify that \( z^6 + z^3 + 1 = g_2(f(z)) \) is irreducible over \( \mathbb{Q} \). Further we checked that \( g_2(f^n(0)) \pmod{7} \) is not a cube for each \( n \geq 2 \). Hence by Lemma 3.1, \( g_2(f^n(z)) \) is irreducible for all \( n \in \mathbb{N} \). Similarly we verified that \( g_2(f^n(z)) \) is irreducible for each \( n \in \mathbb{N} \) when \( m = -1 \). Hence we take \( |m| \geq 2 \). Since \( (x_n(m)) \) is a rigid divisibility sequence and \( x_2(m) \) is not a cube, for \( n \geq 1 \), \( x_{2n}(m) \) is also not a cube in \( \mathbb{Z} \). Again with the help of SAGE we verify for each \( j \in \mathbb{N} \) that \( (g_1(f^{2j}(0))) \) is not a cube for \( m \) belonging to the congruences classes modulo \( k \in \{7, 13, 19, 31, 37\} \) that are listed in Table 2.

| \( k \) | \( m \pmod{k} \) |
|---|---|
| 7 | \( m \equiv \pm 1, \pm 2, \pm 3 \) |
| 13 | \( m \equiv \pm 1, \pm 2, \pm 3, \pm 4, \pm 5 \) |
| 19 | \( m \equiv \pm 3, \pm 5 \) |
| 31 | \( m \equiv \pm 1, \pm 4, \pm 7, \pm 8, \pm 9, \pm 11, \pm 14 \) |
| 37 | \( m \equiv \pm 4, \pm 7, \pm 9, \pm 12, \pm 16, \pm 17, \pm 18 \) |

Table 2

One can verify that the congruence classes in Table 2, cover all integers belonging to the interval \([1, 10^4]\) except for 88 of them. For each of the remaining integers, we could find a prime \( p < 150 \) such that \( g_1(f^n(0)) \pmod{p} \) is not a cube for every even integer \( n \). For example, \( p = 67 \) works for \( m = 2730 \). Hence \( g_2(f^n(z)) \) is irreducible for each \( n \in \mathbb{N} \) by Lemma 3.1. This proves Theorem 3.

4. Proof of Theorems 1 and 2

For the proof of Theorems 1 and 2, we need the following lemma.

**Lemma 4.1.** Let \( g(z) \) be a monic irreducible polynomial over a number field \( K \) and let \( f(z) = z^d + \frac{1}{z} \in K[z] \). Then for \( m \geq 1 \), \( g(f^m(z)) \) is irreducible if \( g(f^{m-1}(z)) \) is irreducible and \( g(f^m(0)) \) is not a \( p \)-th power in \( K \) for each prime \( p \) dividing \( d \). Hence for \( m \geq 1 \), \( g(f^m(z)) \) is irreducible if \( g(f^2(0)) \) is not a \( p \)-th power in \( K \) for each prime \( p \) dividing \( d \) and for each \( 1 \leq j \leq m \).

**Proof.** Assume \( g(f^{m-1}(z)) \) be irreducible. By Lemma 2.2 we have \( g(f^m(z)) \) is irreducible if and only if for every root \( \beta \) of \( g(f^{m-1}(z)) \), \( f(z) - \beta = z^d + 1/c - \beta \) is irreducible over \( K(\beta) \). By [17] Theorem 9.1, \( f(z) - \beta \) is irreducible if for every prime \( p \) dividing \( d \) we have \( \beta - 1/c \notin K(\beta)^p \) and if \( 4|d \) then \( \beta - 1/c \notin -4K(\beta)^d \). We know
Stability of Certain Higher Degree Polynomials

that $\beta - \frac{1}{c} \notin K(\beta)^p$ for a prime $p$ if $N_{K(\beta)/K}(\beta - \frac{1}{c}) \notin K^p$. Note that

$$N_{K(\beta)/K}\left(\beta - \frac{1}{c}\right) = \prod_{\alpha \text{ roots of } g(f^{m-1}(z))} \left(\alpha - \frac{1}{c}\right) = (-1)^t g\left(f^{m-1}\left(\frac{1}{c}\right)\right) = (-1)^t g(f^m(0))$$

where $t = \deg\left(g(f^{m-1}(z))\right)$. Hence if $g(f^m(0))$ is not a $p$-th power in $K$ then $\beta - 1/c \notin K(\beta)^p$. Now let $4|d$. Since $g(f^m(0))$ is not a square in $K$ and $4|t$, we have from $N_{K(\beta)/K}(1/c - \beta) = g(f^m(0))$ that $1/c - \beta$ is not a square and hence $1/c - \beta \notin 4K(\beta)^4$. Hence we conclude that if $(g(f^m)(0)$ is not a $p$-th power in $K$ for each prime $p$ dividing $d$ and $g(f^{m-1}(z))$ is irreducible, then $g(f^m(z))$ is irreducible. This proves the first assertion. The latter follows inductively from the first assertion.

Apply Lemma 4.1 to $K = \mathbb{Q}$ and $f(z) = g(z) = z^d + \frac{1}{c}$ whenever it is irreducible over $\mathbb{Q}$. Let $a_n$ denote the numerator of $f^n(0)$. Then $a_n$ satisfies $a_1 = 1$ and for $n > 1$,

$$a_n = a_{n-1}^d + c^{e_{n-1}} - 1 \quad \text{and} \quad f^n(0) = \frac{a_n}{c^{d^n - 1}}.$$

By induction, $a_n, a_{n+1}$ and $c$ are pairwise coprime for $n \in \mathbb{N}$. Note that for any prime $p$ dividing $d$, the denominator of $f^n(0)$ is always of the form $(e^p)^p$ for some positive integer $e$. So, for a prime $p$ that divides $d$, $f^n(0)$ is not a $p$-th power in $\mathbb{Q}$ unless $a_n$ is a $p$-th power in $\mathbb{Z}$. Let $n = 2$. Then $a_1 = 1$ implying $a_2 = 1 + c^{d-1}$. By Lemma 2.4 $a_2$ is a power only when $c = 2, d = 4$ in which case $a_2 = 3^2$. By Lemma 4.1, $f^2(z)$ is irreducible for all $(d, c) \neq (4, 2)$. For $(d, c) = (4, 2)$, we check that $f^2(z) = (x^4 + \frac{1}{2})^4 + \frac{1}{2}$ is irreducible over $\mathbb{Q}$. Thus to prove Theorem 1 it is enough to consider $n \geq 3$.

4.1. Proof of Theorem 1: Let $f(z) = z^d + b$. As in the statement of Proposition 2.2, let $S(d, m)$ be the set of $b \in \mathbb{Q}$ for which $f^m(z)$ is irreducible but $f^{m+1}(z)$ is not and set $S(d) = \bigcup_{m=1}^\infty S(d, m)$. By Proposition 2.2, $S(d) = \emptyset$ for all $d$ not divisible by 2 or 3. In other words, for $d$ not divisible by 2 or 3, if $f(z) = z^d + \frac{1}{c}$ is irreducible then all its iterates are also irreducible. Hence for the proof of Theorem 1 we may suppose that $2|d$ or $3|d$.

Let $d = 2$. We apply Proposition 2.1 to $K = \mathbb{Q}$, $\phi(z) = f(z) = z^2 + \frac{1}{c}$ and $\nu = \nu_2$, the 2-adic valuation on $\mathbb{Q}$. Here the corresponding residue field is $\mathbb{F}_2$. $f$ has good reduction when $c$ is odd in which case $\tilde{f}(z) = z^2 + 1$. Let $c$ be odd. Then $\tilde{f}(0) = 1, \tilde{f}(1) = 0$ so that the period $i = 2$ by Proposition 2.1. That is $f^n(z)$ has at most $\nu_2(f^2(0))$ irreducible factors. Now $f(0) = \frac{1}{c}, f^2(0) = \frac{l+c}{c}$ so that $\nu_2(f^2(0)) = \nu_2(1+c)$. When $c \equiv 1 \pmod{4}$, we have $\nu_2(1+c) = 1$ so that all the iterates $f^n(z)$ are irreducible over $\mathbb{Q}$. This proves (a).

Now suppose $d \geq 3$. As stated after the proof of Lemma 4.1 we need to show for $n \geq 3$ that for no prime $p$ dividing $d$ $a_n$ is a $p$-th power in $\mathbb{Z}$. We consider various cases of (b) one by one.
Let $d$ be an odd integer divisible by 3. Then $d^{n-1} - 1$ is even and $a_n = a_{n-1}^d + c^{d^{n-1}-1} = x_1^3 + y_1^{2k}$ and if $p \neq 3$ is a prime dividing $d$ then we also have $a_n = a_{n-1}^d + c^{d^{n-1}-1} = x_2^3 + y_2^2$ for some integers $x_1, x_2, y_1, y_2, k$ with $k \geq 3$. For each $n \geq 3$, $a_n$ is not a $p$-th power for any prime divisor of $d$ because if $a_n$ is a cube then $a_n + (-x_1)^3 = y_2^{2k}$ and if $a_n$ is a $p$-th power for any odd prime $p \neq 3$ dividing $d$ then $a_n + (-x_2)^p = y_2^2$ which are not possible by Lemma 2.3.

Let $d = 2^r$ with $r \geq 2$. Then $f(z) = z^{2^r} + \frac{1}{c}$ and $a_n = a_{n-1}^2 + c^{2^{r(n-1)}-1}$ for some integers $x, y, k$ with odd $k \geq 5$. Considering equations $a_n + (-y)^k = x^6$ if $a_n$ is a square and $a_n + (-y)^k = x^5$ if $a_n$ is a cube, we get a contradiction by Lemma 2.3. Hence $a_n$ is neither a square nor a cube for $n \geq 3$.

Let $d = 2^r \cdot 3^s$ with $r, s \geq 1$. Then $6|d$ and hence $a_n = a_{n-1}^d + c^{d^{n-1} - 1} = x^6 + y^k$ for some integers $x, y, k$ with odd $k \geq 5$. Considering equations $a_n + (-y)^k = x^6$ if $a_n$ is a square and $a_n + (-y)^k = x^5$ if $a_n$ is a cube, we get a contradiction by Lemma 2.3. Hence $a_n$ is not a $p$-th power for any odd prime $p$ dividing $d$.

Let $d = 2^r \cdot 5^s \cdot 7^t$ with $r \geq 1, s, t \geq 0$ and $d \equiv 1 \pmod{3}$. We assume that either $s > 0$ or $t > 0$ since $d = 2^r$ is already considered. If $a_n = z^p$ for a prime $p|d$, we have

$$a_n = a_{n-1}^d + c^{d^{n-1} - 1} = \begin{cases} x_1^{10} + y^3 & \Rightarrow z^2 + (-y)^3 = x_1^{10} \quad \text{if } s > 0 \text{ and } a_n = z^2 \\ x_3^7 + y^3 & \Rightarrow z^2 + (-y)^3 = x_3^7 \quad \text{if } s = 0 \text{ and } a_n = z^2 \\ x_2^7 + y^3 & \Rightarrow z^5 + (-x_2)^5 = y^3 \quad \text{if } s > 0 \text{ and } a_n = z^5 \\ x_3^7 + y^3 & \Rightarrow x_3^7 + (-z)^7 = x_3^7 \quad \text{if } t > 0 \text{ and } a_n = z^7. \end{cases}$$

We get a contradiction by Lemma 2.3.

Let $d \equiv 4 \pmod{12}$ with $d > 4$. Then $3|(d-1)$ and $4|d$ and we have

$$a_n = a_{n-1}^d + c^{d^{n-1} - 1} = x_1^4 + y^k = x_2^3 + y_2^3$$

some integers $x_1, x_2, y_1, y_2, k, p$ with odd $k \geq 6$ and for any odd prime $p|d$. Considering equations $a_n + (-y)^k = x_1^4$ if $a_n$ is a square and $a_n + (-x)^p = y_2^3$ if $a_n$ is a $p$-th power for an odd prime $p|d$, we get a contradiction by Lemma 2.3. Hence $a_n$ is not a $p$-the power for any prime divisor of $d$. This proves Theorem 1.

4.2. **Proof of Theorem 2:** We may assume, by Theorem 1 that $d$ is an even integer which is not considered in Theorem 1. As stated after the proof of Lemma 4.1 we need aWe already noted, that it is enough to show that for $n \geq 3$, $a_n$ is not a $p$-th power in $\mathbb{Z}$ for any prime $p$ dividing $d$. Let $p|d$ and suppose that $a_n = z^p$ for some integer $z$. Then

$$z^p = a_n = a_{n-1}^d + c^{d^{n-1} - 1} = x^p + y^k$$

for some integers $x, y, k$ with odd $k \geq 5$. 


From now on, we assume explicit abc Conjecture\[1\]. By Proposition\[2.3\] \(z^p + (-x)^p = y^q\) has no primitive solutions when \(p\) is odd. Hence we assume that \(p = 2\) and therefore we have \(z^2 = a_{n-1}^d + c^{d^{n-1}-1}\). It suffices to show that this equation is not possible. We have \(c < z^{a_{n-1}^d - 1}\) and \(a_{n-1} < z^{2}\) so that

\[
N = N(z^2 \cdot a_{n-1}^d \cdot c^{d^{n-1}-1}) = N(z \cdot a_{n-1} \cdot c) < z^{1 + \frac{2}{d} + \frac{2}{d^{n-1}-1}}
\]

where \(N(r)\) is the radical of \(r\). By Theorem\[2.3\] applied to \(a_{n-1}^d + c^{d^{n-1}-1} = z^2\), we obtain \(z^2 < N^{\frac{2}{d}}\) implying

\[(z^2)^{\frac{d}{2}} < z^{1 + \frac{2}{d} + \frac{2}{d^{n-1}-1}} \implies \frac{d}{2} < 1 + \frac{2}{d} + \frac{2}{d^{n-1}-1} \implies \frac{1}{14} < \frac{1}{d} + \frac{1}{d^2 - 1}.
\]

since \(n \geq 3\). Clearly \(d > 14\) so that \(d^2 - 1 > 2d\) and hence

\[
\frac{1}{14} < \frac{1}{d} + \frac{1}{2d} = \frac{3}{2d} \implies d < 21.
\]

By Theorem\[1\] we need to consider \(d = 14\) where we have the equation \(x^2 = a_n = a_{n-1}^{14} + c^{14^{n-1}-1}\). For \(n\) odd, considering the equation \(x^2 + (-y)^3 = (a_{n-1}^2)^7\) where \(y^3 = c^{14^{n-1}-1}\), we get a contradiction by Lemma\[2.3\]. Hence we assume that \(n\) is even. In particular \(n \geq 4\). Also \(c = \pm 1\) is not possible by Lemma\[2.4\] since \(a_{n-1} \neq 0, \pm 1\). Thus \(|c| \geq 2\) and \(n \geq 4\). We apply Theorem\[2.3\] to \(a_{n-1}^{14} + c^{14^{n-1}-1} = z^2\). If

\[N = N(z^2 \cdot a_{n-1}^{14} \cdot c^{14^{n-1}-1}) < \exp(204.75),\]

we obtain

\[2^{14^{n-1}-1} \leq |c|^{14^{n-1}-1} \leq N^{\frac{7}{d}} \leq \exp(204.75 \cdot \frac{7}{d}),\]

which is a contradiction. Hence \(N \geq \exp(204.75)\). Taking \(\epsilon = \frac{7}{12}\) in Theorem\[2.3\] again, we obtain \(z^2 < N^{1 + \frac{7}{14}}\) implying

\[(z^2)^{\frac{14}{2}} < N \leq z^{1 + \frac{7}{14} + \frac{2}{14^{n-1}-1}} \implies \frac{24}{19} < 1 + \frac{1}{7} + \frac{2}{14^{3}-1} < 1 + \frac{1}{7} + \frac{2}{19},\]

since \(n \geq 4\). This is a contradiction again. This proves Theorem\[2\].

\begin{flushright}
REFERENCES
\end{flushright}

[1] Baker, Alan, \textit{Experiments on the abc-conjecture}, Publ. Math. Debrecen, 65(3-4):253-260, 2004.
[2] Benedetto, Robert and Ingram, Patrick and Jones, Rafe and Manes, Michelle and Silverman, Joseph and Tucker, Thomas, \textit{Current trends and open problems in arithmetic dynamics}, Bulletin of the American Mathematical Society, 56(4):611-685, 2019.
[3] Bennett, Michael A and Chen, Imin and Dahmen, Sander R and Yazdani, Soroosh, \textit{Generalized Fermat equations: a miscellany}, International Journal of Number Theory, 11(01):1-28, 2015.
[4] Bridy, Andrew and Doyle, John and Ghioca, Dragos and Hsia, Liang-Chung and Tucker, Thomas, \textit{Finite index theorems for iterated Galois groups of unicritical polynomials}, Transactions of the American Mathematical Society, 374(1):733-752, 2021.
[5] Bridy, Andrew and Tucker, Thomas J, \textit{Finite index theorems for iterated Galois groups of cubic polynomials}, Mathematische Annalen, 373(1):37-72, 2019.
Stability of Certain Higher Degree Polynomials

[6] Collaboration, LMFDB, The L-Functions and Modular Forms Database (2013), Online Accessed, 16, 2013.

[7] Danielson, Lynda and Fein, Burton, On the irreducibility of the iterates of $x^n - b$, Proceedings of the American Mathematical Society, 130(6):1589-1596, 2002.

[8] DeMark, David and Hindes, Wade and Jones, Rafe and Misplon, Moses and Stoll, Michael and Stoneman, Michael, Eventually stable quadratic polynomials over $\mathbb{Q}$, New York J. Math., 26:526-561, 2020.

[9] Faber, Xander and Granville, Andrew, Prime factors of dynamical sequences, J. Reine Angew. Math., 661:189-214, 2011.

[10] Gratton, Chad and Nguyen, Khoa and Tucker, Thomas J, ABC implies primitive prime divisors in arithmetic dynamics, Bulletin of the London Mathematical Society, 45(6):1194-1208, 2013.

[11] Hamblen, Spencer and Jones, Rafe and Madhu, Kalyani, The density of primes in orbits of $z^d + c$, International Mathematics Research Notices, (7):1924-1958, 2015.

[12] Ingram, Patrick and Silverman, Joseph H, Primitive divisors in arithmetic dynamics, Mathematical Proceedings of the Cambridge Philosophical Society, 146(2):289-302, 2009.

[13] Jones, Rafe and Levy, Alon, Eventually stable rational functions, International Journal of Number Theory, 13(09):2299-2318, 2017.

[14] Jones, Rafe, The density of prime divisors in the arithmetic dynamics of quadratic polynomials, Journal of the London Mathematical Society, 78(2):523-544, 2008.

[15] Krieger, Holly, Primitive prime divisors in the critical orbit of $z^d + c$, International Mathematics Research Notices, (23):5498-5525, 2013.

[16] Laishram, Shanta and Shorey, TN, Baker’s explicit abc-conjecture and applications, Acta Arithmetica, 155(4): 419–429, 2012.

[17] Lang, Serge, Algebra, Revised third edition, volume 211 of Graduate Texts in Mathematics, Springer-Verlag, New York, 2002.

[18] Mihăilescu, Preda, Primary Cyclotomic Units and a Proof of Catalan’s Conjecture, J. reine angew. Math. 572: 167-195, 2004.

[19] Rice, Brian, Primitive prime divisors in polynomial arithmetic dynamics, Integers, 7(1):A26, 2007.

[20] Silverman, Joseph H, The arithmetic of dynamical systems, volume 241 of Graduate Texts in Mathematics. Springer, New York, 2007.

STAT MATH UNIT, INDIAN STATISTICAL INSTITUTE, NEW DELHI 110016, INDIA

Email address: shanta@isid.ac.in

DEPARTMENT OF MATHEMATICS, INDIAN INSTITUTE OF TECHNOLOGY DELHI, NEW DELHI-110016, INDIA

Email address: ritumoni@gmail.com

DEPARTMENT OF MATHEMATICS, INDIAN INSTITUTE OF TECHNOLOGY DELHI, NEW DELHI-110016, INDIA

Email address: himanshusharma985@gmail.com