# ANALOGOUS RESULTS TO ZSIGMONDY'S THEOREM IN ABC-FIELDS

YOUSSEF MARRAKCHI

Abstract. In this paper, we will explore two implications of the *abc*−conjecture on Zsigmondy sets of polynomial and rational functions over number fields.

Contents



## 1. Introduction and Motivation

1.1. **Introduction.** The *abc*−conjecture proposed by Joseph Oesterle and David Masser in 1985 is one of the most famous conjectures in number theory. It originated as an attempt to understand the Szpiro's conjecture and was proven to be equivalent to the modified Szpiro's conjecture. Since then, there have been a couple of claimed proofs for the conjecture, the most famous was the one by Shinichi Mochizuki [Moc21a, Moc21b, Moc21c, Moc21d] in 2012, who claimed to have proven the modified Szpiro's conjecture. However, Mochizuki's attempt was not accepted by the mathematical community, his proof was also shown to have severe gaps in 2018 by Peter Scholze and Jakob Stix [SS18] but it still remained controversial. Despite the fact that the *abc*−conjecture has not been proved neither in its original form nor in its number field version, it does have some interesting implications in various fields in number theory including arithmetic dynamics. Before looking at the implications of the conjecture, we start by looking at the motivation for these results.

*Date*: May 14, 2025.

1.2. **Motivation: Zsigmondy's theorem.** As a motivation for this paper, we will be looking at one of the most useful theorems in number theory and one of the foundational results in the study of prime divisibility which is the Zsigmondy's theorem[Zsi92].

THEOREM 1.1 (Zsigmondy's theorem). *Let $a > b > 0$ be coprime integers. Then for any integer $n > 1$, there is a prime number $p$ that divides $a^n - b^n$ but does not divide $a^m - b^m$ for any $n > m \geq 1$ with the following trivial exceptions:*

*(1) $a - b = 1$ and $n = 1$,*

*(2) $a + b = 2^m$ for some $m \geq 1$ and $n = 2$,*

*(3) $(a, b, n) = (2, 1, 6)$.*

It is easy to see why these exceptions fail to satisfy the mentioned rule:

- When $a - b = 1$ and $n = 1$, $a^n - b^n = 1$ which does not have any prime divisors.
- When $a + b = 2^m$ for some $m \geq 1$ and $n = 2$, we have $a^n - b^n = a^2 - b^2 = (a - b)(a + b)$. So if $p$ divides $a^2 - b^2$ but not $a - b$ then we get $p \mid a + b$. However, if $a + b$ is a power of 2, then $p = 2$ and we already have $2 \mid a - b$ since $a$ and $b$ need to have the same parity to sum up to a power of 2.
- When $(a, b, n) = (2, 1, 6)$, we have $2^6 - 1^6 = 63 = 3^2 \cdot 7$ but $7 \mid 2^3 - 1$ and $3 \mid 2^2 - 1$.

This theorem reveals a deep regularity in the way primes are distributed. There is also a handful of similar results applied to different series like the Fibonacci sequence where we get, using Carmichael's theorem [Car14a, Car14b], that $\mathcal{F}_n$ introduces a new prime divisor $p$ whenever $n \notin \{1, 2, 6, 12\}$ or Pell sequence where $P_n$ has a primitive prime divisor for all $n > 1$. In this paper, we will be looking for analogous results on dynamical sequences introduced on number fields where the *abc*−conjecture holds. We will look at how these results tie to many questions of interest in arithmetic dynamics such as orbits of points and preperiodicity. It is however worth noting that the results we will be looking at rely on the *abc*−conjecture in the corresponding fields, however, the result above is not a conjecture but a theorem that has been proved in 1892 by Zsigmondy in [Zsi92] without using *abc*−conjecture.

## 2. Conjecture Statement and Definitions

In this section, we will look into the statement of the *abc*−conjecture. First, we will look into its known version for natural numbers, then we will look into its version for number fields. Finally, we will see how the two definitions relate to each other.

2.1. ***abc*−conjecture for natural numbers.** To understand the statement of the *abc*−conjecture, we need to first define the notion of a radical of an integer.

DEFINITION 2.1 (Radical function). Let $n$ be a positive integer. We denote by $\mathrm{Rad}(n)$ the product of all prime factors of $n$. In other words, we get

$$\mathrm{Rad}(n) = \prod_{p \mid n} p$$

EXAMPLE 2.2 (Examples of radical of integers).

- $\text{Rad}(24) = 6$,
- $\text{Rad}(2^n) = 2 \qquad \forall n \geq 1$,
- $\text{Rad}(p) = p \qquad$ for all prime $p$.

With definition 2.1 in hand, we can now present the $abc-$conjecture.

CONJECTURE 2.3. Let $\epsilon$ be a positive real number. Then, exists a constant $C_\epsilon$ such that for every triple $(a, b, c)$ of coprime positive satisfying $a + b = c$, we have

$$c \leq \text{Rad}(abc)^{1+\epsilon} \cdot C_\epsilon$$

This conjecture claims a very deep relationship between addition and multiplication of natural numbers. It tells us that for triplet $(a, b, c)$, if we have the property that $a + b = c$, the product of their prime factors cannot be too small compared to their magnitude. It is also worth noting that for the statement of the theorem, having $\epsilon > 0$ is necessary because for $\epsilon = 0$ it is easy to prove that there is no such constant $C_0$. In fact, if we take $a = 1, b = 2^{p(p-1)} - 1$ and $c = 2^{p(p-1)}$ for some odd prime $p$, then, we will have $\text{Rad}(abc) = 2 \cdot \text{Rad}(b)$. However, we have by Fermat's little theorem that $p \mid 2^{p-1} - 1$. And using LTE (lifting the exponent lemma), we have that $v_p\left(\left(2^{p-1}\right)^p - 1\right) = v_p(p) + v_p(2^{p-1} - 1) \geq 1 + 1 = 2$. So $\text{Rad}(b) \leq \frac{b}{p}$. Therefore, we get $\text{Rad}(abc) \leq \frac{2b}{p} \leq \frac{2c}{p}$. So we will need $C_0 \geq \frac{p}{2}$. But since this must hold for every odd prime number, then there is no such $C_0$.

2.2. **abc-conjecture in number fields.** Throughout this paper, we will denote by $K$ a number field and $\mathcal{O}_K$ the ring of integers of $K$. Moreover, for any prime $p$ of $K$, we will denote by $k_p$ the residue field of $p$ and we will set $N_p = \frac{\log |k_p|}{[K:\mathbb{Q}]}$. With this in hand, we can define our height functions.

DEFINITION 2.4 (Weil height function). Let $(a_1, a_2, \dots a_n) \in K^n \backslash \{(0, 0, 0 \dots 0)\}$, then we have

$$\begin{aligned} h(a_1, a_2 \dots a_n) = &- \sum_{p \in \mathcal{O}_K} \min(v_p(a_1), v_p(a_2) \dots v_p(a_n)) N_p \\ &+ \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma: K \to \mathbb{C}} \max(\log|\sigma(a_1)|, \log|\sigma(a_2)|, \dots \log|\sigma(a_n)|) \end{aligned}$$

where the notation $\sigma : K \to \mathbb{C}$ refers to the embeddings from $K$ to $\mathbb{C}$.

Note that in the case where $K = \mathbb{Q}$ and $n = 3$, we get

$$\begin{aligned} h(a, b, c) = &- \sum_p \min(v_p(a), v_p(b), v_p(c)) \log p \\ &+ \max(\log(|a|), \log(|b|), \log(|c|)). \end{aligned}$$

For the case $K = \mathbb{Q}$, it is easy to see from the definition that for any $\alpha \in \mathbb{Q}$, we have $h(\alpha a, \alpha b, \alpha c) = h(a, b, c)$. So, if we choose the unique $\alpha$ such that $\alpha a, \alpha b$ and $\alpha c$ are integers with greatest common divisor 1, we get

$$- \sum_p \min(v_p(\alpha a), v_p(\alpha b), v_p(\alpha c)) = 0$$

$$\Rightarrow h(a, b, c) = h(\alpha a, \alpha b, \alpha c) = \log(|\alpha|) + \log \max(|a|, |b|, |c|). \tag{1}$$

EXAMPLE 2.5. Suppose we have $K = \mathbb{Q}$ and $(a, b, c) = (\frac{21}{8}, \frac{119}{5}, \frac{161}{9})$ then we get

$$h(a, b, c) = 3\log 2 + 2\log 3 + \log 5 - \log 7 + \log \frac{119}{5} = \log 1224. \tag{2}$$

But equation (2) could have also been obtained by looking for the unique $\alpha$ mentioned above which in this case would be $\frac{360}{7}$.

PROPOSITION 2.6 (Properties of the height function). *Let $\alpha \in K$, $f, g \in K[x, y]$ with degree $d$, then we have by* [GNT13, Eq (2.0.2)] *and* [GNT13, Proposition 3.3]*:*

$$\sum_{v_p(\alpha)>0} v_p(\alpha) N_p \leq h(\alpha, 1) \tag{3}$$

$$h(f(x, y), 1) \leq d \cdot h(x, y) + O(1) \tag{4}$$

$$h(f(x, y), g(x, y)) + O(1) \geq d \cdot h(x, y) \tag{5}$$

DEFINITION 2.7 (Radical function in number field). Again, let $(a, b, c) \in K^3 \backslash \{(0, 0, 0)\}$ and let $I(a, b, c) = \{p \text{ prime of } \mathcal{O}_K | v_p(a) \neq v_p(b) \text{ or } v_p(a) \neq v_p(c)\}$. Then we have

$$\mathrm{rad}(a, b, c) = \sum_{p \in I} N_p$$

.

It is also easy to see from this definition that $\mathrm{rad}(a, b, c) = \mathrm{rad}(\alpha a, \alpha b, \alpha c)$. Notice that this definition of the radical function is not directly analogous to our definition of Rad in 2.1. In other words, when $K = \mathbb{Q}$, we don't have $\mathrm{rad}(a, b, c) = \mathrm{Rad}(abc)$. In fact, we actually get $\mathrm{rad}(a, b, c) = \log(\mathrm{Rad}(abc))$.

EXAMPLE 2.8. Looking at the same example from above, we get

$$\mathrm{rad}\left(\frac{21}{8}, \frac{119}{5}, \frac{161}{9}\right) = \log(2)+\log(3)+\log(5)+\log(7)+\log(17)+\log(23) = \log(82110)$$

With definitions 2.4 and 2.7 in hand, we can now look at conjecture statement in number fields [GNT13, Conjecture 3.1] which relates the height of the triplet $(a, b, c)$ with their radical :

CONJECTURE 2.9 ($abc-$conjecture). Let $\epsilon > 0$, there exists $c_{K,\epsilon} > 0$ such that for all non-zero $a, b, c \in K$ such that $a + b = c$, we have

$$h(a, b, c) < (1 + \epsilon) \cdot \mathrm{rad}(a, b, c) + c_{K,\epsilon}$$

We call an ***abc*-field** any number field where conjecture 2.9 holds. To give more intuition about this conjecture and how it is related to its more known version in $\mathbb{Z}$, we can look at what it means when $K = \mathbb{Q}$. By choosing the same $\alpha$ as above, we get $A = \alpha a, B = \alpha b$ and $C = \alpha c$ are coprime integers such that $A + B = C$ and

$$h(A, B, C) = h(a, b, c) < (1 + \epsilon) \cdot \mathrm{rad}(a, b, c) + c_{K,\epsilon} = (1 + \epsilon) \cdot \mathrm{rad}(A, B, C) + c_{K,\epsilon}$$

But since $A, B$ and $C$ are coprime integers, then we have from (1) $h(A, B, C) = \log(\max(A, B, C)$ and $\mathrm{rad}(A, B, C) = \log(\mathrm{Rad}(ABC))$. Therefore, we get

$$\log(\max(A, B, C)) < (1 + \epsilon) \cdot \log(\mathrm{Rad}(ABC)) + c_{\mathbb{Q},\epsilon}$$

And by taking the exponential of both sides we obtain

$$\max(A, B, C) < \mathrm{Rad}(ABC)^{1+\epsilon} \cdot C_{\mathbb{Q},\epsilon} \tag{6}$$

where $C_{K,\epsilon} = \exp(c_{K,\epsilon})$. Then, by simple manipulation of the signs of $A, B, C$, we can force the relationship $C > \max\{A, B\}$ while keeping the same absolute values,

and then by taking $C_\epsilon = C_{\mathbb{Q},\epsilon}$ we get from (6) the formulation we had in Conjecture 2.3.

## 3. Main Results

3.1. **Preliminaries.** Before looking into our 2 main results, we will look at a couple of definitions that will help us understand them. In this paper, we will be dealing with functions $\phi : K \to K$. In our first result, $\phi(x) \in K(x)$ and in our second result we will deal with unicritical polynomials (polynomials of the form $\phi(x) = (x-\lambda)^d + \gamma$).

Definition 3.1 (Primitive prime divisor). Let $\phi$ be our function of interest, and let $p$ be a prime in $\mathcal{O}_K$, $n$ be an integer and $\alpha \in K$. We say that $p$ is a primitive prime divisor of $\phi^n(\alpha)$ if the following is satisfied:

(1) $\phi^n(\alpha) \neq 0$,

(2) $v_p(\phi^n(\alpha)) > 0$,

(3) $v_p(\phi^m(\alpha)) \leq 0$ for all integers $m$ such that $1 \leq m < n$.

If $\phi^n(\alpha)$ does not have a primitive prime divisor, we say that $n$ is in the Zsigmondy set of the forward orbit $\{\phi^i(\alpha)\}_{i\geq 0}$. We can see from the definition that if $\alpha$ is a preperiodic point of $\phi$, then $\exists N \in \mathbb{N}$ such that $\forall n \geq N$, we have $n$ is in the Zsigmondy set of $\{\phi^i(\alpha)\}_{i\geq\alpha}$. We can choose this $N$ to be the index of the first repeated value in the orbit of $\alpha$.

3.2. **Analogous result on rational functions.** In this section we will be looking at [GNT13, Theorem 1.1] which deals with rational functions in $K$. The result in the following.

Theorem 3.2. *Let $K$ be an abc−field, let $\phi \in K(x)$ have degree strictly bigger than 1, and let $\alpha \in K$ such that $h_\phi(\alpha) > 0$ and there is no $n \in \mathbb{N}$ such that $\phi^n(\alpha) = 0$. We also suppose that $\phi(z) \neq cz^{\pm d}$. Then Zsigmondy set of $\{\phi^i(\alpha)\}_{i\geq\alpha}$ is finite.*

The canonical height function here is defined as the following:

$$h_\phi(z) = \lim_{n\to\infty} \frac{h_0(\phi^n(z))}{d^n} \tag{7}$$

where $d$ is the degree of $\phi$ and $h_0$ is defined using the height function in 2.4 the following way:

$$h_0(z) = h(z,1) = -\sum_{p \text{ prime of } \mathcal{O}_K} \min(v_p(z),0)N_p + \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma:K\to\mathbb{C}} \max(\log|\sigma(z)|,0)$$

In the case where $K = \mathbb{Q}$, if we write $z$ as $\frac{a}{b}$ where $a$ and $b$ are coprime integers, we will get $h_0(z) = \log(\max(|a|,|b|))$.

The result of theorem 3.2 is really strong because it starts from the *abc*−conjecture which constrains how prime divisors are distributed in diophantine equations, but helps us govern prime behavior in dynamical systems.

EXAMPLE 3.3. We can take $\phi(x)$ to be as simple as $x^2+1$. Using our theorem in $\mathbb{Q}$ and assuming that the $abc-$conjecture holds. It is easy to see that $\forall x \in \mathbb{Q}$, we have $h_\phi(x) > 0$ and that 0 is not part of the orbit of $\alpha$ under $\phi$ so we have for $x \in \mathbb{Q}$ the Zsigmondy set of $\{\phi^n(x)\}_{n\geq 1}$ has finite size.

3.2.1. *Proof strategy for thorem 3.2.* In the proof introduced by [GNT13], they start by writing $\phi(x) = \frac{P(x)}{Q(x)}$ such that $P, Q \in \mathcal{O}_K[x]$. Then we can also get $\phi^i(x) = \frac{P_i(x)}{Q_i(x)}$ in the following way: We start by taking $p$ and $q$ as the degree $d$ homogenizations of $P$ and $Q$. So $p$ and $q$ are homogeneous polynomials such that $p(x,1) = P(x)$ and $q(x,1) = Q(x)$. We also take $p_1 = p, q_1 = q$ and $p_i(x,y) = p(p_{i-1}(x,y), q_{i-1}(x,y))$ and $q_i(x,y) = q(p_{i-1}(x,y), q_{i-1}(x,y))$. We will prove by induction on $i$ that by taking $P_i(x) = p_i(x,1)$ and $Q_i(x) = q_i(x,1)$ we get

$$\phi^i(x) = \frac{P_i(x)}{Q_i(x)} \tag{8}$$

*Proof of result (8).* The result holds for $i = 1$ by definition. Suppose it holds for $i$. We have

$$\frac{P_{i+1}(x)}{Q_{i+1}(x)} = \frac{p_{i+1}(x,1)}{q_{i+1}(x,1)} = \frac{p(p_i(x,1), q_i(x,1))}{q(p_i(x,1), q_i(x,1))} = \frac{p(P_i(x), Q_i(x))}{q(P_i(x), Q_i(x))}$$

Notice however, that since $p$ and $q$ are homogeneous of degree $d$, then we have $p(\alpha x, \alpha y) = \alpha^d p(x,y)$. So by taking $\alpha = \frac{1}{Q_i(x)}$ the result above is equal to

$$\begin{aligned}
\frac{p(P_i(x), Q_i(x))}{q(P_i(x), Q_i(x))} &= \frac{Q_i(x)^d p\left(\frac{P_i(x)}{Q_i(x)}, 1\right)}{Q_i(x)^d q\left(\frac{P_i(x)}{Q_i(x)}, 1\right)} \\
&= \frac{p\left(\frac{P_i(x)}{Q_i(x)}, 1\right)}{q\left(\frac{P_i(x)}{Q_i(x)}, 1\right)} \\
&= \frac{P\left(\frac{P_i(x)}{Q_i(x)}\right)}{Q\left(\frac{P_i(x)}{Q_i(x)}\right)} \\
&= \frac{P(\phi^i(x))}{Q(\phi^i(x))} \\
&= \phi^{i+1}(x)
\end{aligned}$$

□

After that, the paper proves the following result which bounds the product of all primes $p$:

LEMMA 3.4. *Let $\delta > 0$, let $\alpha \in K$ such that $\lim_{s\to\infty} h_0(\phi^s(\alpha)) = \infty$ and let $F$ be a factor of $P_i$ (so $P_i(x) = F(x) \cdot G(x)$ for some polynomial $G$) such that all roots of $F$ are non-periodic and do not have 0 in their orbit, then there is a constant $C_\delta$ such that for all positive integers $n$, we have*

$$\sum_{p \in Z} N_p \leq \delta h_0(\phi^n(\alpha)) + C_\delta \tag{9}$$

*Where $Z$ is the set of primes $p$ such that* $\min(v_p(\phi^m(\alpha)), v_p(F(\phi^{n-i}(\alpha)))) > 0$ *for some* $m < n$.

To give more intuition about how this lemma can be used to prove the theorem we need to rewrite $\phi^i(x) = \frac{F(x)\cdot G(x)}{Q_i(x)}$, where $F, G$ and $Q_i$ are coprime. So we get that for all but finitely many primes $p$, we have $v_p(\phi^i(z)) > 0$ whenever $v_p(F(z)) > 0$. Therefore, if we find that for all but finitely many $n$ there is prime $p$ such that $v_p(F(\phi^{n-i}(\alpha)) > 0$ and $v_p(\phi^m(\alpha)) \leq 0$ for all $1 \leq m < n$, then we get a proof to the theorem. Let $J$ be the set of primes $p$ such that $v_p(F(\phi^{n-i}(\alpha))) > 0$. So the last statement on $n$ (existence of $p$ such that $v_p(F(\phi^{n-i}(\alpha)) > 0$ and $v_p(\phi^m(\alpha)) \leq 0$ for all $1 \leq m < n$) is equivalent to the existence of $p$ such that $p \in J$ but $p \notin Z$. But since we have by definition that $Z \subset J$ then this is equivalent to

$$\sum_{p \in Z} N_p < \sum_{p \in J} N_p \tag{10}$$

So the first lemma 3.4 is used to upper bound the LHS while the next result lower bounds the RHS:

PROPOSITION 3.5. *If $F$ has degree at least 4 then*

$$\sum_{p \in J} N_p \geq h_0(\phi^{n-i}(\alpha)) + C_1 \tag{11}$$

*for some constant $C_1$*

To prove proposition 3.5, we make use of the following lemma that shows a strong result for homogenous polynomials in number fields:

LEMMA 3.6. *Given any homogeneous $f(x, y) \in K[x, y]$, there are homogeneous polynomials $a(x, y), b(x, y), c(x, y)$ all of degree $D$ such that:*

*(1) $a(x, y)b(x, y)c(x, y)$ has exactly $D+2$ non proportional linear factors over $\overline{K}$,*

*(2) $a(x, y)b(x, y)c(x, y)$contains all the linear factors in $f$,*

*(3) $a(x, y) + b(x, y) = c(x + y)$.*

EXAMPLE 3.7. For $K = \mathbb{Q}$ and let $f(x, y) = x^2 - y^2$. Then we can choose

- $a(x, y) = xy - y^2$,
- $b(x, y) = xy + y^2$,
- $c(x, y) = 2xy$.

Then we get $a, b, c$ are all homogeneous with degree 2 and

$$a(x, y)b(x, y)c(x, y) = 2 \cdot x \cdot y^3 \cdot (x - y)(x + y)$$

So the product has $D + 2$ non proportional linear factors including the ones in $f$.

Using lemma 3.6, we can prove the following proposition:

PROPOSITION 3.8. *If $f(x,y) \in \mathcal{O}_K[x,y]$ is homogeneous polynomial of degree 3 or more without repeated factors. Let $z_1, z_2 \in \mathcal{O}_K$ and $S$ be a finite set of primes in $K$ such that for all prime $p \notin S$, we have $\min(v_p(z_1), v_p(z_2)) = 0$. Finally, let $\epsilon > 0$. Then we get*

$$(\deg f - 2 - \epsilon) \cdot h(z_1, z_2) \leq \sum_{v_p(f(z_1,z_2))>0} N_p + O(1)$$

*The $O(1)$ will depend on $f, K$ and $S$ but not on $z_1$ and $z_2$.*

*Proof.* We start by applying lemma 3.6 to get our homogeneous polynomials $a, b, c \in \mathcal{O}_K[x,y]$ of degree $D = \deg f$ such that $a(x,y)b(x,y)c(x,y)$ has $D+2$ non-proportional linear factors including all the factors in $f$. Given that $f$ has no repeated factors, then we can write $a(x,y)b(x,y)c(x,y)$ as $f(x,y)g(x,y)$ for some polynomial $g$. Then, we get to apply the $abc-$conjecture (finally) on $a(z_1,z_2), b(z_1,z_2)$ and $c(z_1,z_2)$ to get the following result:

$$\left(1 - \frac{\epsilon}{D}\right) \cdot h(a(z_1,z_2), b(z_1,z_2)) \leq \sum_{p \in I(a(z_1,z_2), b(z_1,z_2), c(z_1,z_2))} N_p + O(1) \tag{12}$$

In fact to get inequality (12) from the conjecture, we plugged in $\frac{\epsilon}{D}$ for $\epsilon$ and we used the fact that $\frac{1}{1-\epsilon} \geq 1 + \epsilon$ and $h(a_1, a_2) \leq h(a_1, a_2, a_3)$ which can be seen from the definition of $h$.
Now because for all prime $p \notin S$, we have $\min(v_p(z_1), v_p(z_2)) = 0$, then we enlarge $S$ such that for all prime $p \notin S$, we have

$$p \in I(a(z_1,z_2), b(z_1,z_2), c(z_1,z_2)) \iff v_p(a(z_1,z_2)b(z_1,z_2)c(z_1,z_2)) > 0$$

But since $a(z_1,z_2)b(z_1,z_2)c(z_1,z_2) = f(x,y)g(x,y)$, then we have

$$\begin{aligned}
\sum_{p \in I(a(z_1,z_2), b(z_1,z_2), c(z_1,z_2))} N_p &= \sum_{p \in I(a(z_1,z_2), b(z_1,z_2), c(z_1,z_2)) \setminus S} N_p + \sum_{p \in S \cap I(a(z_1,z_2), b(z_1,z_2), c(z_1,z_2))} N_p \\
&\leq \sum_{p \notin S | v_p(f(x,y)g(x,y))>0} N_p + \sum_{p \in S} N_p \\
&\leq \sum_{v_p(f(x,y))>0} N_p + \sum_{v_p(g(x,y))>0} N_p + O(1)
\end{aligned}$$

Where $O(1)$ is just a constant upper bounded by $\sum_{p \in S} N_p$. Now combining this result with inequality (12) we get

$$\left(1 - \frac{\epsilon}{D}\right) \cdot h(a(z_1,z_2), b(z_1,z_2)) \leq \sum_{v_p(f(x,y))>0} N_p + \sum_{v_p(g(x,y))>0} N_p + O(1) \tag{13}$$

Now using properties (3) and (4) we have:

$$\sum_{v_p(g(z_1,z_2))>0} N_p \leq h_0(g(z_1,z_2)) \leq (D + 2 - \deg f) \cdot h(z_1,z_2) + O(1) \tag{14}$$

And using (5) we also get:

$$h(a(z_1,z_2), b(z_1,z_2)) + O(1) \geq D \cdot h(z_1,z_2) \tag{15}$$

Plugging (14) and (15) in (13) we get the desired

$$(\deg f - 2 - \epsilon) \cdot h(z_1, z_2) \leq \sum_{v_p(f(z_1,z_2))>0} N_p + O(1)$$

which finishes the proof of proposition 3.8. □

Now, with a direct application of proposition 3.8, we can prove the following result:

PROPOSITION 3.9. *Let $F(x) \in \mathcal{O}_K[x]$ be a polynomial of degree 3 or more without repeated factors. Then, for any $\epsilon > 0$ there is a constant $C_{f,\epsilon}$ such that*

$$\sum_{v_p(F(z))>0} N_p \geq (\deg F - 2 - \epsilon) h_0(z) + C_{F,\epsilon}$$

*Proof of 3.9.* Take $f$ to be the homogenization of $F$. We use the fact that $F(z) = f(z, 1)$ and $h_0(z) = h(z, 1)$. Using $\epsilon = 1$, we get

$$\sum_{v_p(F(z))>0} N_p \geq (\deg F - 3) h_0(z) + C_{F,\epsilon}$$

□

Using proposition 3.9, when when $F$ has degree at least 4, we get 11 which concludes the proof of proposition 3.5.
Combining (11) with lemma 3.4 used with $\delta = \frac{1}{2}$, we get that whenever $h_0(\phi^{n-i}(\alpha)) > 2(C_2 - C_1)$, we have the inequality (10). Therefore, by taking $\alpha$ such that $h_\phi(\alpha) > 0$, we know that $\lim_{n\to\infty} h_0(\phi^n(\alpha)) = \infty$. So, there is $N \in \mathbb{N}$ such that $h_0(\phi^{n-i}(\alpha)) > 2(C_2 - C_1)$ whenever $n \geq N$, so (10) holds for all but finitely many $n$, which concludes the proof.

3.3. **Analogous result on unicritical polynomials.** In this section we will be looking at a different theorem proved in [Loo20] that bounds the size of the Zsigmondy set for unicritical polynomials on $abc-$field $K$ even further. For the statement of the next theorem, we will refer by multiplicity 1 prime divisor of $\phi^n(\alpha)$ any prime $p$ that satifies all the conditions of definition 3.1 but also satisfies the following:

$$v_p(\phi^n(\alpha)) = 1$$

THEOREM 3.10. *Assume $K$ is an $abc-$ field such that $K = \mathbb{Q}$ or $K$ is an imaginary quadratic field. Let $d \geq 3$ and $\phi(x) = (x-\lambda)^d + c \in K[x]$ such that $\lambda - c \in \mathcal{O}_K$. Let*

$$v(\phi) = \frac{h(\lambda)}{\max\{1, h_0(c-\lambda)\}}$$

*Then , $\exists D_1, D_2$ depending only on $d$ and $K$ such for all non-preperiodic $\alpha \in K$, there is a multiplicity 1 prime divisor of $\phi^n(\alpha)$ for all $n > D_1 \max(\log(v(\phi)), 0) + D_2$.*

We see that theorem 3.10 adds two stronger results for unicritical polynomials to the results mentioned in theorem 3.2 which are:

(1) Bounding the size of the Zsigmondy sets
(2) Proving the existence of multiplicity 1 prime divisor of $\phi^n(\alpha)$ starting from some index $N$.

## 4. Relation to Zsigmondy's Theorem

Although the 2 results shown share a thematic resemblance to Zsigmondy's theorem, in that they concern the existence of primitive prime divisors in dynamical settings, they do not imply Zsigmondy's theorem in $\mathbb{Q}$ because we cannot write $a^n - b^n$ for integers $a, b$ as $\phi^n(\alpha)$ for some function $\phi \in \mathbb{Q}(x)$ and $\alpha \in \mathbb{Q}$ except for the case where $b = 1$ where we can take $\phi(x) = a(x+1) - 1$ and $\alpha = 0$. However, even in this case, the polynomial mentioned is of degree 1 which is not covered by either 3.2 or 3.10. In the case $b \neq 1$, we can also take $\phi(x) = \frac{a}{b} \cdot (x+1) - 1$, which would give $\phi^n(0) = \frac{a^n - b^n}{b^n}$, but it is also of degree 1. By choosing other polynomials we can prove the result (assuming $abc-$conjecture holds) where $n$ takes values only in a strict subset of $\mathbb{N}$ with density 0 and also $b = 1$ again.

Example 4.1. For any integer $a > 1$, we take $\phi(x) = a(x+1)^2 - 1$ and $\alpha = 0$. Then we get $\phi^n(\alpha) = a^{2^n - 1} - 1$. Theorem 3.2 here will tell us that for all but finitely many $n$, $\phi^n(\alpha)$ will have a primitive prime divisor, which means that there is a $p$ such that $v_p(a^{2^n-1} - 1)$ and $v_p(a^{2^m-1} - 1) \leq 0$ for all $m < n$. Notice that this does not mean that $v_p(a^k - 1) \leq 0$ for all $k \leq 2^n - 1$, it is only true for values of $k$ that can be written as $k = 2^m - 1$ for some $m$ such that $n < m \geq 1$. So using this result alone, we cannot conclude that $2^n - 1$ is not in the Zsigmondy set of the sequence $c_n = a^n - b^n$.

Although, as it turns out, Zsigmondy's theorem cannot be proved using a direct application of the results presented here. The question remains open to whether there is a way to adapt the proof in [GNT13] or [Loo20] in order to come up with another proof for the Zsigmondy's theorem in $abc-$fields.

## References


[Car14a] R. D. Carmichael. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math. (2)*, 15(1-4):30–48, 1913/14.

[Car14b] R. D. Carmichael. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math. (2)*, 15(1-4):49–70, 1913/14.

[GNT13] C. Gratton, K. Nguyen, and T. J. Tucker. *ABC* implies primitive prime divisors in arithmetic dynamics. *Bull. Lond. Math. Soc.*, 45(6):1194–1208, 2013.

[Loo20] Nicole R. Looper. The *ABC*-conjecture implies uniform bounds on dynamical Zsigmondy sets. *Trans. Amer. Math. Soc.*, 373(7):4627–4647, 2020.

[Moc21a] Shinichi Mochizuki. Inter-universal Teichmüller theory I: Construction of Hodge theaters. *Publ. Res. Inst. Math. Sci.*, 57(1-2):3–207, 2021.

[Moc21b] Shinichi Mochizuki. Inter-universal Teichmüller theory II: Hodge-Arakelov-theoretic evaluation. *Publ. Res. Inst. Math. Sci.*, 57(1-2):209–401, 2021.

[Moc21c] Shinichi Mochizuki. Inter-universal Teichmüller theory III: Canonical splittings of the log-theta-lattice. *Publ. Res. Inst. Math. Sci.*, 57(1-2):403–626, 2021.

[Moc21d] Shinichi Mochizuki. Inter-universal Teichmüller theory IV: Log-volume computations and set-theoretic foundations. *Publ. Res. Inst. Math. Sci.*, 57(1-2):627–723, 2021.

[SS18] Peter Scholze and Jakob Stix. Why abc is still a conjecture. *URL http://www. kurims. kyoto-u. ac. jp/motizuki/SS2018-08. pdf*, 2018.

[Zsi92] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.



Massachusetts Institute of Technology
*Email address*: youss24@mit.edu