Binary polynomial power sums vanishing at roots of unity

Yuri Bilu
IMB, Université de Bordeaux & CNRS
E-mail: yuri@math.u-bordeaux.fr,

Florian Luca
School of Maths, Wits University, South Africa
Research Group in Algebraic Structures and Applications,
King Abdulaziz University, Jeddah, Saudi Arabia
Centro de Ciencias Matemáticas,
UNAM, Morelia, Mexico
E-mail: Florian.Luca@wits.ac.za

Abstract

Let $c_1(x), c_2(x), f_1(x), f_2(x)$ be polynomials with rational coefficients. The "obvious" exceptions being excluded, there can be at most finitely many roots of unity among the zeros of the polynomials $c_1(x)f_1(x)^n + c_2(x)f_2(x)^n$ with $n = 1, 2 \ldots$. We estimate the orders of these roots of unity in terms of the degrees and the heights of the polynomials c_i and f_i.

2020 *Mathematics Subject Classification*: Primary 11D61; Secondary 11G50, 11J86.

Key words and phrases: polynomial power sums, roots of unity, primitive divisors.

Contents

1 Introduction **2**

2 Heights **5**

3 Cyclotomic polynomials **8**

4 Schinzel's Primitive Divisor Theorem **11**

5 Proof of Theorems 1.2 and 1.3 **16**

6 Proof of Theorem 1.6 **25**

1 Introduction

Let $c_1(x), c_2(x), f_1(x), f_2(x)$ be non-zero polynomials in $\mathbb{Q}[x]$. We denote by $\mathbf{u} := \{u_n(x)\}_{n\geq 1} \subset \mathbb{Q}[x]$ the sequence of polynomials given by

$$u_n(x) = c_1(x)f_1(x)^n + c_2(x)f_2(x)^n \quad \text{for all} \quad n \geq 1. \tag{1.1}$$

We study roots of unity ζ such that $u_n(\zeta) = 0$ for some n. It can happen accidentally that $u_n(x)$ is the zero polynomial for some n. We ignore these n. We would like to show that aside from some exceptional situations, the following holds true: there exist at most finitely many roots of unity ζ such that for some n the polynomial $u_n(x)$ is not identically zero but $u_n(\zeta) = 0$.

The following example shows that we indeed have to exclude some exceptional cases.

Example 1.1. *Let a, b be integers with b non-zero, and assume that*

$$c_2(x)/c_1(x) = \delta x^a, \qquad f_2(x)/f_1(x) = \varepsilon x^b, \qquad \delta, \varepsilon \in \{1, -1\}.$$

We then get

$$u_n(x) = c_1(x)f_1(x)^n(1 + \delta\varepsilon^n x^{a+bn})$$

and we see that if $x = \zeta$ is such that $\zeta^{a+bn} = -\delta\varepsilon^n$, then $u_n(\zeta) = 0$. The condition that $b \neq 0$ insures that $u_n(x)$ is non-zero for n sufficiently large (in fact, for all n except eventually one of them, namely $n = -a/b$), and every $u_n(x)$ vanishes at the roots of unity of order $|a + bn|$ or $2|a + bn|$ depending on the sign of $\delta\varepsilon^n$.

It turns out that this example is the only case when the polynomials $u_n(x)$ vanish at infinitely many roots of unity. We have the following theorem.

Theorem 1.2. *Let $c_1(x), c_2(x), f_1(x), f_2(x) \in \mathbb{Q}[x]$ be non-zero polynomials. For a positive integer n define $u_n(x)$ as in (1.1). Then the following two conditions are equivalent.*

1. *There exist infinitely many roots of unity ζ such that for some n the polynomial $u_n(x)$ is not identically zero but $u_n(\zeta) = 0$.*

2. *There exist $a, b \in \mathbb{Z}$ with $b \neq 0$ and $\delta, \varepsilon \in \{1, -1\}$ such that*

$$c_2(x)/c_1(x) = \delta x^a, \qquad f_2(x)/f_1(x) = \varepsilon x^b.$$

It is not hard to derive this theorem from classical results on unlikely intersection like the Theorem of Bombieri-Masser-Zannier-Maurin [5, 6, 9]. See also the recent work of Ostafe and Shparlinski [10, 11], especially Theorem 2.11 and Corollary 2.14 in [11].

However, we are mainly interested in a quantitative statement: when condition 2 of Theorem 1.2 is not satisfied, we want to bound the orders of the roots of unity ζ such that $u_n(\zeta) = 0$ for some n, in terms of the degrees and the heights of our polynomials f_i, c_i. To the best of our knowledge, no quantitative version of the Bombieri-Masser-Zannier-Maurin theorem is available which would imply such a bound.

To state our result, let us recall the definition of the height of a non-zero polynomial in $\mathbb{Q}[x]$. The height of a primitive vector $\mathbf{a} = (a_1, \ldots, a_k) \in \mathbb{Z}^k$ (*primitive* means that $\gcd(a_1, \ldots, a_k) = 1$) is defined by

$$\mathrm{h}(\mathbf{a}) := \log \max\{|a_1|, \ldots, |a_k|\}.$$

In general, given a non-zero vector $\mathbf{a} \in \mathbb{Q}^{k+1}$, there exists $\lambda \in \mathbb{Q}^\times$, well defined up to multiplication by ± 1, such that $\mathbf{a}^* = \lambda \mathbf{a}$ is primitive, and we set $\mathrm{h}(\mathbf{a}) := \mathrm{h}(\mathbf{a}^*)$.

We define the height of a non-zero polynomial $g(x) \in \mathbb{Q}[x]$ as the height of the vector of its coefficients. More generally, we define the height of a non-zero vector $(g_1, \ldots, g_k) \in \mathbb{Q}[x]^k$ as the height of the vector formed of the coefficients of all polynomials $g_1, \ldots, g_k$.

We have the following theorem.

Theorem 1.3. *Let $c_1(x), c_2(x), f_1(x), f_2(x) \in \mathbb{Q}[x]$ be non-zero polynomials such that condition 2 of Theorem 1.2 is not satisfied. Set*

$$\begin{aligned} D &:= \max\{\deg c_1, \deg c_2, \deg f_1, \deg f_2\}, \\ X &:= \max\{3, \mathrm{h}(c_1, c_2), \mathrm{h}(f_1, f_2)\}. \end{aligned}$$

Let m be a positive integer and ζ a primitive mth root of unity such that for some n the polynomial $u_n(x)$ is not identically zero but $u_n(\zeta) = 0$. Then

$$m \le e^{100D(X+D)}. \tag{1.2}$$

The numerical constant 100 here is rather loose; probably, one can replace it by 4 or so.

One may ask whether there is a bound for m which depends only on one of the parameters D or X. The following examples show that this is not the case.

Example 1.4. *Consider* $u_n(x) = (2x)^n - 2^m$, *for which*

$$(c_1(x), c_2(x), f_1(x), f_2(x)) = (1, -2^m, 2x, 1), \qquad X = \max\{3, m \log 2\}.$$

Then $u_m(x) = 2^m(x^m - 1)$ *vanishes at primitive* m*th roots of unity, and we have* $m \ge X/\log 2$ *(provided* $m \ge 5$*). Hence no bound independent of* X *is possible.*

Example 1.5. *Consider* $u_n(x) = x^n + x^D + 1$, *for which*

$$(c_1(x), c_2(x), f_1(x), f_2(x)) = (1, x^D + 1, x, 1).$$

Then $u_{2D} = (x^{3D} - 1)/(x^D - 1)$ *vanishes at primitive* $3D$*th roots of unity, so we have* $m \ge 3D$. *Hence no bound independent of* D *is possible.*

One may also ask whether in Theorem 1.3 one can bound n such that $u_n(x)$ vanishes at a root of unity. The answer is "no" in general. Indeed, if polynomials $c_1(x)f_1(x)$ and $c_2(x)f_2(x)$ have a common root, then every $u_n(x)$ will vanish at that root. But even if $c_1(x)f_1(x)$ and $c_2(x)f_2(x)$ do not simultaneously vanish at some root of unity, it is still possible that $u_n(x)$ vanishes at a root of unity for infinitely many n. This is, for instance, the case for the sequence $u_n(x) = x^n + x^D + 1$ from Example 1.5: it vanishes at primitive $3D$th roots of unity whenever $n \equiv 2D \bmod 3D$. Nevertheless, we can bound the *smallest* n with this property. Here is the precise statement.

Theorem 1.6. *In the set-up of Theorem 1.2, assume that, for a given* m, *the set of positive integers* n *with the property "the polynomial* $u_n(x)$ *is not identically* 0 *but vanishes at an* m*th root of unity" is not empty. Then the smallest* n *in this set satisfies*

$$n \le m(\log m)^3(X + \log D).$$

More precisely, either there exists n *in this set satisfying* $n \le 2m$, *or every* n *in this set satisfies* $n \le m(\log m)^3(X + \log D)$.

Throughout the article we use standard notation. We denote $\varphi(n)$ the Euler function, $\mu(n)$ the Möbius function, $\Lambda(n)$ the von Mangoldt function and $\omega(n)$ the number of prime divisors of n counted without multiplicities.

Theorems 1.2 and 1.3 are proved in Section 5, and Theorem 1.6 is proved in Section 6. In Sections 2, 3 and 4 we collect various auxiliary facts used in the proof. In particular, in Section 4 we revisit Schinzel's classical Primitive Divisor Theorem [15]. We obtain a version of this theorem fully explicit in all parameters, which is key ingredient in our proof of Theorem 1.3.

2 Heights

All results of this section are well-known, but sometimes we prefer to give a short proof than to look for a bibliographical reference.

Recall the definition of the absolute logarithmic (projective) height. Let

$$\bar{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_k) \in \bar{\mathbb{Q}}^{k+1}$$

be a non-zero vector of algebraic numbers. Pick a number field K containing all α_i and normalize the absolute values of K to extend the standard absolute values of $\mathbb{Q}$. With this normalization, the height of $\bar{\alpha}$ is defined by

$$\mathrm{h}(\bar{\alpha}) = d^{-1} \sum_{v \in M_K} d_v \log \max\{|\alpha_0|_v, \ldots, |\alpha_k|_v\}, \tag{2.1}$$

where $d = [K : \mathbb{Q}]$ and $d_v = [K_v : \mathbb{Q}_v]$ is the local degree. This definition is known to be independent of the choice of K and invariant under multiplication of $\bar{\alpha}$ by a non-zero algebraic number: $\mathrm{h}(\lambda\bar{\alpha}) = \mathrm{h}(\bar{\alpha})$ for $\lambda \in \bar{\mathbb{Q}}^{\times}$. When $\alpha \in \mathbb{Q}^{n+1}$ this definition coincides with the definition of height from Section 1.

Separating the contributions of infinite and finite places, we can rewrite equation (2.1) as

$$\begin{aligned} \mathrm{h}(\bar{\alpha}) = {} & d^{-1} \sum_{K \overset{\sigma}{\hookrightarrow} \mathbb{C}} \log \max\{|\alpha_0^\sigma|, \ldots, |\alpha_k^\sigma|\} \\ & + d^{-1} \sum_{\mathfrak{p}} \max\{-\nu_{\mathfrak{p}}(\alpha_0), \ldots, -\nu_{\mathfrak{p}}(\alpha_k)\} \log \mathcal{N}\mathfrak{p}, \end{aligned} \tag{2.2}$$

where the first sum is over the complex embeddings of K, the second sum is over the finite primes of K, and $\mathcal{N}\mathfrak{p}$ denotes the absolute norm of $\mathfrak{p}$.

Now we define the height $\mathrm{h}(g)$ of a non-zero polynomial g with algebraic coefficients (in one or in several variables), or, more generally, the height $\mathrm{h}(g_1, \ldots, g_k)$ of a vector of such polynomials as the height of the vector of all coefficients of those polynomials (ordered somehow).

With a standard abuse of notation, for $\alpha \in \bar{\mathbb{Q}}$ we write $\mathrm{h}(\alpha)$ for $\mathrm{h}(1, \alpha)$. If α belongs to a number field K then

$$\mathrm{h}(\alpha) = d^{-1} \sum_{v \in M_K} d_v \log^+ |\alpha|_v \tag{2.3}$$

$$= d^{-1} \sum_{v \in M_K} -d_v \log^- |\alpha|_v \qquad (\alpha \neq 0), \tag{2.4}$$

where $\log^+ = \max\{\log, 0\}$ and $\log^- = \min\{\log, 0\}$.

Lemma 2.1. *Let $\alpha \in \bar{\mathbb{Q}}$ and $f(x) \in \bar{\mathbb{Q}}[x]$ a polynomial of degree less or equal to D. Then*

$$\mathrm{h}(f(\alpha)) \le D\mathrm{h}(\alpha) + \mathrm{h}(1,f) + \log(D+1). \tag{2.5}$$

More generally, if $g(x) \in \bar{\mathbb{Q}}[x]$ is another polynomial of degree less or equal to D and $g(\alpha) \ne 0$ then

$$\mathrm{h}(f(\alpha)/g(\alpha)) \le D\mathrm{h}(\alpha) + \mathrm{h}(g,f) + \log(D+1). \tag{2.6}$$

If $f(\alpha) = 0$ then

$$\mathrm{h}(\alpha) \le \mathrm{h}(f) + \log 2. \tag{2.7}$$

Furthermore, let r be a non-negative integer. Then

$$\mathrm{h}(1, f^{(r)}/r!) \le \mathrm{h}(1,f) + D\log 2. \tag{2.8}$$

Proof. We start by proving (2.6). By definition,

$$\mathrm{h}(f(\alpha)/g(\alpha)) = \mathrm{h}(1, f(\alpha)/g(\alpha)) = \mathrm{h}(g(\alpha), f(\alpha)).$$

Write

$$f(x) = a_D x^D + \cdots + a_0, \qquad g(x) = b_D x^D + \cdots + b_0.$$

Let K be a number field containing α and the coefficients of f, g. We set $d = [K : \mathbb{Q}]$. For $v \in M_K$ we have

$$|f(\alpha)|_v \le \begin{cases} (D+1)|f|_v \max\{1, |\alpha|_v\}^D, & v \mid \infty, \\ |f|_v| \max\{1, |\alpha|_v\}^D, & v < \infty, \end{cases}$$

where $|f|_v = \max\{|a_0|_v, \ldots, |a_D|_v\}$, and similarly for $g(\alpha)$. Hence

$$\begin{aligned} \mathrm{h}(g(\alpha), f(\alpha)) &\le d^{-1} \sum_{v \in M_K} d_v \log\max\{|g(\alpha)|_v, |f(\alpha)|_v\} \\ &\le d^{-1} \sum_{v \in M_K} d_v (\log\max\{|f_v|, |g|_v\} + D\log^+ |\alpha|_v) \\ &+ d^{-1} \sum_{\substack{v \in M_K \\ v\mid\infty}} d_v \log(D+1) \\ &= \mathrm{h}(g,f) + D\mathrm{h}(\alpha) + \log(D+1), \end{aligned}$$

which proves (2.6).

For (2.7) see [2, Proposition 3.6(1)]. Finally, we have

$$\frac{f^{(r)}}{r!}(x) = \sum_{k=r}^{D} \binom{k}{r} a_k x^{k-r}.$$

Since
$$\binom{k}{r} \le 2^k \le 2^D,$$
we have
$$\left|\frac{f^{(r)}}{r!}\right|_v \le \begin{cases} 2^D|f|_v, & v \mid \infty, \\ |f|_v, & v < \infty. \end{cases}$$
Hence
$$\begin{aligned} \mathrm{h}\left(1, \frac{f^{(r)}}{r!}\right) &= d^{-1} \sum_{v \in M_K} d_v \log^+ \left|\frac{f^{(r)}}{r!}\right|_v \\ &\le d^{-1} \sum_{v \in M_K} d_v \log^+ |f_v| + d^{-1} \sum_{\substack{v \in M_K \\ v \mid \infty}} d_v D \log 2 \\ &= \mathrm{h}(1, f) + D \log 2. \end{aligned}$$
The lemma is proved. □

Lemma 2.2. *Let $f_1(x), \dots, f_k(x) \in \bar{\mathbb{Q}}[x]$ be non-zero polynomials of degrees not exceeding D, and let $g(x) \in \bar{\mathbb{Q}}[x]$ be a common divisor of $f_1, \dots, f_k$ (in the ring $\bar{\mathbb{Q}}[x]$). Then*
$$\mathrm{h}(f_1/g, \dots, f_k/g) \le \mathrm{h}(f_1, \dots, f_k) + (D + k - 1) \log 2.$$

Proof. Consider the polynomial
$$f(x, y_1, \dots, y_{k-1}) := f_1(x)y_1 + \dots + f_{k-1}(x)y_{k-1} + f_k(x) \in \bar{\mathbb{Q}}[x, y_1, \dots, y_{k-1}].$$
Applying Theorem 1.6.13 from [4], we obtain
$$\mathrm{h}(f/g) \le \mathrm{h}(f/g) + \mathrm{h}(g) \le \mathrm{h}(f) + (D + k - 1) \log 2.$$
Since
$$\mathrm{h}(f_1/g, \dots, f_k/g) = \mathrm{h}(f/g), \qquad \mathrm{h}(f_1, \dots, f_k) = \mathrm{h}(f),$$
the result follows. □

Lemma 2.3. *Let K be a number field of degree d and $\alpha \in K$. Then*
$$\sum_{\nu_{\mathfrak{p}}(\alpha) < 0} \log \mathcal{N}\mathfrak{p} \le d\mathrm{h}(\alpha), \qquad \sum_{\nu_{\mathfrak{p}}(\alpha) > 0} \log \mathcal{N}\mathfrak{p} \le d\mathrm{h}(\alpha), \tag{2.9}$$
where the first sum is over (finite) primes $\mathfrak{p}$ of K with $\nu_{\mathfrak{p}}(\alpha) < 0$, the second sum over those with $\nu_{\mathfrak{p}}(\alpha) > 0$, and in the second sum we assume $\alpha \ne 0$. More generally, let $\alpha_1, \dots, \alpha_k \in K$. Then
$$\sum_{\substack{\nu_{\mathfrak{p}}(\alpha_i) < 0 \text{ for} \\ \text{some } i \in \{1, \dots, k\}}} \log \mathcal{N}\mathfrak{p} \le d\mathrm{h}(\bar{\alpha}), \qquad \bar{\alpha} = (1, \alpha_1, \dots, \alpha_k). \tag{2.10}$$

Proof. Inequality (2.10) is immediate from (2.2) (note that $\alpha_0 = 1$), and both statements in (2.9) are special cases of (2.10). □

Lemma 2.4 ("Liouville's inequality"). *Let K and α be as in Lemma 2.3, $\alpha \neq 0$. Let $S \subset M_K$ be any set of places of K (finite or infinite). Then*

$$e^{-d\mathrm{h}(\alpha)} \le \prod_{v\in M_K} |\alpha|_v^{d_v} \le e^{d\mathrm{h}(\alpha)}.$$

In particular, if $\sigma_1, \dots \sigma_r : K \hookrightarrow \mathbb{C}$ are some distinct complex embeddings of K then

$$\prod_{i=1}^{r} |\alpha^{\sigma_i}| \ge e^{-d\mathrm{h}(\alpha)}.$$

We omit the proof, which is well-known and easy.

3 Cyclotomic polynomials

We denote $\Phi_m(T)$ the mth cyclotomic polynomial. We will systematically use the identity

$$\Phi_m(T) = \prod_{d|m} (T^d - 1)^{\mu(m/d)}, \tag{3.1}$$

In this section we study values of cyclotomic polynomials at algebraic points. We give an asymptotic expression for the height of $\Phi_m(\gamma)$ as $\gamma \in \bar{\mathbb{Q}}$ is fixed and $m \to \infty$. We also estimate the absolute value of $\Phi_m(\gamma)$ from below.

The results of this section can be viewed as totally explicit versions of some results from [1, Section 3], and we follow [1] rather closely. We note however that all this goes back to the 1974 work of Schinzel [15] or even earlier.

3.1 The height

Theorem 3.1. *Let γ be an algebraic number. Then*

$$\mathrm{h}(\Phi_m(\gamma)) = \varphi(m)\mathrm{h}(\gamma) + O_1\bigl(2^{\omega(m)} \log(\pi m)\bigr).$$

Recall that $A = O_1(B)$ means that $|A| \le B$.

To prove this theorem we need some preparations. We follow [1, Section 3] with some changes.

Proposition 3.2. *For a positive integer m we have*

$$\max_{|z|\le 1}\log|\Phi_m(z)| \le 2^{\omega(m)}\log(\pi m), \tag{3.2}$$

the maximum being over the unit disc on the complex plane. (We use the convention $\log 0 = -\infty$.) For $0<\varepsilon\le 1/2$ we also have

$$\min_{|z|\le 1-\varepsilon}\log|\Phi_m(z)| \ge -2^{\omega(m)}\log\frac{1}{\varepsilon}. \tag{3.3}$$

Proof. By the maximum principle, it suffices to prove that (3.2) holds for complex z with $|z|=1$. Thus, fix such z. We will actually prove a slightly sharper bound

$$\log|\Phi_m(z)| \le (2^{\omega(m)-1}+1)\log m + 2^{\omega(m)}\log\pi. \tag{3.4}$$

We can write z in a unique way as $z=\zeta e^{2\pi i\theta/m}$, where ζ is an mth root of unity (not necessarily primitive) and $-1/2<\theta\le 1/2$. We may assume $\theta\ne 0$, because for the finitely many z with $\theta=0$ the bound extends by continuity.

Let ℓ be the exact order of ζ; thus, $\ell\mid m$ and ζ is a primitive ℓth root of unity. Let d be any other divisor of m. If $\ell\nmid d$ then $d\le m/2$ and

$$2\ge |z^d-1|\ge 2\sin(\pi d/2m)\ge 2d/m.$$

(We use the inequality $|\sin x|\ge (2/\pi)x$ which holds for $|x|\le\pi/2$.) This implies that

$$\bigl|\log|z^d-1|\bigr| \le \log(m/d). \tag{3.5}$$

And if $\ell\mid d$ then we have $|z^m-1| = 2\sin(\pi\theta d/m)$, which implies that

$$2\pi\theta d/m \ge |z^d-1| \ge 4\theta d/m.$$

Writing $d=d'\ell$, this implies that

$$\log|z^{d'\ell}-1| = \log d' - \log\frac{m}{2\ell\theta} + O_1(\log\pi). \tag{3.6}$$

Using (3.1) we obtain

$$\begin{aligned}
\log|\Phi_m(z)| &= \sum_{\substack{d\mid m\\ \ell\nmid d}}\mu\left(\frac{m}{d}\right)\log|z^d-1| + \sum_{d'\mid m/\ell}\mu\left(\frac{m/\ell}{d'}\right)\log|z^{\ell d'}-1|\\
&\le \sum_{d\mid m}\left|\mu\left(\frac{m}{d}\right)\right|\log\frac{m}{d} + \sum_{d'\mid m/\ell}\mu\left(\frac{m/\ell}{d'}\right)\left(\log d' - \log\frac{m}{2\ell\theta}\right)\\
&\quad + O_1(2^{\omega(n/\ell)}\log\pi)\\
&= 2^{\omega(m)-1}\sum_{p\mid m}\log p + \Lambda\left(\frac{m}{\ell}\right) + \delta\log(2\theta) + O_1(2^{\omega(m/\ell)}\log\pi),
\end{aligned}$$

where $\delta = 0$ if $\ell < m$ and $\delta = 1$ if $\ell = m$. Since $\log(2\theta) \le 0$, this proves (3.4).

The proof of (3.3) is much easier. When $|z| \le 1-\varepsilon$, we have

$$2 \ge |z^d - 1| \ge 1 - |z|^d \ge 1 - |z| \ge \varepsilon.$$

Since $0 < \varepsilon \le 1/2$ this implies that $\bigl|\log|z^d-1|\bigr| \le \log(1/\varepsilon)$. We obtain

$$\bigl|\log|\Phi_m(z)|\bigr| = \left|\sum_{d|m} \mu\left(\frac{m}{d}\right)\log|z^d-1|\right| \le 2^{\omega(m)}\log\frac{1}{\varepsilon}.$$

In particular, (3.3) holds. □

Corollary 3.3. *Let m be a positive integer and $z \in \mathbb{C}$. Then*

$$\log^+|\Phi_m(z)| = \varphi(m)\log^+|z| + O_1\bigl(2^{\omega(m)}\log(\pi m)\bigr),$$

where $\log^+ = \max\{\log, 0\}$.

Proof. For $|z| \le 1$ this is Proposition 3.2. If $|z| > 1$ then

$$\log|\Phi_m(z)| = \varphi(m)\log|z| + \log|\Phi_m(z^{-1})|, \tag{3.7}$$

and $\log|\Phi_m(z^{-1})| \le 2^{\omega(m)}\log(\pi m)$ by Proposition 3.2. This already implies the upper bound

$$\log^+|\Phi_m(z)| \le \varphi(m)\log^+|z| + 2^{\omega(m)}\log(\pi m).$$

The lower bound

$$\log^+|\Phi_m(z)| \ge \varphi(m)\log^+|z| - 2^{\omega(m)}\log(\pi m) \tag{3.8}$$

is trivial when $m = 1$, so we will assume $m \ge 2$ in the sequel. In the case $1 < |z| \le m/(m-1)$ we have

$$\log^+|\Phi_m(z)| \ge 0 \ge \varphi(m)\log\frac{m}{m-1} - 1 \ge \varphi(m)\log^+|z| - 1,$$

which is much better than wanted. Finally, if $|z| \ge m/(m-1)$, then

$$\log|\Phi_m(z^{-1})| \ge -2^{\omega(m)}\log m$$

by (3.3) with $\varepsilon = 1/m$. Hence (3.8) follows from (3.7) in this case. □

Proof of Theorem 3.1. We use (2.3) with $\alpha = \Phi_m(\gamma)$. For $v \in M_K$ we have

$$\log^+|\Phi_m(\gamma)|_v = \begin{cases} \varphi(m)\log^+|\gamma|_v + O_1\bigl(2^{\omega(m)}\log(\pi m)\bigr), & v \mid \infty, \\ \varphi(m)\log^+|\gamma|_v, & v < \infty. \end{cases}$$

Indeed, the archimedean case is Corollary 3.3, and the non-archimedean case is obvious. Summing up, the result follows. □

3.2 The lower bound

The following result is proved in [3, Corollary 4.2] as a consequence of Baker's theory of logarithmic forms.

Proposition 3.4. *Let γ be a complex algebraic number of degree d, not a root of unity, and n a positive integer. Then*

$$|\gamma^n - 1| \ge e^{-10^{12}d^4(\mathrm{h}(\gamma)+1)\log(n+1)}.$$

Corollary 3.5. *Let γ and m be as in Proposition 3.4. Then*

$$\log|\Phi_m(\gamma)| \ge -10^{12}d^4(\mathrm{h}(\gamma)+1)\cdot 2^{\omega(m)}\log(m+1). \tag{3.9}$$

Proof. If $|\gamma| \ge 1$ then

$$\log|\Phi_m(\gamma)| = \varphi(m)\log|\gamma| + \log|\Phi(\gamma^{-1})| \ge \log|\Phi(\gamma^{-1})|.$$

Hence, replacing, if necessary, γ by γ^{-1}, we may assume $|\gamma| \le 1$. We have

$$\log|\Phi_m(\gamma)| = \sum_{n|m}\mu\left(\frac{m}{n}\right)\log|\gamma^n - 1|. \tag{3.10}$$

Proposition 3.4 implies that

$$2 \ge |\gamma^n - 1| \ge e^{-10^{12}d^4(\mathrm{h}(\gamma)+1)\log(n+1)}.$$

Hence for $1 \le n \le m$ we have

$$\big|\log|\gamma^n - 1|\big| \le 10^{12}d^4(\mathrm{h}(\gamma)+1)\log(m+1).$$

Substituting this to (3.10), we obtain

$$\big|\log|\Phi_m(\gamma)|\big| \le 10^{12}d^4(\mathrm{h}(\gamma)+1)\cdot 2^{\omega(m)}\log(m+1).$$

In particular, we proved (3.9). □

4 Schinzel's Primitive Divisor Theorem

Let γ be a non-zero algebraic number, not a root of unity. We consider the sequence

$$u_n = u_n(\gamma) = \gamma^n - 1.$$

(Note that in this section (u_n) is a numerical sequence, while in the other sections it is a sequence of polynomials.) A prime $\mathfrak{p}$ of the number field $K = \mathbb{Q}(\gamma)$ is called *primitive divisor* for u_n if

$$\nu_{\mathfrak{p}}(u_n) > 0, \qquad \nu_{\mathfrak{p}}(u_k) = 0 \quad (k = 1, \dots, n-1).$$

For further use, let us fix here some basic properties of primitive divisors. Recall that $\Phi_n(T)$ denotes the nth cyclotomic polynomial, and $\mathcal{N}\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$.

Proposition 4.1. *Assume that $\mathfrak{p}$ is a primitive divisor of u_n. Then n divides $\mathcal{N}\mathfrak{p}-1$ and $\nu_\mathfrak{p}(\Phi_n(\gamma))\ge 1$. In particular, $n<\mathcal{N}\mathfrak{p}$.*

The proofs are very easy and we omit them.

Schinzel [15] proved that u_n admits a primitive divisor for $n\ge n_0(d)$, where d is the degree of γ. This was an improvement upon the earlier work [12], where the same was proved under the assumption $n\ge n_0(\gamma)$.

Stewart [16] made Schinzel's result explicit, but he imposed an additional hypothesis $\gamma=\alpha/\beta$, where $\alpha,\beta\in\mathcal{O}_K$ are coprime algebraic integers. Here we obtain a fully explicit version of Schinzel's result without any extra hypothesis.

Theorem 4.2. *Let γ be an algebraic number of degree d, not a root of unity. Assume that*

$$n\ge \max\{2^{d+1},10^{30}d^9\}. \tag{4.1}$$

Then $u_n=\gamma^n-1$ admits a primitive divisor.

Theorem 4.2 is a consequence of the following result, appearing, albeit in a different setting, in Schinzel's work.

Proposition 4.3. *In the above set-up, assume that u_n does not admit a primitive divisor. Then*

$$\mathrm{h}(\Phi_n(\gamma))\le 10^{13}d^4(\mathrm{h}(\gamma)+1)\cdot 2^{\omega(n)}\log(n+1). \tag{4.2}$$

4.1 Proof of Proposition 4.3

We start from the following well-known fact.

Lemma 4.4. *Let K be a number field of degree d and p a prime number. Let $\mathfrak{p}$ be a prime of K above p of ramification index $e_\mathfrak{p}$ (that is, $e_\mathfrak{p}=\nu_\mathfrak{p}(p)$). Let $\xi\in K$ satisfy*

$$\nu_\mathfrak{p}(\xi-1)>\frac{e_\mathfrak{p}}{p-1}.$$

Then for any positive integer n we have

$$\nu_\mathfrak{p}(\xi^n-1)=\nu_\mathfrak{p}(\xi-1)+\nu_\mathfrak{p}(n).$$

The proof of the lemma can be found, for instance, in [12, Lemma 1].

Lemma 4.5. *Let γ be an algebraic number of degree d, not a root of unity, and n an integer satisfying $n \ge 2^{d+1}$. Let $\mathfrak{p}$ be a prime of the field $\mathbb{Q}(\gamma)$ which is not a primitive divisor of $u_n = \gamma^n - 1$. Then $\nu_{\mathfrak{p}}(\Phi_n(\gamma)) \le \nu_{\mathfrak{p}}(n)$.*

This is Schinzel's [15] crucial "Lemma 4". Since his set-up is slightly different, we reproduce the proof here.

Proof. We may assume that $\nu_{\mathfrak{p}}(\gamma^n - 1) > 0$, since there is nothing to prove otherwise. In particular, $\nu_{\mathfrak{p}}(\gamma) = 0$.

For $k = 0, 1, 2\ldots$ denote ℓ_k the multiplicative order of γ mod $\mathfrak{p}^k$; that is, ℓ_k is the smallest positive integer ℓ with the property $\nu_{\mathfrak{p}}(\gamma^\ell - 1) \ge k$. Clearly, $\nu_{\mathfrak{p}}(\gamma^n - 1) \ge k$ if and only if $\ell_k \mid n$. Together with (3.1) this implies that for every k the following holds:

$$\nu_{\mathfrak{p}}\bigl(\Phi_n(\gamma)\bigr) = \sum_{i=1}^{k} \sum_{\ell_i \mid m \mid n} \mu\left(\frac{n}{m}\right) + \sum_{\ell_{k+1} \mid m \mid n} \mu\left(\frac{n}{m}\right) \bigl(\nu_{\mathfrak{p}}(\gamma^m - 1) - k\bigr) \tag{4.3}$$

Let p be the rational prime below $\mathfrak{p}$ and $e_{\mathfrak{p}} = \nu_{\mathfrak{p}}(p)$ the ramification index. We will apply (4.3) with

$$k = \left\lfloor \frac{e_{\mathfrak{p}}}{p-1} \right\rfloor,$$

which will be our choice of k from now on. We claim that

$$n > \ell_{k+1}. \tag{4.4}$$

We postpone the proof of (4.4) (which is a bit messy) until later, and now complete the proof of the lemma assuming validity of (4.4).

Since $n > \ell_{k+1} \ge \ell_i$ for $i = 1, \ldots, k$, the double sum in (4.3) vanishes. Also, if $\ell_{k+1} \mid m$ then

$$\nu_{\mathfrak{p}}(\gamma^m - 1) = \nu_{\mathfrak{p}}(\gamma^{\ell_{k+1}} - 1) + \nu_{\mathfrak{p}}\left(\frac{m}{\ell_{k+1}}\right)$$

by Lemma 4.4. Hence (4.3) can be rewritten as

$$\nu_{\mathfrak{p}}\bigl(\Phi_n(\gamma)\bigr) = \sum_{\ell_{k+1} \mid m \mid n} \mu\left(\frac{n}{m}\right) \bigl(\nu_{\mathfrak{p}}(\gamma^{\ell_{k+1}} - 1) - k\bigr) + \sum_{\ell_{k+1} \mid m \mid n} \mu\left(\frac{n}{m}\right) \nu_{\mathfrak{p}}\left(\frac{m}{\ell_{k+1}}\right). \tag{4.5}$$

Since $n > \ell_{k+1}$, the first sum in (4.5) vanishes. As for the second sum, it vanishes (just being empty) if $\ell_{k+1} \nmid n$. From now on assume that $\ell_{k+1} \mid n$ and set $n' = n/\ell_{k+1}$. We obtain

$$\nu_{\mathfrak{p}}\bigl(\Phi_n(\gamma)\bigr) = e_{\mathfrak{p}} \sum_{m' \mid n'} \mu\left(\frac{n'}{m'}\right) \nu_p(m') = \begin{cases} e_{\mathfrak{p}}, & n' \text{ is a power of } p, \\ 0, & \text{otherwise.} \end{cases}$$

In any case we obtain $\nu_{\mathfrak{p}}\bigl(\Phi_n(\gamma)\bigr) \le \nu_{\mathfrak{p}}(n)$. This proves the lemma.

We are left with the claim (4.4). Note first of all that

$$n > \ell_1 \tag{4.6}$$

because $\mathfrak{p}$ is not a primitive divisor of u_n. Another useful observation is that

$$\ell_{i+1} \le p\ell_i \qquad (i = 1, 2, \ldots). \tag{4.7}$$

Indeed,

$$\gamma^{p\ell_i} - 1 = \sum_{j=1}^{p-1} \binom{p}{j} (\gamma^{\ell_i} - 1)^j + (\gamma^{\ell_i} - 1)^p,$$

which implies that $\nu_{\mathfrak{p}}(\gamma^{p\ell_i} - 1) > \nu_{\mathfrak{p}}(\gamma^{\ell_i} - 1)$, proving (4.7).

If $k = 0$ then (4.4) is (4.6). Now assume that $k \ge 1$. In this case

$$p - 1 \le e_{\mathfrak{p}} \le d. \tag{4.8}$$

On the other hand, let $p^{f_{\mathfrak{p}}} = \mathcal{N}\mathfrak{p}$ be the absolute norm of $\mathfrak{p}$. Clearly,

$$\ell_1 \le p^{f_{\mathfrak{p}}} - 1 \le p^{d/e_{\mathfrak{p}}} - 1.$$

In the special case $p = 3$, $e_{\mathfrak{p}} = d = 2$ we have $k = 1$ and $\ell_2 \le p\ell_1 \le 6$. Since $n \ge 2^{d+1} = 8$ by the hypothesis, this proves (4.4) in this special case. From now on we assume that $d \ge 3$ for $p = 3$.

Using (4.7) iteratively, we obtain

$$\ell_{k+1} \le p^k \ell_1 < p^{e_{\mathfrak{p}}/(p-1) + d/e_{\mathfrak{p}}} \le \max_{p-1 \le t \le d} p^{t/(p-1) + d/t} = p^{1 + d/(p-1)}.$$

We have to show that

$$p^{1+d/(p-1)} \le 2^{d+1}.$$

This is true by inspection in the cases

$$p = 2, \qquad p = 3,\ d \ge 3, \qquad p = 5,\ d \ge 4.$$

Now assume that $p \ge 7$, in which case $d \ge 6$. Since $p \le d + 1$, we have

$$p^{1+d/(p-1)} \le (d+1) \cdot 7^{d/6}.$$

A calculation shows that $(d+1) \cdot 7^{d/6} \le 2^{d+1}$ for $d \ge 6$. This completes the proof of (4.4). □

Proof of Proposition 4.3 We use (2.4) with $\alpha = \Phi_n(\gamma)$. For $v \in M_K$ we have

$$-\log^- |\Phi_n(\gamma)|_v \le \begin{cases} 10^{12}d^4(\mathrm{h}(\gamma)+1)\cdot 2^{\omega(n)}\log(n+1), & v \mid \infty,\\ -\log|n|_v, & v < \infty. \end{cases}$$

Indeed, the archimedean case is Corollary 3.5, and the non-archimedean case is Lemma 4.5. Summing up, we obtain

$$\mathrm{h}(\Phi_n(\gamma)) \le 10^{12}d^4(\mathrm{h}(\gamma)+1)\cdot 2^{\omega(n)}\log(n+1)+\log n,$$

which is sharper than (4.2). □

4.2 Proof of Theorem 4.2

Assume u_n does not have a primitive divisor, but n satisfies (4.1). We have, in particular, $n \ge 10^{30}$. Comparing Proposition 4.3 and Theorem 3.1, we obtain

$$\begin{aligned}\varphi(n)\mathrm{h}(\gamma) &\le 10^{13}d^4(\mathrm{h}(\gamma)+1)\cdot 2^{\omega(n)}\log(n+1)+2^{\omega(n)}\log(\pi n)\\ &\le 10^{14}d^4(\mathrm{h}(\gamma)+1)\cdot 2^{\omega(n)}\log(n+1).\end{aligned}$$

Since γ is not a root of unity, we have

$$d\mathrm{h}(\gamma) \ge 2(\log(3d))^{-3}, \tag{4.9}$$

see [18, Corollary 2]. Hence

$$\varphi(n)\mathrm{h}(\gamma) \le 10^{15}d^5(\log(3d))^3\mathrm{h}(\gamma)\cdot 2^{\omega(n)}\log(n+1),$$

which implies

$$\varphi(n) \le 10^{15}d^5(\log(3d))^3\cdot 2^{\omega(n)}\log(n+1). \tag{4.10}$$

For $n \ge 10^{30}$ we have

$$\varphi(n) \ge 0.5\frac{n}{\log\log n}, \qquad \omega(n) \le \frac{\log n}{\log\log n - 1.2}, \tag{4.11}$$

see [14, Theorem 15] and [13, Theorem 13]. Hence for $n \ge 10^{30}$

$$\begin{aligned}2^{\omega(n)}\frac{n}{\varphi(n)}\log(n+1) &\le n^{(\log 2)/(\log\log(10^{30})-1.2)}\cdot 2(\log\log n)\cdot\log(n+1)\\ &\le n^{1/3}.\end{aligned}$$

Using this, we deduce from (4.10) the inequality $n^{2/3} \le 10^{15}d^5(\log(3d))^3$. A quick calculation shows that this inequality is incompatible with (4.1). □

5 Proof of Theorems 1.2 and 1.3

Since condition 2 of Theorem 1.2 trivially implies condition 1 (see Example 1.1) it suffices to prove Theorem 1.3. Thus, in the sequel:

- $c_i(x)$ and $f_i(x)$ are polynomials not satisfying condition 2 of Theorem 1.2 and

$$u_n(x) = c_1(x)f_1(x)^n + c_2(x)f_2(x)^n \qquad (n = 1, 2, \ldots);$$

- m and n are positive integers such that $u_n(\zeta) = 0$ for a primitive mth root of unity ζ; since $u_n(x) \in \mathbb{Q}[x]$, this is equivalent to

$$\Phi_m(x) \mid u_n(x). \tag{5.1}$$

5.1 Some reductions

We start by some general observations.

- We may assume that

$$c_1(\zeta)c_2(\zeta)f_1(\zeta)f_2(\zeta) \neq 0. \tag{5.2}$$

  Otherwise $\varphi(m) \leq D$, and, using

$$\varphi(m) \geq m^{1/2} \qquad (m \neq 2, 6) \tag{5.3}$$

  (see [17]), we obtain $m \leq \max\{6, D^2\}$, which is much sharper than what we want to prove.

- We may assume that at least one of f_1, f_2 is a non-constant polynomial. Otherwise $\deg u_n(x) \leq D$, and we again obtain $\varphi(m) \leq D$.

- We may assume that $n > D$. Otherwise $\deg u_n(x) \leq D + D^2$, and, using (5.3) we obtain $m \leq \max\{6, (D + D^2)^2\}$, again much sharper than the wanted result.

- Replacing $c_i(x)$ and $f_i(x)$ by

$$\tilde{c}_i(x) := c_i(x)/\gcd(c_1(x), c_2(x)), \qquad \tilde{f}_i(x) := f_i(x)/\gcd(f_1(x), f_2(x)),$$

  respectively, we may assume that the polynomials c_1, c_2 are coprime in the ring $\mathbb{Q}[x]$, and so are f_1, f_2:

$$\gcd(c_1(x), c_2(x)) = \gcd(f_1(x), f_2(x)) = 1. \tag{5.4}$$

Lemma 2.2 implies that

$$\mathrm{h}(\tilde{c}_1, \tilde{c}_2) \le \mathrm{h}(c_1, c_2) + (D+1)\log 2 \le X + (D+1)\log 2,$$

and similarly for $\mathrm{h}(\tilde{f}_1, \tilde{f}_2)$. Hence, to prove (1.2) in the general case, it suffices to prove

$$m \le e^{30D(X+D)} \tag{5.5}$$

in the "coprime case", that is, assuming (5.4).

We distinguish several cases according to the nature of roots of our polynomials:

1. $f_1(x)f_2(x)$ admits a root which is non-zero and not a root of unity;
2. $f_1(x)f_2(x)$ vanishes at a root of unity;
3. $f_1(x)f_2(x)$ vanishes only at 0.

These cases are treated separately in the subsequent subsections.

5.2 The polynomial $f_1(x)f_2(x)$ admits a root γ which is non-zero and not a root of unity

By symmetry, we may assume that γ is a root of $f_1(x)$. Since the statement of Theorem 1.3 is invariant under multiplication of the polynomials c_1, c_2 by the same non-zero rational number, we may assume that the polynomial $c_1(x)$ is monic. Similarly, we may assume that $f_1(x)$ is monic.

Denote $K = \mathbb{Q}(\gamma)$. Then

$$d := [K : \mathbb{Q}] \le D.$$

Since $X \ge 3$, the right-hand side of (5.5) exceeds $10^{30}D^9$. Hence we may assume that

$$m > \max\{2^{d+1}, 10^{30}d^9\}.$$

Theorem 4.2 together with Proposition 4.1 implies now that there exists a prime $\mathfrak{p}$ of K such that $\nu_{\mathfrak{p}}(\Phi_m(\gamma)) > 0$ and

$$m < \mathcal{N}\mathfrak{p}.$$

So we only have to bound $\mathcal{N}\mathfrak{p}$.

5.2.1 The numbers β and δ

We have $f_2(\gamma) \neq 0$ by (5.4). However, it it possible that $c_2(\gamma) = 0$. Denote r the order of γ as a root of $c_2(x)$, and set

$$\beta = \frac{c_2^{(r)}(\gamma)}{r!}, \qquad \delta = f_2(\gamma),$$

These are non-zero elements of the number field K.

We claim that one of the following holds:

(5.6) $\nu_{\mathfrak{p}}(\alpha) < 0$ for some coefficient α of c_1 or f_1 or c_2 or f_2;

(5.7) $\nu_{\mathfrak{p}}(\beta) > 0$;

(5.8) $\nu_{\mathfrak{p}}(\delta) > 0$.

Indeed, since $\nu_{\mathfrak{p}}(\Phi_m(\gamma)) > 0$, there exists a primitive mth rooth of unity ζ and a prime $\mathfrak{P} \mid \mathfrak{p}$ of the field $K(\zeta)$ such that

$$\nu_{\mathfrak{P}}(\zeta - \gamma) > 0.$$

Now, if (5.6) does not hold, then our four polynomials belong to $\mathcal{O}_{\mathfrak{P}}[x]$, where $\mathcal{O}_{\mathfrak{P}}$ is the local ring of $\mathfrak{P}$. Moreover, since f_1 is monic, $\gamma \in \mathcal{O}_{\mathfrak{P}}$. Hence the polynomials

$$F(x) := \frac{c_1(x) f_1(x)^n}{(x-\gamma)^r}, \qquad G(x) := \frac{c_2(x)}{(x-\gamma)^r}$$

belong to $\mathcal{O}_{\mathfrak{P}}[x]$ as well. Note that $F(x)$ is indeed a polynomial, and moreover

$$F(\gamma) = 0,$$

because $n > D \geq r$.

We have $\beta = G(\gamma)$ and $F(\zeta) = -G(\zeta) f_2(\zeta)^n$ (because $u_n(\zeta) = 0$). This implies the following congruences in the ring $\mathcal{O}_{\mathfrak{P}}$:

$$\beta\delta^n \equiv G(\zeta) f_2(\zeta)^n \equiv -F(\zeta) \equiv -F(\gamma) \equiv 0 \mod \mathfrak{P}.$$

Hence either $\beta \equiv 0 \bmod \mathfrak{P}$ or $\delta \equiv 0 \bmod \mathfrak{P}$, which means that one of (5.7) or (5.8) holds true.

5.2.2 Estimates

Now we are ready to estimate $\mathcal{N}\mathfrak{p}$. Using Lemma 2.3, we obtain

(5.9) $\log \mathcal{N}\mathfrak{p} \leq \max\{\mathrm{h}(1, c_1), \mathrm{h}(1, c_2), \mathrm{h}(1, f_1), \mathrm{h}(1, f_2), \mathrm{h}(\beta), \mathrm{h}(\delta)\}.$

Since $f_1(x)$ is a monic polynomial, we have

$$\mathrm{h}(1, f_1), \mathrm{h}(1, f_2) \le \mathrm{h}(f_1, f_2) \le X, \tag{5.10}$$

and similarly for c_1, c_2. Furthermore, using Lemma 2.1, we find

$$\begin{aligned} \mathrm{h}(\gamma) &\le \mathrm{h}(f_1) + \log 2 \\ &\le X + \log 2, \\ \mathrm{h}(\delta) &\le \mathrm{h}(1, f_2) + D\mathrm{h}(\gamma) + \log(D+1) \\ &\le (D+1)X + 2D, \\ \mathrm{h}(\beta) &\le \mathrm{h}(1, c_2^{(r)}/r!) + D\mathrm{h}(\gamma) + \log(D+1) \\ &\le \mathrm{h}(1, c_2) + D\log 2 + DX + D\log 2 + \log(D+1) \\ &\le (D+1)X + 2D. \end{aligned}$$

This implies that

$$\log \mathcal{N}\mathfrak{p} \le (D+1)X + 2D < 3DX.$$

Since $m < \mathcal{N}\mathfrak{p}$, this proves (5.5).

5.3 The polynomial $f_1(x)f_2(x)$ vanishes at a root of unity ξ

We may assume that $f_1(\xi) = 0$. Then $f_2(\xi) \ne 0$ by (5.4).

Let us describe our argument informally. Since $f_1(\xi)/f_2(\xi) = 0$, there exists $\varepsilon > 0$ such that $|f_1(z)/f_2(z)| \le 1/2$ when $|z - \xi| \le \varepsilon$.

Now assume that $u_n(\zeta) = 0$ for some primitive mth root of unity ζ. Using (5.2), we may write

$$0 \ne \alpha := \frac{c_2(\zeta)}{c_1(\zeta)} = -\left(\frac{f_1(\zeta)}{f_2(\zeta)}\right)^n. \tag{5.11}$$

Let $\mathbb{Q}(\zeta) \overset{\sigma}{\hookrightarrow} \mathbb{C}$ be a complex embedding of the field $\mathbb{Q}(\zeta)$ such that ζ^σ belongs to the ε-neighborhood of ξ. Then $|\alpha^\sigma| \le (1/2)^n$. Define

$$\beta := \prod_{|\zeta^\sigma - \xi| \le \varepsilon} \alpha^\sigma, \tag{5.12}$$

the product being over all σ as above. Since the ε-neighborhood of ξ contains a positive proportion of primitive mth roots of unity, we have

$$-\log|\beta| \gg n\varphi(m),$$

where the implied constant depends on our polynomials c_i and f_i and on our choice of ε.

On the other hand, $\alpha \neq 0$, and $\mathrm{h}(\alpha) \ll 1$ by Lemma 2.1. Hence Liouville's inequality (Lemma 2.4) implies that

$$-\log|\beta| = \sum_{|\zeta^\sigma - \xi| \le \varepsilon} -\log|\alpha^\sigma| \ll [\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(m).$$

This bounds n.

This all will be made explicit in Subsection 5.3.2. But first, we establish some simple lemmas.

5.3.1 Some lemmas

Lemma 5.1. *Let $a, b \in \mathbb{R}$, $a < b$, and m a positive integer. Denote $\varphi(m,a,b)$ the number of integers k coprime with m and satisfying $a \le k \le b$. Then*

$$\varphi(m,a,b) = (b-a)\varphi(m) + O_1(2^{\omega(m)}).$$

For the proof, see [7, Lemma 2.3].

Lemma 5.2. *Let ε satisfy $0 < \varepsilon \le 1$ and let ξ be a complex number on the unit circle; that is, $|\xi| = 1$. Let m be a positive integer. Then there exist at least $\pi^{-1}\varepsilon\varphi(m) - 2^{\omega(m)}$ primitive mth roots of unity ζ satisfying $|\zeta - \xi| \le \varepsilon$.*

Proof. Write $\xi = e^{2\pi\theta i}$ with $\theta \in \mathbb{R}$, and let $\eta > 0$ be the smallest positive real number with the property $2\sin(\pi\eta) = \varepsilon$. Note that $1/6 \ge \eta > (2\pi)^{-1}\varepsilon$. If k is an integer satisfying

$$m(\theta - \eta) \le k \le m(\theta + \eta), \qquad \gcd(m,k) = 1,$$

then $\zeta := e^{2\pi i k/m}$ is a primitive mth root of unity satisfying $|\zeta - \xi| \le \varepsilon$.

Lemma 5.1 implies that there is at least $2\eta\varphi(m) - 2^{\omega(m)}$ choices for k, with distinct k giving rise to distinct ζ (this is because $\eta \le 1/6$). Since $\eta \ge (2\pi)^{-1}\varepsilon$, the result follows. □

Lemma 5.3. *Let $f_1(x), f_2(x) \in \mathbb{C}[x]$ be polynomials of degrees bounded by D, and with coefficients bounded by $H \ge 1$ in absolute value. Let $\xi \in \mathbb{C}$ be such that*

$$|\xi| \le 1, \qquad f_1(\xi) = 0, \qquad f_2(\xi) = \delta \neq 0.$$

Set

$$\varepsilon = \frac{\min\{|\delta|, 1\}}{3D^2H}.$$

Then for $z \in \mathbb{C}$ satisfying $|z - \xi| \le \varepsilon$ we have $|f_1(z)/f_2(z)| \le 1/2$.

Proof. Since $|\xi| \le 1$ and $\varepsilon \le 1/3D$, we have for $|z-\xi| \le \varepsilon$ trivial estimates

$$|f_i'(z)| \le \frac{1}{2}D(D+1)H(1+\varepsilon)^{D-1} \le D^2H \qquad (i=1,2).$$

Hence for $|z-\xi| \le \varepsilon$ we have

$$|f_1(z)| \le D^2H\varepsilon \le \frac{1}{3}|\delta|, \qquad |f_2(z)| \ge |\delta| - D^2H\varepsilon \ge \frac{2}{3}|\delta|.$$

This proves the lemma. □

5.3.2 The estimates

As in Subsection 5.2 we may assume that f_1 is monic, which implies that we have (5.10). In particular, the coefficients of f_1 and f_2 are bounded in absolute value by $H := e^X$. Set $\delta = f_2(\xi)$.

Note that the degree of ξ is at most D and the height is 0, because it is a root of unity. Using Lemmas 2.1 and 2.4, we estimate

$$|\delta| \ge e^{-\mathrm{h}(f_2(\xi))} \ge e^{-\mathrm{h}(1,f_2)-\log(D+1)} \ge ((D+1)H)^{-1}.$$

Setting $\varepsilon = (6D^3H^2)^{-1}$, Lemma 5.3 implies that

$$\left|\frac{f_1(z)}{f_2(z)}\right| \le 1/2$$

for $z \in \mathbb{C}$ with $|z-\xi| \le \varepsilon$.

Now define α and β as in (5.11), (5.12). Then

$$-\log|\beta| \ge nr\log 2, \tag{5.13}$$

where r is the number of embeddings $\mathbb{Q}(\zeta) \overset{\sigma}{\hookrightarrow} \mathbb{C}$ such that $|\zeta^\sigma - \xi| \le \varepsilon$. Denote $\sigma_1, \dots, \sigma_r$ all those σ. Lemmas 2.4 and 2.1 imply that

$$\begin{aligned} -\log|\beta| &= \sum_{i=1}^{r} -\log|\alpha^{\sigma_i}| \\ &\le [\mathbb{Q}(\zeta):\mathbb{Q}]\mathrm{h}(\alpha) \\ &\le \varphi(m)(\mathrm{h}(c_1,c_2)+\log(D+1)) \\ &\le \varphi(m)(X+\log(D+1)). \end{aligned}$$

Together with (5.13) this implies that

$$n \le \frac{\varphi(m)}{r\log 2}(X+\log(D+1)), \tag{5.14}$$

so we only have to bound r from below.

Lemma 5.2 implies that

$$r \geq \pi^{-1}\varepsilon\varphi(m) - 2^{\omega(m)},$$

where we recall that $\varepsilon = (6D^3H^2)^{-1}$ with $H = e^X$. Using (4.11) with n replaced by m, a messy but trivial calculation shows that either $m \leq e^{30D(X+D)}$ (as we want) or $2^{\omega(m)} \leq (2\pi)^{-1}\varepsilon\varphi(m)$. Thus, $r \geq (2\pi)^{-1}\varepsilon\varphi(m)$, which, substituted to (5.14), gives

$$n \leq 100D^4e^{3X}.$$

Then

$$\varphi(m) \leq \deg u_n(x) \leq 200D^5e^{3X},$$

and, using (5.3), we deduce from this an estimate much sharper than (5.5).

5.4 The only root of $f_1(x)f_2(x)$ is 0

We may assume that $f_1(x) = 1$ and $f_2(x) = \kappa x^b$, where $\kappa \in \mathbb{Q}^\times$ and

$$1 \leq b \leq D < n.$$

We recall the following theorem of Mann [8].

Theorem 5.4. *Let $a_0, a_1, \ldots, a_k \in \mathbb{Q}^\times$ and $x_0 = 1, x_1, \ldots, x_k$ be roots of unity such that*

$$a_0x_0 + a_1x_1 + \cdots + a_kx_k = 0. \tag{5.15}$$

Assume that

$$\sum_{i\in I} a_ix_i \neq 0 \tag{5.16}$$

for every non-empty proper subset $I \subset \{0, \ldots, k\}$. Then $x_i^m = 1$ where

$$m = \prod_{p\leq k+1} p.$$

For us, we label

$$c_i(x) = \sum_{j=0}^{D} c_{i,j}x^j \quad \text{for} \quad i = 1, 2,$$

and we get

$$\sum_{j=0}^{D} c_{1,j}\zeta^j + \sum_{j=0}^{D} c_{2,j}\kappa^n\zeta^{j+nb} = 0. \tag{5.17}$$

This almost looks like the equation from Mann's theorem (5.15) except that the non-degeneracy condition (5.16) might fail. So, let us study (5.17). Let C be the set of non-zero coefficients among $c_{1,j}$ and $c_{2,j}\kappa^n$ for $0 \le j \le D$. If $c \in C$ then $c = c_{\ell,j}\kappa^{\delta n}$ for some $\ell \in \{1, 2\}$ and $j \in \{0, \dots, j\}$, then put $x_c = \zeta^{j+\delta nb}$. Here, we take $\delta = 0$ if $\ell = 1$ and $\delta = 1$ if $\ell = 2$. With these conventions, equation (5.17) is

$$\sum_{c \in C} c x_c = 0.$$

This splits into a certain number of non-degenerate equations. That is, there is a partition $C_1 \cup C_2 \cup \dots \cup C_t = C$ such that $\sum_{c \in C_i} c x_c = 0$ for $i = 1, \dots, t$ and each of these sub-equations is non-degenerate in the sense that it has no zero proper sub-sums. Clearly, $\#C_i \ge 2$ for each i. We analyze two sub-cases.

5.4.1 We have $\#C_i \ge 3$ for some $i \in \{1, \dots, t\}$

Then C_i contains two coefficients with the same ℓ. We assume that $\ell = 1$ (the case $\ell = 2$ reduces to $\ell = 1$ replacing ζ by ζ^{-1}) and let $j_1 < j_2$ be the smallest such that c_{1,j_1}, c_{1,j_2} belong to C_i. Then the equation is

$$c_{1,j_1}\zeta^{j_1} + c_{1,j_2}\zeta^{j_2} + \sum_{\substack{c_{\ell,j}\kappa^{\delta n} \in C_i \\ \ell = 2 \text{ or } j > j_2}} c_{\ell,j}\kappa^{n\delta}\zeta^{j+n\delta b} = 0.$$

Dividing by ζ^{j_1}, we get

$$c_{1,j_1} + c_{1,j_2}\zeta^{j_2 - j_1} + \sum_{\substack{c_{\ell,j}\kappa^{\delta n} \in C_i \\ \ell = 2 \text{ or } j > j_2}} c_{\ell,j}\kappa^{n\delta}\zeta^{j - j_1 + n\delta b} = 0.$$

We are now in the position to apply Mann's theorem to conclude that

$$\zeta^{(j_2 - j_1)m_1} = 1, \qquad m_1 \mid \prod_{p \le \#C_i} p \mid \prod_{p \le 2D+2} p,$$

because $\#C_i \le 2D + 2$. Since $|j_2 - j_1| \le D$, we have

$$m \le D \prod_{p \le 2D+2} p. \tag{5.18}$$

The inequality $\sum_{p \le x} \log p \le 1.02x$ holds for all $x > 0$, see [14, Theorem 9]. Hence

$$\log m \le \log D + \sum_{p \le 2D+2} \log p \le 4D,$$

which is much sharper than what we need.

5.4.2 We have $\#C_i = 2$ for all $i = 1, \ldots, t$

In fact, we may assume not only that $\#C_i = 2$ but also that each C_i contains exactly one c_{1,j_1} and one $c_{2,j_2}\kappa^n$; otherwise the argument from Subsection 5.4.1 applies, and we again have (5.18). So, let

$$c_{1,j_1}\zeta^{j_1} + c_{2,j_2}\kappa^n\zeta^{j_2+nb} = 0.$$

We then get $\zeta^{j_2-j_1+nb} = -c_{1,j_1}/c_{2,j_2}\kappa^{-n}$. The pair (j_1, j_2) depends on i. Assume first that, as we loop over i, the differences $j_2 - j_1$ are not the same over all i; that is, there are two values of i corresponding to say (j_1, j_2) and (j_1', j_2') such that $j_2' - j_1' \neq j_2 - j_1$. We obtain

$$\zeta^{(j_2-j_1)-(j_2'-j_1')} = \frac{c_{1,j_1}/c_{2,j_2}}{c_{1,j_1'}/c_{2,j_2'}}$$

and the number on the right is a root of unity belonging to $\mathbb{Q}$. Hence it is ±1. The exponent on the left satisfies

$$0 \neq \left|(j_2 - j_1) - (j_2' - j_1')\right| \leq 2D.$$

Hence $m \leq 4D$, again better than wanted.

Now let us assume that $j_2 = j_1 + a$ with the same a for all i. In this case $c_{2,j_1+a} = \lambda c_{1,j_1}$ with the same $\lambda \in \mathbb{Q}^\times$ holds for all the i as well. This makes the rational function $c_2(x)/c_1(x)$ equal to λx^a, and so

$$u_n(x) = c_1(x)(1 + \lambda\kappa^n x^{a+nb}).$$

Since $u_n(\zeta) = 0$ but $c_1(\zeta) \neq 0$, we must have $1 + \lambda\kappa^n\zeta^{a+nb} = 0$, which means that $\lambda\kappa^n$ is a root of unity, so ±1. Now we have two options: either both λ and κ are ±1, or none is. The first option means that condition 2 of Theorem 1.2 is satisfied, which is against our hypothesis. Hence $\lambda\kappa^n = \pm1$, but $\lambda, \kappa \neq \pm1$.

We have clearly $\mathrm{h}(\kappa) = \mathrm{h}(f_1, f_2) \leq X$ and $\mathrm{h}(\lambda) = \mathrm{h}(c_1, c_2) \leq X$. Since κ is a rational number, distinct from 0 and from ±1, its numerator or denominator (say, the former) is at least 2 in absolute value. It follows that the denominator of $\lambda = \pm\kappa^{-n}$ is at least 2^n in absolute value. But the denominator of λ cannot exceed $e^{\mathrm{h}(\lambda)} \leq e^X$. We obtain $2^n \leq e^X$, which implies $n \leq \log X$. Hence

$$\varphi(m) \leq \deg u_n(x) \leq D + D\log X,$$

which implies a much sharper estimate for m than the wanted (5.5).

Theorem 1.3 is proved.

6 Proof of Theorem 1.6

Let ζ be an mth primitive root of unity such that the set

$$\{n \in \mathbb{Z}_{>0} : u_n(x) \text{ is not identically } 0, \text{ but } u_n(\zeta) = 0\} \tag{6.1}$$

is not empty. If $c_1(\zeta)f_1(\zeta) = c_2(\zeta)f_2(\zeta) = 0$ then set (6.1) consists of all positive integers, and includes 1 in particular.

If, say, $c_1(\zeta)f_1(\zeta) \neq 0$, and set (6.1) is non-empty, then

$$c_1(\zeta)f_1(\zeta)c_2(\zeta)f_2(\zeta) \neq 0.$$

Denoting

$$\eta = \frac{f_1(\zeta)}{f_2(\zeta)}, \qquad \theta = -\frac{c_2(\zeta)}{c_1(\zeta)},$$

set (6.1) consists of n with the property $\eta^n = \theta$. If η is a root of unity, then its order divides $2m$, and there exists a positive $n \leq 2m$ such that $\eta^n = \theta$. If η is not a root of unity, then $n = \mathrm{h}(\theta)/\mathrm{h}(\eta)$. We have $\mathrm{h}(\theta) \leq X + \log(D+1)$ by Lemma 2.1, and $\varphi(m)\mathrm{h}(\eta) \geq 2(\log\varphi(m))^{-3}$, see (4.9). Hence

$$n \leq m(\log m)^3(X + \log D).$$

Theorem 1.6 is proved.

Acknowledgements

Yu. B. was partially supported by the Indian Government SPARC Project P445. F. L. was supported in part by Grant NUM2020 from the Wits CoEMaSS. Part of this work was done while F. L. was visiting the Max Planck Institute for Mathematics in Bonn from September 2019 to February 2020. He thanks this institution for its support, hospitality and excellent working conditions.

We thank Yann Bugeaud, Philipp Habegger, Alina Ostafe and Igor Shparlinski for helpful discussions. We also thank the referee for the encouraging report and many useful suggestions that helped us to improve the presentation.

References

[1] B. Bartolome, Yu. Bilu, and F. Luca, *On the exponential local-global principle*, Acta Arith. **159** (2013), no. 2, 101–111. MR 3062909

[2] Yu. Bilu and A. Borichev, *Remarks on Eisenstein*, J. Aust. Math. Soc. **94** (2013), no. 2, 158–180. MR 3109740

[3] Yu. Bilu and F. Luca, *Trinomials with given roots*, Indag. Math. (N.S.) **31** (2020), no. 1, 33–42. MR 4052259

[4] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006. MR 2216774

[5] E. Bombieri, P. Habegger, D. Masser, and U. Zannier, *A note on Maurin's theorem*, Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl. **21** (2010), no. 3, 251–260. MR 2677603

[6] E. Bombieri, D. Masser, and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Internat. Math. Res. Notices (1999), no. 20, 1119–1140. MR 1728021

[7] L. Fukshansky, P. Guerzhoy, and F. Luca, *On arithmetic lattices in the plane*, Proc. Amer. Math. Soc. **145** (2017), no. 4, 1453–1465. MR 3601538

[8] H. B. Mann, *On linear relations between roots of unity*, Mathematika **12** (1965), 107–117. MR 191892

[9] G. Maurin, *Courbes algébriques et équations multiplicatives*, Math. Ann. **341** (2008), no. 4, 789–824. MR 2407327

[10] A. Ostafe, *On some extensions of the Ailon-Rudnick theorem*, Monatsh. Math. **181** (2016), no. 2, 451–471. MR 3539944

[11] A. Ostafe and I. Shparlinski, *On the Skolem problem and some related questions for parametric families of linear recurrence sequences*, arXiv:2005.06713 (2020).

[12] L. P. Postnikova and A. Schinzel, *Primitive divisors of the expression $a^n - b^n$ in algebraic number fields*, Mat. Sb. (N.S.) **75 (117)** (1968), 171–177. MR 0223330

[13] G. Robin, *Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n*, Acta Arith. **42** (1983), no. 4, 367–389. MR 736719

[14] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94. MR 0137689

[15] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. **268(269)** (1974), 27–33. MR 344221

[16] C. L. Stewart, *Primitive divisors of Lucas and Lehmer numbers*, Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976), 1977, pp. 79–92. MR 0476628

[17] A. M. Vaidya, *An inequality for Euler's totient function*, Math. Student **35** (1967), 79–80 (1969). MR 252314

[18] P. Voutier, *An effective lower bound for the height of algebraic numbers*, Acta Arith. **74** (1996), no. 1, 81–95. MR 1367580