Binary polynomial power sums vanishing at roots of unity

by

YURI BILU (Bordeaux) and
FLORIAN LUCA (Johannesburg, Jeddah and Morelia)

Contents

1. Introduction ............................................. 1
2. Heights .................................................. 4
3. Cyclotomic polynomials ................................ 7
4. Schinzel’s Primitive Divisor Theorem ............... 10
5. Proof of Theorems 1.2 and 1.3 ....................... 14
6. Proof of Theorem 1.6 ................................ 21
References .................................................. 22

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 $u := \{u_n(x)\}_{n \geq 1} \subset \mathbb{Q}[x]$ the sequence of polynomials given by

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

We study roots of unity $\zeta$ 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 $\zeta$ 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
\[
c_2(x)/c_1(x) = \delta x^a, \quad f_2(x)/f_1(x) = \varepsilon x^b, \quad \delta, \varepsilon \in \{1, -1\}.
\]

We then get
\[
u_n(x) = c_1(x)f_1(x)^n(1 + \delta \varepsilon^n x^{a+bm})
\]
and we see that if $x = \zeta$ is such that $\zeta^{a+bn} = -\delta \varepsilon^n$, then $u_n(\zeta) = 0$. The condition that $b \neq 0$ ensures 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 $\zeta$ 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 $c_2(x)/c_1(x) = \delta x^a$, $f_2(x)/f_1(x) = \varepsilon x^b$.

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 [11, Theorem 2.11 and Corollary 2.14].

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 $\zeta$ 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 $a = (a_1, \ldots, a_k) \in \mathbb{Z}^k$ (primitive means that $\gcd(a_1, \ldots, a_k) = 1$) is defined by

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

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

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 by 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
Binary polynomial power sums vanishing at roots of unity

\[ D := \max\{\deg c_1, \deg c_2, \deg f_1, \deg f_2\}, \]
\[ X := \max\{3, h(c_1, c_2), h(f_1, f_2)\}. \]

Let \( m \) be a positive integer and \( \zeta \) a primitive \( m \)th root of unity such that for some \( n \) the polynomial \( u_n(x) \) is not identically zero but \( u_n(\zeta) = 0 \). Then
\[ m \leq e^{100D(X+D)}. \]

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
\[ (c_1(x), c_2(x), f_1(x), f_2(x)) = (1, -2^m, 2x, 1), \quad X = \max\{3, m \log 2\}. \]
Then \( u_m(x) = 2^m(x^m - 1) \) vanishes at primitive \( m \)th roots of unity, and we have \( m \geq X/\log 2 \) (provided \( m \geq 5 \)). 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 \( m \geq 3D \). 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 \( n \equiv 2D \mod 3D \). 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
\[ n \leq m(\log m)^3(X + \log D). \]

More precisely, either there exists \( n \) in this set satisfying \( n \leq 2m \), or every \( n \) in this set satisfies \( n \leq m(\log m)^3(X + \log D) \).
Throughout the article we use standard notation. We denote by $\varphi(n)$ the Euler function, by $\mu(n)$ the Möbius function, by $\Lambda(n)$ the von Mangoldt function and by $\omega(n)$ 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 2–4 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 the 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 $\alpha_i$ 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

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

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: $h(\lambda \bar{\alpha}) = h(\bar{\alpha})$ 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 (2.1) as

\[
h(\bar{\alpha}) = d^{-1} \sum_{K \rightarrow \mathbb{C}} \log \max\{|\alpha_0^\sigma|, \ldots, |\alpha_k^\sigma|\}
\]

\[+ d^{-1} \sum_{p} \max\{-\nu_p(\alpha_0), \ldots, -\nu_p(\alpha_k)\} \log N_p,
\]

where the first sum is over the complex embeddings of $K$, the second sum is over the finite primes of $K$, and $N_p$ denotes the absolute norm of $p$.

Now we define the height $h(g)$ of a non-zero polynomial $g$ with algebraic coefficients (in one or in several variables), or, more generally, the height $h(g_1, \ldots, g_k)$ 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 $h(\alpha)$ for $h(1, \alpha)$. If $\alpha$ belongs to a number field $K$ then
\[ h(\alpha) = d^{-1} \sum_{v \in M_K} d_v \log^+ |\alpha|_v \]
\[ = d^{-1} \sum_{v \in M_K} -d_v \log^- |\alpha|_v \quad (\alpha \neq 0), \]

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

**Lemma 2.1.** Let \( \alpha \in \bar{\mathbb{Q}} \) and \( f(x) \in \bar{\mathbb{Q}}[x] \) be a polynomial of degree less than or equal to \( D \). Then
\[ h(f(\alpha)) \leq Dh(\alpha) + h(1, f) + \log(D + 1). \]

More generally, if \( g(x) \in \bar{\mathbb{Q}}[x] \) is another polynomial of degree less than or equal to \( D \) and \( g(\alpha) \neq 0 \) then
\[ h(f(\alpha)/g(\alpha)) \leq Dh(\alpha) + h(g, f) + \log(D + 1). \]

If \( f(\alpha) = 0 \) then
\[ h(\alpha) \leq h(f) + \log 2. \]

Furthermore, let \( r \) be a non-negative integer. Then
\[ h(1, f^{(r)}/r!) \leq h(1, f) + D \log 2. \]

**Proof.** We start by proving (2.6). By definition,
\[ h(f(\alpha)/g(\alpha)) = h(1, f(\alpha)/g(\alpha)) = h(g(\alpha), f(\alpha)). \]

Write
\[ f(x) = a_D x^D + \cdots + a_0, \quad g(x) = b_D x^D + \cdots + b_0. \]

Let \( K \) be a number field containing \( \alpha \) and the coefficients of \( f, g \). We set \( d = [K : \mathbb{Q}] \). For \( v \in M_K \) we have
\[ |f(\alpha)|_v \leq \begin{cases} (D + 1)|f|_v \max\{1, |\alpha|_v\}^D, & v | \infty, \\ |f|_v \max\{1, |\alpha|_v\}^D, & v < \infty, \end{cases} \]

where \( |f|_v = \max\{|a_0|_v, \ldots, |a_D|_v\} \), and similarly for \( g(\alpha) \). Hence
\[ h(g(\alpha), f(\alpha)) \leq d^{-1} \sum_{v \in M_K} d_v \log \max\{|g(\alpha)|_v, |f(\alpha)|_v\} \]
\[ \leq d^{-1} \sum_{v \in M_K} d_v (\log \max\{|f|_v, |g|_v\} + D \log^+ |\alpha|_v) \]
\[ + d^{-1} \sum_{v \in M_K} d_v \log(D + 1) \]
\[ = h(g, f) + Dh(\alpha) + \log(D + 1), \]

which proves (2.6).
For (2.7) see [2, Proposition 3.6(1)]. Finally, we have
\[ f^{(r)}(x) = \sum_{k=r}^{D} \binom{k}{r} a_k x^{k-r}. \]
Since\( \binom{k}{r} \leq 2^k \leq 2^D, \)
we have
\[ \left| \frac{f^{(r)}}{r!} \right|_v \leq \begin{cases} 2^D |f|_v, & v \mid \infty, \\ |f|_v, & v < \infty. \end{cases} \]
Hence
\[
\begin{align*}
\h(1, \frac{f^{(r)}}{r!}) &= d^{-1} \sum_{v \in M_K} d_v \log^+ \left| \frac{f^{(r)}}{r!} \right|_v \\
&\leq d^{-1} \sum_{v \in M_K} d_v \log^+ |f_v| + d^{-1} \sum_{v \in M_K} d_v D \log 2 \\
&= \h(1, f) + D \log 2.
\end{align*}
\]
The lemma is proved. ■

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

**Proof.** Consider the polynomial
\[ f(x, y_1, \ldots, y_{k-1}) := f_1(x)y_1 + \cdots + f_{k-1}(x)y_{k-1} + f_k(x) \in \mathbb{Q}[x, y_1, \ldots, y_{k-1}]. \]
Applying [4, Theorem 1.6.13], we obtain
\[ \h(f/g) \leq \h(f/g) + \h(g) \leq \h(f) + (D + k - 1) \log 2. \]
Since
\[ \h(f_1/g, \ldots, f_k/g) = \h(f/g), \quad \h(f_1, \ldots, f_k) = \h(f), \]
the result follows. ■

**Lemma 2.3.** Let \( K \) be a number field of degree \( d \) and \( \alpha \in K \). Then
\[ \sum_{\nu_p(\alpha) < 0} \log \mathcal{N} p \leq d \h(\alpha), \quad \sum_{\nu_p(\alpha) > 0} \log \mathcal{N} p \leq d \h(\alpha), \]
where the first sum is over (finite) primes \( p \) of \( K \) with \( \nu_p(\alpha) < 0 \), the second sum over those with \( \nu_p(\alpha) > 0 \), and in the second sum we assume \( \alpha \neq 0 \).
More generally, let $\alpha_1, \ldots, \alpha_k \in K$. Then

$$\sum_{\nu_p(\alpha_i) < 0 \text{ for some } i \in \{1, \ldots, k\} \atop some i \in \{1, \ldots, k\}} \log Np \leq dh(\bar{\alpha}), \quad \bar{\alpha} = (1, \alpha_1, \ldots, \alpha_k).$$

**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). \hfill \square

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

$$e^{-dh(\alpha)} \leq \prod_{v \in S} |\alpha|_{v}^d \leq e^{dh(\alpha)}.$$

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

$$\prod_{i=1}^{r} |\alpha^{\sigma_i}| \geq e^{-dh(\alpha)}.$$

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

**3. Cyclotomic polynomials.** We denote by $\Phi_m(T)$ the $m$th cyclotomic polynomial. We will systematically use the identity

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

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 $\gamma \in \mathbb{Q}$ 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 $\gamma$ be an algebraic number. Then

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

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

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

$$\max_{|z| \leq 1} \log |\Phi_m(z)| \leq 2^{\omega(m)} \log(\pi m),$$
the maximum being over the unit disc on the complex plane. (We use the convention \( \log 0 = -\infty \).) For \( 0 < \varepsilon \leq 1/2 \) we also have

\[
\min_{|z| \leq 1-\varepsilon} \log |\Phi_m(z)| \geq -2^{\omega(m)} \log \frac{1}{\varepsilon}.
\] (3.3)

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

\[
\log |\Phi_m(z)| \leq (2^{\omega(m)-1} + 1) \log m + 2^{\omega(m)} \log \pi.
\] (3.4)

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

Let \( \ell \) be the exact order of \( \zeta \); thus, \( \ell | m \) and \( \zeta \) is a primitive \( \ell \)th root of unity. Let \( d \) be any other divisor of \( m \). If \( \ell \nmid d \) then \( d \leq m/2 \) and

\[
2 \geq |z^d - 1| \geq 2 \sin(\pi d/2m) \geq 2d/m.
\]

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

\[
|\log |z^d - 1|| \leq \log(m/d).
\] (3.5)

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

\[
2\pi \theta d/m \geq |z^d - 1| \geq 4\theta d/m.
\]

Writing \( d = d' \ell \), this implies that

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

Using (3.1) we obtain

\[
\log |\Phi_m(z)| = \sum_{d|m} \mu\left(\frac{m}{d}\right) \log |z^d - 1| + \sum_{d' | m/\ell} \mu\left(\frac{m/\ell}{d'}\right) \log |z^{\ell d'} - 1|
\]

\[
\leq \sum_{d|m} \left|\mu\left(\frac{m}{d}\right)\right| \log \frac{m}{d} + \sum_{d' | m/\ell} \mu\left(\frac{m/\ell}{d'}\right) \left( \log d' - \log \frac{m}{2\ell \theta} \right)
\]

\[
+ O_1(2^{\omega(m/\ell)} \log \pi)
\]

\[
= 2^{\omega(m)-1} \sum_{p|m} \log p + A\left(\frac{m}{\ell}\right) + \delta \log(2\theta) + O_1(2^{\omega(m/\ell)} \log \pi),
\]

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

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

\[
2 \geq |z^d - 1| \geq 1 - |z|^d \geq 1 - |z| \geq \varepsilon.
\]
Since $0 < \varepsilon \leq 1/2$ this implies that $|\log |z^d - 1|| \leq \log(1/\varepsilon)$. We obtain

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

In particular, (3.3) holds. ■

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

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

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

**Proof.** For $|z| \leq 1$ this is (3.2). If $|z| > 1$ then

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

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

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

The lower bound

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

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

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

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

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

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

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

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 $\gamma$ be a complex algebraic number of degree $d$, not a root of unity, and $n$ a positive integer. Then

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

**Corollary 3.5.** Let $\gamma$ and $m$ be as in Proposition 3.4. Then

(3.9) $$\log |\Phi_m(\gamma)| \geq -10^{12}d^4(h(\gamma) + 1) \cdot 2^{\omega(m)} \log(m + 1).$$
Proof. If $|\gamma| \geq 1$ then
\[
\log |\Phi_m(\gamma)| = \varphi(m) \log |\gamma| + \log |\Phi(\gamma^{-1})| \geq \log |\Phi(\gamma^{-1})|.
\]
Hence, replacing $\gamma$ by $\gamma^{-1}$ if necessary, we may assume $|\gamma| \leq 1$. We have
\[
(3.10) \quad \log |\Phi_m(\gamma)| = \sum_{n|m} \mu \left( \frac{m}{n} \right) \log |\gamma^n - 1|.
\]
Proposition 3.4 implies that
\[
2 \geq |\gamma^n - 1| \geq e^{-10^{12}d^4(h(\gamma)+1)\log(n+1)}.
\]
Hence for $1 \leq n \leq m$ we have
\[
|\log |\Phi_m(\gamma)|| \leq 10^{12}d^4(h(\gamma) + 1) \log(m + 1).
\]
Substituting this into (3.10), we obtain
\[
|\log |\Phi_m(\gamma)|| \leq 10^{12}d^4(h(\gamma) + 1) \cdot 2^{\omega(m)} \log(m + 1).
\]
In particular, we have proved (3.9). 

4. Schinzel’s Primitive Divisor Theorem. Let $\gamma$ be a non-zero algebraic number, not a root of unity. We consider the sequence
\[
u_p(u_n) > 0, \quad \nu_p(u_k) = 0 \quad (k = 1, \ldots, n - 1).
\]
For further use, let us fix here some basic properties of primitive divisors. Recall that $\Phi_n(T)$ denotes the $n$th cyclotomic polynomial, and $N_p$ is the absolute norm of $p$.

**Proposition 4.1.** Assume that $p$ is a primitive divisor of $u_n$. Then $n$ divides $N_p - 1$ and $\nu_p(\Phi_n(\gamma)) \geq 1$. In particular, $n < N_p$.

The proofs are very easy and we omit them.

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

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 $\gamma$ be an algebraic number of degree $d$, not a root of unity. Assume that
\[
n \geq \max\{2^{d+1}, 10^{30}d^9\}.
\]
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

\begin{equation}
(4.2) \quad h(\Phi_n(\gamma)) \leq 10^{13}d^4(h(\gamma) + 1) \cdot 2^{\omega(n)} \log(n + 1).
\end{equation}

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 $e_p$ (that is, $e_p = \nu_p(p)$). Let $\xi \in K$ satisfy

$$
\nu_p(\xi - 1) > \frac{e_p}{p - 1}.
$$

Then for any positive integer $n$ we have

$$
\nu_p(\xi^n - 1) = \nu_p(\xi - 1) + \nu_p(n).
$$

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

LEMMA 4.5. Let $\gamma$ be an algebraic number of degree $d$, not a root of unity, and $n$ an integer satisfying $n \geq 2^{d+1}$. 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 $\nu_p(\Phi_n(\gamma)) \leq \nu_p(n)$.

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 $\nu_p(\gamma^n - 1) > 0$, since there is nothing to prove otherwise. In particular, $\nu_p(\gamma) = 0$.

For $k = 0, 1, \ldots$ denote by $\ell_k$ the multiplicative order of $\gamma$ mod $\mathfrak{p}^k$; that is, $\ell_k$ is the smallest positive integer $\ell$ with $\nu_p(\gamma^\ell - 1) \geq k$. Clearly, $\nu_p(\gamma^n - 1) \geq k$ if and only if $\ell_k | n$. Together with (3.1) this implies that for every $k$,

\begin{equation}
(4.3) \quad \nu_p(\Phi_n(\gamma)) = \sum_{i=1}^{k} \sum_{\ell_i | m | n} \mu\left(\frac{n}{m}\right) + \sum_{\ell_{k+1} | m | n} \mu\left(\frac{n}{m}\right) \left(\nu_p(\gamma^m - 1) - k\right)
\end{equation}

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

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

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

\begin{equation}
(4.4) \quad n > \ell_{k+1}.
\end{equation}

We postpone the proof of (4.4) (which is a bit messy) until later, and now complete the proof of the lemma assuming the validity of (4.4):
Since \( n > \ell_{k+1} \geq \ell_i \) for \( i = 1, \ldots, k \), the double sum in (4.3) vanishes. Also, if \( \ell_{k+1} \mid m \) then

\[
\nu_p(\gamma^m - 1) = \nu_p(\gamma^{\ell_{k+1}} - 1) + \nu_p\left(\frac{m}{\ell_{k+1}}\right)
\]

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

\[
(4.5) \quad \nu_p(\Phi_n(\gamma)) = \sum_{\ell_{k+1} \mid m \mid n} \mu\left(\frac{n}{m}\right) \left(\nu_p(\gamma^{\ell_{k+1}} - 1) - k\right) + \sum_{\ell_{k+1} \mid m \mid n} \mu\left(\frac{n}{m}\right) \nu_p\left(\frac{m}{\ell_{k+1}}\right).
\]

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

\[
\nu_p(\Phi_n(\gamma)) = e_p \sum_{m' \mid n'} \mu\left(\frac{n'}{m'}\right) \nu_p(m') = \begin{cases} e_p & \text{if } n' \text{ is a power of } p, \\ 0 & \text{otherwise}. \end{cases}
\]

In any case we obtain \( \nu_p(\Phi_n(\gamma)) \leq \nu_p(n) \). This proves the lemma.

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

\[
(4.6) \quad n > \ell_1
\]

because \( p \) is not a primitive divisor of \( u_n \). Another useful observation is that

\[
(4.7) \quad \ell_{i+1} \leq p\ell_i \quad (i = 1, 2, \ldots).
\]

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 \( \nu_p(\gamma^{p\ell_i} - 1) > \nu_p(\gamma^{\ell_i} - 1) \), proving (4.7).

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

\[
(4.8) \quad p - 1 \leq e_p \leq d.
\]

On the other hand, let \( p^{f_p} = N_p \) be the absolute norm of \( p \). Clearly,

\[
\ell_1 \leq p^{f_p} - 1 \leq p^{d/e_p} - 1.
\]

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

Using (4.7) iteratively, we obtain

\[
\ell_{k+1} \leq p^k \ell_1 \leq p^{e_p/(p-1)+d/e_p} \leq \max_{p-1 \leq t \leq d} p^{t/(p-1)+d/t} = p^{1+d/(p-1)}.
\]
We have to show that
\[ p^{1+d/(p-1)} \leq 2^{d+1}. \]
This is true by inspection in the cases
\[ p = 2, \quad p = 3, \quad d \geq 3, \quad p = 5, \quad d \geq 4. \]
Now assume that \( p \geq 7 \), in which case \( d \geq 6 \). Since \( p \leq d + 1 \), we have
\[ p^{1+d/(p-1)} \leq (d + 1) \cdot 7^{d/6}. \]
A calculation shows that \((d + 1) \cdot 7^{d/6} \leq 2^{d+1}\) for \( d \geq 6 \). 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
\[- \log |\Phi_n(\gamma)|_v \leq \begin{cases} 10^{12} d^4 (h(\gamma) + 1) \cdot 2^{\omega(n)} \log(n + 1), & v \mid \infty, \\ - \log |n|_v, & v < \infty. \end{cases} \]
Indeed, the archimedean case is Corollary 3.5, and the non-archimedean case is Lemma 4.5. Summing up, we obtain
\[ h(\Phi_n(\gamma)) \leq 10^{12} d^4 (h(\gamma) + 1) \cdot 2^{\omega(n)} \log(n + 1) + \log n, \]
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, \( n \geq 10^{30} \). Comparing Proposition 4.3 and Theorem 3.1, we obtain
\[ \varphi(n) h(\gamma) \leq 10^{13} d^4 (h(\gamma) + 1) \cdot 2^{\omega(n)} \log(n + 1) + 2^{\omega(n)} \log(\pi n) \leq 10^{14} d^4 (h(\gamma) + 1) \cdot 2^{\omega(n)} \log(n + 1). \]
Since \( \gamma \) is not a root of unity, we have
\[ (4.9) \quad d h(\gamma) \geq 2 (\log(3d))^{-3} \]
(see [18 Corollary 2]). Hence
\[ \varphi(n) h(\gamma) \leq 10^{15} d^5 (\log(3d))^3 h(\gamma) \cdot 2^{\omega(n)} \log(n + 1), \]
which implies
\[ (4.10) \quad \varphi(n) \leq 10^{15} d^5 (\log(3d))^3 \cdot 2^{\omega(n)} \log(n + 1). \]
For \( n \geq 10^{30} \) we have
\[ (4.11) \quad \varphi(n) \geq 0.5 \frac{n}{\log \log n}, \quad \omega(n) \leq \frac{\log n}{\log \log n - 1.2} \]
(see [14 Theorem 15] and [13 Theorem 13]). Hence for \( n \geq 10^{30} \),
\[ 2^{\omega(n)} \frac{n}{\varphi(n)} \log(n + 1) \leq n^{(\log 2)/((\log \log n)^{1.2})} \cdot 2 (\log \log n) \cdot \log(n + 1) \leq n^{1/3}. \]
Using this, we deduce from \((4.10)\) the inequality \(n^{2/3} \leq 10^{15} d^5 (\log(3d))^3\). A quick calculation shows that this is incompatible with \((4.1)\) \(\blacksquare\).

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 what follows:

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

\[
u_n(x) = c_1(x)f_1(x)^n + c_2(x)f_2(x)^n \quad (n = 1, 2, \ldots);
\]

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

\[
\Phi_m(x) | \nu_n(x).
\]

5.1. Some reductions. We start by some general observations.

- We may assume that

\[
c_1(\zeta)c_2(\zeta)f_1(\zeta)f_2(\zeta) \neq 0.
\]

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

\[
\varphi(m) \geq m^{1/2} \quad (m \neq 2, 6)
\]

(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 \(\deg \nu_n(x) \leq D\), and we again obtain \(\varphi(m) \leq D\).

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

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

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

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

\[
\gcd(c_1(x), c_2(x)) = \gcd(f_1(x), f_2(x)) = 1.
\]

Lemma 2.2 implies that

\[
\h(\tilde{c}_1, \tilde{c}_2) \leq \h(c_1, c_2) + (D + 1) \log 2 \leq X + (D + 1) \log 2,
\]

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

\[
m \leq e^{30D(X + D)}
\]

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 which is non-zero and not a root of unity. By symmetry, we may assume that \( \gamma \) 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 \( c_1(x) \) is monic. Similarly, we may assume that \( f_1(x) \) is monic.

Denote \( K = \mathbb{Q}(\gamma) \). Then
\[
d := \left[ K : \mathbb{Q} \right] \leq D.
\]
Since \( X \geq 3 \), 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 \( p \) of \( K \) such that \( \nu_p(\Phi_m(\gamma)) > 0 \) and
\[
m < \mathcal{N}p.
\]

So we only have to bound \( \mathcal{N}p \).

5.2.1. The numbers \( \beta \) and \( \delta \). We have \( f_2(\gamma) \neq 0 \) by (5.4). However, it can happen that \( c_2(\gamma) = 0 \). Denote by \( r \) the order of \( \gamma \) as a root of \( c_2(x) \), and set
\[
\beta = c_2^{(r)}(\gamma)/r!, \quad \delta = f_2(\gamma),
\]
These are non-zero elements of the number field \( K \).

We claim that one of the following holds:

(5.6) \( \nu_p(\alpha) < 0 \) for some coefficient \( \alpha \) of \( c_1 \) or \( f_1 \) or \( c_2 \) or \( f_2 \);
(5.7) \( \nu_p(\beta) > 0 \);
(5.8) \( \nu_p(\delta) > 0 \).

Indeed, since \( \nu_p(\Phi_m(\gamma)) > 0 \), there exists a primitive \( m \)th root of unity \( \zeta \) and a prime \( \mathfrak{P} | p \) 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
\[
F(x) := \frac{c_1(x)f_1(x)^n}{(x - \gamma)^r}, \quad G(x) := \frac{c_2(x)}{(x - \gamma)^r}
\]
belong to $O_P[x]$ 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 $O_P$:
\[ \beta \delta^n \equiv G(\zeta)f_2(\zeta)^n \equiv -F(\zeta) \equiv -F(\gamma) \equiv 0 \mod \mathfrak{P}. \]
Hence either $\beta \equiv 0 \mod \mathfrak{P}$ or $\delta \equiv 0 \mod \mathfrak{P}$, which means that one of (5.7) or (5.8) holds true.

### 5.2.2. Estimates
Now we are ready to estimate $N_p$. Using Lemma 2.3, we obtain
\[ \log N_p \leq \max\{h(1, c_1), h(1, c_2), h(1, f_1), h(1, f_2), h(\beta), h(\delta)\}. \]
Since $f_1(x)$ is monic, we have
\[ h(1, f_1), h(1, f_2) \leq h(f_1, f_2) \leq X, \]
and similarly for $c_1, c_2$. Furthermore, using Lemma 2.1, we find
\begin{align*}
    h(\gamma) &\leq h(f_1) + \log 2 \leq X + \log 2, \\
    h(\delta) &\leq h(1, f_2) + Dh(\gamma) + \log(D + 1) \leq (D + 1)X + 2D, \\
    h(\beta) &\leq h(1, c_2^{(r)/r!}) + Dh(\gamma) + \log(D + 1) \\
    &\leq h(1, c_2) + D \log 2 + DX + D \log 2 + \log(D + 1) \\
    &\leq (D + 1)X + 2D.
\end{align*}
This implies that
\[ \log N_p \leq (D + 1)X + 2D < 3DX. \]
Since $m < N_p$, this proves (5.5).

### 5.3. The polynomial $f_1(x)f_2(x)$ vanishes at a root of unity $\xi$.
We may assume that $f_1(\xi) = 0$. Then $f_2(\xi) \neq 0$ by (5.4).
Let us describe our argument informally. Since $f_1(\xi)/f_2(\xi) = 0$, there exists $\varepsilon > 0$ such that $|f_1(z)/f_2(z)| \leq 1/2$ when $|z - \xi| \leq \varepsilon$.
Now assume that $u_n(\zeta) = 0$ for some primitive $m$th root of unity $\zeta$. Using (5.2), we may write
\[ 0 \neq \alpha := \frac{c_2(\zeta)}{c_1(\zeta)} = -\left( \frac{f_1(\zeta)}{f_2(\zeta)} \right)^n. \]
Let $Q(\zeta) \hookrightarrow \mathbb{C}$ be a complex embedding such that $\zeta^\sigma$ belongs to the $\varepsilon$-neighborhood of $\xi$. Then $|\alpha^\sigma| \leq (1/2)^n$. Define
\[ \beta := \prod_{|\zeta^\sigma - \xi| \leq \varepsilon} \alpha^\sigma, \]
the product being over all $\sigma$ as above. Since the $\varepsilon$-neighborhood of $\xi$ contains a positive proportion of primitive $m$th 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 $\varepsilon$.

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

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

This bounds $n$.

All of this 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 by $\varphi(m, a, b)$ the number of integers $k$ coprime with $m$ and satisfying $a \leq k \leq b$. 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 $\varepsilon$ satisfy $0 < \varepsilon \leq 1$ and let $\xi$ be a complex number on the unit circle; that is, $|\xi| = 1$. Let $m$ be a positive integer. Then there exist at least $\pi \varepsilon^{-1} \varphi(m) - 2^{\omega(m)}$ primitive $m$th roots of unity $\zeta$ satisfying $|\zeta - \xi| \leq \varepsilon$.

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

$$m(\theta - \eta) \leq k \leq m(\theta + \eta), \quad \gcd(m, k) = 1,$$

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

Lemma 5.1 implies that there are at least $2\eta \varphi(m) - 2^{\omega(m)}$ choices for $k$, with distinct $k$ giving rise to distinct $\zeta$ (this is because $\eta \leq 1/6$). Since $\eta \geq (2\pi)^{-1} \varepsilon$, 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 $H \geq 1$ in absolute value. Let $\xi \in \mathbb{C}$ be such that

$$|\xi| \leq 1, \quad f_1(\xi) = 0, \quad f_2(\xi) = \delta \neq 0.$$  

Set

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

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


Proof. Since $|\xi| \leq 1$ and $\varepsilon \leq 1/3D$, we have for $|z - \xi| \leq \varepsilon$ trivial estimates
$$|f_i'(z)| \leq \frac{1}{2} D(D+1)H(1+\varepsilon)^{D-1} \leq D^2 H \quad (i = 1, 2).$$
Hence for $|z - \xi| \leq \varepsilon$ we have
$$|f_1(z)| \leq D^2 H \varepsilon \leq \frac{1}{2}|\delta|, \quad |f_2(z)| \geq |\delta| - D^2 H \varepsilon \geq \frac{2}{3}|\delta|.$$  
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 $\xi$ 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
$$|\delta| \geq e^{-h(f_2(\xi))} \geq e^{-h(1,f_2)-\log(D+1)} \geq ((D+1)H)^{-1}.$$  
For $\varepsilon = (6D^3H^2)^{-1}$, Lemma 5.3 implies that
$$\left|\frac{f_1(z)}{f_2(z)}\right| \leq 1/2$$  
for $z \in \mathbb{C}$ with $|z - \xi| \leq \varepsilon$.

Now define $\alpha$ and $\beta$ as in (5.11), (5.12). Then
$$- \log |\beta| \geq nr \log 2,$$
where $r$ is the number of embeddings $\mathbb{Q}(\zeta) \stackrel{\sigma}{\rightarrow} \mathbb{C}$ such that $|\zeta^\sigma - \xi| \leq \varepsilon$. Denote by $\sigma_1, \ldots, \sigma_r$ all those $\sigma$. Lemmas 2.4 and 2.1 imply that
$$- \log |\beta| = \sum_{i=1}^r - \log |\alpha^{\sigma_i}| \leq [\mathbb{Q}(\zeta) : \mathbb{Q}] h(\alpha)$$  
$$\leq \varphi(m)(h(c_1, c_2) + \log(D + 1)) \leq \varphi(m)(X + \log(D + 1)).$$
Together with (5.13) this implies that
$$n \leq \frac{\varphi(m)}{r \log 2}(X + \log(D + 1)),$$
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

$$(5.15) \quad a_0 x_0 + a_1 x_1 + \cdots + a_k x_k = 0.$$  

Assume that

$$(5.16) \quad \sum_{i \in I} a_i x_i \neq 0$$

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

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

and we get

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

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 $0 \leq j \leq D$. If $c \in C$ then $c = c_{\ell,j} \kappa^\delta n$ for some $\ell \in \{1, 2\}$ and $j \in \{0, \ldots, j\}$, and we 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

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

This splits into a certain number of non-degenerate equations. That is, there is a partition $C_1 \cup \cdots \cup C_t = C$ such that $\sum_{c \in C_i} cx_c = 0$ for $i = 1, \ldots, t$ and each of these subequations is non-degenerate in the sense that it has no zero proper subsums. Clearly, $\#C_i \geq 2$ for each $i$. We analyze two subcases.

**5.4.1.** $\#C_i \geq 3$ for some $i \in \{1, \ldots, t\}$. Then $C_i$ contains two coefficients with the same $\ell$. We assume that $\ell = 1$ (the case $\ell = 2$ reduces to $\ell = 1$ after replacing $\zeta$ by $\zeta^{-1}$) 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
\[ c_{1,j_1} \zeta^{j_1} + c_{1,j_2} \zeta^{j_2} + \sum_{\substack{\ell, j \in C_i \\ \ell = 2 \text{ or } j > j_2}} c_{\ell,j} \zeta^{n,j+n}b = 0. \]

Dividing by $\zeta^{j_1}$, we get
\[ c_{1,j_1} + c_{1,j_2} \zeta^{j_2-j_1} + \sum_{\substack{\ell, j \in C_i \\ \ell = 2 \text{ or } j > j_2}} c_{\ell,j} \zeta^{n,j-j_1+n}b = 0. \]

We are now in a position to apply Mann’s theorem to conclude that
\[ \zeta^{(j_2-j_1)m_1} = 1, \quad m_1 \mid \prod_{p \leq \#C_i} p \mid \prod_{p \leq 2D+2} p, \]

because $\#C_i \leq 2D + 2$. Since $|j_2 - j_1| \leq D$, we have
\[ (5.18) \quad m \leq D \prod_{p \leq 2D+2} p. \]

The inequality $\sum_{p \leq x} \log p \leq 1.02x$ holds for all $x > 0$ (see [14, Theorem 9]). Hence
\[ \log m \leq \log D + \sum_{p \leq 2D+2} \log p \leq 4D, \]

which is much sharper than what we need.

5.4.2. $\#C_i = 2$ 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 $c_{2,j_2} \zeta^n$; otherwise the argument from Subsection 5.4.1 applies, and we again have $(5.18)$. So, let
\[ c_{1,j_1} \zeta^{j_1} + c_{2,j_2} \zeta^n \zeta^{j_2+n}b = 0. \]

We then get $\zeta^{j_2-j_1+n}b = -c_{1,j_1}/c_{2,j_2} \zeta^{-n}$. 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
\[ \zeta^{(j_2-j_1)-(j_2'-j_1')} = c_{1,j_1}/c_{2,j_2} \]

and the number on the right is a root of unity belonging to $\mathbb{Q}$. Hence it is $\pm 1$. The exponent on the left satisfies
\[ 0 \neq |(j_2 - j_1) - (j_2' - j_1')| \leq 2D. \]

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

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

We have clearly $h(\kappa) = h(f_1, f_2) \leq X$ and $h(\lambda) = h(c_1, c_2) \leq X$. Since $\kappa$ is a rational number, distinct from 0 and from $\pm 1$, 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 $\lambda$ cannot exceed $e^{h(\lambda)} \leq e^X$. 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 desired (5.5).

Theorem 1.3 is proved.

6. Proof of Theorem 1.6 Let $\zeta$ be an $m$th primitive root of unity such that the set
\[ \{ n \in \mathbb{Z}_{>0} : u_n(x) \text{ is not identically 0, but } u_n(\zeta) = 0 \} \]
is not empty. If $c_1(\zeta)f_1(\zeta) = c_2(\zeta)f_2(\zeta) = 0$ then the set (6.1) consists of all positive integers, and includes 1 in particular.

If, say, $c_1(\zeta)f_1(\zeta) \neq 0$, and (6.1) is non-empty, then
\[ c_1(\zeta)f_1(\zeta)c_2(\zeta)f_2(\zeta) \neq 0. \]
Denote
\[ \eta = \frac{f_1(\zeta)}{f_2(\zeta)}, \quad \theta = -\frac{c_2(\zeta)}{c_1(\zeta)}; \]
then (6.1) consists of $n$ with the property $\eta^n = \theta$. If $\eta$ is a root of unity, then its order divides $2m$, and there exists a positive $n \leq 2m$ such that $\eta^n = \theta$. If $\eta$ is not a root of unity, then $n = h(\theta)/h(\eta)$. We have $h(\theta) \leq X + \log(D + 1)$ by Lemma 2.1 and $\varphi(m)h(\eta) \geq 2(\log \varphi(m))^{-3}$ (see (4.9)). Hence
\[ n \leq m(\log m)^3(X + \log D). \]
Theorem 1.6 is proved.

Acknowledgements. 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.
Yu. B. was partially supported by the Indian Government SPARC Project P445. F. L. was supported in part by Grant NUM2020 from the Wits Co-EMaSS. 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.

References

[1] B. Bartolome, Yu. Bilu, and F. Luca, *On the exponential local-global principle*, Acta Arith. 159 (2013), 101–111.
[2] Yu. Bilu and A. Borichev, *Remarks on Eisenstein*, J. Austral. Math. Soc. 94 (2013), 158–180.
[3] Yu. Bilu and F. Luca, *Trinomials with given roots*, Indag. Math. (N.S.) 31 (2020), 33–42.
[4] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, New Math. Monogr. 4, Cambridge Univ. Press, Cambridge, 2006.
[5] E. Bombieri, P. Habegger, D. Masser, and U. Zannier, *A note on Maurin’s theorem*, Rend. Lincei Mat. Appl. 21 (2010), no. 3, 251–260.
[6] E. Bombieri, D. Masser, and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Int. Math. Res. Notices 1999, 1119–1140.
[7] L. Fukshansky, P. Guerzhoy, and F. Luca, *On arithmetic lattices in the plane*, Proc. Amer. Math. Soc. 145 (2017), 1453–1465.
[8] H. B. Mann, *On linear relations between roots of unity*, Mathematika 12 (1965), 107–117.
[9] G. Maurin, *Courbes algébriques et équations multiplicatives*, Math. Ann. 341 (2008), 789–824.
[10] A. Ostafe, *On some extensions of the Ailon–Rudnick theorem*, Monatsh. Math. 181 (2016), 451–471.
[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 (in Russian).
[13] G. Robin, *Estimation de la fonction de Tchebychef $\theta$ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de $n$*, Acta Arith. 42 (1983), 367–389.
[14] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.
[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.
[16] C. L. Stewart, *Primitive divisors of Lucas and Lehmer numbers*, in: Transcendence Theory: Advances and Applications (Cambridge, 1976), 1977, 79–92.
[17] A. M. Vaidya, *An inequality for Euler’s totient function*, Math. Student 35 (1967), 79–80 (1969).
[18] P. Voutier, *An effective lower bound for the height of algebraic numbers*, Acta Arith. 74 (1996), 81–95.
