International Journal of Number Theory

The non-cyclotomic part of $f(x)x^n + g(x)$ and roots of reciprocal polynomials off the unit circle

E. Dobrowolski

Department of Mathematics and Statistics,
University of Northern British Columbia,
Prince George BC V2N 4Z9, Canada
dobrowolski@cnc.bc.ca

M. Filaseta*

Department of Mathematics, University of South Carolina,
Columbia, SC 29208, U.S.A.
filaseta@math.sc.edu

A. F. Vincent

Department of Mathematics, University of South Carolina,
Columbia, SC 29208, U.S.A.
vincenta@email.sc.edu

Given relatively prime polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$ with non-zero constant terms, we show that for n greater than an explicitly determined bound depending on $f(x)$ and $g(x)$, if the polynomial $f(x)x^n + g(x)$ is non-reciprocal, then its *non-cyclotomic part* is irreducible except for some explicit cases where a known factorization of $f(x)x^n + g(x)$ can easily be described. Prior work of a similar nature is discussed which shows under similar circumstances the *non-reciprocal part of* $f(x)x^n + g(x)$ is irreducible. The current paper establishes and makes use of a result which shows that a reciprocal polynomial $f(x)$ with a root off the unit circle must have a root bounded away from the unit circle by an explicitly given function of the degree of $f(x)$, the leading coefficient a of $f(x)$ and the discriminant of $f(x)$. Notably in this result, a need not be 1.

Keywords: reciprocal; cyclotomic; irreducible; Mahler measure.

Mathematics Subject Classification 2000: 11C08, 11R06, 11R09, 12E05

1. Introduction

For a non-zero $f(x) \in \mathbb{R}[x]$, we define $\tilde{f}(x) = x^{\deg f} f(1/x)$. The polynomial $\tilde{f}(x)$ is called the *reciprocal* of $f(x)$. The constant term of $\tilde{f}(x)$ is the leading coefficient of $f(x)$ and, hence, non-zero. If $\alpha \neq 0$ is a root of $f(x)$, then $1/\alpha$ is a root of $\tilde{f}(x)$. If $f(x) = \pm\tilde{f}(x)$, then necessarily each root of $f(x)$ is non-zero. Thus, $f(x) = \pm\tilde{f}(x)$ implies that α is a root of $f(x)$ if and only if $1/\alpha$ is a root of $f(x)$. We call such

*The second author expresses his gratitude to the NSA for funding for this research.

an $f(x)$ *reciprocal*. If $f(x)$ is not reciprocal, we say that $f(x)$ is *non-reciprocal*. The *content* of a non-zero polynomial $f(x) \in \mathbb{Z}[x]$ is the greatest common divisor of its coefficients. For $f(x) \in \mathbb{Z}[x]$, we are interested in the polynomial obtained by removing the content of $f(x)$ and those reciprocal factors of $f(x)$ in $\mathbb{Z}[x]$ that are irreducible over the rationals and that have content 1 and positive leading coefficient. We refer to what remains as the *non-reciprocal part of* $f(x)$. For example, the non-reciprocal part of $3(-x+1)x(x^2+2)$ is $-x(x^2+2)$ (the content 3 and the irreducible reciprocal factor $x-1$ have been removed from the polynomial $3(-x+1)x(x^2+2)$). We similarly refer to the *non-cyclotomic part of an* $f(x) \in \mathbb{Z}[x]$ as the polynomial $f(x)$ removed of its cyclotomic factors. For

$$f(x) = \sum_{j=0}^{r} a_j x^j = a_r \prod_{1 \le j \le r} (x - \alpha_j) \in \mathbb{R}[x],$$

we recall that the *Mahler measure of* $f(x)$ is given by

$$M(f) = |a_r| \prod_{\substack{1 \le j \le r \\ |\alpha_j| > 1}} |\alpha_j|.$$

Furthermore, the *Euclidean norm of* $f(x)$ is defined by

$$\|f\| = \sqrt{\sum_{j=0}^{r} a_j^2}.$$

Finally, for two polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$, we use the notation $\gcd_{\mathbb{Z}}(f(x), g(x))$ to denote the polynomial $h(x) \in \mathbb{Z}[x]$ with largest degree and largest leading coefficient that divides both $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$. In particular, $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$ implies that the content of $f(x)$ and the content of $g(x)$ are relatively prime.

Based on early work by Schinzel [10,11], which in particular connected the study of polynomials of the form $x^n + g(x)$ to a problem of P. Turán and a problem on covering systems of the integers (see also [4]), one can find an explicit $B_1 = B_1(f, g)$ such that, for $n \ge B_1$, the non-reciprocal part of the polynomial $f(x)x^n + g(x)$ is either irreducible or ± 1 provided $f(x)x^n + g(x)$ itself does not factor in a precisely given way (see (i) and (ii) and the examples after Theorem 1.1 below). Motivated to strengthen what can be said in this direction, Ford, Konyagin, and the second author [5] obtained the following explicit estimate.

Theorem 1.1. *Let* $f(x)$ *and* $g(x)$ *be in* $\mathbb{Z}[x]$ *with* $f(0) \ne 0$, $g(0) \ne 0$, *and* $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$. *Let* r_1 *and* r_2 *denote the number of non-zero terms in* $f(x)$ *and* $g(x)$, *respectively. If*

$$n \ge B_1 := \max\left\{2 \times 5^{2N-1}, 2\max\left\{\deg f, \deg g\right\}\left(5^{N-1} + \frac{1}{4}\right)\right\}$$

where

$$N = 2\|f\|^2 + 2\|g\|^2 + 2r_1 + 2r_2 - 7,$$

then the non-reciprocal part of $f(x)x^n + g(x)$ *is irreducible or identically* 1 *or* -1 *unless one of the following holds:*

(i) *The polynomial* $-f(x)g(x)$ *is a pth power for some prime* p *dividing* n.
(ii) *For either* $\varepsilon = 1$ *or* $\varepsilon = -1$, *one of* $\varepsilon f(x)$ *or* $\varepsilon g(x)$ *is a* 4*th power, the other is* 4 *times a* 4*th power, and* n *is divisible by* 4.

The conditions (i) and (ii) above are necessary. We illustrate this necessity with two examples. In each example, m denotes a positive integer. For $n = 6m$, we have

$$(x+5)^3x^n - 8 = ((x+5)x^{2m} - 2)((x+5)^2x^{4m} + 2(x+5)x^{2m} + 4),$$

giving an example illustrating (i). For an example illustrating (ii), we take $n = 4m$ and note that

$$4x^n + 81(x+1)^4 = (2x^{2m} + 6(x+1)x^m + 9(x+1)^2)(2x^{2m} - 6(x+1)x^m + 9(x+1)^2).$$

The same work of Schinzel in [10,11] more specifically addresses, in the case that $f(x) = 1$, the existence of a $B_2 = B_2(f,g)$ such that $n \geq B_2$ implies that the non-*cyclotomic* part of the polynomial $f(x)x^n + g(x)$ is either irreducible or ± 1 when (i) and (ii) of Theorem 1.1 do not hold. An explicit estimate for such a B_2 is not given there. On the other hand, the work by Schinzel in [12] (as a consequence of Theorem 3) or [13] (as a consequence of Theorem 4) would allow for one to obtain such an explicit value of $B_2(f,g)$ for general $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$ when $f(x)x^n + g(x)$ is non-reciprocal. Note that for $n > \max\{\deg f, \deg g\}$, the condition that $f(x)x^n + g(x)$ is non-reciprocal is equivalent to $g(x) \neq \pm\tilde{f}(x)$. To elaborate on how the material from [12] can be used for this problem, we include an argument in Appendix A that gives a bound associated with Corollary 1.3 below.

One goal of ours is to supply an explicit estimate for $B_2 = B_2(f,g)$. We will also require here the condition $g(x) \neq \pm\tilde{f}(x)$ mentioned above. In this direction, we show the following.

Theorem 1.2. *Let* $f(x)$ *and* $g(x)$ *be in* $\mathbb{Z}[x]$ *with* $f(0) \neq 0$, $g(0) \neq 0$, $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$ *and* $g(x) \neq \pm\tilde{f}(x)$. *Let* $b = \gcd\big(\tilde{f}(0), g(0)\big)$. *Define*

$$m_1 = \sqrt{\|f\|^2 + \|g\|^2}$$

and

$$m_2 = \max\{\deg f + 2\deg g, 2\deg f + \deg g, 2\}.$$

If

$$n > B_2 := \max\Big\{2^{2m_2^3 - 2m_2^2 + m_2} m_2^{m_2^2 + m_2} m_1^{2m_2^2} + \deg g, \\ \frac{\log m_1}{\log 2}(\deg g + 2m_2)\, b^{m_2 - 1} 2^{m_2 - 1}(m_2 - 1)^{(m_2-1)/2}\omega\Big\}$$

where $\omega = 1.216134\ldots$ *denotes the positive real root of* $64x^3 - 64x^2 - 16x - 1$, *then every irreducible reciprocal divisor of* $f(x)x^n + g(x)$ *with positive leading coefficient is cyclotomic.*

As an immediate consequence of Theorem 1.1 and Theorem 1.2, we have the following.

Corollary 1.3. *Let $f(x)$ and $g(x)$ be in $\mathbb{Z}[x]$ with $f(0) \neq 0$, $g(0) \neq 0$, $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$ and $g(x) \neq \pm\tilde{f}(x)$. In the notation of Theorem 1.1 and 1.2, we have that if*

$$n > \max\{B_1, B_2\},$$

then the non-cyclotomic part of $f(x)x^n + g(x)$ is irreducible or identically 1 or -1 unless either (i) or (ii) holds.

In order to obtain Theorem 1.2, we will want information about roots near the unit circle, reminiscent of prior work on the subject such as that of P. E. Blanksby and H. L. Montgomery [1], C. J. Smyth [15] and the first author [3]. Specifically, we want an estimate for the maximum absolute value of a root of $f(x) \in \mathbb{Z}[x]$ when $f(x)$ is reciprocal and contains a root off the unit circle. What sets this apart from the work cited above is that we are interested in the case that $f(x)$ is not necessarily monic. As the example $2x^2+x+2$ shows, it is possible for $f(x)$ to be non-monic, to be non-cyclotomic and to have all its roots on the unit circle. So the condition that $f(x)$ has at least one root off the unit circle is of significance here. We will show the following.

Theorem 1.4. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible reciprocal polynomial with leading coefficient a and roots $\alpha_1, \dots, \alpha_d$. If $f(x)$ has a root off the unit circle, then*

$$\max_{1 \le j \le d}\{|\alpha_j|\} \ge \min\left\{1 + \frac{1}{2^{d-1}\omega}, 1 + \frac{\sqrt{|\Delta(f)|}}{|a|^{d-1}2^{d-1}(d-1)^{(d-1)/2}\omega}\right\}$$

where $\Delta(f)$ is the discriminant of $f(x)$ and ω is as in Theorem 1.2.

Since $|\Delta(f)|$ is greater than the minimum absolute value of a discriminant of a field of degree d over $\mathbb{Q}$, then for sufficiently large d, we note that one can use lower bounds for this minimum obtained by Odlyzko and others (cf. [9]) to rewrite the lower bound in Theorem 1.4 in terms of the leading coefficient of $f(x)$ and the number of real and complex conjugate roots of $f(x)$.

2. Proof of Theorem 1.4

For the proof of Theorem 1.4, we begin by observing that the conditions in the theorem that $f(x)$ is reciprocal and that a root of $f(x)$ exists off the unit circle imply that the degree d of $f(x)$ is greater than 1. Since a reciprocal polynomial of odd degree has 1 or -1 as a root, the condition that $f(x)$ is irreducible implies further that d is even. We suppose as we may that a, the leading coefficient of $f(x)$, is positive. The discriminant of $f(x)$ is given by

$$\Delta(f) = a^{2(d-1)} \prod_{1 \le u < v \le d} (\alpha_u - \alpha_v)^2.$$

Since $f(x)$ is reciprocal, the product of its roots has absolute value 1 (that the product of the roots of $f(x)$ equals 1 is also true but slightly harder to see and not needed here). Thus,

$$\begin{aligned}\Bigg|\prod_{1\le u<v\le d}(\alpha_u-\alpha_v)^2\Bigg| &= \Bigg|(\alpha_1\cdots\alpha_d)^{d-1}\prod_{\substack{1\le u\le d\\1\le v\le d\\u\ne v}}(1-\alpha_u^{-1}\alpha_v)\Bigg| \\ &= \Bigg|\prod_{\substack{1\le u\le d\\1\le v\le d\\u\ne v}}(1-\alpha_u^{-1}\alpha_v)\Bigg|.\end{aligned} \tag{2.1}$$

We use again that $f(x)$ is reciprocal, observing that if $re^{i\theta}$ is a root of $f(x)$, then so is the conjugate of its inverse, namely $(1/r)e^{i\theta}$. Since also $f(x)$ is irreducible, we deduce that for each $u \in \{1,2,\ldots,d\}$, there is a unique $w(u) \in \{1,2,\ldots,d\}$ for which $\alpha_{w(u)} = 1/\overline{\alpha}_u$. Furthermore, if $|\alpha_u| \ne 1$, then we have $w(u) \ne u$, $w(w(u)) = u$ and exactly one of $|\alpha_u| > 1$ and $|\alpha_{w(u)}| > 1$ holds. In this case, we also have

$$\begin{aligned}(1-\alpha_u^{-1}\alpha_{w(u)})(1-\alpha_{w(u)}^{-1}\alpha_u) &= 2-|\alpha_u|^2-|\alpha_{w(u)}|^2 \\ &= (1-|\alpha_u|^2)(1-|\alpha_{w(u)}|^2) \\ &= (1-|\alpha_u|^2)(1-|\alpha_u|^{-2}).\end{aligned}$$

Therefore, the right-hand side of (2.1) can be written as

$$\begin{aligned}&\Bigg|\prod_{\substack{1\le u\le d\\w(u)\ne u}}(1-\alpha_u^{-1}\alpha_{w(u)})\Bigg|\cdot\Bigg|\prod_{\substack{1\le u\le d\\1\le v\le d\\v\notin\{u,w(u)\}}}(1-\alpha_u^{-1}\alpha_v)\Bigg| \\ &\qquad = \Bigg|\prod_{\substack{1\le u\le d\\|\alpha_u|>1}}(1-|\alpha_u|^2)(1-|\alpha_u|^{-2})\Bigg|\cdot\Bigg|\prod_{\substack{1\le u\le d\\1\le v\le d\\v\notin\{u,w(u)\}}}(1-\alpha_u^{-1}\alpha_v)\Bigg|.\end{aligned}$$

Let k denote the number of roots α_u satisfying $|\alpha_u| > 1$. By relabeling if needed, we take these k roots to be $\alpha_1, \alpha_2, \ldots, \alpha_k$. Noting that there are then exactly k roots α_u satisfying $|\alpha_u| < 1$, we relabel if need be to take these k roots to be $\alpha_d, \alpha_{d-1}, \ldots, \alpha_{d-k+1}$. For $1 \le u \le k$, we define ε_u by $|\alpha_u| = 1 + \varepsilon_u$. In particular, each $\varepsilon_u > 0$. Note also that, by the conditions in the theorem, $k \ge 1$. To obtain our result, we suppose as we may that $\varepsilon_u < 1$ for $1 \le u \le k$. We deduce then that

$$\big|(1-(1+\varepsilon_u)^2)(1-(1+\varepsilon_u)^{-2})\big| \le 4\,\varepsilon_u^2 \qquad \text{for } 1 \le u \le k.$$

Thus,

$$\Bigg|\prod_{\substack{1\le u\le d\\|\alpha_u|>1}}(1-|\alpha_u|^2)(1-|\alpha_u|^{-2})\Bigg| = \Bigg|\prod_{u=1}^{k}(1-|\alpha_u|^2)(1-|\alpha_u|^{-2})\Bigg| \le 4^k(\varepsilon_1\cdots\varepsilon_k)^2.$$

We use again that the product of the roots of $f(x)$ has absolute value 1, and note that $|\alpha_u \alpha_{w(u)}| = 1$. Hence,

$$\left| \prod_{\substack{1\le u\le d\\ 1\le v\le d\\ v\notin\{u,w(u)\}}} (1-\alpha_u^{-1}\alpha_v) \right| = \left| \prod_{\substack{1\le u\le d\\ 1\le v\le d\\ v\notin\{u,w(u)\}}} (\alpha_u-\alpha_v) \right| = P_1\cdot P_2,$$

where

$$P_1 = \left| \prod_{\substack{1\le u\le d-k\\ 1\le v\le d-k\\ v\ne u}} (\alpha_u-\alpha_v) \right| \quad \text{and} \quad P_2 = \left| \prod_{\substack{1\le u\le d\\ 1\le v\le d\\ v\notin\{u,w(u)\}\\ \max\{u,v\}>d-k}} (\alpha_u-\alpha_v) \right|.$$

Observe that the product in P_1 is restricted to α_u and α_v both having absolute value ≥ 1 and the product in P_2 is restricted to α_u and α_v with at least one having absolute value < 1. We find an upper bound for each of P_1 and P_2.

The value of P_1 can be interpreted as the square of the determinant of the $(d-k)\times(d-k)$ Vandermonde matrix

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{d-k-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{d-k-1} \\ 1 & \alpha_3 & \alpha_3^2 & \dots & \alpha_3^{d-k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{d-k} & \alpha_{d-k}^2 & \dots & \alpha_{d-k}^{d-k-1} \end{pmatrix}.$$

By applying Hadamard's inequality, we obtain

$$P_1 \le (d-k)^{d-k} M_0(f)^{2(d-k-1)},$$

where $M_0(f) = M(f)/|a|$.

In P_2, we consider first the factors $\alpha_u - \alpha_v$ with $u > d-k$. For a fixed α_u, there are $d-2$ possibilities for α_v since $v \notin \{u, w(u)\}$. Thus, there are a total of $k(d-2)$ factors of the form $\alpha_u - \alpha_v$ with $u > d-k$. Similarly, there are a total of $k(d-2)$ factors of the form $\alpha_u - \alpha_v$ with $v > d-k$. Together, this gives $2k(d-2)$ factors of the form $\alpha_u - \alpha_v$, but the ones with both $u > d-k$ and $v > d-k$ have been counted twice. There are $k(k-1)$ such factors counted twice, so the product in P_2 consists of exactly $2k(d-2) - k(k-1)$ factors $\alpha_u - \alpha_v$. Observe that if $u \le k$ in a factor $\alpha_u - \alpha_v$, then $v > d-k$ and $v \ne w(u)$; similarly, if $v \le k$, then $u > d-k$ and $u \ne w(v)$. Thus, each $j \le k$ appears as a u or v in exactly $2(k-1)$ factors $\alpha_u - \alpha_v$. Bounding $|\alpha_u - \alpha_v|$ by $2\max\{|\alpha_u|, |\alpha_v|\}$ in P_2, we deduce

$$P_2 \le \left(\prod_{j=1}^{k} (2|\alpha_j|) \right)^{2(k-1)} 2^{2k(d-2)-k(k-1)-2k(k-1)} = 2^{2kd-k^2-3k} M_0(f)^{2(k-1)}.$$

Combining the above, we now obtain that

$$|\Delta(f)| \le a^{2(d-1)} (\varepsilon_1 \cdots \varepsilon_k)^2 2^{2kd-k^2-k} (d-k)^{d-k} M_0(f)^{2(d-2)}.$$

Hence,

$$\varepsilon_1 \cdots \varepsilon_k \geq \frac{\sqrt{|\Delta(f)|}}{a^{d-1} 2^{(d-\frac{k+1}{2})k} (d-k)^{(d-k)/2} M_0(f)^{d-2}}.$$

Now, if

$$x_1 \cdots x_k = B,$$

where B is fixed and each $x_j > 0$, then

$$(1+x_1)\cdots(1+x_k) \geq (1+B^{1/k})^k. \tag{2.2}$$

There are a variety of approaches to verifying the above inequality; we simply note here that (2.2) is a consequence of a classical inequality of Maclaurin (see Theorem 52 of [7]). From (2.2), we deduce

$$\begin{aligned} M_0(f) &= (1+\varepsilon_1)\cdots(1+\varepsilon_k) \\ &\geq \left(1 + \left(\frac{\sqrt{|\Delta(f)|}}{a^{d-1} 2^{(d-\frac{k+1}{2})k} (d-k)^{(d-k)/2} M_0(f)^{d-2}}\right)^{1/k}\right)^k. \end{aligned}$$

Let $\alpha = \max_{1 \leq u \leq d}\{|\alpha_u|\}$. Since $f(x)$ has exactly k roots outside the unit circle we have $\alpha^k \geq M_0(f)$. Hence,

$$\begin{aligned} \alpha &\geq 1 + \left(\frac{\sqrt{|\Delta(f)|}}{a^{d-1} 2^{(d-\frac{k+1}{2})k} (d-k)^{(d-k)/2} \alpha^{k(d-2)}}\right)^{1/k} \\ &\geq 1 + \left(\frac{\sqrt{|\Delta(f)|}}{a^{d-1}(d-k)^{(d-k)/2}}\right)^{1/k} \frac{1}{2^{d-1}\alpha^{d-2}}. \end{aligned}$$

We set $X = \sqrt{|\Delta(f)|}/(a^{d-1}(d-k)^{(d-k)/2})$, and consider separately the case that $X \geq 1$ and $X < 1$. In the latter case, we observe that $X^{1/k}$ is minimized when $k = 1$. Thus, we deduce

$$\alpha \geq \min\left\{1 + \frac{1}{2^{d-1}\alpha^{d-2}}, 1 + \frac{\sqrt{|\Delta(f)|}}{a^{d-1}2^{d-1}(d-1)^{(d-1)/2}\alpha^{d-2}}\right\}. \tag{2.3}$$

To complete the proof we show that we can replace α^{d-2} in the denominators above with ω, where ω is as stated in Theorem 1.2. To do this, we set γ_d to be the positive real root of $x^{d-1} - x^{d-2} - (1/2^{d-1})$. Then $\gamma_d > 1$, and we get

$$\frac{1}{(\gamma_d - 1)2^{d-1}} = \gamma_d^{d-2} \geq 1.$$

Thus,

$$\gamma_d \leq 1 + \frac{1}{2^{d-1}}.$$

For $d \geq 6$, one checks that $(d-2)/2^{d-1} \leq 1/8$. Since $(1+(1/x))^x < e$ for all $x > 0$, we deduce that, for $d \geq 6$, we have

$$\gamma_d^{d-2} \leq \left(1 + \frac{1}{2^{d-1}}\right)^{d-2} = \left(\left(1 + \frac{1}{2^{d-1}}\right)^{2^{d-1}}\right)^{(d-2)/2^{d-1}} < e^{1/8} < 1.2. \qquad (2.4)$$

Recall d is even. We claim that

$$\gamma_d^{d-2} \leq \gamma_4^2 = \omega.$$

The equality above is an exercise in arithmetic. As $\omega > 1.2$ and (2.4) holds for $d \geq 6$, the inequality above is verified by simply considering $d = 2$ and $d = 4$, both of which clearly are satisfied.

Now, we consider two possibilities $\alpha^{d-2} \leq \omega$ and $\alpha^{d-2} > \omega$. In the case that $\alpha^{d-2} \leq \omega$, the theorem follows as the bound in (2.3) is decreased by replacing α^{d-2} with ω. Suppose now that $\alpha^{d-2} > \omega$. Then $d \neq 2$ and

$$\alpha > \exp\left(\frac{\log \omega}{d-2}\right) > 1 + \frac{\log \omega}{d-2}.$$

For $d \geq 6$, one checks that

$$\frac{\log \omega}{d-2} > \frac{1}{2^{d-1}\omega},$$

so that the theorem follows for such d. Recall that $\omega = \gamma_4^2$. Thus, for $d = 4$, we use that $\alpha^2 > \omega$ and the definition of γ_4 to obtain

$$\alpha > \omega^{1/2} = \gamma_4 = 1 + \frac{1}{2^3\gamma_4^2} = 1 + \frac{1}{2^{d-1}\omega},$$

and again the theorem follows. Thus, Theorem 1.4 holds for all d.

3. Proof of Theorem 1.2

In what follows, let $P(x) = P_n(x) = f(x)x^n + g(x)$, where $f(x)$ and $g(x)$ are as in the statement of Theorem 1.2. We suppose, as we may, that $n > \deg g$. In particular, this implies $m_1 = \|P\|$. We make use of the following two preliminary results found in [6, Lemma 1 and Lemma 3].

Lemma 3.1. *Suppose $h(x)$ is irreducible and has a root with absolute value < 1. If $h(x) \mid P(x)$ and $h(x) \nmid g(x)$, then*

$$n \leq C(\deg g + 2\deg h)$$

where $C = \log m_1 / \log(M(h)/|h(0)|)$.

Lemma 3.2. *Suppose the roots of $h(x)$ are distinct and all have absolute value ≥ 1. Suppose further that no root of $h(x)$ is a root of unity. Let $d = \deg h$. If $h(x) \mid P(x)$ and $h(x) \nmid g(x)$, then*

$$n \leq 2^d d^{d^2+d} m_1^{2d} \|h\|^{2d^2-2d} + \deg g.$$

Note that any irreducible reciprocal divisor of $P(x)$ must divide the reciprocal of $P(x)$, which is

$$\tilde{g}(x)x^{n+\deg f-\deg g} + \tilde{f}(x).$$

Hence, any irreducible reciprocal divisor of $P(x)$ divides

$$\begin{aligned} A(x) &= (\tilde{g}(x)x^{n+\deg f-\deg g} + \tilde{f}(x))f(x)x^{\deg g} - (f(x)x^n + g(x))\tilde{g}(x)x^{\deg f} \\ &= f(x)\tilde{f}(x)x^{\deg g} - g(x)\tilde{g}(x)x^{\deg f}. \end{aligned}$$

The conditions $f(0) \neq 0$, $g(0) \neq 0$, $g(x) \neq \pm\tilde{f}(x)$ and $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$ imply that $A(x) \neq 0$. Thus, any irreducible reciprocal factor of $P(x)$ has degree less than or equal to m_2.

Suppose now that $h(x)$ is an irreducible reciprocal non-cyclotomic factor of $P(x)$ with a positive leading coefficient. Note that the condition $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$ implies that the content of $h(x)$ is 1. From the analysis above, $h(x)|A(x)$ so that $\deg h \leq m_2$. Let a denote the leading coefficient of $h(x)$. Since $h(x)$ is reciprocal, the constant term of $h(x)$ is $\pm a$. Since $h(x)$ divides $P(x)$, we deduce that a divides the leading coefficient and the constant term of $P(x)$. Since $\tilde{f}(0)$ is the leading coefficient of $f(x)$ and $g(0)$ is the constant term of $g(x)$, we deduce $a|\tilde{f}(0)$ and $a|g(0)$. Thus, $a \leq b = \gcd\big(\tilde{f}(0), g(0)\big)$. We also note that since $g(0) \neq 0$ and $\gcd(f(x), g(x)) = 1$, we have that $h(x) \nmid g(x)$.

We first consider the case that $h(x)$ has a root off the unit circle. Since $h(x)$ is reciprocal, it must then have a root with absolute value > 1, a root with absolute value < 1, and a leading coefficient equal to $\pm h(0)$. Setting $d = \deg h$ and denoting the roots of $h(x)$ by $\alpha_1, \dots, \alpha_d$, we see that

$$\frac{M(h)}{|h(0)|} = \prod_{\substack{1\leq j\leq d \\ |\alpha_j|>1}} |\alpha_j| \geq \max_{1\leq j\leq d}\{|\alpha_j|\}.$$

Thus, Lemma 3.1 implies

$$n \leq C(\deg g + 2d),$$

where

$$C = \frac{\log m_1}{\log(M(h)/|h(0)|)} \leq \frac{\log m_1}{\log\big(\max_{1\leq j\leq d}\{|\alpha_j|\}\big)}.$$

We apply Theorem 1.4 to obtain

$$C \leq \log m_1 \Big/ \log\left(\min\left\{1 + \frac{1}{2^{d-1}\omega}, 1 + \frac{\sqrt{|\Delta(h)|}}{a^{d-1}2^{d-1}(d-1)^{(d-1)/2}\omega}\right\}\right).$$

The graph of $y = \log(1+x)$ lies above $y = (\log 2)x$ for $0 < x < 1$ so that $\log(1+x) \geq (\log 2)x$ for $0 \leq x \leq 1$. Also, $\sqrt{|\Delta(h)|} \geq 1$. Thus, we can deduce from the estimate above that

$$C \leq \frac{\log m_1}{\log 2}\, a^{d-1}2^{d-1}(d-1)^{(d-1)/2}\omega.$$

This establishes that n is at most

$$\frac{\log m_1}{\log 2}(\deg g + 2d)\, a^{d-1}2^{d-1}(d-1)^{(d-1)/2}\omega.$$

In the case that all roots of $h(x)$ are on the unit circle, we make use of an inequality of M. Mignotte [8] to deduce

$$\|h\| \le 2^d \|f(x)x^n + g(x)\| = 2^d m_1.$$

From Lemma 3.2, we obtain

$$\begin{aligned} n &\le 2^d d^{d^2+d} m_1^{2d} \|h\|^{2d^2-2d} + \deg g \\ &\le 2^d d^{d^2+d} m_1^{2d} 2^{2d^3-2d^2} m_1^{2d^2-2d} + \deg g \\ &\le 2^{2d^3-2d^2+d} d^{d^2+d} m_1^{2d^2} + \deg g. \end{aligned}$$

Recalling that $a \le b$ and $d \le m_2$, Theorem 1.2 follows.

Acknowledgment: The authors thank the referee for pointing out the nice application of Theorem 3 in [12] as described in the Appendix.

References

[1] P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith. 18 (1971), 355–369.
[2] E. Bombieri, D. Masser and U. Zannier, *Anomalous subvarieties - structure theorems and applications*, International Mathematics Research Notices, Vol. 2007, Article ID rnm057, 33 pages. doi:10.1093/imrn/rnm057
[3] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401.
[4] Michael Filaseta, *Coverings of the integers associated with an irreducibility theorem of A. Schinzel*, In Number theory for the millennium, II (Urbana, IL, 2000), pp. 1–24, A K Peters, Natick, MA, 2002.
[5] M. Filaseta, K. Ford, and S. Konyagin, *On an irreducibility theorem of A. Schinzel associated with coverings of the integers*, Illinois J. Math. 44 (2000), 633–643.
[6] M. Filaseta and I. Solan, *Norms of factors of polynomials*, Acta Arith. 82 (1997), 243–255.
[7] G. H. Hardy, J. E. Littlewood and G. Pólya, Inequalities, Second Edition, Cambridge Univ. Press, Cambridge, 1952.
[8] M. Mignotte, *Some useful bounds*, in Computer Algebra, Symbolic and Algebraic Computation, B. Buchberger et al. (eds.), Springer, New York, 1982, 259–263.
[9] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, Sém. Théor. Nombres Bordeaux 2 (1990), 119–141.
[10] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. 11 (1965), 1–34.
[11] A. Schinzel, *Reducibility of polynomials and covering systems of congruences*, Acta Arith. 13 (1967), 91–101.
[12] A. Schinzel, *Reducibility of lacunary polynomials, I*, Acta Arith. 16 (1969), 123–159.
[13] A. Schinzel, *Reducibility of lacunary polynomials, XII*, Acta Arith. 90 (1999), 273–289.

[14] A. Schinzel, Polynomials with Special Regard to Reducibility, Encyclopedia of Mathematics and its Applications, 77, Cambridge University Press, 2000.
[15] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. 3 (1971), 169–175.

Appendix A.

Let m_1 and m_2 be as defined in Theorem 1.2. We show here how Theorem 3 of [12] can be used to obtain Corollary 1.3 but with the lower bound $\max\{B_1, B_2\}$ on n replaced by

$$\exp\left(500m_1^4(2m_2)^{2m_1^2+1}\right).$$

In Theorem 3 of [12], set

$$F(x_1, x_2) = f(x_1)x_2 + g(x_1), \quad n_1 = 1 \quad \text{and} \quad n_2 = n.$$

We make use of the notation in [12]; in particular, see how K, L, J and canonical factorizations are defined there. Recall the conditions $f(0) \neq 0$, $g(0) \neq 0$, $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$ and $g(x) \neq \pm\tilde{f}(x)$ in Corollary 1.3. We deduce

$$K\,F(x_1, x_2) = L\,F(x_1, x_2) = F(x_1, x_2).$$

One further checks that, in the notation of [12] (which differs from our own),

$$\|F\| = m_1^2 \quad \text{and} \quad |F|^* \leq m_2.$$

Theorem 3 of [12] now implies that there is an $r \times 2$ integral matrix $N = \left(a_{ij}\right)$ of rank $r \in \{1, 2\}$ and an integral vector $\overrightarrow{v} = \langle v_1, v_r\rangle$, that is

$$\overrightarrow{v} = \begin{cases} \langle v_1\rangle & \text{if } r = 1, \\ \langle v_1, v_2\rangle & \text{if } r = 2, \end{cases}$$

with $\langle 1, n\rangle = \overrightarrow{v} N$ and

$$\max_{i,j}\{|a_{ij}|\} \leq \begin{cases} \exp\left(9 \cdot 2^{m_1^2-4}\right) & \text{if } r = 2, \\ \exp\left(500m_1^4(2m_2)^{2m_1^2+1}\right) & \text{if } r = 1, \end{cases}$$

such that the canonical factorization

$$K\left(f\left(\prod_{j=1}^r y_j^{a_{j1}}\right)\prod_{j=1}^r y_j^{a_{j2}} + g\left(\prod_{j=1}^r y_j^{a_{j1}}\right)\right) \overset{\text{can}}{=} \text{const}\prod_{\sigma=1}^s F_\sigma(y_1, y_r)^{e_\sigma}$$

implies the single variable canonical factorization

$$K\left(f(x)x^n + g(x)\right) \overset{\text{can}}{=} \text{const}\prod_{\sigma=1}^s K\,F_\sigma(x^{v_1}, x^{v_r})^{e_\sigma}.$$

If $r = 1$, then $1 = v_1a_{11}$ and $n = v_1a_{12}$. We deduce in this case that $v_1 = \pm1$ and

$$n = |a_{12}| \leq \exp\left(500m_1^4(2m_2)^{2m_1^2+1}\right).$$

It remains to consider the case that $r = 2$. Let

$$G(y_1, y_2) = f(y_1^{a_{11}} y_2^{a_{21}})\, y_1^{a_{12}} y_2^{a_{22}} + g(y_1^{a_{11}} y_2^{a_{21}}).$$

We show next that $J\,G$ is irreducible unless (i) or (ii) of Theorem 1.1 holds. Suppose that the polynomial $J\,G$ in y_1 and y_2 is reducible in $\mathbb{Q}[y_1, y_2]$. We make the substitution

$$y_1 = x^{v_1} y^{-a_{21}} \quad \text{and} \quad y_2 = x^{v_2} y^{a_{11}}$$

in $G(y_1, y_2)$ to obtain

$$H(x, y) = f(x)\, x^n y^{a_{11}a_{22} - a_{12}a_{21}} + g(x).$$

Observe that $\langle 1, n \rangle = \overrightarrow{v} N$ implies $v_1 a_{11} + v_2 a_{21} = 1$ so that the terms $y_1^k y_2^\ell$ in $G(y_1, y_2)$ correspond to different terms $x^{k'} y^{\ell'}$ in $H(x, y)$ with

$$k' = k v_1 + \ell v_2 \quad \text{and} \quad \ell' = -k a_{21} + \ell a_{11}.$$

Since the definition of J implies $J\,G$ has no non-constant monomial factors, each irreducible factor of $J\,G$ corresponds to a factor of $J\,H$ with at least two terms. In particular, the reducibility of $J\,G$ in $\mathbb{Q}[y_1, y_2]$ implies the reducibility of $J\,H$ in $\mathbb{Q}[x, y]$.

Since the rank of N is $r = 2$, we deduce that $a_{11}a_{22} - a_{12}a_{21} \neq 0$. Since $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$ and $g(0) \neq 0$, we deduce from $J\,H$ being reducible in $\mathbb{Q}[x, y]$ that $J\,H$ is reducible as a polynomial in y over the field $\mathbb{Q}(x)$ of rational functions in x. Recalling also that $f(0) \neq 0$, we deduce from Capelli's theorem (see [14]) that either (i) of Theorem 1.1 holds for some prime p dividing $a_{11}a_{22} - a_{12}a_{21}$ or (ii) of Theorem 1.1 holds and 4 divides $a_{11}a_{22} - a_{12}a_{21}$.

We consider now the case that $r = 2$ and $J\,G$ is irreducible. Hence, $K\,G$ is either irreducible or a constant. The application of Theorem 3 of [12] above implies $K\big(f(x)x^n + g(x)\big)$ is either irreducible or a constant. For

$$n > \exp\left(500 m_1^4 (2m_2)^{2m_1^2+1}\right) > m_2 \geq \deg g,$$

the terms in $f(x)x^n$ and $g(x)$ have different degrees so that the condition $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$ implies that the greatest common divisor of the coefficients of $f(x)x^n + g(x)$ equals 1. We deduce in this case that $K\big(f(x)x^n + g(x)\big)$ is either irreducible or ± 1, giving the desired conclusion.