TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 339, Number 2, October 1993

THE NUMBER OF IRREDUCIBLE FACTORS OF A POLYNOMIAL. I

CHRISTOPHER G. PINNER AND JEFFREY D. VAALER

ABSTRACT. Let $F(x)$ be a polynomial with coefficients in an algebraic number field k. We estimate the number of irreducible cyclotomic factors of F in $k[x]$, the number of irreducible noncyclotomic factors of F, the number of nth roots of unity among the roots of F, and the number of primitive nth roots of unity among the roots of F. All of these quantities are counted with multiplicity and estimated by expressions which depend explicitly on k, on the degree of F and height of F, and (when appropriate) on n. We show by constructing examples that some of our results are essentially sharp.

1. INTRODUCTION

Let k be an algebraic number field and $F(x)$ a polynomial in $k[x]$ with degree $\partial(F)$ and $F(0) \neq 0$. We consider the problem of estimating the number of irreducible factors of F in $k[x]$ in terms of $\partial(F)$ and of the height of F. We write $H(F)$ for the absolute homogeneous height of the vector of coefficients of F and define this precisely in (2.3). In the present paper we count irreducible factors of F with multiplicity. In a later paper of this series we give estimates for the number of distinct irreducible factors, that is, we count irreducible factors without multiplicity. Both of these problems have been studied in the case $k = \mathbb{Q}$ by Schinzel [11, 12] and Dobrowolski [7]. As is clear from their work it is natural to give separate estimates for the number of cyclotomic factors and for the number of noncyclotomic factors.

Let $\Phi_n(x)$ in $\mathbb{Z}[x]$ denote the nth cyclotomic polynomial. We assume that Φ_n factors in $k[x]$ as

$$\Phi_n(x) = \prod_{s=1}^{\delta(k;n)} \Phi_{n,s}(x),$$

where each factor $\Phi_{n,s}$ is monic and irreducible in $k[x]$. If ζ_n is a primitive nth root of unity then each factor $\Phi_{n,s}$ has degree $[k(\zeta_n) : k]$. As $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois we have

$$[k(\zeta_n) : k] = [\mathbb{Q}(\zeta_n) : k \cap \mathbb{Q}(\zeta_n)] = \frac{\varphi(n)}{[k \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}]}. \tag{1.1}$$

It follows that

$$\delta(k; n) = [k \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq [k' : \mathbb{Q}], \tag{1.2}$$

Received by the editors July 18, 1991.
1991 *Mathematics Subject Classification.* Primary 11R09; Secondary 11J25, 11C08.

0002-9947/93 $1.00 + $.25 per page

where $k' \subseteq k$ is the maximum abelian subfield of k. Indeed, $\delta(k'; n) = \delta(k; n)$ since each factor $\Phi_{n,s}(x)$ occurs in $k'[x]$. Next we suppose that $F(x)$ factors into irreducible polynomials in $k[x]$ as

$$F(x) = \left\{ \prod_{n=1}^{\infty} \prod_{s=1}^{\delta(k;n)} \Phi_{n,s}(x)^{e(n,s)} \right\} \left\{ \prod_{i=1}^{I} f_i(x)^{m(i)} \right\}. \tag{1.3}$$

Here $e(n, s) \geq 0$, $m(i) \geq 1$, and $f_i(x)$, $i = 1, 2, \ldots, I$, are distinct, irreducible, noncyclotomic polynomials in $k[x]$. There will be no loss of generality if we assume that F is monic and hence that each f_i is monic and has $\partial(f_i) \geq 1$. Of course $e(n, s) = 0$ for all but finitely many pairs $\{n, s\}$, $1 \leq s \leq \delta(k; n)$. Thus the total number of cyclotomic factors of F counted with multiplicity is $\sum_{n=1}^{\infty} \sum_{s=1}^{\delta(k;n)} e(n, s)$, and the total number of noncyclotomic factors counted with multiplicity is $\sum_{i=1}^{I} m(i)$. Obviously we have the trivial bound

$$\sum_{n=1}^{\infty} \sum_{s=1}^{\delta(k;n)} e(n, s) + \sum_{i=1}^{I} m(i) \leq \partial(F), \tag{1.4}$$

and in general nothing more can be said. However, if $\partial(F)$ is large compared with $\log H(F)$ we may expect to obtain sharper bounds. In this regard it will be convenient to set

$$r = r(F) = \max\left\{ \frac{\partial(F)}{\log \nu(F)}, 3 \right\},$$

where $\nu(F)$ is defined in (2.3). The quantity $\nu(F)$ is technically more convenient for our purposes than the height of F. In fact we have

$$\log H(F) \leq \log \nu(F) \leq 2 \log H(F)$$

so that the two are interchangeable in some of our results. We note, however, that our bounds (1.7) and (1.8) contain constants which require us to use $\nu(F)$. Also, we let ξ_i denote an algebraic number which is a root of f_i.

Our main result is a system of five inequalities which give upper bounds for certain sums containing the multiplicities $e(n, s)$ and $m(i)$. Here and throughout this paper the constants implied by the Vinogradov symbol $\ll$ are absolute and computable constants. In particular they do not depend on the field k. In two of our bounds a nontrivial field constant $c(k)$ occurs. This is defined by

$$\begin{aligned} c(k) &= \lim_{X \to \infty} X^{-1} \sum_{\substack{n=1 \\ [k(\zeta_n) : k] \leq X}}^{\infty} \delta(k; n) \\ &= \left\{ \prod_{\substack{p \\ p \nmid J}} \left(1 + \frac{1}{p(p-1)} \right) \right\} \sum_{l \mid J} \frac{\delta(k; l)^2 \phi(J/l)}{\varphi(l)(J/l)}, \end{aligned} \tag{1.5}$$

where $J = J(k) = \min\{j \geq 1 : k' \subseteq \mathbb{Q}(\zeta_j)\}$. Of course the integer J is finite by the theorem of Kronecker-Weber. In particular we have

$$c(\mathbb{Q}) = \frac{\zeta(2)\zeta(3)}{\zeta(6)}$$

and more generally there is the upper bound

$$c(k) \le \frac{\zeta(2)\zeta(3)}{\zeta(6)} \min\{[k' : \mathbb{Q}]^2,\ \tau(J)[k' : \mathbb{Q}],\ J\}, \tag{1.6}$$

where τ is the divisor function. We prove the identity (1.5) and the estimate (1.6) in Lemma 12.

Theorem 1. *Let $F(x)$ in $k[x]$ satisfy $F(0) \neq 0$ and factor into irreducible polynomials in $k[x]$ as in* (1.3). *Then the multiplicities of the irreducible factors of F satisfy the following five inequalities:*

For every $\varepsilon > 0$ and $r \ge r_0(\varepsilon)$,

$$\sum_{n=1}^{\infty} \delta(k; n)^{-1} \sum_{s=1}^{\delta(k;n)} e(n, s) \le (1+\varepsilon)\partial(F) \left(\frac{c(\mathbb{Q}) \log r}{r}\right)^{1/2}, \tag{1.7}$$

for every $\varepsilon > 0$ and $r \ge r_1(\varepsilon, k)$,

$$\sum_{n=1}^{\infty} \sum_{s=1}^{\delta(k;n)} e(n, s) \le (1+\varepsilon)\partial(F) \left(\frac{c(k) \log r}{r}\right)^{1/2}, \tag{1.8}$$

$$\sum_{i=1}^{I} m(i)[k(\xi_i) : \mathbb{Q}(\xi_i)] \ll \partial(F)[k : \mathbb{Q}] \frac{(\log r)^3}{r(\log\log r)^3}, \tag{1.9}$$

for each positive integer $n \le r$,

$$\sum_{m|n} \sum_{s=1}^{\delta(k;m)} e(m, s)\partial(\Phi_{m,s}) \ll \partial(F) \left(\frac{n}{r}\right)^{1/2}, \tag{1.10}$$

and for each integer n such that $\varphi(n) \le r$,

(1.11)

$$\sum_{s=1}^{\delta(k;n)} e(n, s)\partial(\Phi_{n,s}) \ll \partial(F) \left(\frac{\varphi(n)}{r}\right)^{1/2} \left\{1 + \left(\frac{\log\log 20n}{\log\left(\frac{r \log\log 20n}{\varphi(n)}\right)}\right)^{1/2}\right\}.$$

As will be shown by examples which we give in §4, the bounds (1.7) and (1.8) are essentially sharp. In case $k = \mathbb{Q}$ these bounds coalesce. In this case they were obtained by Schinzel [12, Theorem 2] but with an extra factor of $\log\log r$ on the right-hand side. The constant

$$c(\mathbb{Q})^{1/2} = \left(\frac{\zeta(2)\zeta(3)}{\zeta(6)}\right)^{1/2} = 1.39412\cdots$$

which occurs in (1.7) and (1.8) when $k = \mathbb{Q}$ may not be best possible. However, we will show that it cannot be replaced by a constant smaller than

$$\frac{3(3)^{1/2}}{4} = 1.299038\cdots.$$

More generally, let L be a positive integer, $L \not\equiv 2 \bmod 4$, and set

$$K = \begin{cases} 2L & \text{if } L \equiv 1 \text{ or } L \equiv 3 \bmod 4, \\ L & \text{if } L \equiv 0 \bmod 4. \end{cases} \tag{1.12}$$

If $k = \mathbb{Q}(\zeta_L)$ then $J(\mathbb{Q}(\zeta_L)) = L$ and

$$c(\mathbb{Q}(\zeta_L))^{1/2} = \left\{ \frac{\zeta(2)\zeta(3)L}{\zeta(6)} \prod_{p|L} \left(1 - \frac{1}{p^2}\right) \left(1 + \frac{1}{p(p-1)}\right)^{-1} \right\}^{1/2}. \tag{1.13}$$

In this case we will show that the constant given by (1.13) and occurring in (1.8) cannot be replaced by a constant smaller than

$$\left(\frac{3K}{2}\right)^{1/2} \prod_{p|K} \left(1 - \frac{1}{p^2}\right).$$

It may be of interest to note that the ratio

$$c(\mathbb{Q}(\zeta_L))^{-1/2} \left(\frac{3K}{2}\right)^{1/2} \prod_{p|K} \left(1 - \frac{1}{p^2}\right) = \left\{ \frac{3\zeta(6)}{2\zeta(2)\zeta(3)} \prod_{p|K} \left(1 + \frac{1}{p^3}\right) \right\}^{1/2}$$

$$\geq \left\{ \frac{27\zeta(6)}{16\zeta(2)\zeta(3)} \right\}^{1/2} = 0.9317917\cdots.$$

The inequality (1.9) sharpens a result of Dobrowolski [7, Theorem 2], who also considered the case $k = \mathbb{Q}$. In fact our result simply reflects a more efficient use of Dobrowolski's lower bound for the height of a nonzero algebraic integer which is not a root of unity.

The inequality (1.10) bounds the total number counted with multiplicity of nth roots of unity among the roots of F. In a similar manner (1.11) gives a bound on the number of primitive nth roots of unity among the roots of F. Both of these results follow from slightly stronger but more complicated inequalities which are sharp except for a precise determination of the implied constants. We give further examples in §4 to indicate this. In the case $k = \mathbb{Q}$ Schinzel [12, Theorem 2] has shown that the maximum multiplicity of an irreducible factor is $\ll \partial(F) r^{-1/2}$. Our inequalities (1.9), (1.10) and (1.11) give more precise information and plainly imply Schnizel's bound.

2. Inequalities for polynomials

In this section we develop some of the main tools which we use to establish Theorem 1. At each place v of the number field k we write k_v for the completion of k at v, $\overline{k}_v$ for an algebraic closure of k_v, and Ω_v for the completion of $\overline{k}_v$. As is well known, the field Ω_v is then complete as a metric space and algebraically closed. Also, we introduce two normalized absolute values $|\ |_v$ and $\|\ \|_v$ on Ω_v which are related by

$$|\ |_v = \|\ \|_v^{d_v/d},$$

where $d = [k : \mathbb{Q}]$ and $d_v = [k_v : \mathbb{Q}_v]$ is the local degree. If $v|\infty$ then $\|\ \|_v$ restricted to $\mathbb{Q}$ is the usual Archimedean absolute value. If p is a prime number and $v|p$ then $\|\ \|_v$ restricted to $\mathbb{Q}$ is the usual p-adic absolute value. Let

$$F(x) = \sum_{l=0}^{L} a_l x^l = a_L \prod_{l=1}^{L} (x - \alpha_l) \tag{2.1}$$

be a polynomial in $\Omega_v[x]$ and not identically zero. We define the local Mahler measure of F to be $\mu_v(F)$ where

$$\log \mu_v(F) = \log |a_L|_v + \sum_{l=1}^{L} \log^+ |\alpha_l|_v \,. \tag{2.2}$$

We define the local height of F by

$$H_v(F) = \max_l |a_l|_v \,, \qquad \text{if } v \nmid \infty \,,$$

and

$$H_v(F) = \left\{ \sum_{l=0}^{L} \|a_l\|_v^2 \right\}^{d_v/2d} \,, \qquad \text{if } v|\infty \,.$$

There is a third local measure of F which we require and define by

$$\nu_v(F) = \sup\{|F(z)|_v : z \in \Omega_v \text{ and } |z|_v = 1\} \,.$$

Now suppose that F is given by (2.1) but has its coefficients in k and hence in Ω_v for all places v of k. In this case we define the global Mahler measure $\mu(F)$, the global height $H(F)$, and the global measure $\nu(F)$ by

$$\mu(F) = \prod_v \mu_v(F) \,, \quad H(F) = \prod_v H_v(F) \,, \quad \text{and} \quad \nu(F) = \prod_v \nu_v(F) \,, \tag{2.3}$$

respectively. It can easily be shown that in each of these products only finitely many factors are different from 1. Because of the way we have normalized our absolute values $|\ |_v$ and $\|\ \|_v$, the global quantities μ, H and ν do not depend on the number field k which contains the coefficients of F. Thus we may regard them as positive real valued functions defined on the not identically zero polynomials in $\overline{\mathbb{Q}}[x]$. For completeness we set $\mu(F) = \nu(F) = H(F) = 0$ if F is the zero polynomial.

If F is a monic, irreducible polynomial in $\mathbb{Q}[x]$ then by a result of Kronecker we have $\mu(F) = 1$ if and only if $F(x) = x$ or $F(x)$ is cyclotomic. If F is not x and not cyclotomic then it is known that $\log \mu(F)$ can be bounded away from zero by a positive quantity which depends only on the degree of F. In fact, Dobrowolski [7] has shown that if F is not x and not cyclotomic then

$$\min\left\{1 \,, \left(\frac{\log\log L}{\log L}\right)^3\right\} \ll \log \mu(F) \tag{2.4}$$

where $L = \partial(F)$ is the degree of F. Simpler proofs of (2.4) have been given by Cantor and Straus [5], Rausch [10] and Louboutin [9].

We now give several basic inequalities which relate the local and global functions we have defined on polynomials. It will be useful to define

$$N(F) = \sum_{\substack{l=0 \\ a_l \neq 0}}^{L} 1 \,,$$

so that $N(F)$ is the number of nonzero coefficients of F.

Lemma 2. *Let F be a polynomial in $\Omega_v[x]$ which is not identically zero. If $v \nmid \infty$ then*

$$\mu_v(F) = H_v(F) = \nu_v(F), \tag{2.5}$$

and if $v|\infty$ then

$$\begin{aligned} \log H_v(F) - \frac{d_v}{d}\partial(F)\log 2 \le \log \mu_v(F) \le \log H_v(F) \\ \le \log \nu_v(F) \le \log H_v(F) + \frac{d_v}{2d}\log N(F). \end{aligned} \tag{2.6}$$

Moreover, if F is in $k[x]$ we have

$$\log H(F) \le \log \nu(F) \le 2\log H(F). \tag{2.7}$$

Proof. Let F be given by (2.1) and $v \nmid \infty$. Then $\mu_v(F) = H_v(F)$ by [3, Lemma 2]. The ring $\mathscr{R}_v = \{z \in \Omega_v : |z|_v \le 1\}$ has maximal ideal $\mathscr{M}_v = \{z \in \Omega_v : |z|_v < 1\}$ and the index of $\mathscr{M}_v$ in $\mathscr{R}_v$ is infinite. It follows that there exists z_0 in $\mathscr{R}_v$, $|z_0|_v = 1$, such that

$$\prod_{l=1}^{L} |z_0 - \alpha_l|_v = \prod_{l=1}^{L} \max\{1, |\alpha_l|_v\}.$$

Then we have

$$\mu_v(F) = |F(z_0)|_v \le \sup_{|z|_v=1} |F(z)| = \nu_v(F) \le \max_l |a_l|_v = H_v(F),$$

and (2.5) follows immediately.

If $v|\infty$ then

$$\log H_v(F) - \frac{d_v}{d}\partial(F)\log 2 \le \log \mu_v(F) \le \log H_v(F)$$

as in [3, Theorem 1 and Lemma 2]. Let $\mathscr{U}_v = \{z \in \Omega_v : |z|_v = 1\}$ be the compact group of units in Ω_v and let m_v denote a Haar measure on the Borel subsets of $\mathscr{U}_v$ normalized so that $m_v(\mathscr{U}_v) = 1$. Then by Parseval's formula and Cauchy's inequality,

$$\begin{aligned} H_v(F) &= \left\{ \int_{\mathscr{U}_v} \|F(z)\|_v^2 dm_v(z) \right\}^{d_v/2d} \le \nu_v(F) \\ &= \sup_{|z|_v=1} \left\| \sum_{l=0}^{L} a_l z^l \right\|_v^{d_v/d} \le \left\{ \sum_{l=0}^{L} \|a_l\|_v^2 \right\}^{d_v/2d} N(F)^{d_v/2d}. \end{aligned}$$

This establishes the remaining inequalities in (2.6).

If F is a polynomial in $k[x]$ we have

$$\log H(F) \le \log \nu(F) \le \log H(F) + \tfrac{1}{2}\log N(F)$$

from the local estimates already proved. We now show that

$$\tfrac{1}{2}\log N(F) \le \log H(F) \tag{2.8}$$

and thereby establish (2.7). By the product formula,

$$N(F) = \sum_{l=0}^{L} \left(\prod_v |a_l|_v^2 \right) \le \left\{ \prod_{v \nmid \infty} H_v(F)^2 \right\} \left\{ \sum_{l=0}^{L} \left(\prod_{v|\infty} |a_l|_v^2 \right) \right\}.$$

Since $\sum_{v|\infty} d_v/d = 1$ we may apply Hölder's inequality to obtain

$$\sum_{l=0}^{L}\left(\prod_{v|\infty}|a_l|_v^2\right) \le \prod_{v|\infty}\left(\sum_{l=0}^{L}|a_l|_v^{2d/d_v}\right)^{d_v/d}$$

$$= \prod_{v|\infty}\left(\sum_{l=0}^{L}\|a_l\|_v^2\right)^{d_v/d} = \prod_{v|\infty}H_v(F)^2.$$

Now (2.8) follows by combining these estimates.

Again we suppose that F in $\Omega_v[x]$ has the form (2.1). If $n \ge 0$ is an integer we write

$$D^{(n)} = (n!)^{-1}\left(\frac{d}{dx}\right)^n$$

for the corresponding differential operator and note that

$$\{D^{(n)}F\}(x) = \sum_{l=n}^{L} a_l\binom{l}{n}x^{l-n}.$$

Lemma 3. *Let F be a polynomial in $\Omega_v[x]$. For each nonnegative integer n we have*

$$\nu_v(D^{(n)}F) \le \nu_v(F) \quad \text{if } v \nmid \infty,$$

and

$$\nu_v(D^{(n)}F) \le \binom{L}{n}^{d_v/d}\nu_v(F) \quad \text{if } v|\infty,$$

where $L = \partial(F)$ is the degree of F.

Proof. If $v \nmid \infty$ then

$$\nu_v(D^{(n)}F) = H_v(D^{(n)}F) = \max_{n\le l\le L}\left|a_l\binom{l}{n}\right|_v$$

$$\le \max_{0\le l\le L}|a_l|_v = H_v(F) = \nu_v(F).$$

If $v|\infty$ then by a well-known inequality of Bernstein (see [15, Vol. II, p. 11])

$$\nu_v(D^{(1)}F) \le L^{d_v/d}\nu_v(F). \tag{2.9}$$

The general result now follows easily by an n-fold application of (2.9).

Lemma 4. *Let F be a polynomial in $\Omega_v[x]$, n a nonnegative integer and $\xi \in \Omega_v$. If $v \nmid \infty$ then*

$$|\{D^{(n)}F\}(\xi)|_v \le \nu_v(F)\max\{1, |\xi|_v\}^{L-n}, \tag{2.10}$$

and if $v|\infty$ then

$$|\{D^{(n)}F\}(\xi)|_v \le \nu_v(F)\binom{L}{n}^{d_v/d}\max\{1, |\xi|_v\}^{L-n}, \tag{2.11}$$

where $L = \partial(F)$ is the degree of F.

Proof. It plainly suffices to prove the result for $n = 0$ and then the general case follows from the previous lemma. If $n = 0$ and $v \nmid \infty$ we have

$$|F(\xi)|_v \le \max_{0\le l\le L}|a_l\xi^l|_v \le H_v(F)\max\{1, |\xi|_v\}^L = \nu_v(F)\max\{1, |\xi|_v\}^L.$$

Now suppose that $n = 0$, $v|\infty$ and $|\xi|_v \leq 1$. Then

$$|F(\xi)|_v \leq \sup_{|z|_v \leq 1} |F(z)|_v = \nu_v(F)$$

by the maximum modulus theorem. If $n = 0$, $v|\infty$ and $1 \leq |\xi|_v$ we have

$$|F(\xi)|_v = |\xi|_v^L \left| \sum_{l=0}^{L} a_l (\xi^{-1})^{L-l} \right|_v \leq |\xi|_v^L \left(\sup_{|z|_v=1} \left| \sum_{l=0}^{L} a_l z^{L-l} \right|_v \right),$$

again using the maximum modulus theorem. But

$$\sup_{|z|_v=1} \left| \sum_{l=0}^{L} a_l z^{L-l} \right|_v = \sup_{|z|_v=1} \left| \sum_{l=0}^{L} a_l z^{l} \right|_v = \nu_v(F),$$

which completes the proof of (2.11).

Next we suppose that F and G are not identically zero polynomials in $\Omega_v[x]$, $v \nmid \infty$, with F given by (2.1) and

$$G(x) = b_M \prod_{m=1}^{M} (x - \beta_m), \qquad b_M \neq 0. \tag{2.12}$$

If $\gamma \in \Omega_v$ we set

$$\partial(F, \gamma) = \sum_{\substack{l=1 \\ \alpha_l \neq \gamma}}^{L} 1,$$

and similarly for $\partial(G, \gamma)$. Then we define

$$\mathscr{L}_v(F, G) = \sum_{l=1}^{L} \partial(G, \alpha_l) \log^+ |\alpha_l|_v + \sum_{m=1}^{M} \partial(F, \beta_m) \log^+ |\beta_m|_v$$
$$- \sum_{l=1}^{L} \sum_{\substack{m=1 \\ \beta_m \neq \alpha_l}}^{M} \log |\alpha_l - \beta_m|_v .$$

Obviously $\mathscr{L}_v$ is a symmetric function of its polynomial arguments and

$$\mathscr{L}_v(\gamma F, G) = \mathscr{L}_v(F, G) \tag{2.13}$$

for all $\gamma \neq 0$ in Ω_v. In view of the inequality

$$\log |\alpha_l - \beta_m|_v \leq \log(\max\{|\alpha_l|_v, |\beta_m|_v\}) \leq \log^+ |\alpha_l|_v + \log^+ |\beta_m|_v,$$

we have

$$0 \leq \mathscr{L}_v(F, G). \tag{2.14}$$

Also, the additive identity

$$\mathscr{L}_v(F_1 F_2, G) = \mathscr{L}_v(F_1, G) + \mathscr{L}_v(F_2, G) \tag{2.15}$$

is easily verified.

Lemma 5. *Let F and G be not identically zero polynomials in $\Omega_v[x]$, $v \nmid \infty$. If F and G have no common zeros in Ω_v then*

$$\mathscr{L}_v(F, G) = \partial(G)\log H_v(F) + \partial(F)\log H_v(G) - \log|\operatorname{Res}\{F, G\}|_v, \tag{2.16}$$

where $\operatorname{Res}\{F, G\}$ is the resultant of F and G. If F has no multiple zeros in Ω_v then

$$\mathscr{L}_v(F, F) = (2\partial(F) - 2)\log H_v(F) - \log|\operatorname{Disc}(F)|_v, \tag{2.17}$$

where $\operatorname{Disc}(F)$ is the discriminant of F.

Proof. If F and G are given by (2.1) and (2.12) and have no common zeros then

$$\begin{aligned}\mathscr{L}_v(F,G) &= \partial(G)\left\{\log|a_L|_v + \sum_{l=1}^{L}\log^+|\alpha_l|_v\right\} + \partial(F)\left\{\log|b_M|_v + \sum_{m=1}^{M}\log^+|\beta_m|_v\right\} \\ &\quad - \left\{\partial(G)\log|a_L|_v + \partial(F)\log|b_M|_v + \sum_{l=1}^{L}\sum_{m=1}^{M}\log|\alpha_l - \beta_m|_v\right\} \\ &= \partial(G)\log\mu_v(F) + \partial(F)\log\mu_v(G) - \log|\operatorname{Res}\{F, G\}|_v.\end{aligned}$$

Now (2.16) follows from (2.5).

If F has no multiple zero we derive (2.17) in a similar manner using

$$(2\partial(F) - 2)\log|a_L|_v + \sum_{l=1}^{L}\sum_{\substack{m=1\\ m\neq l}}^{L}\log|\alpha_l - \alpha_m|_v = \log|\operatorname{Disc}(F)|_v.$$

Let F and G be not identically zero polynomials in $k[x]$. Then $\mathscr{L}_v(F, G)$ is defined for all finite places v of k. If we factor F and G into products of irreducible polynomials in $k[x]$ then (2.15) and Lemma 5 imply that $\mathscr{L}_v(F, G) = 0$ for all but finitely many v. We therefore define

$$\mathscr{L}: (k[x]\setminus\{0\}) \times (k[x]\setminus\{0\}) \to [0, \infty)$$

by

$$\mathscr{L}(F, G) = \sum_{v\nmid\infty}\mathscr{L}_v(F, G).$$

It is clear that $\mathscr{L}$ satisfies the three elementary conditions (2.13), (2.14) and (2.15) which already hold for each $\mathscr{L}_v$. If F and G are not identically zero polynomials in $\overline{\mathbb{Q}}[x]$ we may compute $\mathscr{L}(F, G)$ with respect to any number field k containing the coefficients of F and G. Because of the way we have normalized the absolute values $|\ |_v$, the value of $\mathscr{L}(F, G)$ is independent of our choice of k. Thus we may regard $\mathscr{L}$ as a map,

$$\mathscr{L}: (\overline{\mathbb{Q}}[x]\setminus\{0\}) \times (\overline{\mathbb{Q}}[x]\setminus\{0\}) \to [0, \infty).$$

Theorem 6. *Let F and G be not identically zero polynomials in $\overline{\mathbb{Q}}[x]$. If $\sigma \in \mathscr{G}(\overline{\mathbb{Q}}/\mathbb{Q})$ is an automorphism of $\overline{\mathbb{Q}}$ then*

$$\mathscr{L}(F, G) = \mathscr{L}(\sigma^{-1}F, \sigma^{-1}G). \tag{2.18}$$

Proof. Let K be a number field which is a Galois extension of $\mathbb{Q}$, v a finite place of $\mathbb{Q}$, and $V_{K,v}$ the set of places of K which lie over v. Recall that

the Galois group $\mathcal{G}(K/\mathbb{Q})$ acts on $V_{K,v}$ (see [14, §1]). More precisely, if $w \in V_{K,v}$ and $\tau \in \mathcal{G}(K/\mathbb{Q})$ then $\tau w \in V_{K,v}$ is the place determined by the map $\gamma \to \|\tau^{-1}\gamma\|_w$ on K, which is easily seen to be an absolute value. In fact the map $\gamma \to \|\tau^{-1}\gamma\|_w$ is already normalized so that

$$\|\gamma\|_{\tau w} = \|\tau^{-1}\gamma\|_w \tag{2.19}$$

for all $\gamma \in K$. This is so because both sides of (2.19) plainly equal $\|\gamma\|_v$ when γ is restricted to $\mathbb{Q}$. For a Galois extension all local degrees over a fixed place are equal. It follows that $|\gamma_{\tau w}| = |\tau^{-1}\gamma|_w$ for all $\gamma \in K$. In particular, if $\gamma \neq 0$ then

$$\sum_{w \in V_{K,v}} \log|\gamma|_w = \sum_{w \in V_{K,v}} \log|\gamma|_{\tau w} = \sum_{w \in V_{K,v}} \log|\tau^{-1}\gamma|_w, \tag{2.20}$$

and similarly with log replaced by $\log^+$. If we select K so as to contain the coefficients and roots of F and G, if we select $\tau \in \mathcal{G}(K/\mathbb{Q})$ to be the restriction of σ to K, then (2.18) follows easily from (2.20).

The main inequality which we require for $\mathscr{L}$ is the following upper bound.

Theorem 7. *Let F and G be polynomials in $k[x]$ having positive degree. Suppose that G is irreducible and that $G^e \| F$, that is, $e \geq 0$ is an integer and is the highest power of G which divides F. Then*

$$\mathscr{L}(F, G) \leq (\partial(F) - e)\log\mu(G) + \partial(G)\log\nu(F) + \partial(G)\log\binom{\partial(F)}{e}. \tag{2.21}$$

Proof. We may assume without loss of generality that F and G are monic. Let K be a finite extension of k in which F and G split completely as in (2.1) and (2.12), respectively. For each fixed integer m, $1 \leq m \leq M$, we may write F as

$$F(x) = (x - \beta_m)^e \prod_{l=1}^{L-e} (x - \gamma_{l,m}),$$

where $\beta_m \neq \gamma_{l,m}$ for $l = 1, 2, \ldots, L - e$. It follows that

$$(D^{(e)}F)(\beta_m) = \prod_{l=1}^{L-e} (\beta_m - \gamma_{l,m}).$$

By our previous remarks we may compute $\mathscr{L}$ using places w of K. Then applying the product formula in K we have

(2.22)

$$\begin{aligned}
&\mathscr{L}(F, (x - \beta_m)) \\
&\quad = \sum_{w \nmid \infty} \left\{ \sum_{l=1}^{L-e} \log^+|\gamma_{l,m}|_w + (L - e)\log^+|\beta_m|_w - \sum_{l=1}^{L-e} \log|\gamma_{l,m} - \beta_m|_w \right\} \\
&\quad = \sum_{w \nmid \infty} \left\{ \sum_{l=1}^{L-e} \log^+|\gamma_{l,m}|_w + (L - e)\log^+|\beta_m|_w \right\} + \sum_{w \mid \infty} \log|(D^{(e)}F)(\beta_m)|_w .
\end{aligned}$$

It is trivial that

$$\sum_{w \nmid \infty} \sum_{l=1}^{L-e} \log^+|\gamma_{l,m}|_w \leq \sum_{w \nmid \infty} \log\mu_w(F) = \sum_{w \nmid \infty} \log\nu_w(F). \tag{2.23}$$

Applying (2.11) we find that

$$\sum_{w|\infty} \log |(D^{(e)}F)(\beta_m)|_w$$

$$\leq \sum_{w|\infty} \log \nu_w(F) + \sum_{w|\infty} (L-e) \log^+ |\beta_m|_w + \log \binom{L}{e}. \tag{2.24}$$

Combining (2.22), (2.23) and (2.24), we conclude that

$$\mathscr{L}(F, (x-\beta_m)) \leq (L-e) \sum_{w} \log^+ |\beta_m|_w + \log \nu(F) + \log \binom{L}{e}. \tag{2.25}$$

Finally, we sum both sides of (2.25) over $1 \leq m \leq M$ to obtain the inequality (2.21).

Lemma 8. *Let Φ_n denote the nth cyclotomic polynomial. If $1 \leq m < n$ then*

$$\mathscr{L}(\Phi_m, \Phi_n) = \begin{cases} \varphi(m)\Lambda(n/m) & \text{if } m|n, \\ 0 & \text{if } m \nmid n, \end{cases} \tag{2.26}$$

where Λ is von Mangoldt's function. For $m = n$ we have

$$\mathscr{L}(\Phi_n, \Phi_n) = \varphi(n) \log n - \sum_{l|n} \varphi(n/l)\Lambda(l). \tag{2.27}$$

Proof. Using (2.16), (2.17) and the product formula in $\mathbb{Q}$ we find that

$$\mathscr{L}(\Phi_m, \Phi_n) = \log |\operatorname{Res}\{\Phi_m, \Phi_n\}|_\infty \tag{2.28}$$

if $1 \leq m < n$, and

$$\mathscr{L}(\Phi_n, \Phi_n) = \log |\operatorname{Disc}\{\Phi_n\}|_\infty. \tag{2.29}$$

Here $|\ |_\infty$ in (2.28) and (2.29) is the usual Archimedean absolute value on $\mathbb{Q}$. Explicit formulas for the resultant and discriminant of cyclotomic polynomials were derived by E. T. Lehmer [8] and, more simply, by T. Apostol [1]. These formulas lead immediately to the identities (2.26) and (2.27) in the statement of the theorem.

We are now in position to prove some basic inequalities for the multiplicities of the irreducible cyclotomic factors of a polynomial. If $F(x)$ factors as in (1.3) we write

$$a(n) = \delta(k; n)^{-1} \sum_{s=1}^{\delta(k;n)} e(n, s) \tag{2.30}$$

for the average multiplicity of the cyclotomic factors $\Phi_{n,s}$, $1 \leq s \leq \delta(k; n)$.

Theorem 9. *Let $F(x)$ in $k[x]$ satisfy $F(0) \neq 0$ and factor into irreducible polynomials in $k[x]$ as in (1.3). Then for each positive integer n we have*

$$\sum_{m|n} a(m)\varphi(m)\Lambda(n/m)$$

$$+ a(n) \sum_{m|n} \{\varphi(n) - \varphi(n/m)\}\Lambda(m) + \varphi(n) \sum_{l=1}^{\infty} a(ln)\Lambda(l) \tag{2.31}$$

$$\leq \varphi(n) \log \nu(F) + \varphi(n)\delta(k; n)^{-1} \sum_{s=1}^{\delta(k;n)}{}' e(n, s) \log \left(\frac{3\partial(F)}{e(n, s)} \right),$$

where $\sum_{s=1}^{\prime\delta(k;n)}$ *indicates a sum in which terms with* $e(n, s) = 0$ *are omitted.*

Proof. From Theorem 6 it is clear that $\mathscr{L}(\Phi_{m,s}, \Phi_n)$ is constant for $1 \le s \le \delta(k; m)$. In particular

$$\mathscr{L}(\Phi_m, \Phi_n) = \delta(k; m)\mathscr{L}(\Phi_{m,s}, \Phi_n)$$

for each s, $1 \le s \le \delta(k; m)$. Using the additivity and nonnegativity of $\mathscr{L}$ we obtain the lower bound

$$\begin{aligned}\mathscr{L}(F, \Phi_n) &= \sum_{m=1}^{\infty} \sum_{s=1}^{\delta(k;m)} e(m, s)\mathscr{L}(\Phi_{m,s}, \Phi_n) + \sum_{i=1}^{I} m(i)\mathscr{L}(f_i, \Phi_n) \\ &\ge \sum_{m=1}^{\infty} a(m)\mathscr{L}(\Phi_m, \Phi_n).\end{aligned}$$

Using the identities (2.26) and (2.27) we find that $\mathscr{L}(F, \Phi_n)$ is bounded from below by exactly the expression on the left-hand side of (2.31).

Next we apply Theorem 7 to establish an upper bound for $\mathscr{L}(F, \Phi_n)$. Since $\log \mu(\Phi_{n,s}) = 0$ we have

$$\begin{aligned}\mathscr{L}(F, \Phi_n) &= \sum_{s=1}^{\delta(k;n)} \mathscr{L}(F, \Phi_{n,s}) \\ &\le \sum_{s=1}^{\delta(k;n)} \left\{ \partial(\Phi_{n,s}) \log \nu(F) + \partial(\Phi_{n,s}) \log \binom{\partial(F)}{e(n, s)} \right\} \\ &= \varphi(n) \log \nu(F) + \varphi(n)\delta(k; n)^{-1} \sum_{s=1}^{\delta(k;n)} \log \binom{\partial(F)}{e(n, s)}.\end{aligned}$$

Finally, for $e(n, s) \ge 1$ we use the inequality

$$\log \binom{\partial(F)}{e(n, s)} \le e(n, s) \log \left(\frac{3\partial(F)}{e(n, s)} \right)$$

for binomial coefficients (see [4]). The result follows by comparing the lower bound and upper bound for $\mathscr{L}(F, \Phi_n)$.

Next we derive an inequality which will be used in our proof of (1.10). If $n \ge 1$ is an integer and p is a prime number we set

$$T(n, p) = \{np/m : m|n \text{ and } p \nmid m\}.$$

Theorem 10. *Let* F *be as in Theorem* 9 *and let* p *be a prime number. Then for each positive integer* n *we have*

$$(2.32) \quad (\log p) \sum_{m|n} a(m)\varphi(m) \le np \log \nu(F) + \sum_{t \in T(n,p)}{}' a(t)\varphi(t) \log \left(\frac{6\partial(F)}{npa(t)} \right),$$

where $\sum'_{t \in T(n,p)}$ *indicates a sum in which terms with* $a(t) = 0$ *are omitted.*

Proof. Let $b(n)$ be the expression on the left-hand side of (2.31). For each positive integer t we have

$$\begin{aligned}\sum_{u|t} b(u) &= \sum_{u|t} a(u)\varphi(u) \sum_{m|\frac{t}{u}} \Lambda(m) + \sum_{u|t} a(u)\varphi(u)\log u \\ &\quad + \sum_{l=1}^{\infty} \sum_{u|t} a(lu)\varphi(u)\Lambda(l) - \sum_{l=1}^{\infty} \sum_{\substack{m=1 \\ lm|t}}^{\infty} a(lm)\varphi(m)\Lambda(l) \\ &= (\log t) \sum_{u|t} a(u)\varphi(u) + \sum_{l=1}^{\infty} \sum_{\substack{u|t \\ lu\nmid t}} a(lu)\varphi(u)\Lambda(l).\end{aligned} \tag{2.33}$$

It follows that

$$\begin{aligned}\sum_{t\in T(n,p)} b(t) &= \sum_{u|np} b(u) - \sum_{u|n} b(u) \\ &= (\log np) \sum_{u|np} a(u)\varphi(u) - (\log n) \sum_{u|n} a(u)\varphi(u) \\ &\quad + \sum_{l=1}^{\infty} \sum_{\substack{u|np \\ lu\nmid np}} a(lu)\varphi(u)\Lambda(l) - \sum_{l=1}^{\infty} \sum_{\substack{u|n \\ lu\nmid n}} a(lu)\varphi(u)\Lambda(l) \\ &= (\log np) \sum_{t\in T(n,p)} a(t)\varphi(t) + (\log p) \sum_{m|n} a(m)\varphi(m) \\ &\quad + \sum_{l=1}^{\infty} \sum_{\substack{u|np \\ u\nmid n,\, lu\nmid np}} a(lu)\varphi(u)\Lambda(l) - \sum_{l=1}^{\infty} \sum_{\substack{u|n \\ lu\nmid n,\, lu|np}} a(lu)\varphi(u)\Lambda(l).\end{aligned} \tag{2.34}$$

In order to obtain a lower bound for this expression we discard the third sum on the right of (2.34) and note that the fourth sum is

$$\begin{aligned}-\sum_{l=1}^{\infty} \sum_{\substack{u|n \\ lu\nmid n,\, lu|np}} a(lu)\varphi(u)\Lambda(l) &= -\sum_{t\in T(n,p)} a(t) \sum_{\substack{l|t \\ p|l}} \varphi(t/l)\Lambda(l) \\ &= -(\log p) \sum_{t\in T(n,p)} a(t) \sum_{\substack{p^{\alpha}|t \\ 1\le\alpha}} \varphi(t/p^{\alpha}) \\ &= -\left(\frac{\log p}{p-1}\right) \sum_{t\in T(n,p)} a(t)\varphi(t) \\ &\ge -(\log 2) \sum_{t\in T(n,p)} a(t)\varphi(t).\end{aligned} \tag{2.35}$$

Thus we have

$$\sum_{t\in T(n,p)} b(t) \ge \left(\log\left(\frac{np}{2}\right)\right) \sum_{t\in T(n,p)} a(t)\varphi(t) + (\log p) \sum_{m|n} a(m)\varphi(m) \tag{2.36}$$

by combining (2.34) and (2.35). For an upper bound we use (2.31), the concavity of the logarithm and the simple identity

$$\sum_{t\in T(n,p)} \varphi(t) = n\varphi(p).$$

In this way we find that

$$\sum_{t\in T(n,p)} b(t) \le n\varphi(p)\log\nu(F) + \sum_{t\in T(n,p)}{}' a(t)\varphi(t)\log\left(\frac{3\partial(F)}{a(t)}\right). \tag{2.37}$$

Now the lower bound (2.36) and the upper bound (2.37) may be taken together to establish the inequality (2.32) in the statement of the theorem.

Our proof of (1.11) requires a simple variation of Theorem 10. Here it will be convenient to define $\rho(n)$ for $n \ge 1$ by

$$\rho(n) = \exp\left\{\sum_{p|n} \frac{\log p}{p-1}\right\}$$

so that

$$\sum_{m|n} \varphi(n/m)\Lambda(m) = \varphi(n)\log\rho(n).$$

Theorem 11. *Let F be as in Theorem 9 and let p be a prime number. Then for each positive integer n we have*

$$(\log p)a(n)\varphi(n) \le \varphi(n)p\log\nu(F) + a(np)\varphi(np)\log\left\{\frac{3\rho(np)\partial(F)}{npa(np)}\right\}, \tag{2.38}$$

where the second term on the right of (2.38) *is omitted if $a(np) = 0$.*

Proof. As before let $b(n)$ denote the expression on the left of (2.31). By discarding obviously nonnegative terms we obtain

$$b(np) \ge a(n)\varphi(n)(\log p) + a(np)\varphi(np)(\log np) - a(np)\varphi(np)\log\rho(np). \tag{2.39}$$

If $a(np) = 0$ the result is now clear. Otherwise we use the concavity of the logarithm to conclude that

$$b(np) \le \varphi(np)\log\nu(F) + a(np)\varphi(np)\log\left\{\frac{3\partial(F)}{a(np)}\right\}. \tag{2.40}$$

The inequality plainly follows from (2.39) and (2.40).

Next we establish (1.5), (1.6) and a related identity.

Lemma 12. *Let $k' \subseteq k$ be the maximum abelian subfield of k and define $J = J(k)$ by*

$$J(k) = \min\{j \ge 1 : k' \subseteq \mathbb{Q}(\zeta_j)\}.$$

Then we have

$$\lim_{X\to\infty} X^{-1} \sum_{\substack{n=1\\ [k(\zeta_n):k]\le X}}^{\infty} \delta(k;n) = \left\{\prod_{\substack{p\\ p\nmid J}} \left(1 + \frac{1}{p(p-1)}\right)\right\} \sum_{l|J} \frac{\delta(k;l)^2\varphi(\frac{J}{l})}{\varphi(l)(\frac{J}{l})}. \tag{2.41}$$

Moreover, if $c(k)$ *is the value of the limit in* (2.41) *then*

$$\lim_{X\to\infty} X^{-2} \sum_{\substack{n=1 \\ [k(\zeta_n):k]\le X}}^{\infty} \varphi(n) = \frac{1}{2}c(k) \tag{2.42}$$

and

$$c(k) \le \frac{\zeta(2)\zeta(3)}{\zeta(6)} \min\{[k':\mathbb{Q}]^2, \tau(J)[k':\mathbb{Q}], J\}, \tag{2.43}$$

where τ *is the divisor function.*

Proof. We begin by determining the asymptotic behavior of sums of the form

$$\mathscr{U}(X; J, m) = \sum_{\substack{n=1 \\ \varphi(n)\le X \\ (n,J)=m}}^{\infty} 1, \qquad m|J.$$

Following a method of Bateman [2] we write

$$\mathscr{U}(X; J, m) = \sum_{n\le X} u(n; J, m),$$

where

$$u(n; J, m) = \sum_{\substack{l=1 \\ \varphi(l)=n \\ (l,J)=m}}^{\infty} 1,$$

and consider the Dirichlet series

$$\begin{aligned}\sum_{n=1}^{\infty} u(n; J, m)n^{-s} &= \left\{\prod_{p\nmid J}(1+\varphi(p)^{-s}+\varphi(p^2)^{-s}+\cdots)\right\} \\ &\quad\cdot\left\{\prod_{\substack{p^\alpha\| J \\ p^\beta\| m \\ \beta<\alpha}}\varphi(p^\beta)^{-s}\right\}\left\{\prod_{\substack{p^\beta\| J \\ p^\beta\| m}}(\varphi(p^\beta)^{-s}+\varphi(p^{\beta+1})^{-s}+\cdots)\right\} \\ &= \left\{\prod_{p\nmid J}(1+(p-1)^{-s}(1-p^{-s})^{-1})\right\}\varphi(m)^{-s}\left\{\prod_{\substack{p|J \\ p\nmid \frac{J}{m}}}(1-p^{-s})^{-1}\right\} \\ &= \zeta(s)\left\{\prod_{p\nmid J}(1-p^{-s}+(p-1)^{-s})\right\}\varphi(m)^{-s}\left\{\prod_{p|\frac{J}{m}}(1-p^{-s})\right\} \\ &= \zeta(s)g(s; J, m).\end{aligned} \tag{2.44}$$

Writing $s = \sigma + it$ we find that

$$|(p-1)^{-s} - p^{-s}| = \left|s\int_{p-1}^{p} x^{-s-1}\,dx\right| \le |s|(p-1)^{-\sigma-1}. \tag{2.45}$$

It follows in a standard manner using (2.45) that $g(s; J, m)$ is an analytic function of s in the half plane $0 < \sigma$. Applying the Weiner-Ikehara theorem (see [6]) to (2.44) we conclude that

(2.46)
$$\lim_{x\to\infty} X^{-1}\mathscr{Z}(X; J, m) = g(1; J, m) = \left\{\prod_{p\nmid J}\left(1+\frac{1}{p(p-1)}\right)\right\}\frac{\varphi(J/m)}{\varphi(m)(J/m)}.$$

Since $\delta(k; n) = \delta(k'; n)$ and $k' \subseteq \mathbb{Q}(\zeta_J)$ we have $\delta(k; n) = \delta(k; (n, J))$ and similarly $[k(\zeta_n) : k] = \varphi(n)/\delta(k; (n, J))$. This allows us to write

(2.47)
$$\begin{aligned} X^{-1}\sum_{\substack{n=1\\ [k(\zeta_n):k]\le X}}^{\infty}\delta(k; n) &= X^{-1}\sum_{m\mid J}\delta(k; m)\sum_{\substack{n=1\\ \varphi(n)\le\delta(k;m)X\\ (n,J)=m}}^{\infty} 1 \\ &= \sum_{m\mid J}\delta(k; m)^2\left\{\frac{\mathscr{Z}(\delta(k; m)X; J, m)}{\delta(k; m)X}\right\}. \end{aligned}$$

Now (2.41) follows from (2.46) and (2.47).

Let

$$b(k; m) = \sum_{\substack{n=1\\ [k(\zeta_n):k]=m}}^{\infty}\delta(k; n)$$

and observe that

(2.48)
$$\sum_{\substack{n=1\\ [k(\zeta_n):k]\le X}}^{\infty}\varphi(n) = \sum_{\substack{n=1\\ [k(\zeta_n):k]\le X}}^{\infty}\delta(k; n)[k(\zeta_n) : k] = \sum_{m\le X} mb(k; m).$$

By (2.41) we have

(2.49)
$$\lim_{X\to\infty} X^{-1}\sum_{m\le X} b(k; m) = c(k),$$

and (2.42) follows easily from (2.48) and (2.49).

We now prove the inequality (2.43). From (1.2) we have the simple bound

$$\delta(k; n) \le \min\{[k' : \mathbb{Q}], \varphi(n)\}.$$

Using (2.41) and $\delta(k; n)^2 \le [k' : \mathbb{Q}]^2$ we obtain

(2.50)
$$\begin{aligned} c(k) &\le \left\{\prod_{p\nmid J}\left(1+\frac{1}{p(p-1)}\right)\right\}[k' : \mathbb{Q}]^2\sum_{m\mid J}\frac{\varphi(J/m)}{\varphi(m)(J/m)} \\ &= \left\{\prod_{p}\left(1+\frac{1}{p(p-1)}\right)\right\}[k' : \mathbb{Q}]^2 \\ &= \frac{\zeta(2)\zeta(3)}{\zeta(6)}[k' : \mathbb{Q}]^2. \end{aligned}$$

Alternatively using

$$\delta(k\,;\,n)^2 \le [k' : \mathbb{Q}]\varphi(n)$$

we find

$$\begin{aligned} c(k) &\le \left\{\prod_{p\nmid J}\left(1+\frac{1}{p(p-1)}\right)\right\}[k' : \mathbb{Q}]\sum_{m|J}\frac{\varphi(J/m)}{(J/m)} \\ &\le \frac{\zeta(2)\zeta(3)}{\zeta(6)}[k' : \mathbb{Q}]\tau(J)\,. \end{aligned} \tag{2.51}$$

Finally we use $\delta(k\,;\,n)^2 \le \varphi(n)^2$ and deduce that

$$\begin{aligned} c(k) &\le \left\{\prod_{p\nmid J}\left(1+\frac{1}{p(p-1)}\right)\right\}\sum_{m|J}\frac{\varphi(m)\varphi(J/m)}{(J/m)} \\ &\le \frac{\zeta(2)\zeta(3)}{\zeta(6)}\sum_{m|J}\varphi(m) = \frac{\zeta(2)\zeta(3)}{\zeta(6)}J\,. \end{aligned} \tag{2.52}$$

The estimates (2.50), (2.51) and (2.52) may be combined to establish (2.43).

3. Proof of Theorem 1

To begin with we prove (1.8) and now it will be convenient to write (2.31) as

$$\begin{aligned} &\sum_{m|n}a(m)\varphi(m)\Lambda(n/m) - a(n)\varphi(n)\log\rho(n) + \varphi(n)\sum_{l=1}^{\infty}a(ln)\Lambda(l) \\ &\qquad \le \varphi(n)\log\nu(F) + \varphi(n)\delta(k\,;\,n)^{-1}\sum_{s=1}^{\delta(k\,;\,n)}{}'\, e(n\,,\,s)\log\left(\frac{3\partial(F)}{ne(n\,,\,s)}\right). \end{aligned} \tag{3.1}$$

We sum both sides of inequality (3.1) over the set of positive integers n such that $[k(\zeta_n) : k] \le X$ where X is a sufficiently large positive parameter. In making our estimates we employ the elementary inequalities

$$[k(\zeta_m) : k] \le [k(\zeta_{lm}) : k] \le l[k(\zeta_m) : k]\,.$$

We also assume that $0 < \varepsilon \le \frac{1}{2}$ and then by the prime number theorem there exists $Y = Y(\varepsilon) \ge 2$ so that

$$\psi(X) = \sum_{n\le X}\Lambda(n) \ge (1 - \tfrac{1}{6}\varepsilon)X$$

whenever $X \geq Y$. The first sum on the left of (3.1) contributes

(3.2)
$$\begin{aligned}\sum_{\substack{n=1\\ [k(\zeta_n):k]\leq X}}^{\infty} \sum_{m|n} a(m)\varphi(m)\Lambda(n/m) &= \sum_{m=1}^{\infty} a(m)\varphi(m) \sum_{\substack{l=1\\ [k(\zeta_{lm}):k]\leq X}}^{\infty} \Lambda(l)\\ &\geq \sum_{m=1}^{\infty} a(m)\varphi(m)\psi\left(\frac{X}{[k(\zeta_m):k]}\right)\\ &\geq (1-\tfrac{1}{6}\varepsilon)X \sum_{\substack{m=1\\ [k(\zeta_m):k]\leq X/Y}}^{\infty} \frac{a(m)\varphi(m)}{[k(\zeta_m):k]}\\ &= (1-\tfrac{1}{6}\varepsilon)X \sum_{\substack{m=1\\ [k(\zeta_m):k]\leq X/Y}}^{\infty} \sum_{s=1}^{\delta(k;m)} e(m,s).\end{aligned}$$

The remaining terms on the left of (3.1) are

(3.3)
$$\begin{aligned}&\sum_{\substack{n=1\\ [k(\zeta_n):k]\leq X}}^{\infty} \left\{-a(n)\varphi(n)\log\rho(n) + \varphi(n)\sum_{l=1}^{\infty} a(ln)\Lambda(l)\right\}\\ &\quad\geq -\sum_{\substack{n=1\\ [k(\zeta_n):k]\leq X}}^{\infty} a(n)\varphi(n)\log\rho(n)\\ &\qquad + \sum_{\substack{m=1\\ [k(\zeta_m):k]\leq X}}^{\infty} \left\{\sum_{\substack{n=1\\ [k(\zeta_n):k]\leq X}}^{\infty} \sum_{\substack{l=1\\ ln=m}}^{\infty} a(ln)\varphi(n)\Lambda(l)\right\}\\ &\quad= -\sum_{\substack{n=1\\ [k(\zeta_n):k]\leq X}}^{\infty} a(n)\varphi(n)\log\rho(n) + \sum_{\substack{m=1\\ [k(\zeta_m):k]\leq X}}^{\infty} a(m)\sum_{l|m}\varphi(m/l)\Lambda(l)\\ &\quad= 0.\end{aligned}$$

On the right of (3.1) we have

(3.4)
$$\sum_{\substack{n=1\\ [k(\zeta_n):k]\leq X}}^{\infty} \varphi(n)\log\nu(F) \leq \frac{1}{2}\left(1+\frac{1}{3}\varepsilon\right)c(k)X^2\log\nu(F)$$

by (2.42), provided $X \geq X_0(\varepsilon, k)$ is sufficiently large. To estimate the remaining terms on the right of (3.1) we use the trivial bound

$$\sum_{\substack{n=1\\ [k(\zeta_n):k]\leq X}}^{\infty} \varphi(n)\delta(k;n)^{-1} {\sum_{s=1}^{\delta(k;n)}}' e(n,s) \leq \sum_{n=1}^{\infty}\sum_{s=1}^{\delta(k;n)} e(n,s)\partial(\Phi_{n,s}) \leq \partial(F)$$

together with the monotonicity and concavity of the logarithm. It follows that

$$\sum_{\substack{n=1\\ [k(\zeta_n):k]\le X}}^{\infty} \varphi(n)\delta(k;n)^{-1} \sum_{s=1}^{\delta(k;n)}{}' e(n,s)\log\left(\frac{3\partial(F)}{ne(n,s)}\right)$$

$$\le \partial(F)\log\left\{3\sum_{\substack{n=1\\ [k(\zeta_n):k]\le X}}^{\infty}\frac{\varphi(n)}{n}\right\} \tag{3.5}$$

$$\le (1+\tfrac{1}{6}\varepsilon)\partial(F)\log\{c(k)^{1/2}X\},$$

again assuming that $X \ge X_1(\varepsilon, k)$ is sufficiently large. By combining (3.1), (3.2), (3.3), (3.4) and (3.5) we arrive at the bound

$$(1-\tfrac{1}{6}\varepsilon)X \sum_{\substack{n=1\\ [k(\zeta_n):k]\le X/Y}}^{\infty} \sum_{s=1}^{\delta(k;n)} e(n,s) \tag{3.6}$$

$$\le \tfrac{1}{2}(1+\tfrac{1}{3}\varepsilon)c(k)X^2\log\nu(F) + (1+\tfrac{1}{6}\varepsilon)\partial(F)\log\{c(k)^{1/2}X\},$$

provided $X \ge \max\{Y, X_0, X_1\}$. We also have the trivial estimate

$$(1-\tfrac{1}{6}\varepsilon)X \sum_{\substack{n=1\\ X/Y<[k(\zeta_n):k]}}^{\infty} \sum_{s=1}^{\delta(k;n)} e(n,s) \le Y\sum_{n=1}^{\infty}[k(\zeta_n):k]\sum_{s=1}^{\delta(k;n)} e(n,s)$$

$$= Y\sum_{n=1}^{\infty}\sum_{s=1}^{\delta(k;n)} e(n,s)\partial(\Phi_{n,s}) \le Y\partial(F) \le \tfrac{1}{6}\varepsilon\partial(F)\log\{c(k)^{1/2}X\}, \tag{3.7}$$

whenever $X \ge X_2(\varepsilon, k)$. Finally, we add the inequalities (3.6) and (3.7). In this way we find that

$$\sum_{n=1}^{\infty}\sum_{s=1}^{\delta(k;n)} e(n,s) \le \left(1+\frac{2}{3}\varepsilon\right)\left(\frac{1}{2}c(k)X\log\nu(F) + \partial(F)X^{-1}\log\{c(k)^{1/2}X\}\right). \tag{3.8}$$

We choose $X = (r\log r/c(k))^{1/2}$ in (3.8). If $r \ge r_1(\varepsilon, k)$ is sufficiently large the bound (1.8) follows easily.

We now deduce (1.7) from (1.8). Let $\sigma_1, \sigma_2, \ldots, \sigma_M$ be the distinct embeddings of k into $\overline{\mathbb{Q}}$. We have

$$\prod_{m=1}^{M}\sigma_m\Phi_{n,s}(x) = \Phi_n(x)^{M/\delta(k;n)} \tag{3.9}$$

for each pair $\{n, s\}$, $1 \le s \le \delta(k;n)$. If $F(x)$ is given by (1.3) then $G(x) = \prod_{m=1}^{M}\sigma_m F(x)$ is clearly in $\mathbb{Q}[x]$. Using (3.9) we have the factorization

$$G(x) = \left\{\prod_{n=1}^{\infty}\Phi_n(x)^{E(n)}\right\}g(x),$$

where

$$E(n) = M\delta(k;n)^{-1}\sum_{s=1}^{\delta(k;n)} e(n,s)$$

and $g(x)$ in $\mathbb{Q}[x]$ is not divisible by any cyclotomic polynomial. As $\partial(G) = M\partial(F)$ and

$$\nu(G) \leq \prod_{m=1}^{M} \nu(\sigma_m F) = \nu(F)^M,$$

it follows that

$$r(G) = \max\left\{\frac{\partial(G)}{\log \nu(G)}, 3\right\} \geq \max\left\{\frac{\partial(F)}{\log \nu(F)}, 3\right\} = r(F).$$

If $r(F) \geq r_1(\varepsilon, \mathbb{Q})$ we may apply (1.8) to the polynomial $G(x)$ with $k = \mathbb{Q}$. We find that

$$\begin{aligned}\sum_{n=1}^{\infty} M\delta(k; n)^{-1} \sum_{s=1}^{\delta(k;n)} e(n, s) &= \sum_{n=1}^{\infty} E(n) \\ &\leq (1+\varepsilon)\partial(G)\left(\frac{c(\mathbb{Q})\log r(G)}{r(G)}\right)^{1/2} \\ &\leq (1+\varepsilon)M\partial(F)\left(\frac{c(\mathbb{Q})\log r(F)}{r(F)}\right)^{1/2},\end{aligned}$$

which is the inequality (1.7).

Throughout the remainder of this section we assume that

$$r = r(F) = \frac{\partial(F)}{\log \nu(F)} \geq 3,$$

for otherwise the inequalities (1.9), (1.10) and (1.11) follow from the trivial bound (1.4). We now prove (1.9). Let $g_i(x)$ be the monic irreducible polynomial in $\mathbb{Q}[x]$ having a root at ξ_i. We have

$$\frac{\log \mu(g_i)}{\partial(g_i)} = \frac{\log \mu(f_i)}{\partial(f_i)}$$

and

$$\frac{\partial(f_i)}{\partial(g_i)} = \frac{[k(\xi_i) : k]}{[\mathbb{Q}(\xi_i) : \mathbb{Q}]} = \frac{[k(\xi_i) : \mathbb{Q}(\xi_i)]}{[k : \mathbb{Q}]} \tag{3.10}$$

for each $i = 1, 2, \ldots, I$. Also, if $\partial(g_i) \leq r$ then by Dobrowolski's inequality (2.4)

$$\left(\frac{\log\log r}{\log r}\right)^3 \ll \log \mu(g_i).$$

It follows that

$$\sum_{i=1}^{I}\left(\frac{m(i)\partial(f_i)}{\partial(g_i)}\right) \ll \left(\frac{\log r}{\log\log r}\right)^3 \sum_{\substack{i=1\\ \partial(g_i)\le r}}^{I}\left(\frac{m(i)\partial(f_i)\log\mu(g_i)}{\partial(g_i)}\right) + r^{-1}\sum_{\substack{i=1\\ r<\partial(g_i)}}^{I} m(i)\partial(f_i)$$

$$\ll \left(\frac{\log r}{\log\log r}\right)^3 \sum_{i=1}^{I} m(i)\log\mu(f_i) + \partial(F)r^{-1} \tag{3.11}$$

$$= \left(\frac{\log r}{\log\log r}\right)^3 \log\mu(F) + \partial(F)r^{-1}$$

$$\ll \left(\frac{\log r}{\log\log r}\right)^3 \log\nu(F).$$

Now (3.10) and (3.11) taken together establish the desired inequality.

Next we prove (1.10). It will be convenient to set

$$L_n = \partial(F)^{-1}\sum_{p}\sum_{t\in T(n,p)} a(t)\varphi(t). \tag{3.12}$$

If p_1 and p_2 are distinct primes then the sets $T(n, p_1)$ and $T(n, p_2)$ are disjoint. It follows that $L_n \le 1$. We sum (2.32) over primes $p \le X$ where $X \ge 2$ will be selected later. In this way we deduce the inequality

$$\left(\sum_{p\le X}\log p\right)\left(\sum_{m\mid n} a(m)\varphi(m)\right) \le n\left(\sum_{p\le X} p\right)\log\nu(F) + \sum_{p\le X}{\sum_{t\in T(n,p)}}' a(t)\varphi(t)\log\left(\frac{6\partial(F)}{npa(t)}\right). \tag{3.13}$$

If $L_n = 0$ then (1.10) follows trivially from (3.13) upon choosing $X = 2$. Therefore we may proceed under the assumption that $0 < L_n \le 1$. Using the prime number theorem and the concavity and monotonicity of the logarithm in (3.13) we find that

$$X\sum_{m\mid n} a(m)\varphi(m) \ll \frac{nX^2\log\nu(F)}{\log X} + \partial(F)L_n\log\left\{\sum_{p\le X}\sum_{t\in T(n,p)}\frac{\varphi(t)}{npL_n}\right\} \tag{3.14}$$

$$\ll \partial(F)\left\{\left(\frac{n}{r}\right)\left(\frac{X^2}{\log X}\right) + L_n\log\left(\frac{X}{L_n}\right)\right\}.$$

We select $X = (R_n\log R_n)^{1/2}$, where

$$R_n = \max\left\{4,\ L_n\left(\frac{r}{n}\right)\log\left(\frac{r}{n}\right)\right\},$$

and the bound

$$\sum_{m|n} a(m)\varphi(m) \ll \partial(F)\left(\frac{n}{r}\right)\left(\frac{R_n}{\log R_n}\right)^{1/2} \tag{3.15}$$

follows easily. Now the inequality (1.10) in the statement of Theorem 1 is obtained by using (3.15) and $L_n \leq 1$.

Finally we prove (1.11). We set

$$M_n = \partial(F)^{-1}\sum_{p} a(np)\varphi(np) \tag{3.16}$$

and note that $M_n \leq 1$. If $M_n = 0$ the result follows immediately from (2.38) with $p = 2$. Thus we may assume that $0 < M_n \leq 1$. Now we sum both sides of (2.38) over primes $p \leq X$. As before this leads to the bound

$$\begin{aligned} Xa(n)\varphi(n) &\ll \frac{\varphi(n)X^2\log\nu(F)}{\log X} + \partial(F)M_n\log\left\{\sum_{p\leq X}\frac{\varphi(np)\rho(np)}{npM_n}\right\} \\ &\ll \partial(F)\left\{\left(\frac{\varphi(n)}{r}\right)\left(\frac{X^2}{\log X}\right) + M_n\log\left(\frac{\rho(n)X}{M_n}\right)\right\}. \end{aligned}$$

We select $X = (S_n\log S_n)^{1/2}$ where

$$S_n = \max\left\{4,\ M_n\left(\frac{r}{\varphi(n)}\right)\log\left(\frac{\rho(n)r}{\varphi(n)}\right)\right\}.$$

It follows that

$$a(n)\varphi(n) \ll \partial(F)\left(\frac{\varphi(n)}{r}\right)\left(\frac{S_n}{\log S_n}\right)^{1/2}. \tag{3.17}$$

To complete the proof we use $M_n \leq 1$ and the simple bound $\log\rho(n) \ll \log\log 20n$.

4. Examples

In this section we consider the extent to which the inequalities in Theorem 1 are sharp. Plainly an improvement in Dobrowolski's bound (2.4) would lead immediately to a corresponding improvement in (1.9). In fact Schinzel [11] has formulated such an improvement for the restricted class of noncyclotomic factors which are also nonreciprocal by appealing to the well-known inequality of C. J. Smyth [13]. In general, however, the sharpness of (1.9) remains an open problem. We therefore consider only the inequalities in Theorem 1 which bound the multiplicities of cyclotomic factors.

We will make use of the polynomials

$$F_{N,K}(x) = \prod_{n=1}^{N}(x^{nK} - 1)^{N+1-n} \tag{4.1}$$

where $N \geq 2$ and $K \geq 1$. These were also employed by Dobrowolski [7], at least when $K = 1$. We will show that the polynomials $F_{N,K}(x)$ have a large number of irreducible cyclotomic factors and yet $\log\nu(F_{N,K})$ is relatively small. A somewhat related problem concerning polynomials was considered in [4].

Lemma 13. *The polynomials* $F_{N,K}$ *satisfy*

$$\partial(F_{N,K}) = K\binom{N+2}{3} = \frac{1}{6}KN^3 + O(KN^2), \tag{4.2}$$

$$\log \nu(F_{N,K}) = \tfrac{1}{2}(N+1)\log(N+1), \tag{4.3}$$

$$\log H(F_{N,K}) = \tfrac{1}{2}N\log N + O(\log N), \tag{4.4}$$

$$r(F_{N,K}) = \frac{1}{3}\left(\frac{KN^2}{\log N}\right) + O\left(\frac{KN}{\log N}\right). \tag{4.5}$$

Proof. Only (4.3) is nontrivial and in proving it we may clearly suppose that $K = 1$. Since $F_{N,1}$ is monic we have $\nu_p(F_{N,1}) = 1$ at each (finite) prime p. It remains to consider $\nu_\infty(F_{N,1})$.

Let $V(x)$ denote the $(N+1) \times (N+1)$ matrix $V(x) = (x^{mn})$, where $m = 0, 1, 2, \ldots, N$ indexes rows and $n = 0, 1, 2, \ldots, N$ indexes columns. We have

$$\det(V(x)) = \prod_{l=0}^{N-1} \prod_{m=l+1}^{N} (x^m - x^l) = \prod_{l=0}^{N-1} \prod_{n=1}^{N-l} x^l(x^n - 1)$$

$$= \prod_{n=1}^{N} x^{\binom{N+1-n}{2}}(x^n - 1)^{N+1-n} = x^{\binom{N+1}{3}}F_{N,1}(x).$$

By Hadamard's inequality

$$\nu_\infty(F_{N,1}) = \sup_{|x|_\infty = 1} |F_{N,1}(x)|_\infty = \sup_{|x|_\infty = 1} |\det(V(x))|_\infty \leq (N+1)^{\frac{1}{2}(N+1)}.$$

Let $\mathbf{1}_{N+1}$ denote the $(N+1) \times (N+1)$ identity matrix. We find that

$$V(\zeta_{N+1})V(\zeta_{N+1})^* = (N+1)\mathbf{1}_{N+1},$$

where $V(\zeta_{N+1})^*$ is the complex conjugate transpose matrix. As there is equality in Hadamard's inequality in this case, we conclude that

$$\nu_\infty(F_{N,1}) = (N+1)^{\frac{1}{2}(N+1)}.$$

This proves (4.3) and then (4.4) follows using (2.6).

The polynomials $F_{N,K}(x)$ clearly factor in $\mathbb{Q}[x]$ as

$$F_{N,K}(x) = \prod_{n=1}^{N} \left\{ \prod_{m|nK} \Phi_m(x) \right\}^{N+1-n} = \prod_{m=1}^{NK} \Phi_m(x)^{e(m)},$$

where

$$e(m) = \sum_{\substack{n=1 \\ m|nK}}^{N} (N+1-n).$$

Over an arbitrary number field k we have

$$F_{N,K}(x) = \prod_{m=1}^{NK} \prod_{s=1}^{\delta(k;m)} \Phi_{m,s}(x)^{e(m,s)}$$

with $e(m, s) = e(m)$ for $1 \le s \le \delta(k; m)$. Now suppose that $L \not\equiv 2 \bmod 4$, $k = \mathbb{Q}(\zeta_L)$ and therefore $J(\mathbb{Q}(\zeta_L)) = L$. Using (1.2) we find that

$$\delta(\mathbb{Q}(\zeta_L); m) = [\mathbb{Q}(\zeta_{(m,L)}) : \mathbb{Q}] = \varphi((m, L)).$$

It follows that the constant defined by (1.5) is

$$c(\mathbb{Q}(\zeta_L)) = \frac{\zeta(2)\zeta(3)L}{\zeta(6)} \prod_{p|L} \left(1 - \frac{1}{p^2}\right) \left(1 + \frac{1}{p(p-1)}\right)^{-1}.$$

Also, the total number of irreducible cyclotomic factors of $F_{N,K}$ in $\mathbb{Q}(\zeta_L)[x]$ is

$$\sum_{m=1}^{\infty} \sum_{s=1}^{\varphi((m,L))} e(m, s) = \sum_{n=1}^{N} (N + 1 - n) \sum_{m|nK} \varphi((m, L)). \tag{4.6}$$

From (4.2) and (4.5) we deduce that

$$\partial(F_{N,K}) \left(\frac{\log r(F_{N,K})}{r(F_{N,K})}\right)^{1/2} = \left(\frac{K}{6}\right)^{1/2} N^2 \log N + O_K(N^2 \log\log N). \tag{4.7}$$

At this point we select K so as to satisfy (1.12). Then it follows without difficulty that

$$\begin{aligned} &\sum_{n=1}^{N} (N + 1 - n) \sum_{m|nK} \varphi((m, L)) \\ &\quad = \left\{ \frac{K}{2} \prod_{p|K} \left(1 - \frac{1}{p^2}\right) \right\} N^2 \log N + O_K(N^2). \end{aligned} \tag{4.8}$$

Now (4.6), (4.7) and (4.8) imply that the constant $c(\mathbb{Q}(\zeta_L))^{1/2}$ which occurs on the right of (1.8) cannot be replaced by a constant smaller than

$$\left(\frac{3K}{2}\right)^{1/2} \prod_{p|K} \left(1 - \frac{1}{p^2}\right).$$

This verifies our earlier remark concerning the sharpness of (1.8) and also, by taking $L = 1$ and $K = 2$, that of (1.7).

Next we consider our two estimates (1.10) and (1.11) for the number of nth roots of unity and the number of primitive nth roots of unity among the roots of F. In our proof of Theorem 1 these were immediate consequences of the more elaborate bounds

$$\sum_{m|n} a(m)\varphi(m) \ll \partial(F) \left(\frac{n}{r}\right) \left(\frac{R_n}{\log R_n}\right)^{1/2} \tag{4.9}$$

and

$$a(n)\varphi(n) \ll \partial(F) \left(\frac{\varphi(n)}{r}\right) \left(\frac{S_n}{\log S_n}\right)^{1/2}, \tag{4.10}$$

respectively. Here we will show that (4.9) and (4.10) are sharp except for a precise determination of the implied constant. We note, however, that these more

elaborate bounds depend on considerably more information than is contained in $\partial(F)$ and $r(F)$.

Let k be a fixed number field and let $n|K$ with $K/n \ll N/\log N$. The left-hand side of (4.9) is

$$\sum_{m|n}\sum_{s=1}^{\delta(k;m)} e(m,s)\partial(\Phi_{m,s}) = \sum_{l=1}^{N}(N+1-l)\sum_{\substack{m|n\\ m|lK}}\varphi(m) \tag{4.11}$$

$$= \frac{n}{2}(N^2+N).$$

In this case the quantity L_n given by (3.12) is

$$\begin{aligned}
L_n &= \partial(F_{N,K})^{-1}\sum_{p}\sum_{t\in T(n,p)} a(t)\varphi(t)\\
&\ll K^{-1}N^{-3}\sum_{p}\sum_{t\in T(n,p)}\varphi(t)\sum_{\substack{l=1\\ t|lK}}^{N}(N+1-l)\\
&\ll K^{-1}N^{-3}\left\{N^2\sum_{p|\frac{K}{n}}\sum_{t\in T(n,p)}\varphi(t)+\sum_{p\nmid\frac{K}{n}}\sum_{\substack{l=1\\ p|l}}^{N}(N+1-l)\sum_{t\in T(n,p)}\varphi(t)\right\}\\
&\ll K^{-1}N^{-1}\left\{n\sum_{p|\frac{K}{n}}(p-1)\right\}+K^{-1}N^{-1}\sum_{p\le N}\left\{\frac{1}{p}\sum_{t\in T(n,p)}\varphi(t)\right\}\\
&\ll N^{-1}+nK^{-1}N^{-1}\sum_{p\le N}1\\
&\ll nK^{-1}(\log N)^{-1}.
\end{aligned}$$

From Lemma 14 and the definition of R_n we have $R_n \ll N^2(\log N)^{-1}$. Thus our bound (4.9) takes the form

$$\sum_{m|n}\sum_{s=1}^{\delta(k;m)} e(m,s)\partial(\Phi_{m,s}) \ll nN^2,$$

and in view of (4.11) it cannot be substantially improved. The analysis for (4.10) is very similar but now we find that

$$\sum_{s=1}^{\delta(k;n)} e(n,s)\partial(\Phi_{n,s}) = \frac{\varphi(n)}{2}(N^2+N) \tag{4.12}$$

and (using (3.16))

$$M_n \ll \varphi(n)K^{-1}(\log N)^{-1}.$$

This leads to $S_n \ll N^2(\log N)^{-1}$ and finally to

$$\sum_{s=1}^{\delta(k;n)} e(n,s)\partial(\Phi_{n,s}) \ll \varphi(n)N^2. \tag{4.13}$$

Of course (4.12) and (4.13) show that no significant improvement in (4.10) is possible.

REFERENCES

1. T. M. Apostol, *Resultants of cyclotomic polynomials*, Proc. Amer. Math. Soc. **24** (1970), 457–462.
2. P. T. Bateman, *The distribution of values of the Euler function*, Acta Arith. **21** (1972), 329–345.
3. E. Bombieri, *Lectures on the Thue principle*, Analytic Number Theory and Diophantine Problems, Progress in Math., vol. 70, (A. C. Adolphson, J. B. Convey, A. Ghosh, and R. I. Yager, eds.), Birkhäuser, 1987, pp. 15–52.
4. E. Bombieri and J. Vaaler, *Polynomials with low height and prescribed vanishing*, Analytic Number Theory and Diophantine Problems, Progress in Math., vol. 70, (A. C. Adolphson, J. B. Convey, A. Ghosh, and R. I. Yager, eds.), Birkhäuser, 1987, pp. 53–73.
5. D. C. Cantor and E. G. Straus, *On a conjecture of D. H. Lehmer*, Acta Arith. **42** (1982), 97–100, Correction to the paper *On a conjecture of D. H. Lehmer*, Acta Arith. **42** (1983).
6. K. Chandrasekharan, *Introduction to analytic number theory*, Springer-Verlag, 1968.
7. E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401.
8. E. T. Lehmer, *A numerical function applied to cyclotomy*, Bull. Amer. Math. Soc. **36** (1930), 291–298.
9. R. Louboutin, *Sur la mesure de Mahler d'un nombre algébrique*, C. R. Acad. Sci. Paris Sér. I Math. **296** (1983), 707–708.
10. U. Rausch, *On a theorem of Dobrowolski about conjugate numbers*, Colloq. Math. **50** (1985), 137–142.
11. A. Schinzel, *On the number of irreducible factors of a polynomial*, Colloq. Math. Soc. János Bolyai, Debrecen (Hungary), 1974.
12. ———, *On the number of irreducible factors of a polynomial*. II, Ann. Polon. Math. **42** (1983), 309–320.
13. 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.
14. J. T. Tate, *Global class field theory*, Algebraic Number Theory (Proceedings of an instructional conference, University of Sussex, Brighton, U.K.), (J.W.S. Cassels and A. Fröhlich, eds.), Academic Press, 1967.
15. A. Zygmund, *Trigonometric series*, vols. I, II, Cambridge Univ. Press, 1968.

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF TEXAS AT AUSTIN, AUSTIN, TEXAS 78712
E-mail address, C. G. Pinner: pinner@math.utexas.edu
E-mail address, J. D. Vaaler: vaaler@math.utexas.edu