ACTA ARITHMETICA
LXXVIII.2 (1996)

The number of irreducible factors of a polynomial, II

by

Christopher G. Pinner (Vancouver and Burnaby, B.C.) and
Jeffrey D. Vaaler (Austin, Tex.)

1. Introduction. Let k be an algebraic number field and $F(x)$ a polynomial in $k[x]$ with degree $\partial(F)$ and $F(0) \neq 0$. In [5] we considered the problem of estimating the number of irreducible factors of F in $k[x]$ in terms of $\partial(F)$ and of the height $H(F)$ of the vector of coefficients of F. As is already clear from earlier work of Schinzel [6] and Dobrowolski [1], it is natural in problems of this type to give separate estimates for the number of cyclotomic factors and for the number of noncyclotomic factors. In the present paper we estimate the number of irreducible, cyclotomic factors of F in terms of $\partial(F)$ and of the number $N(F)$ of monomials which occur in F. In particular, our bounds do not depend on the coefficients of F and they depend only minimally on $\partial(F)$.

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

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

Here we suppose that 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 noted already in [5], equation (1.2), the number of distinct irreducible factors of Φ_n in $k[x]$ is

$$\delta(k;n) = [k \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq [k' : \mathbb{Q}], \tag{1.1}$$

where $k' \subseteq k$ is the maximum abelian subfield of k. Now suppose that $F(x)$ factors into irreducible cyclotomic polynomials in $k[x]$ as

$$F(x) = \Big\{ \prod_{n=1}^{\infty} \prod_{s=1}^{\delta(k;n)} \Phi_{n,s}(x)^{e(n,s)} \Big\} G(x). \tag{1.2}$$

Here each $e(n,s)$ is a nonnegative integer, $e(n,s) = 0$ for all but finitely

many pairs $\{n,s\}$, $n=1,2,\dots$, $1\le s\le \delta(k;n)$, and G has only noncyclotomic factors. Then the 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 number of distinct cyclotomic factors of F counted without multiplicity is $\sum_{n=1}^{\infty}\sum_{s=1}^{\delta(k;n)} \min\{1,e(n,s)\}$. Let

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

where the integer J is finite by the theorem of Kronecker–Weber, and define

$$C(k)=\sum_{j\mid J}\delta(k;j).$$

THEOREM 1. *Let $F(x)$ in $k[x]$ satisfy $F(0)\neq 0$ and factor in $k[x]$ as in* (1.2). *Then for every $\varepsilon>0$ the multiplicities of the irreducible, cyclotomic factors of F satisfy*

$$\sum_{n=1}^{\infty}\sum_{s=1}^{\delta(k;n)} e(n,s)\ll_{\varepsilon} C(k)\partial(F)^{\varepsilon}N(F)^2, \tag{1.3}$$

and

$$\sum_{n=1}^{\infty}\sum_{s=1}^{\delta(k;n)} \min\{1,e(n,s)\}\ll_{\varepsilon} C(k)\partial(F)^{\varepsilon}N(F). \tag{1.4}$$

Here the constant implied by the Vinogradov symbol $\ll_{\varepsilon}$ depends only on ε and not on k. By a result of Hajós [2] (see also [4], Lemma 2) we have

$$e(n,s)\le \min\{1,e(n,s)\}N(F),$$

and therefore (1.3) follows from (1.4).

It should be noted when counting distinct cyclotomic factors that degree considerations give us a trivial estimate of the form

$$\sum_{n=1}^{\infty}\sum_{s=1}^{\delta(k;n)} \min\{1,e(n,s)\}\ll_{k} \partial(F)^{1/2}.$$

Thus our bounds are primarily of interest when

$$N(F)\ll_{k,\varepsilon}\partial(F)^{1/2-\varepsilon}.$$

We observe that our estimates have only polynomial growth in $N(F)$ as compared to previous bounds where the growth was essentially exponential. Notice that a fusion of Theorem 1 and the trivial bound easily gives

$$\sum_{n=1}^{\infty}\sum_{s=1}^{\delta(k;n)} \min\{1,e(n,s)\}\ll_{k} \partial(F)^{1/2}\left(\frac{\log N(F)}{\log \partial(F)}\right)^{1/2}.$$

This is of course much weaker than Theorem 1 (it follows from any bound with only polynomial growth in $N(F)$). We record it primarily for comparison with an inequality of Schinzel [6] for polynomials in $\mathbb{Q}[x]$:

$$\sum_{n=1}^{\infty} \min\{1, e(n,1)\} \ll \partial(F)^{1/2} \left(\frac{\log H(F)}{\log\log \partial(F)} \right)^{1/2}.$$

Since $\log N(F) \leq 2 \log H(F)$ (as in (2.8) of [5]), our result confirms Schinzel's prediction that the $\log\log \partial(F)$ in his bound could be replaced by $\log \partial(F)$.

To the other part of the prediction, concerning noncyclotomic polynomials we shall return in a later paper.

It would be surprising if our bounds are sharp since, as we shall see in the next section, (1.4) is really a bound on the number of cyclotomic polynomials which occur as factors of some polynomial with given exponents but arbitrary coefficients in k. We conjecture that the bound (1.3) can be improved to

$$\sum_{n=1}^{\infty} \sum_{s=1}^{\delta(k;n)} e(n,s) \ll_{\varepsilon,k} \partial(F)^{\varepsilon} N(F), \tag{1.5}$$

and that the bound (1.4) can be improved to

$$\sum_{n=1}^{\infty} \sum_{s=1}^{\delta(k;n)} \min\{1, e(n,s)\} \ll_{\varepsilon,k} \partial(F)^{\varepsilon} N(F)^{1/2}. \tag{1.6}$$

If these estimates are correct then the exponents on $N(F)$ would be best possible. This can be seen by considering the polynomials $(x^n - 1)^L$ and $\prod_{l=1}^{L}(x^{nl} - 1)$, respectively, for large values of L.

We actually prove a more precise form of Theorem 1 in which the factor $\partial(F)^{\varepsilon}$ is expressed explicitly in terms of the number of divisors of differences of pairs of exponents. The simple example $x^n - x^m$ suggests the appropriateness of such parameters. We give several bounds in which the complexity of this term is contrasted against the degree of dependence on $N(F)$:

THEOREM 2. *Let $F(x)$ in $k[x]$ satisfy $F(0) \neq 0$, factor in $k[x]$ as in* (1.2), *and let*

$$F(x) = \sum_{i=1}^{N(F)} a_i x^{n_i}. \tag{1.7}$$

Then the number of distinct cyclotomic factors

$$\sum_{n=1}^{\infty} \sum_{s=1}^{\delta(k;n)} \min\{1, e(n,s)\} \tag{1.8}$$

can be bounded by the following three quantities:

(i) *For any exponent* n_I, *the expression* (1.8) *is at most*

$$C(k)\Big(\sum_{i=1}^{N(F)}\tau(n_i-n_I)\Big)2^{\pi(N(F))}, \tag{1.9}$$

where $\pi(N(F))$ *denotes the number of primes less than or equal to* $N(F)$, *and* $\tau(n)$ *is the number of positive divisors of* n.

(ii) *Alternatively, the expression* (1.8) *is bounded from above by*

$$C(k)\Big(\sum_{i=1}^{N(F)}\sum_{j<i}\tau(n_i-n_j)\Big) \times\left(0.287+O\left(\frac{1}{\log\log N(F)}\right)\right)N(F)\log N(F). \tag{1.10}$$

(iii) *If* $N(F)\ge 3$ *then, for any pair of distinct exponents* n_I, n_J, *the number of distinct cyclotomic factors* (1.8) *can also be bounded by*

$$C(k)\Big(\sum_{i=1}^{N(F)}\tau((n_I-n_J)^2(n_I-n_i)^2(n_J-n_i)^2)\Big)(\log\log N(F)+O(1)). \tag{1.11}$$

Moreover, the factor $\log\log N(F)$ *may be omitted for any pairs* n_I, n_J *with* a_I/a_J *not a root of unity.*

It is clear that Theorem 1 follows easily from (1.11) and is the most that can be obtained from these bounds when little is known about the exponents.

2. Linear forms in roots of unity. In this section we describe the main technical results of the paper. These extend in various ways the work of H. B. Mann [3] on vanishing sums of roots of unity. Let $L\subseteq M\subseteq\mathbb{Z}$, with $1\le|L|\le|M|<\infty$. For each irreducible cyclotomic polynomial $\Phi_{n,s}(x)$ in $k[x]$ we wish to determine if there exists a vector $(\xi_m)_{m\in M}$ in $k^{|M|}$ such that

$$\sum_{m\in M}\xi_m\zeta_n^m=0 \quad\text{and}\quad \xi_l\ne 0 \text{ for all } l \text{ in } L, \tag{2.1}$$

where $\Phi_{n,s}(\zeta_n)=0$. If $(\xi_m)_{m\in M}$ is a vector in $k^{|M|}$ then it is clear that (2.1) holds for one root of $\Phi_{n,s}(x)$ if and only if (2.1) holds for all roots of $\Phi_{n,s}(x)$. The situation is further clarified by the following result, which we prove in Section 3.

Lemma 3. *Let* $\Phi_{n,s}(x)$ *and* $\Phi_{n,t}(x)$ *be distinct irreducible cyclotomic polynomials in* $k[x]$. *If there exists a vector* $(\xi_m^{(s)})_{m\in M}$ *in* $k^{|M|}$ *such that* (2.1) *is satisfied for each root of* $\Phi_{n,s}$, *then there exists a vector* $(\xi_m^{(t)})_{m\in M}$ *in* $k^{|M|}$ *such that* (2.1) *is satisfied for each root of* $\Phi_{n,t}$.

We define $Z(L;M) \subseteq \{1,2,3,\ldots\}$ to be the set of positive integers n such that there exists a primitive nth root of unity ζ_n and a vector $(\xi_m)_{m\in M}$ in $k^{|M|}$ such that

$$\sum_{m\in M} \xi_m \zeta_n^m = 0 \quad \text{and} \quad \xi_l \neq 0 \text{ for all } l \text{ in } L. \tag{2.2}$$

By Lemma 3 the existence of a vector $(\xi_m)_{m\in M}$ in $k^{|M|}$ which satisfies (2.2) depends on n and not on the choice of ζ_n. It will be convenient to write $Y(M) = Z(M;M)$ and

$$Z(M) = \bigcup_{\substack{L\subseteq M \\ L\neq\emptyset}} Z(L;M).$$

Our objective is to describe $Z(M)$ in terms of M and $Z(L;M)$ in terms of L and M, at least when $|L| = 1$ or $|L| = 2$. Toward this end we define

$$P = P(k,|M|) = \prod_{\substack{p\leq |M| \\ p\nmid J}} p,$$

where the product on the right is over prime numbers p. We will show that if n belongs to $Z(M)$ or to $Z(L;M)$ then n factors as

$$n = (n,J)ab, \qquad a \mid P,$$

where the integers a and b are further restricted by divisibility conditions which may depend on L or M. To begin with we have the following generalization of Mann's result [3] to the number field k.

THEOREM 4. *Suppose that m_1 belongs to M and n belongs to $Z(\{m_1\};M)$. Then there exists an integer m_2 in $M\setminus\{m_1\}$ and a factorization*

$$n = (n,J)ab, \qquad a \mid P, \tag{2.3}$$

such that $b|(m_1 - m_2)$.

By modifying the proof of Theorem 4 we can further restrict the factor a in (2.3) but relax the condition imposed on b.

THEOREM 5. *Suppose that n belongs to $Z(M)$. Then there exist distinct integers m_1 and m_2 in M and a factorization*

$$n = (n,J)ab, \qquad a \mid P, \tag{2.4}$$

such that $a \leq \tau(a)|M|$ and $b \mid (m_1 - m_2)$.

If we assume that n belongs to $Z(\{m_1,m_2\};M)$, we can make more elaborate restrictions on both a and b.

THEOREM 6. *Suppose that* $3 \le |M|$, m_1 *and* m_2 *are distinct elements of* M, *and* n *belongs to* $Z(\{m_1, m_2\}; M)$. *Then there exists a factorization*

$$n = (n, J)ab, \qquad a \mid P, \tag{2.5}$$

for which one of the following holds:

(i) $a \mid b$ *and there exists* m_3 *in* $M \setminus \{m_1, m_2\}$ *with* $b \mid (m_1 - m_2)(m_2 - m_3) \times (m_3 - m_1)$, *or*

(ii) a *has exactly one odd prime divisor* p *and there exist* $p - 2$ *distinct elements* $m_3, m_4, \dots, m_p$ *in* $M \setminus \{m_1, m_2\}$ *such that* $b \mid (m_1 - m_2)(m_2 - m_j) \times (m_j - m_1)$ *for each* $j = 3, 4, \dots, p$.

Moreover, *if* (ii) *holds then* $m_1, m_2, \dots, m_p$ *form a complete set of incongruent residue classes in* $\mathbb{Z}/p\mathbb{Z}$.

Although we have not concerned ourselves here with estimates which depend on the coefficients, it is worth noting that the awkward case (ii) of Theorem 6 does not occur except in the special case where ξ_{m_1}/ξ_{m_2} is a $2(n, J)$th root of unity in the relation (2.2) assumed for ζ_n. We comment further on this in the proof of (1.11).

Next we define

$$S(L; M) = \sum_{n \in Z(L;M)} \delta(k; n) \quad \text{and} \quad S(M) = \sum_{n \in Z(M)} \delta(k; n).$$

In view of Lemma 3, $S(L; M)$ is exactly the number of distinct, irreducible cyclotomic polynomials $\Phi_{n,s}(x)$ in $k[x]$ for which there exists a vector $(\xi_m)_{m \in M}$ in $k^{|M|}$ satisfying the conditions in (2.2). A similar interpretation applies to $S(M)$. Since $\delta(k; n) = \delta(k'; n)$ and $k' \subseteq \mathbb{Q}(\zeta_J)$, it follows (see Lemma 8) that $\delta(k; n) = \delta(k; (n, J))$. Thus the factorizations given in the previous theorems lead to estimates for these sums. Let

$$\partial(M) = \max\{|m_1 - m_2| : m_1 \in M,\ m_2 \in M\}$$

denote the diameter of M.

COROLLARY 7. *Suppose that* m_1 *and* m_2 *are distinct elements of* M. *Then for every* $\varepsilon > 0$ *we have*

$$S(\{m_1, m_2\}; M) \ll_\varepsilon C(k)\partial(M)^\varepsilon |M|, \tag{2.6}$$

and

$$S(M) \ll_\varepsilon C(k)\partial(M)^\varepsilon |M|^{7/3}. \tag{2.7}$$

We note that (2.6) also provides an estimate for $S(\{m_1\}; M)$. For clearly,

$$S(\{m_1\}; M) \le \sum_{\substack{m_2 \in M \\ m_2 \ne m_1}} S(\{m_1, m_2\}; M). \tag{2.8}$$

It is obvious that Corollary 7 implies Theorem 1. For suppose that $F(x)$ in $k[x]$ satisfies $F(0) \neq 0$. Then we can write

$$F(x) = \sum_{m \in M} \xi_m x^m,$$

where $\{0, \partial(F)\} \subseteq M \subseteq \mathbb{Z}$, $\xi_m \neq 0$ for each m in M, $\partial(F) = \partial(M)$, and $N(F) = |M|$. Now (2.6) plainly implies (1.4), and by our previous remarks we get (1.3) as well.

3. Preliminary lemmas. Let $M \subseteq \mathbb{Z}$ be a finite subset, p a prime and $r_1, \dots, r_l$ a collection of residue classes in $\mathbb{Z}/p\mathbb{Z}$. Then we define

$$M(r_1, \dots, r_l; p) = \{m \in M : m \equiv r_i \bmod p \text{ for some } i,\ 1 \leq i \leq l\}.$$

We shall need a simple lemma describing the degrees of various cyclotomic extensions over the number field k.

Lemma 8. *For each prime p and coprime integer m*

$$[k(\zeta_{mp^{i+1}}) : k(\zeta_{mp^i})] = \begin{cases} p-1 & \text{if } p \nmid J \text{ and } i = 0, \\ p & \text{if } p \nmid J \text{ and } i \geq 1, \\ p & \text{if } p^\alpha \| J \text{ and } i \geq \alpha \geq 1. \end{cases}$$

P r o o f. We first observe that $K = \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{(n,m)})$. This follows directly from the familiar fact that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, the more easily seen relation $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{[n,m]})$ and, since the extensions are Galois,

$$\begin{aligned}[K : \mathbb{Q}(\zeta_{(n,m)})] &= \frac{\phi(n)}{\phi((n,m))[\mathbb{Q}(\zeta_n) : K]} \\ &= \frac{\phi(n)}{\phi((n,m))[\mathbb{Q}(\zeta_{[n,m]}) : \mathbb{Q}(\zeta_m)]} = \frac{\phi(n)\phi(m)}{\phi((n,m))\phi([n,m])} = 1.\end{aligned}$$

Now for each n we have

$$[k(\zeta_n) : k] = \frac{\phi(n)}{\delta(k; n)}$$

where, by the definition of J,

$$\begin{aligned}\delta(k; n) &= [k \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] = [k \cap \mathbb{Q}(\zeta_J) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] \\ &= [k \cap \mathbb{Q}(\zeta_{(n,J)}) : \mathbb{Q}] = \delta(k; (n, J)).\end{aligned}$$

In all the above cases we have $(mp^{i+1}, J) = (mp^i, J)$. Hence $\delta(k; mp^{i+1}) = \delta(k; p^i)$,

$$[k(\zeta_{mp^{i+1}}) : k(\zeta_{mp^i})] = \frac{\phi(p^{i+1})}{\phi(p^i)},$$

and the result is clear.

Our proofs of Theorems 4 and 5 require the following lemma.

LEMMA 9. *Suppose that n belongs to $Y(M)$ and p is a prime divisor of $n/(n,J)$.*

(A) *If $p\nmid J$ and $p^2\nmid n$ then one of the following holds*:

(i) *For each r in $\mathbb{Z}/p\mathbb{Z}$ the subset $M(r;p)$ satisfies $|M(r;p)|\neq 1$. If $|M(r;p)|\geq 2$ then n/p belongs to $Y(M(r;p))$.*

(ii) *For each r in $\mathbb{Z}/p\mathbb{Z}$ the subset $M(r;p)$ satisfies $|M(r;p)|\geq 1$. If $r_1\not\equiv r_2 \bmod p$ then n/p belongs to $Y(M(r_1,r_2;p))$. Also, p satisfies $p\leq |M|$.*

(B) *If $p\,|\,J$ or if $p^2\,|\,n$ then*

(iii) *for each r in $\mathbb{Z}/p\mathbb{Z}$ the subset $M(r;p)$ satisfies $|M(r;p)|\neq 1$. If $|M(r;p)|\geq 2$ then n/p belongs to $Y(p^{-1}(M(r;p)-r))$.*

Proof. For each m in M let ξ_m be nonzero elements of k such that

$$\sum_{m\in M}\xi_m\zeta_n^m=0 \tag{3.1}$$

for some primitive nth root of unity ζ_n. Assume that $p\nmid J$ and $p^2\nmid n$ and then write $n=n'p$. Select a primitive n'th root of unity $\zeta_{n'}$ and a primitive pth root of unity ζ_p such that $\zeta_n=\zeta_{n'}\zeta_p$. Now (3.1) can be written as

$$\sum_{r=0}^{p-1}\Big\{\sum_{m\in M(r;p)}\xi_m\zeta_{n'}^m\Big\}\zeta_p^r=0. \tag{3.2}$$

We have $k(\zeta_n)=k(\zeta_{n'},\zeta_p)$ and, using $p\nmid J$ and $p^2\nmid n$, we see from Lemma 8 that

$$[k(\zeta_n):k(\zeta_{n'})]=p-1,$$

in particular the minimal polynomial for ζ_p over $k(\zeta_p)$ is simply $\Phi_p(x)$. It follows then from (3.2) that

$$r\to\sum_{m\in M(r;p)}\xi_m\zeta_{n'}^m \tag{3.3}$$

is constant for r in $\mathbb{Z}/p\mathbb{Z}$. If (3.3) is constantly zero for r in $\mathbb{Z}/p\mathbb{Z}$ then the conclusion (i) follows immediately. If (3.3) is a nonzero constant for all r in $\mathbb{Z}/p\mathbb{Z}$ then clearly $|M(r;p)|\geq 1$ for all r. If $r_1\not\equiv r_2 \bmod p$ then

$$\sum_{m\in M(r_1;p)}\xi_m\zeta_{n'}^m-\sum_{m\in M(r_2;p)}\xi_m\zeta_{n'}^m=0$$

and therefore $n/p=n'$ belongs to $Y(M(r_1,r_2;p))$. Also, we have

$$|M|=\sum_{r=0}^{p-1}|M(r;p)|\geq p,$$

and this verifies the conclusion (ii).

Next we assume that either $p \mid J$ or $p^2 \mid n$, and again we write $n = n'p$. We change our previous notation and set $\zeta_{n'} = \zeta_n^p$ because ζ_n^p is a primitive n'th root of unity in this case. Then (3.2) can be written as

$$\sum_{r=0}^{p-1} \Big\{ \sum_{m \in M(r;p)} \xi_m \zeta_{n'}^{(\frac{m-r}{p})} \Big\} \zeta_n^r = 0. \tag{3.4}$$

Using $p \mid J$ or $p^2 \mid n$ we find that

$$[k(\zeta_n) : k(\zeta_{n'})] = p.$$

It follows from (3.4) that

$$\sum_{m \in M(r;p)} \xi_m \zeta_{n'}^{(\frac{m-r}{p})} = 0$$

for all r in $\mathbb{Z}/p\mathbb{Z}$. This establishes the conclusion (iii).

If n belongs to $Y(M)$ then prime divisors p of $n/(n, J)$ which satisfy $p \nmid J$ and $p^2 \nmid n$ will be called *type A prime divisors*. The remaining prime divisors which must satisfy $p \mid J$ or $p^2 \mid n$ will be called *type B prime divisors*.

LEMMA 10. *Suppose that* $3 \le |M|$, m_1 *and* m_2 *are distinct elements of* M, *and* n *belongs to* $Y(M)$. *Let* $L \ge 0$ *be the number of distinct type A prime divisors of* $n/(n, J)$ *and write* $q_0 = 1$. *If* $L \ge 1$ *let* $p_1, \dots, p_L$ *be the distinct type A prime divisors of* $n/(n, J)$ *and write*

$$q_l = p_1 \dots p_l, \qquad 1 \le l \le L.$$

Then there exists a nested collection of $L + 1$ *subsets*

$$M = M_0 \supseteq M_1 \supseteq \dots \supseteq M_L \supseteq \{m_1, m_2\}$$

such that

(iv) n/q_l *belongs to* $Y(M_l)$ *for each* l, $0 \le l \le L$, *and*

(v) $q_l \mid (m_1 - m_2)(m_2 - m)(m - m_1)$ *for each* m *in* M_l *and each* l, $0 \le l \le L$.

Moreover, if $2 = |M_l| < |M_{l-1}|$ *for some* l, $1 \le l \le L$, *then* $3 \le p_l \le |M_{l-1}|$, $m_1 \not\equiv m_2 \bmod p_l$, *and* M_{l-1} *contains a complete set of incongruent residue classes modulo* p_l.

Proof. We argue by induction on l. As n belongs to $Y(M_0)$ and $q_0 = 1$, both (iv) and (v) are trivial when $l = 0$. Therefore we assume that $1 \le l \le L$, and that a nested collection of subsets

$$M = M_0 \supseteq M_1 \supseteq \dots \supseteq M_{l-1} \supseteq \{m_1, m_2\}$$

has been determined which satisfies the conclusion of the lemma. If $|M_{l-1}| = 2$ then $M_{l-1} = \{m_1, m_2\}$ and we must select $M_l = \{m_1, m_2\}$. Then (iv)

follows from Lemma 9(A) and, of course, (v) is trivial. Thus we may assume throughout the remainder of the proof that $3 \le |M_{l-1}|$.

If $m_1 \not\equiv m_2 \bmod p_l$ or $m_1 \equiv m_2 \bmod p_l$ and $M_{l-1}(m_1; p_l) = M_{l-1}$ we set

$$M_l = M_{l-1}(m_1, m_2; p_l).$$

If $m_1 \equiv m_2 \bmod p_l$ and $M_{l-1}(m_1; p_l) \neq M_{l-1}$ we select a residue class s_l in $\mathbb{Z}/p_l\mathbb{Z}$, $s_l \not\equiv m_1 \bmod p_l$, so that $3 \le |M_{l-1}(m_1, s_l; p_l)|$ and then set

$$M_l = M_{l-1}(m_1, s_l; p_l).$$

In either case it is obvious that

$$p_l \,|\, (m_1 - m_2)(m_2 - m)(m - m_1)$$

for each m in M_l. As

$$q_{l-1} \,|\, (m_1 - m_2)(m_2 - m)(m - m_1)$$

for each m in M_l, it follows that (v) holds also at l.

Now p_l is a type A prime divisor of n/q_{l-1} and by the inductive hypothesis n/q_{l-1} belongs to $Y(M_{l-1})$. Therefore we can apply Lemma 9. In case (i) we have $|M_{l-1}(r; p_l)| \neq 1$ for all r in $\mathbb{Z}/p_l\mathbb{Z}$. In particular,

$$2 \le |M_{l-1}(m_1; p_l)| \quad \text{and} \quad 2 \le |M_{l-1}(m_2; p_l)|.$$

If $m_1 \not\equiv m_2 \bmod p_l$ then $4 \le |M_l|$ and it is clear that n/q_l belongs to $Y(M_l)$. If $m_1 \equiv m_2 \bmod p_l$ then $3 \le |M_l|$, and again we find that n/q_l belongs to $Y(M_l)$. In case (ii) we conclude that $1 \le |M_{l-1}(r; p_l)|$ for all r in $\mathbb{Z}/p_l\mathbb{Z}$ and so n/q_l belongs to $Y(M_l)$. In case (ii), however, it may happen that $|M_l| = 2$. Plainly this requires that $m_1 \not\equiv m_2 \bmod p_l$, $M_{l-1}(m_1; p_l) = \{m_1\}$ and $M_{l-1}(m_2; p_l) = \{m_2\}$. As $M_{l-1} = M_{l-1}(0, 1; 2)$, we must have $3 \le p_l$ and in case (ii) we also have $p_l \le |M_{l-1}|$. Since $1 \le |M_{l-1}(r; p_l)|$ for all r in $\mathbb{Z}/p_l\mathbb{Z}$, it is obvious that M_{l-1} contains a complete set of incongruent residue classes modulo p_l.

Proof of Lemma 3. Let ζ_n be any primitive nth root of unity. Then $k(\zeta_n)/k$ is a Galois extension. For each σ in $G = \mathrm{Gal}\{k(\zeta_n)/k\}$ there exists a unique $i = i(\sigma)$ in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ such that $\sigma(\zeta_n) = \zeta_n^{i(\sigma)}$. Clearly $i(\sigma)$ does not depend on our choice of ζ_n. It follows easily that $\sigma \to i(\sigma)$ is an isomorphism from G onto a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. Let $U(\zeta_n) = (\zeta_n^{i(\sigma)m})$ denote the $|G| \times |M|$ matrix in which σ in G indexes rows and m in M indexes columns. The determinant of any square submatrix of $U(\zeta_n)$ is a polynomial with integer coefficients evaluated at ζ_n. Therefore

$$\zeta_n \to \text{ rank } U(\zeta_n) \tag{3.5}$$

is constant on the set of primitive nth roots of unity. Let $\psi_1, \dots, \psi_{|G|}$ be a basis for $k(\zeta_n)/k$ and write $\Psi = (\sigma(\psi_j))$ for the corresponding nonsingular

$|G| \times |G|$ matrix in which σ in G indexes rows and $j = 1, \ldots, |G|$ indexes columns. Then we have

$$\zeta_n^m = \sum_{j=1}^{|G|} v_n(j,m)\psi_j,$$

where $V(\zeta_n) = (v_n(j,m))$ is an $|G| \times |M|$ matrix with entries in k. From the matrix identity

$$U(\zeta_n) = \Psi V(\zeta_n) \tag{3.6}$$

we conclude that

$$\zeta_n \to \text{ rank } V(\zeta_n) \tag{3.7}$$

is constant on primitive nth roots of unity.

Let $\mathfrak{X}(n,s;M)$ denote the k-subspace of $k^{|M|}$ containing all vectors $\mathbf{x}$ such that

$$\sum_{m\in M} x_m \zeta_n^m = 0, \tag{3.8}$$

where $\Phi_{n,s}(\zeta_n) = 0$. Applying σ in G to (3.8) we see that $\mathfrak{X}(n,s;M)$ is the null space of $U(\zeta_n)$ and so also the null space of $V(\zeta_n)$. As $V(\zeta_n)$ has entries in k, (3.6) implies that

$$s \to \dim\{\mathfrak{X}(n,s;M)\} \tag{3.9}$$

is constant for $0 \le s \le \delta(k;n)$. If the right hand side of (3.9) is zero the result is trivial, hence we may assume that this dimension is positive. For each l in L let $\mathfrak{X}_l(n,s;M)$ be the subspace of vectors $\mathbf{x}$ in $k^{|M|}$ such that

$$\sum_{m\in M} x_m \zeta_n^m = 0, \qquad x_l = 0,$$

where $\Phi_{n,s}(\zeta_n) = 0$. In a similar manner we find that

$$s \to \dim\{\mathfrak{X}_l(n,s;M)\} \tag{3.10}$$

is constant for $0 \le s \le \delta(k;n)$. Now observe that

$$\mathfrak{X}(n,s;M) \setminus \bigcup_{l\in L} \mathfrak{X}_l(n,s;M) \tag{3.11}$$

is exactly the set of vectors $\mathbf{x}$ in $k^{|M|}$ such that

$$\sum_{m\in M} x_m \zeta_n^m = 0 \quad \text{and} \quad x_l \neq 0 \quad \text{for all } l \text{ in } L,$$

where $\Phi_{n,s}(\zeta_n) = 0$. Recall that an infinite vector space cannot be a finite union of proper subspaces. If (3.11) is empty for some s' then there exists l' in L such that

$$\dim\{\mathfrak{X}(n,s';M)\} = \dim\{\mathfrak{X}_{l'}(n,s';M)\}. \tag{3.12}$$

We conclude from (3.9) and (3.10) that

$$\dim\{\mathfrak{X}(n,s;M)\} = \dim\{\mathfrak{X}_{l'}(n,s;M)\}$$

for all s, $1 \le s \le \delta(k;n)$. Thus (3.11) is empty for one s if and only if it is empty for all s, $1 \le s \le \delta(k;n)$, and this verifies the lemma.

4. Proof of Theorems 4 and 5. Let $\Omega(n)$ denote the number of prime divisors of n counted with multiplicity. We begin by proving Theorem 4 under the stronger hypothesis that n belongs to $Y(M)$. We argue by induction on $\Omega(n/(n,J))$. If $\Omega(n/(n,J)) = 0$ then the result is obvious with $a = b = 1$. Assume then that p is a prime divisor of $n/(n,J)$ and write $n = n'p$. We note that $(n',J) = (n,J)$.

As n belongs to $Y(M)$ we can apply Lemma 9. In case (i) we have m_1 in $M(m_1;p)$ and therefore n' belongs to $Y(M(m_1;p))$. It follows from the inductive hypothesis that there exists m_2 in $M(m_1;p) \setminus \{m_1\}$ such that n' factors as

$$n' = (n',J)a'b', \qquad a' \mid P,$$

and $b' \mid (m_1 - m_2)$. Obviously $p \mid (m_1 - m_2)$ and so the desired factorization (2.3) holds with $a = a'$ and $b = b'p$.

In case (ii) we can select m_0 in $M \setminus \{m_1\}$ so that $m_0 \not\equiv m_1 \bmod p$. Then n' belongs to $Y(M(m_0,m_1;p))$ and by the inductive hypothesis there exists m_2 in $M(m_0,m_1;p)$ so that n' factors as

$$n' = (n',J)a'b', \qquad a' \mid P,$$

with $b' \mid (m_1 - m_2)$. Clearly $p \nmid a'$ and in case (ii) we have $p \le |M|$. Thus the factorization (2.3) holds with $a = a'p$ and $b = b'$.

In case (iii), n' belongs to $Y(p^{-1}(M(m_1,p) - m_1))$. Therefore we apply the inductive hypothesis to the set $p^{-1}(M(m_1;p) - m_1)$ and the element 0, which plainly occurs in this set. We conclude that there exists $p^{-1}(m_2 - m_1)$ in $p^{-1}(M(m_1;p) - m_1) \setminus \{0\}$ such that n' factors as

$$n' = (n',J)a'b', \qquad a' \mid P,$$

with $b' \mid p^{-1}(m_1 - m_2)$. Again this shows that n satisfies (2.3) with $a = a'$ and $b = b'p$.

Finally, if n belongs to $Z(\{m_1\};M)$ then there exists a subset M' such that $\{m_1\} \subseteq M' \subseteq M$ and n belongs to $Y(M')$. The desired factorization of n now follows from the special case of the theorem which was already proved.

The proof of Theorem 5 is identical to the proof of Theorem 4 except in the treatment of case (ii). We assume that n belongs to $Y(M)$ and that p is a prime divisor of $n/(n,J)$. Then we apply Lemma 9. In case (ii) we

see that $n' = n/p$ belongs to $Y(M(r_1, r_2; p))$ whenever $r_1 \not\equiv r_2 \bmod p$. We select r_1 and r_2 in $\mathbb{Z}/p\mathbb{Z}$ so that $r_1 \not\equiv r_2 \bmod p$ and so that

$$|M(r_1, r_2; p)| = |M(r_1; p)| + |M(r_2; p)|$$

is minimized. As

$$\begin{aligned} 2(p-1)|M| &= \sum_{s=0}^{p-1} \sum_{\substack{t=0 \\ t \neq s}}^{p-1} \{|M(s; p)| + |M(t; p)|\} \\ &\geq (p^2 - p)\{|M(r_1; p)| + |M(r_2; p)|\} \end{aligned}$$

we conclude that

$$2|M| \geq p|M(r_1, r_2; p)|. \tag{4.1}$$

By the inductive hypothesis there exist distinct elements m_1 and m_2 in $M(r_1, r_2; p)$ and a factorization

$$n' = (n', J)a'b', \qquad a' \mid P,$$

such that $a' \leq \tau(a')|M(r_1, r_2; p)|$ and $b' \mid (m_1 - m_2)$. Using (4.1) we have $a'p \leq 2\tau(a')|M|$. In case (ii) the prime p does not divide a'. It follows that n factors as (2.4) with $a = a'p$ and $b = b'$.

5. Proof of Theorem 6. First we prove Theorem 6 under the stronger hypothesis that n belongs to $Y(M)$. Let $L \geq 0$ be the number of distinct, type A prime divisors of $n/(n, J)$ and write $q_0 = 1$. If $L \geq 1$ let $p_1, \ldots, p_L$ be the distinct, type A prime divisors of $n/(n, J)$ and write

$$q_l = p_1 \ldots p_l, \qquad 1 \leq l \leq L.$$

Then let

$$M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_L \supseteq \{m_1, m_2\}$$

be the nested collection of $L + 1$ subsets determined as in Lemma 10. We consider two cases.

Assume that $|M_L| \geq 3$. Then n/q_L belongs to $Y(M_L)$ and

$$q_L \mid (m_1 - m_2)(m_2 - m)(m - m_1) \tag{5.1}$$

for all m in M_L. By Theorem 4 there exists m_2' in $M_L \setminus \{m_1\}$ and a factorization

$$\frac{n}{q_L} = \left(\frac{n}{q_L}, J\right)a'b', \qquad a' \mid P,$$

such that

$$b' \mid (m_1 - m_2'). \tag{5.2}$$

Since $(n/q_L)/(n/q_L, J)$ has no type A prime divisors it follows easily that $a' \mid b'$. Now set $a = a'$ and $b = b'q_L$. Then n factors as

$$n = (n, J)ab, \qquad a \mid P, \tag{5.3}$$

and $a \mid b$. If $m_2' \neq m_2$ we set $m_3 = m_2'$. Then (5.1) and (5.2) imply that $b \mid (m_1 - m_2)(m_2 - m_3)(m_3 - m_1)$. If $m_2' = m_2$ we select m_3 arbitrarily in $M_L \setminus \{m_1, m_2\}$. Again (5.1) and (5.2) imply that $b \mid (m_1 - m_2)(m_2 - m_3)(m_3 - m_1)$. Thus the factorization (5.3) satisfies condition (i) in the statement of the theorem.

Next we assume that $|M_L| = 2$ and then there exists l, $1 \leq l \leq L$, such that $2 = |M_l| < |M_{l-1}|$. From Lemma 10 we conclude that n/q_l belongs to $Y(M_l)$, that

$$q_{l-1} \mid (m_1 - m_2)(m_2 - m)(m - m_1) \tag{5.4}$$

for all m in M_{l-1}, and also that $3 \leq p_l \leq |M_{l-1}|$. In this case $M_l = \{m_1, m_2\}$ and so by Theorem 4 there exists a factorization

$$\frac{n}{q_l} = \left(\frac{n}{q_l}, J\right)a'b', \qquad a' \mid 2,$$

such that $b' \mid (m_1 - m_2)$. Set $a = a'p_l$ and $b = b'q_{l-1}$. Then n factors as

$$n = (n, J)ab, \qquad a \mid P,$$

and a has exactly one odd prime factor p_l. Using (5.4) and $(b', q_{l-1}) = 1$, we find that

$$b \mid (m_1 - m_2)(m_2 - m)(m - m_1)$$

for each m in M_{l-1}. Since $m_1 \not\equiv m_2 \bmod p_l$ and M_{l-1} contains a complete set of incongruent residue class representatives in $\mathbb{Z}/p_l\mathbb{Z}$, the conclusion (ii) in the statement of the theorem is verified.

If n belongs to $Z(\{m_1, m_2\}; M)$ then there exists a subset M' such that $\{m_1, m_2\} \subseteq M' \subseteq M$ and n belongs to $Y(M')$. As before the theorem follows from the special case already proved.

6. Proof of Corollary 7 and Theorem 2. Let $\tau(n)$ denote the number of positive divisors of n and $\omega(n)$ the number of distinct prime divisors of n. It will be convenient to set $\tau(0) = 0$ and $\tau(-n) = \tau(n)$. If $|M| = 2$ then Corollary 7 is a trivial consequence of Theorem 4. Thus we may assume that $3 \leq |M|$ and then estimate the number of integers n which factor as in (2.5).

Let m_1, m_2 and m_3 be distinct elements of M and write $m = (m_1 - m_2)(m_2 - m_3)(m_3 - m_1)$. Then we have

$$\sum_{b|m}\sum_{\substack{a|P\\ a|b}} 1 \le \sum_{b|m} 2^{\omega(b)} = \tau(m^2)$$
$$\le \tau(m_1-m_2)^2\tau(m_2-m_3)^2\tau(m_3-m_1)^2 \ll_\varepsilon \partial(M)^\varepsilon.$$

Thus the number of positive integers that can be written as ab, where $a \mid P$ and a and b satisfy condition (i) of Theorem 6 is at most

$$\sum_{m_3\in M}\sum_{b|m}\sum_{\substack{a|P\\ a|b}} 1 \ll_\varepsilon \partial(M)^\varepsilon |M|.$$

The number of positive integers that can be written as ab, where $a \mid P$ and a and b satisfy condition (ii) of Theorem 6 is at most

$$\sum_{3\le p\le |M|} (p-2)^{-1} \sum_{m_3\in M} \tau\{(m_1-m_2)(m_2-m_3)(m_3-m_1)\} \ll_\varepsilon \partial(M)^\varepsilon |M|. \tag{6.1}$$

It follows that

$$S(\{m_1,m_2\};M) = \sum_{n\in Z(\{m_1,m_2\};M)} \delta(k;(n,J)) \ll_\varepsilon \Big\{\sum_{j|J}\delta(k;j)\Big\}\partial(M)^\varepsilon|M|,$$

which is (2.6).

For a positive integer U we define the set

$$Z_U(M) = \bigcup_{|L|\ge U} Z(L;M).$$

Then for $U \ge 2$ we have

$$\sum_{n\in Z_U(M)} \delta(k;(n,J)) \le \frac{1}{U(U-1)} \sum_{m_1\in M}\sum_{\substack{m_2\in M\\ m_2\ne m_1}} S(\{m_1,m_2\};M)$$
$$\ll_\varepsilon C(k)\partial(M)^\varepsilon |M|^3 U^{-2}.$$

To estimate the remaining integers in $Z(M)$ we appeal to Theorem 5. We find that

$$\sum_{n\in Z(M)\setminus Z_U(M)} \delta(k;(n,J)) \le \sum_{j|J}\delta(k;j) \sum_{a\le \tau(a)U} 1 \sum_{b|(m_i-m_j)} 1$$
$$\ll_\varepsilon C(k)U^{1+\varepsilon} \sum_{m_1\in M}\sum_{m_2\in M} \tau(m_1-m_2)$$
$$\ll_\varepsilon C(k)U^{1+\varepsilon}\partial(M)^\varepsilon |M|^2.$$

The bound (2.7) follows by choosing $U = |M|^{1/3}$.

The bounds (1.9)–(1.11) in Theorem 2 follow easily from Theorems 4–6 respectively, on counting the number of a and b satisfying the given conditions. In (1.11) the estimates are almost identical to those in the proof of

Corollary 7 except we use the more precise estimate $\sum_{3\le p\le N(F)} 1/(p-2) = \log\log N(F) + O(1)$ in (6.1). We also make the observation that case (ii) of Theorem 6, and hence the necessity of the $\log\log N(F)$ in (1.11), never occurs unless a_I/a_J is a root of unity. To see this observe that the induction process employed in Lemmas 9 and 10 constructs a relation of the form (2.2) for $\zeta_{n/p}$ from the assumed relation for ζ_n using a subset of the coefficients altered by at most a sign change. In particular, case (ii) of Theorem 6 will not arise unless the induction terminates in a two-term relation

$$a_I\zeta_m^{n_I} \pm a_J\zeta_m^{n_J} = 0,$$

for some integer m. It is perhaps also worth remarking that the proof of Theorem 6(i) actually shows that $a \,|\, (m_1 - m_2)$ or $(m_1 - m_3)$, so that the squares are not required on all the factors in (1.11).

For (1.10) we also need the following lemma to estimate the number of square-free a with $a \le \tau(a)|M|$.

LEMMA 11. *For all $x \ge 3$ we have*

$$S(x) = \sum_{n/\tau(n)\le x} |\mu(n)| = \left(1 + O\left(\frac{1}{\log\log x}\right)\right) Cx\log x, \tag{6.2}$$

where

$$C = \prod_p (1 - 3p^{-2} + 2p^{-3}) < 0.287,$$

and $\prod_p$ indicates a product over all primes p.

P r o o f. We first recall some elementary properties of the divisor function $\tau(n)$. We have

$$\tau(n) \le e^{c\log n/\log\log 3n}$$

for some constant $c > 0$, and

$$\sum_{M\le n\le N} \frac{\tau(n)}{n} = \frac{1}{2}\log\left(\frac{N}{M}\right)\log(NM) + O\left(\log\left(\frac{2N}{M}\right)\right). \tag{6.3}$$

Here (6.3) is a straightforward consequence of the estimate $\sum_{n\le x}\tau(n) = x\log x + O(x)$ and partial summation.

Next we use the estimate $\log n = \log x(1+O(1/\log\log x))$, which holds for all n such that $x/\log x \le n \le x\tau(n)$. Using p to denote primes, we can write

$$\begin{aligned}\left(1 + O\left(\frac{1}{\log\log x}\right)\right) & S(x)\log x \\ &= \sum_{n/\tau(n)\le x} |\mu(n)|\log n = \sum_{n/\tau(n)\le x} |\mu(n)| \sum_{p\mid n} \log p \\ &= \sum_p \log p \sum_{\substack{n\le\tau(n)x \\ p\mid n}} |\mu(n)| = \sum_p \log p \sum_{\substack{pm\le\tau(pm)x \\ p\nmid m}} |\mu(pm)|\end{aligned}$$

$$= \sum_p \log p \sum_{\substack{pm \le 2\tau(m)x \\ p \nmid m}} |\mu(m)| = \sum_{m \le \tau(m)x} |\mu(m)| \sum_{\substack{p \le 2x\tau(m)/m \\ p \nmid m}} \log p$$
$$= S_1 + S_2 - S_3,$$

where

$$S_1 = \sum_{n \le x/\log x} |\mu(n)| \vartheta(2x\tau(n)n^{-1}),$$
$$S_2 = \sum_{x/\log x < n \le \tau(n)x} |\mu(n)| \sum_{\substack{p \le 2x\tau(n)/n \\ p \nmid n}} \log p,$$

and

$$S_3 = \sum_{n \le x/\log x} |\mu(n)| \sum_{\substack{p \le 2x\tau(n)/n \\ p \mid n}} \log p.$$

Now using a weak form of the prime number theorem

$$\vartheta(x) = \sum_{p \le x} \log p = x + O(x/\log x),$$

we have

$$S_1 = \sum_{n \le x/\log x} |\mu(n)| \vartheta(2x\tau(n)n^{-1})$$
$$= 2x\left(1 + O\left(\frac{1}{\log\log x}\right)\right) \sum_{n \le x/\log x} |\mu(n)| \frac{\tau(n)}{n},$$

with

$$0 \le S_2 \le \sum_{x/\log x < n \le x\tau(n)} \vartheta(2x\tau(n)n^{-1})$$
$$\ll x \sum_{x/\log x < n \le xe^{c\frac{\log x}{\log\log x}}} \frac{\tau(n)}{n} \ll x\frac{(\log x)^2}{\log\log x},$$

and

$$0 \le S_3 \le \sum_{n \le x/\log x} \sum_{p \mid n} \log p \le \sum_{n \le x/\log x} \log n \ll x.$$

Finally, to evaluate the remaining sum, we write

$$|\mu(n)|\tau(n) = \sum_{m \mid n} \tau(m) a(n/m)$$

where $a(n)$ is the multiplicative function generated by

$$A(s) = \sum_{n=1}^{\infty} a(n)n^{-s} = \Big(\sum_{n=1}^{\infty} |\mu(n)|\tau(n)n^{-s}\Big)\zeta(s)^{-2} = \prod_{p}(1-3p^{-2s}+2p^{-3s}).$$

Notice that $A(s)$ converges absolutely for $\operatorname{Re} s > 1/2$. Hence

$$\begin{aligned}\sum_{n\le x} |\mu(n)|\frac{\tau(n)}{n} &= \sum_{l\le x}\frac{a(l)}{l}\sum_{m\le x/l}\frac{\tau(m)}{m}\\ &= \frac{1}{2}(\log x)^2\Big(\sum_{l\le x}\frac{a(l)}{l}\Big) + O\Big(\log x\sum_{l\le x}\frac{|a(l)|\log l}{l}\Big)\\ &= \frac{1}{2}(\log x)^2\Big(\sum_{l=1}^{\infty}\frac{a(l)}{l}\Big) + O(\log x),\end{aligned}$$

and the result follows with $C = A(1)$.

References

[1] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401.

[2] G. Hajós, *Solution to problem 41*, Mat. Lapok 4 (1953), 40–41 (in Hungarian).

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

[4] H. L. Montgomery and A. Schinzel, *Some arithmetic properties of polynomials in several variables*, in: Transcendence Theory: Advances and Applications, Academic Press, 1977, 195–203.

[5] C. G. Pinner and J. D. Vaaler, *The number of irreducible factors of a polynomial, I*, Trans. Amer. Math. Soc. 339 (1993), 809–834.

[6] A. Schinzel, *On the number of irreducible factors of a polynomial, II*, Ann. Polon. Math. 42 (1983), 309–320.

Department of Mathematics
University of British Columbia
Vancouver, British Columbia, V6T 1Z2
Canada
E-mail: pinner@math.ubc.ca

Centre for Experimental and Constructive Mathematics
Simon Fraser University
Burnaby, British Columbia, V5A 1S6
Canada
E-mail: pinner@perfect.cecm.sfu.ca

Department of Mathematics
The University of Texas at Austin
Austin, Texas 78712-1082
U.S.A.
E-mail: vaaler@math.utexas.edu

Received on 15.12.1995 (2904)