ACTA ARITHMETICA
130.4 (2007)

Arithmetical applications of an identity for the Vandermonde determinant

by

D. S. Ramana (Allahabad)

1. Introduction. This article is concerned with the following question. Suppose that $\{\alpha_i\}_{1\le i\le m}$ is a sequence of distinct elements in an integral domain A and that γ is a common multiple of the α_i in A. Let ϕ be a function from the nonzero elements of A to $\mathbb{R}_+$ satisfying $\phi(xy) = \phi(x) + \phi(y)$ for all nonzero x, y in A. If, for some s in $[0,1]$, we have $\phi(\alpha_i) \ge s\phi(\gamma)$ for all i, then the question is to obtain a lower bound for $\sup_{1\le i<j\le m} \phi(\alpha_i - \alpha_j)$ in terms of $\phi(\gamma)$, m and s. This question is relevant, for example, to the problem of determining upper bounds for the number of integer points on small arcs of conics considered in [2], [3], [6], [5], and the problem of showing that the number of divisors of an integer N lying in certain arithmetical progressions is bounded independently of N, considered in [8].

In most situations where the aforementioned question is of interest, the integral domain A is either a factorial ring or a Dedekind domain and, indeed, it is by assuming that A has one of these properties that this question has been studied. For instance, when A is a factorial ring we have $\phi(\alpha_i - \alpha_j) \ge \phi((\alpha_i, \alpha_j))$ for $1 \le i < j \le m$, where (α_i, α_j) is the greatest common divisor of α_i and α_j in A. A special case of the overlapping theorem of [7] (see also [8]) then provides a lower bound for $\sup_{1\le i<j\le m} \phi((\alpha_i, \alpha_j))$, and therefore for $\sup_{1\le i<j\le m} \phi(\alpha_i - \alpha_j)$, in terms of $\phi(\gamma)$, m and s. When A is a Dedekind domain, and assuming that ϕ extends in a natural manner to the ideals of A, one uses Theorem 1.1 of [6] which provides a lower bound for $\phi((\mathfrak{a}_i, \mathfrak{a}_j))$, where the ideal $(\mathfrak{a}_i, \mathfrak{a}_j)$ is the greatest common divisor of the ideals $\mathfrak{a}_i$ and $\mathfrak{a}_j$ generated, respectively, by α_i and α_j in A, and passes to a lower bound for $\sup_{1\le i<j\le m} \phi(\alpha_i - \alpha_j)$ in terms of $\phi(\gamma)$, m and s by noting that the ideal generated in A by $\alpha_i - \alpha_j$ is contained in $(\mathfrak{a}_i, \mathfrak{a}_j)$.

In this article we present a simple identity for the Vandermonde determinant that immediately yields, for any integral domain A, a lower bound

2000 *Mathematics Subject Classification*: Primary 11P21.
Key words and phrases: Vandermonde determinant, divisors, integer points.

for $\sup_{1\le i<j\le m}\phi(\alpha_i-\alpha_j)$ in terms of $\phi(\gamma)$, without recourse to factorisation in A. We show in Section 2 that this identity provides rather simple proofs for a number of results given in [6] and [7], and use it to obtain the following version of Theorem 1.2 of [6], which contains Theorem 1 of [2] and improves on the main results of [3], [5].

THEOREM 1.1. *When $d \neq 0,-1$ is a squarefree integer and m, R are integers with $m \ge 2$, there are no more than m integer points on any arc of length $\le |R|^{s(m)}/|d|^{r(m)}$ on the conic*

$$(*) \qquad X^2 + dY^2 = R,$$

where

$$s(m) = \frac{1}{4} - \frac{1}{8[m/2]+4},$$

$$r(m) = \begin{cases} \dfrac{1}{2}\left(1 - \dfrac{\left[\frac{1}{2}\left(\frac{m^2}{2} - m\right)\right]+1}{\binom{m}{2}}\right) & \text{if } m \text{ is odd},\\ r(m+1) & \text{if } m \text{ is even.}\end{cases}$$

We conclude in Section 3 with some notes relating to the contents of this article.

2. An identity for the Vandermonde determinant. Throughout this article, m shall denote an integer ≥ 2.

LEMMA 2.1. *Let A be a commutative ring and $\{\alpha_i\}_{1\le i\le m}$ and $\{\beta_i\}_{1\le i\le m}$ be sequences of m elements in A for which there exists a γ in A satisfying $\alpha_i\beta_i = \gamma$ for all i. For each integer k satisfying $0 \le k \le m-1$,*

$$(1) \qquad \gamma^{k(k+1)/2} \prod_{1\le i<j\le m} (\alpha_i - \alpha_j) = \prod_{1\le i\le m} \alpha_i^k \begin{vmatrix} \beta_1^k & \beta_2^k & \dots & \beta_m^k \\ \vdots & \vdots & & \vdots \\ \beta_1 & \beta_2 & \dots & \beta_m \\ 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \vdots & \vdots & & \vdots \\ \alpha_1^{m-k-1} & \alpha_2^{m-k-1} & \dots & \alpha_m^{m-k-1} \end{vmatrix}.$$

Proof. For $1 \le k \le m-1$ and $1 \le i \le m$, we multiply the ith column of the determinant on the right hand side of (1) by α_i^k. For $1 \le i \le m$ and $1 \le j \le k$ the (i,j)th entry in the resulting determinant is $\beta_i^{k-j+1}\alpha_i^k = (\beta_i\alpha_i)^{k-j+1}\alpha_i^{j-1} = \gamma^{k-j+1}\alpha_i^{j-1}$. Therefore γ^{k-j+1} is common to each entry in the jth row, for $1 \le j \le k$. Since $\prod_{1\le j\le k} \gamma^{k-j+1} = \gamma^{k(k+1)/2}$, (1) now follows on using the well known evaluation of the Vandermonde determinant, to which it reduces when $k = 0$.

DEFINITION 2.1. When A is a commutative ring and $\{\alpha_i\}_{1\le i\le m}$ and $\{\beta_i\}_{1\le i\le m}$ are sequences of elements of A, we write $\det_k(\alpha,\beta)$, for each integer k satisfying $0 \le k \le m-1$, to denote the determinant on the right hand side of (1).

The preceding definition allows us to rewrite the identity (1) in the following form. For all integers k satisfying $0 \le k \le m-1$ and $\{\alpha_i\}_{1\le i\le m}$, $\{\beta_i\}_{1\le i\le m}$ and γ as in Lemma 2.1 we have

$$\gamma^{k(k+1)/2} \prod_{1\le i<j\le m} (\alpha_i - \alpha_j) = \det_k(\alpha,\beta) \prod_{1\le i\le m} \alpha_i^k. \tag{2}$$

In order to choose optimal values of k in the applications of (2) that we consider below, we define, for any real number s in $[0,m]$,

$$K(s,m) = \sup_{0\le k\le m-1} \left(sk - \frac{k(k+1)}{2} \right). \tag{3}$$

In this article $K(s,m)$ plays essentially the same role as $E_k(\gamma)\binom{k}{2}$ in Theorem 1.1 of [6] and, by (i) of Lemma 2.2 below, the same role as $Q_2(x)$ in [7].

PROPOSITION 2.1. *Let A be an integral domain and $\alpha = \{\alpha_i\}_{1\le i\le m}$ and $\beta = \{\beta_i\}_{1\le i\le m}$ be sequences of distinct nonzero elements of A. If γ is an element of A such that $\alpha_i\beta_i = \gamma$ for each i, then $\det_k(\alpha,\beta)$ is a nonzero element of A for all k with $0 \le k \le m-1$.*

Suppose that ϕ is a function from the nonzero elements of A into $\mathbb{R}_+$ satisfying $\phi(xy) = \phi(x) + \phi(y)$ for all nonzero x, y in A, and that for some s in $[0,1]$ we have $\phi(\alpha_i) \ge s\phi(\gamma)$ for all i. If $\phi(\det_k(\alpha,\beta)) \ge L$ for all k with $0 \le k \le m-1$, then

$$\sup_{1\le i<j\le m} \phi(\alpha_i - \alpha_j) \ge \frac{K(sm,m)}{\binom{m}{2}} \phi(\gamma) + \frac{L}{\binom{m}{2}}. \tag{4}$$

Proof. Since A is an integral domain and α, β are sequences of distinct nonzero elements of A, we have $\gamma \ne 0$. The left hand side of (2) is thus distinct from 0 and therefore $\det_k(\alpha,\beta)$ is distinct from 0 for $0 \le k \le m-1$.

To verify (4) we apply ϕ to both sides of (2) and obtain

$$\frac{k(k+1)}{2} \phi(\gamma) + \binom{m}{2} \sup_{1\le i<j\le m} \phi(\alpha_i - \alpha_j) \ge smk\phi(\gamma) + L \tag{5}$$

for $0 \le k \le m-1$. On rearranging terms and using (3) we obtain (4).

Lemma 2.2. *We have the following relations for $K(s,m)$.*

(i) *For all s in* $[0,m]$,

$$K(s,m)=\left(s[s]-\frac{[s]([s]+1)}{2}\right)\geq\frac{s(s-1)}{2}.$$

(ii) *We have*

$$\frac{K(m/2,m)}{\binom{m}{2}}=\frac{1}{4}-\frac{1}{8[m/2]+4}$$

when m is an odd integer.

(iii) *If m is an integer ≥ 2, then for all s in* $[0,1]$,

$$\frac{K(sm,m)}{\binom{m}{2}}\geq s^2-\frac{s(1-s)}{m-1}\geq s^2-\frac{1}{4(m-1)}.$$

Proof. Let us verify (i). The function

$$f(t)=st-\frac{t(t+1)}{2}=\left(s-\frac{1}{2}\right)t-\frac{t^2}{2}$$

is a smooth strictly concave function on $\mathbb{R}$ that satisfies $f(s)=f(s-1)$. The supremum of $f(t)$ over the integers in $[0,m-1]$ is therefore attained at an integer in $[0,m-1]\cap[s-1,s]$. If s is not an integer, then $[s]$ is the unique integer in this intersection and the required supremum is attained at $[s]$. If s is an integer, then $s=[s]$ and $s-1$ are the integers in $[0,m-1]\cap[s-1,s]$ and, since $f(s)=f(s-1)$, we see that the required supremum is attained at $[s]$ as well. Moreover, $f([s])\geq f(s)=s(s-1)/2$. We set $m=2k+1$ and $s=m/2$ in (i) to obtain $K(m/2,m)=k^2/2$, from which (ii) follows on dividing by $\binom{m}{2}$ and rearranging terms. We obtain (iii) from (i) on noting that $s(1-s)\leq 1/4$ when s is in $[0,1]$.

The following corollary to Proposition 2.1 is implicit in [6, proof of Theorem 1.2], where only the case of this corollary for quadratic extensions of $\mathbb{Q}$ is required and this is obtained in [6] by an application of Theorem 1.1 of [6].

Corollary 2.1. *Suppose that K is number field of degree n over $\mathbb{Q}$ and that $\{\alpha_i\}_{1\leq i\leq m}$ is a sequence of distinct nonzero elements of the ring A of integers of K. Let $\mathcal{N}(x)$ denote the norm of an element x of K. If $|\mathcal{N}(\alpha_i)|=R$ for each i then*

$$\sup_{1\leq i<j\leq m}|\mathcal{N}(\alpha_i-\alpha_j)|^{1/n}\geq R^{K(m/n,m)/\binom{m}{2}}. \tag{6}$$

Proof. Since $|\mathcal{N}(\alpha_i)|=R$ for each i, we see that R belongs to the ideal generated by each α_i in A. Thus on setting $\gamma=R$, there exists, for each i, a β_i in A such that $\alpha_i\beta_i=\gamma$. Let ϕ be the function $x\mapsto|\mathcal{N}(x)|^{1/n}$. Since R

is in $\mathbb{Z}$, we have $\phi(R) = R$ and hence $\phi(\alpha_i) = \phi(\gamma)^{1/n}$ for all i. The corollary now follows from Proposition 2.1 applied with $L = 1$ and $s = 1/n$.

The following corollary to Proposition 2.1 is implicit in the proof of Proposition 1 of H. Lenstra [8], whose method is closely related to the overlapping theorem of [7]. Conversely, as is evident from the first paragraph on page 336 of [8], the corollary below easily implies Proposition 1 of [8], and moreover, as shown on pages 6 to 8 of [7], implies Lemma 3.1 of [1].

COROLLARY 2.2. *Let s be a real number in $(0,1)$ and $\{d_i\}_{1\le i\le m}$ be distinct positive divisors of an integer $N \ge 1$ and satisfying $d_i \ge N^s$ for all i. If each d_i belongs to the arithmetic progression $a \bmod q$, where $(a,q) = 1$, $q \ge 1$, then*

$$\sup_{1\le i<j\le m} |d_i - d_j| \ge qN^{K(sm,m)/\binom{m}{2}}. \tag{7}$$

Proof. We take $A = \mathbb{Z}$ and set $\alpha_i = d_i$, $\beta_i = N/d_i$ and $\gamma = N$ and take ϕ to be the function $x \mapsto \log|x|$. Since each $\alpha_i \equiv a \bmod q$, we see that $\prod_{1\le i<j\le m}(\alpha_i - \alpha_j)$ is divisible by $q^{\binom{m}{2}}$. As $(a,q) = 1$, we deduce that $\prod_{1\le i\le m} \alpha_i^k \not\equiv 0 \bmod q$ for any integer $k \ge 0$. The identity (2) then shows that $\det_k(\alpha,\beta)$ is divisible by $q^{\binom{m}{2}}$ for all integers k with $0 \le k \le m-1$, and hence that we may take $L = \binom{m}{2}\log q$ when applying Proposition 2.1.

The following corollary to Proposition 2.1 generalises Theorem 1.4 of [6].

COROLLARY 2.3. *Suppose that E is an integral domain and $X = (X_\iota)_{\iota\in I}$ is a family of indeterminates indexed by a set I. Let $\{P_i(X)\}_{1\le i\le m}$ be a sequence of distinct polynomials in $E[X]$. If $R(X)$ is a common multiple of the polynomials $P_i(X)$ in $E[X]$ and if, for some s in $[0,1]$, $\deg(P_i) \ge s\deg(R)$ for all i, then*

$$\sup_{1\le i<j\le m} \deg(P_i - P_j) \ge \deg(R)\,\frac{K(sm,m)}{\binom{m}{2}}, \tag{8}$$

where $\deg(u)$ denotes the total degree of a polynomial $u(X)$ in $E[X]$.

Proof. Since E is an integral domain, so is $E[X]$, and $\deg(uv) = \deg(u) + \deg(v)$ for u and v in $E[X]$. We apply Proposition 2.1 with $A = E[X]$, $\alpha_i = P_i(X)$, $\beta_i = Q_i(X)$ such that $P_i(X)Q_i(X) = R(X)$, $\gamma = R(X)$, ϕ taken to be the function $u \mapsto \deg(u)$ and $L = 0$.

We shall presently verify Theorem 1.1, the essential point in the proof being a refinement of the lower bound for $|\mathcal{N}(\det_k(\alpha,\beta))|$ used in the proof of Corollary 2.1 when K is a quadratic extension of $\mathbb{Q}$.

Proof of Theorem 1.1. We shall show that when $m \ge 2$ is odd, there are in fact no more than $m-1$ integer points on any arc of length $|R|^{s(m)}/|d|^{r(m)}$ on the conic $X^2 + dY^2 = R$. The theorem for m even follows from this conclusion on applying it to $m+1$ and noting that $s(m)=s(m+1)$ and $r(m)=r(m+1)$ when m is an even integer ≥ 2.

Let us thus assume that m is an odd integer ≥ 2, and that $\{p_i\}_{1\leq i\leq m}$ is a sequence of m integer points $p_i=(x_i,y_i)$ on $X^2+dY^2=R$. If the points p_i lie on an arc of length l, then $l>\|p_i-p_j\|_2$ for all (i,j), where $\|\ \|_2$ denotes the Euclidean distance. We set, for each i, $\alpha_i=x_i+\sqrt{-d}\,y_i$ and $\beta_i=x_i-\sqrt{-d}\,y_i$. Since d is a squarefree integer $\neq 0,-1$, we know that $\mathbb{Q}(\sqrt{-d})$ is a quadratic extension of $\mathbb{Q}$ and the triangle inequality gives

$$|d|l^2>|d|\,\|p_i-p_j\|_2^2\geq|\mathcal{N}(\alpha_i-\alpha_j)| \tag{9}$$

for all (i,j), where $\mathcal{N}$ is the norm on $\mathbb{Q}(\sqrt{-d})$. Plainly, $\alpha_i\beta_i=R$ for all i, $1\leq i\leq m$, and $\alpha=\{\alpha_i\}$ and $\beta=\{\beta_i\}$ sequences of distinct nonzero elements of the ring of integers of $\mathbb{Q}(\sqrt{-d})$. On applying the identity (2) and taking norms of both sides we see, for all integer k satisfying $0\leq k\leq m-1$, that

$$\prod_{1\leq i<j\leq m}\mathcal{N}(\alpha_i-\alpha_j)=R^{km-k(k+1)}\mathcal{N}(\det_k(\alpha,\beta)). \tag{10}$$

Let us verify that for any integer k with $0\leq k\leq m-1$,

$$|\mathcal{N}(\det_k(\alpha,\beta))|\geq|d|^{t(m)},\quad\text{where}\quad t(m)=\left[\frac{1}{2}\left(\frac{m^2}{2}-m\right)\right]+1.$$

Indeed, let p be a prime divisor of d. If h of the x_i belong to the same residue class modulo p, then $v_p(\prod_{1\leq i<j\leq m}\mathcal{N}(\alpha_i-\alpha_j))\geq h(h-1)/2$. Since $x_i^2\equiv R \bmod p$, each x_i lies in one of no more than 2 residue classes modulo p. Consequently, for some integer h, $0\leq h\leq m$, we have

$$v_p\Big(\prod_{1\leq i<j\leq m}\mathcal{N}(\alpha_i-\alpha_j)\Big)\geq\frac{h(h-1)}{2}+\frac{(m-h)(m-h-1)}{2}\geq t(m). \tag{11}$$

Suppose that p divides d but not R. It then follows from (10) that $v_p(\mathcal{N}(\det_k(\alpha,\beta)))=v_p(\prod_{1\leq i<j\leq m}\mathcal{N}(\alpha_i-\alpha_j))$ and hence $v_p(\mathcal{N}(\det_k(\alpha,\beta)))\geq t(m)$ for such primes p. Suppose now that p divides d and R. Then each of the ideals $\langle\alpha_i\rangle$ and $\langle\beta_i\rangle$ in the ring A of integers of $\mathbb{Q}(\sqrt{-d})$ is divisible by $\mathfrak{p}$, the unique prime ideal lying above the ramified prime p in $\mathbb{Q}(\sqrt{-d})$. On expanding the determinants $\det_k(\alpha,\beta)$ with respect to any row, we see that for all integers k with $0\leq k\leq m-1$,

$$v_{\mathfrak{p}}(\langle\det_k(\alpha,\beta)\rangle)\geq\frac{k(k+1)}{2}+\frac{(m-1-k)(m-k)}{2}\geq t(m)\,, \tag{12}$$

where $\langle\det_k(\alpha,\beta)\rangle$ is the ideal generated by $\det_k(\alpha,\beta)$ in A. Thus, we have $v_p(\mathcal{N}(\det_k(\alpha,\beta)))\geq t(m)$ even in the case when p divides d and R. Since d is a squarefree integer, we deduce that $|\mathcal{N}(\det_k(\alpha,\beta))|\geq|d|^{t(m)}$. On combining this lower bound with (9) and (10) we then conclude that for all integers k

satisfying $0 \le k \le m-1$,

$$(|d|l^2)^{\binom{m}{2}} > (R^2)^{(km/2-k(k+1)/2)}|d|^{t(m)}. \tag{13}$$

Finally, on using (ii) of Lemma 2.2 and recalling the definitions of $s(m)$ and $r(m)$, we see that $l > |R|^{s(m)}/|d|^{r(m)}$. In other words, when m is an odd integer ≥ 2 there are no more than $m-1$ integer points on any arc of length $|R|^{s(m)}/|d|^{r(m)}$ on the conic $X^2 + dY^2 = R$.

Remark 2.1. Theorem 1.2 in [6] states that if $d \ne 0, 1$ is a fixed square-free integer, then on the conic $X^2 - dY^2 = N$, an arc of length N^α with $\alpha = 1/4 - 1/(8[k/2]+4)$ contains at most k lattice points. This statement, as well as Theorem 1 of [3], appears to be inaccurate with regard to the dependence of the lengths of the arcs on d. As Example 2.1 below shows, there are infinitely many integers $R \ge 1$ such that there are arcs of length $2^{13/6}R^{1/6}/d^{1/3}$ containing three integer points on the ellipses $X^2+dY^2 = R^2$ for any integer $d \ge 1$, while Theorem 1.2 of [6] implies that there are no more than two integer points on any arc of length $R^{1/6}$ on these conics.

The following example was kindly supplied to the author by Prof. Joseph Oesterlé.

Example 2.1. Let t and d be integers ≥ 1 and let $u = d^2t + dt - d + 1$. Let $p_i = (x_i, y_i)$, $1 \le i \le 3$, be points in the plane with coordinates x_i, y_i given below:

$$\begin{aligned} x_1 &= dt(2dt-1)u - 1, & y_1 &= t(2dt+1)u + 1,\\ x_2 &= x_1 + 2dt + 2, & y_2 &= y_1 - 2dt,\\ x_3 &= x_1 - 2dt, & y_3 &= y_1 + 2dt - 2. \end{aligned} \tag{14}$$

We then verify that $x_i^2 + dy_i^2 = x_1^2 + dy_1^2$ for $1 \le i \le 3$ and, on setting $R = x_1^2+dy_1^2$, we see that all the p_i are integer points on the ellipse $X^2+dY^2 = R$. Set $D = \sup_{1\le i<j\le 3} \|p_i - p_j\|_2$ and let l be the length of the shortest arc on the ellipse containing all the p_i. Then as $t \to +\infty$ we have

$$R \sim 4d^7(d+1)t^6, \qquad D \sim 4\sqrt{2}\,dt, \qquad l \sim D, \tag{15}$$

where the relation $l \sim D$ follows on noting that $D/R^{1/2} \to 0$ as $t \to +\infty$. Since $d \ge 1$, it follows from (15) that

$$l < \frac{2^{13/6}R^{1/6}}{d^{1/3}} \quad \text{for all sufficiently large } t. \tag{16}$$

Example 2.1 shows that the conclusion of Theorem 1.1 is essentially (that is, up to a constant) best possible for $m = 2$. Prof. Cilleruelo kindly informed the author that A. Granville and himself have constructed examples that show that the exponent of R provided by this theorem when $m = 3$ is also best possible when the conic in question is a circle. It is not known if this still is the case for $m \geq 4$. Indeed, a recent conjecture (Conjecture 14 on page 11 of [4]) of J. Cilleruelo and A. Granville predicts a considerable improvement on Theorem 1.1, at least when the conic in question is a circle, when m is large. On page 15 of the same article, Cilleruelo and Granville give a flowchart relating their conjecture to a number of other interesting conjectures on the interface between Fourier analysis and number theory.

3. Notes. The author arrived at the identity $(*)$ of Section 1 as one way of generalising the elementary formula $abc = 4\Delta R$, where a, b and c are the sides of a triangle, Δ its area and R the radius of its circumcircle. Indeed, if one applies the identity with $m = 3$, $k = 1$, α_i elements of $\mathbb{C}$ denoting the vertices of the triangle, $\beta_i = \overline{\alpha}_i$, $\gamma = R^2$, one arrives at the formula $abc = 4\Delta R$ on taking absolute values of both sides of the resulting relation and noting that $|\det_1(\alpha, \beta)| = 4\Delta$. The use of the formula $abc = 4\Delta R$ in obtaining the case of Theorem 1.1 when $m = 2$ and when the conic in this theorem is a circle is described on page 899 of [2].

The use of a relation between matrices of the form $(f_i(x_j))$ and (x_j^{i-1}), where x_j are elements of a commutative ring A—usually a subring of the complex numbers—and f_i suitable functions on this ring, the index i varying over the integers in an interval $[1, k]$ and j in a finite set, to study the gaps between the x_j is well known in the context of the Bombieri–Pila method. Indeed, even the simplest of such relations, namely the case when the f_i are polynomials, may be used to deduce interesting conclusions, as for example, in the second proof of Theorem 10 on page 7 of [4]; the identity $(*)$ may certainly be viewed from this perspective as well.

Finally, we note that there are applications, described in [7], of even the particular case of the overlapping theorem that we have been concerned with here, on which the identity of this article does not shed any light.

Acknowledgments. Throughout the course of preparing this article the author benefitted considerably from correspondence with Prof. J. Cilleruelo, from whose works, in particular those with Prof. G. Tenenbaum and Prof. A. Granville, the author learnt of a number of results relevant to the content of this article. The author expresses his gratitude to these scholars as well as to Prof. Olivier Ramaré, Dr. T. D. Browning and Dr. Gyan Prakash, who very kindly went through a number of versions of this article and provided the author with several useful suggestions.

References

[1] R. de la Bretèche, *Nombre de valeurs polynomiales qui divisent un entier*, Math. Proc. Cambridge Philos. Soc. 131 (2001), 193–209.

[2] J. Cilleruelo and A. Córdoba, *Trigonometric polynomials and lattice points*, Proc. Amer. Math. Soc. 115 (1992), 899–905.
[3] —, —, *Lattice points on ellipses*, Duke Math. J. 76 (1994), 741–750.
[4] J. Cilleruelo and A. Granville, *Lattice points on circles, squares in arithmetic progressions and sumsets of squares*, math.NT/0608109, 2006.
[5] J. Cilleruelo and J. Jiménez-Urroz, *Lattice points on hyperbolas*, J. Number Theory 63 (1997), 267–274.
[6] —, —, *Divisors in a Dedekind domain*, Acta Arith. 85 (1998), 229–233.
[7] J. Cilleruelo and G. Tenenbaum, *An overlapping theorem with applications*, preprint, 2005, 9 pp.
[8] H. W. Lenstra, Jr., *Divisors in residue classes*, Math. Comp. 42 (1984), 331–340.

Harish-Chandra Research Institute
Chhatnag Road, Jhunsi
Allahabad 211 019, India
E-mail: suri@mri.ernet.in

Received on 20.3.2007
and in revised form on 20.10.2007 (5416)