Mathematika 12 (1965), 176-192.

THE DISTRIBUTION OF SOLUTIONS OF CONGRUENCES

J. H. H. Chalk *and* K. S. Williams

1. *Introduction.* Let p be an odd prime and denote by $[p]$, the finite field of residue classes, mod p. In Euclidean n-space, let $\mathscr{L}_n$ denote the lattice of points $\mathbf{x}=(x_1, \ldots, x_n)$ with integral coordinates and $C=C(n, p)$, the set of points of $\mathscr{L}_n$ satisfying

$$0 \leqslant x_i < p, \quad (i=1, 2, \ldots, n). \tag{1}$$

We define a box $\mathfrak{B}=\mathfrak{B}(n, \mathbf{h}, \boldsymbol{\nu})$ as the set of points $\mathbf{x} \in C$ for which

$$\nu_i \leqslant x_i < \nu_i + h_i, \quad (i=1, 2, \ldots, n) \tag{2}$$

where

$$0 \leqslant \nu_i < \nu_i + h_i \leqslant p, \quad (i=1, 2, \ldots, n). \tag{3}$$

For $n \geqslant 2$, let $f(\mathbf{x})=f(x_1, x_2, \ldots, x_n)$ be a polynomial in the n variables $x_1, x_2, \ldots, x_n$ of degree $d \geqslant 2$, fixed independently of p, and with coefficients in $[p]$. If $f(\mathbf{x})$ is not homogeneous in $x_1, \ldots, x_n$, we introduce the associated forms, F and f^*, defined by

$$F(x_0, x_1, \ldots, x_n) = x_0{}^d f(x_1/x_0, \ldots, x_n/x_0) \tag{4}$$

and

$$f^*(x_1, \ldots, x_n) = F(0, x_1, \ldots, x_n). \tag{5}$$

Let $N(\mathfrak{B}) = N(p, n, f, \mathfrak{B})$ denote the number of $\mathbf{x} \in \mathfrak{B}$ for which

$$f(\mathbf{x}) = 0, \quad [p] \tag{6}$$

where, for convenience, we count $\mathbf{x}=\mathbf{0}$ as a solution when $\mathbf{0} \in \mathfrak{B}$ and $f(\mathbf{x})$ is a form. Thus in the special case when $\mathfrak{B}=C$, the integer $N(C)$ is just the number of solutions of the congruence $f(\mathbf{x}) \equiv 0 \pmod p$, while generally, $N(\mathfrak{B})$ represents the number of solutions in certain prescribed residue classes (namely, those defined by the points of $\mathfrak{B}$), of the same congruence. By using a generalization of the inequalities of Vinogradov [**11**] and Mordell [**8**] we shall obtain estimates for $N(\mathfrak{B})$ in terms of $N(C)$ for "general" polynomials $f(\mathbf{x})$, when p is large. This general inequality was established in [**3**] and relevant details are summarized in the following lemma:

Lemma 1. *Let $f(\mathbf{x})$ be a function defined over $[p]$ and taking values in $[p]$ and put*†

$$\mathscr{F}(\mathbf{y}) = \sum_{\mathbf{x} \in C} \sum_{t=0}^{p-1} e\{tf(\mathbf{x}) - \mathbf{x}.\mathbf{y}\}, \tag{7}$$

$$\mathscr{E}(\mathfrak{B}) = \sum_{\mathbf{0} \neq \mathbf{y} \in C} \left| \sum_{\mathbf{z} \in \mathfrak{B}} e(\mathbf{y}.\mathbf{z}) \right|. \tag{8}$$

† For any real t, $e(t)$ stands for $\exp(2\pi i t p^{-1})$.

Suppose that there is a constant Φ, *independent of* $\mathbf{y}$, *such that*

$$|\mathscr{F}(\mathbf{y})| \leqslant \Phi, \textit{ for all non-zero } \mathbf{y} \in C. \tag{9}$$

Then

$$N(\mathfrak{B}) = h_1 \dots h_n p^{-n} N(C) + \theta p^{-n-1} \Phi \mathscr{E}(\mathfrak{B}) \tag{10}$$

for some real number θ *satisfying* $|\theta| \leqslant 1$. *Moreover,* $\mathscr{E}(\mathfrak{B}) \leqslant C p^n \log^n p$, *for some absolute constant* $C > 0$. (11)

For convenience in referring to the inequality (10), we shall speak of $h_1 \dots h_n p^{-n} N(C)$ and $p^{-n-1} \Phi \mathscr{E}(\mathfrak{B})$ as the main and error terms, respectively. Note that the only reference to $\mathfrak{B}$ in the error term occurs in $\mathscr{E}(\mathfrak{B})$, since Φ is merely a bound for the *complete* exponential sum $\mathscr{F}(\mathbf{y})$. We remark that the estimate for $\mathscr{E}(\mathfrak{B})$ in (11) is essentially best possible in the absence of any further restriction on the box $\mathfrak{B}$, for it can be easily verified that $\mathscr{E}(\mathfrak{B}) \geqslant k p^n \log^n p$ for some absolute constant $k > 0$ in the special case $\nu_i = 1$, $h_i = (p-1)/2$, $(i = 1, 2, \dots, n)$, when p is large enough. It is of interest, therefore, to find an estimate Φ for $\mathscr{F}(\mathbf{y})$ which is sufficiently good, for p large, to ensure that the main term dominates the error term when the "sides" h_i of the box $\mathfrak{B}$ are also large but bounded by $O(p^{1-\delta})$, for some fixed $\delta > 0$ depending on n (and possibly on d). This has been done in some special cases, *e.g.* for quadratic and diagonal polynomials (see [**3**], [**8**] and [**9**]). Results can also be obtained for other special polynomials when good estimates are known for the exponential sum in (7). In the general case, however, some restriction on $f(\mathbf{x})$ is essential, *e.g.* we have to exclude polynomials such as $f(\mathbf{x}) = x_1^d$, for then $N(\mathfrak{B}) = 0$ whenever $\nu_1 > 0$. Roughly speaking, we require $N(C)$ large and Φ small. The crude estimate for $\mathscr{F}(\mathbf{y})$ is $pN(C)$, since on taking absolute values in (7) we have

$$|\mathscr{F}(\mathbf{y})| = \left| \sum_{\mathbf{x} \in C} e(-\mathbf{x}.\mathbf{y}) \sum_{t=0}^{p-1} e\big(tf(\mathbf{x})\big) \right| \leqslant \sum_{\mathbf{x} \in C} \left| \sum_{t=0}^{p-1} e\big(tf(\mathbf{x})\big) \right| = pN(C), \tag{12}$$

and inspection of (10) shows that virtually any improvement on this would be effective for our purpose. In Theorem 1 we find that, for forms $f(\mathbf{x})$ which have no linear factor over $[p]$, there is an improvement (by a factor which is about p when $N(C)p^{-n+1}$ is bounded below) on the estimate in (12):

THEOREM† 1. *Let* $f(x)$ *be a form over* $[p]$, *of degree* $d \geqslant 2$, *which admits no linear factors over* $[p]$. *Then*

$$N(\mathfrak{B}) = h_1 \dots h_n p^{-n} N(C) + O(p^{n-2} \log^n p), \textit{ as } p \to \infty. \tag{13}$$

† **Here, and throughout the paper, the constant in the O-symbol depends only upon n and d, unless explicitly stated otherwise.**

COROLLARY 1. *If*

$$f(\mathbf{x}) = \eta \prod_{i=1}^{t} [f_i(\mathbf{x})]^{\alpha_i}, \quad [p], \quad (\eta \text{ a unit}) \tag{14}$$

where $f_i(\mathbf{x})$ *are the irreducible factors of* $f(\mathbf{x})$ *over* $[p]$, $\deg f_i \geqslant 2$ $(i = 1, 2, \ldots, t)$ *and* $s \geqslant 1$ *of these are absolutely irreducible (i.e. irreducible over the algebraic closure of* $[p]$*), then*

$$N(\mathfrak{B}) = h_1 \ldots h_n p^{-n}\{sp^{n-1} + O(p^{n-3/2})\} + O(p^{n-2}\log^n p), \text{ as } p \to \infty. \tag{15}$$

COROLLARY 2. *If* $0 < \epsilon < n^{-1}$, *let* $\nu_i \geqslant 0$ $(i = 1, 2, \ldots, n)$ *be chosen arbitrarily subject only to the condition* $\nu_i + p^{1-n^{-1}+\epsilon} < p$. *Then, provided* (15) *holds, there is an integer* $p_0 = p_0(\epsilon, n, d)$ *and an* $\mathbf{x} \in C$ *for which* $f(\mathbf{x}) = 0$ $[p]$ *and*

$$\nu_i \leqslant x_i < \nu_i + p^{1-n^{-1}+\epsilon}, \quad (i = 1, 2, \ldots, n) \tag{16}$$

if $p \geqslant p_0$.

Our method depends upon an interpretation of $\mathscr{F}(\mathbf{y})$ in terms of the numbers of solutions of pairs of simultaneous equations over $[p]$ (see Lemma 11), and appears to be useful only when $f(\mathbf{x})$ is homogeneous and the number of such pairs reduces to one. As the properties of $\mathscr{F}(\mathbf{y})$ are vital to the effectiveness of the general inequality (10), we include in §3 an alternative, but generally less useful, interpretation of $\mathscr{F}(\mathbf{y})$ in terms of equations obtained from $f(\mathbf{x}) = 0$ $[p]$ by the addition of certain linear terms (again, this works only for forms when the homogeneity can be exploited). If we regard $\mathscr{F}(\mathbf{y})$ as a complete exponential sum over $(n+1)$ variables $(x_1, \ldots, x_n, t)$ the estimates of Davenport and Lewis [**5**] (for $d = 3$) and Birch [**2**] are applicable, but the results will involve the determination of certain invariants of $f(\mathbf{x})$ over $[p]$, or over the algebraic closure of $[p]$. In the latter case, for example, if $K = 2^{-d+1}$ and s is defined as the dimension of the singular locus of $f(\mathbf{x})$ (see [**5**]) in the n-dimensional vector space of points $\mathbf{x}$ over the algebraic closure of $[p]$, then Birch's result gives

$$\mathscr{F}(\mathbf{y}) = O\{p^{n+1-K(n-s)}\}, \tag{17}$$

which is effective in (10) when $N(C)p^{-n+1}$ is bounded below and

$$s < n - 2^{d-1}. \tag{18}$$

So far as estimates for $N(C)$ are concerned, we use the general theorem of Lang and Weil [**6**] on the number of points in an algebraic variety over a finite field. As Birch and Lewis [**1**] have observed, this specializes to the case of forms $f(\mathbf{x})$ over $[p]$, which are absolutely irreducible over $[p]$, to give the asymptotic formula

$$N(C) = p^{n-1} + O(p^{n-3/2}), \text{ as } p \to \infty. \tag{19}$$

Corollary 1 is an elementary deduction from this and Theorem 1 (see Lemma 8). In fact we have $N(C) = O(p^{n-2})$, unless the form f has at least one absolutely irreducible factor over $[p]$. For polynomials $f(\mathbf{x})$ which are not homogeneous we have no direct method of attack, though the simple device of working with the form $F(x_0, x_1, \ldots, x_n)$ in place of $f(x_1, \ldots, x_n)$, and a "flat" box $\mathfrak{B}_0$ in $(n+1)$-dimensions satisfying $x_0 = 1$ is partially successful. However, the formula (13) with $n+1$ in place of n, applied to a form $F(x_0, x_1, \ldots, x_n)$ with $N(C)$ about p^n is clearly ineffective, since the main term is no larger than p^{n-1}, while the error is $p^{n-1}\log^{n+1}p$. This raises the question of whether the error term in (13) itself can be improved. But the example with $f(x) = (x_1^2 + x_2^2)^m, p \equiv 3 \pmod 4)$ $\nu_i = p - h_i = 1$, $(i = 1, 2, \ldots, n)$ in which f has no linear factors over $[p]$ and

$$|N(\mathfrak{B}) - h_1 \ldots h_n p^{-n} N(C)| = (1-p^{-1})^n p^{n-2} \sim p^{n-2} \text{ as } p \to \infty,$$

shows that some further condition on $f(\mathbf{x})$ is essential for such an improvement. In Theorem 2 we impose the restriction that the form $f(\mathbf{x})$ be non-singular† and show that this leads to an improvement of about $p^{-1/2}$ in the error term. In addition, it is easily shown that such forms are in general absolutely irreducible (*cf.* Lemma 9) and consequently (19) is applicable:

THEOREM 2. *If $f(\mathbf{x})$ is a non-singular form of degree d in $n \geqslant 2d+1$ variables then*

$$N(\mathfrak{B}) = h_1 \ldots h_n p^{-n} N(C) + O(p^{n-5/2}\log^n p) \text{ as } p \to \infty. \tag{20}$$

COROLLARY 1. *If $f(\mathbf{x})$ is a non-singular form of degree d in $n \geqslant 2d+1$ variables, then*

$$N(\mathfrak{B}) = h_1 \ldots h_n p^{-n}\{p^{n-1} + O(p^{n-3/2})\} + O(p^{n-5/2}\log^n p), \tag{21}$$

as $p \to \infty$.

COROLLARY 2. *If $0 < \epsilon < 3/2n$, let $\nu_i \geqslant 0$ $(i = 1, 2, \ldots, n)$ be chosen arbitrarily subject only to the condition $\nu_i + p^{1-(3/2n)+\epsilon} < p$. Then, provided (21) holds, there is an integer $p_0 = p_0(\epsilon, n, d)$ and an $\mathbf{x} \in C$ for which $f(\mathbf{x}) = 0$ $[p]$ and*

$$\nu_i \leqslant x_i < \nu_i + p^{1-(3/2n)+\epsilon}, \quad (i = 1, 2, \ldots, n) \tag{22}$$

if $p \geqslant p_0$.

Use of Chevalley's theorem [4] on the existence of a non-trivial zero $[p]$ of a system of simultaneous equations over $[p]$ is a convenient tool in the proof of Theorem 2 and gives rise to the condition on the number n of variables. Then, with the device of the "flat box" in $(n+1)$-dimensions, we deduce

† *i.e.*, for any $\mathbf{x} \neq \mathbf{0}$ of C, the n partial derivatives of the first order do not vanish simultaneously.

Theorem 3. *If $f(\mathbf{x})$ is a polynomial in n variables $x_1, \ldots, x_n$ of degree $d \leqslant n/2$ and*

$$F(x_0, x_1, \ldots, x_n) = x_0^d f(x_1/x_0, \ldots, x_n/x_0)$$

is non-singular, then for $f(\mathbf{x})$,

$$N(\mathfrak{B}) = h_1 \ldots h_n p^{-1} + O(p^{n-3/2} \log^{n+1} p), \text{ as } p \to \infty. \tag{23}$$

Corollary. *If $0 < \epsilon < 1/2n$, let $\nu_i \geqslant 0$ $(i = 1, 2, \ldots, n)$ be chosen arbitrarily only to the condition $\nu_i + p^{1-(2n)^{-1}+\epsilon} < p$. Then provided* (23) *holds, there is an integer $p_0 = p_0(\epsilon, n, d)$ and an $\mathbf{x} \in C$ for which $f(\mathbf{x}) = 0$ $[p]$ and*

$$\nu_i \leqslant x_i < \nu_i + p^{1-(2n)^{-1}+\epsilon}, \quad (i = 1, 2, \ldots, n) \tag{24}$$

if $p \geqslant p_0$.

With regard to the corollaries where the existence of a solution of $f(\mathbf{x}) = 0$ $[p]$ satisfying certain asymmetric inequalities is asserted, it is natural to enquire whether methods from the geometry of numbers are applicable. For the special case when $f(\mathbf{x})$ is homogeneous and the box $\mathfrak{B}$ is symmetric in $\mathbf{0}$, Minkowski's theorem on convex bodies is useful; for if $(\xi_1, \ldots, \xi_n) \neq (0, \ldots, 0)$ $[p]$ is some solution of $f(\mathbf{x}) = 0$ $[p]$, the subset of $\mathscr{L}_n$ defined by

$$(x_1, \ldots, x_n) = h(\xi_1, \ldots, \xi_n) \; [p], \quad h \in [p],$$

is a lattice Λ of determinant p^{n-1} and so there is a point $\mathbf{x} \neq \mathbf{0}$ of Λ in the cube

$$|x_i| \leqslant p^{1-n^{-1}} \quad (i = 1, 2, \ldots, n)$$

and this point will satisfy $f(\mathbf{x}) = 0$ $[p]$, by the homogeneity of† $f(\mathbf{x})$. However, for the general case, we have no information.

2. *Estimation of $N(C)$.* In 1954 Lang and Weil [**6**] deduced (as a consequence of Weil's work on algebraic curves) an estimate for the number of points of an absolutely irreducible variety V, of algebraic dimension r and degree d in m-dimensional projective space P^m over a finite field k_q with q elements. As pointed out by Birch and Lewis [**1**], the following lemma is the special case of this with $r = m - 1 = n - 2$ and $q = p$.

Lemma 2. *If $f(\mathbf{x})$ is an absolutely irreducible form‡ over $[p]$ in n variables and of degree d then*

$$N(C) = p^{n-1} + O(p^{n-3/2}), \text{ as } p \to \infty. \tag{25}$$

They also deduced from Lang and Weil's paper the following two lemmas.

---

† A special case of this was communicated to one of us by Dr. G. L. Watson.

‡ We remark that an absolutely irreducible form in n variables defines an absolutely irreducible variety in projective $(n-1)$-space of dimension $r = n-2$; for this, and the converse, see *e.g.* [**12**; Proposition 2, p. 74].

LEMMA 3. *If $f(\mathbf{x})$ is a form which is irreducible over $[p]$, but not absolutely irreducible, then all the zeros of $f(\mathbf{x})$ are singular.*

LEMMA 4. *If $f(\mathbf{x})$ is a form over $[p]$ of degree d in n variables with no squared factors over $[p]$, then the number N^* of singular zeros of f satisfies*

$$N^* = O(p^{n-2}), \text{ as } p \to \infty. \tag{26}$$

Combining Lemmas 3 and 4, we have

LEMMA 5. *If $f(\mathbf{x})$ is a form which is irreducible over $[p]$, but not absolutely irreducible, then*

$$N(C) = O(p^{n-2}), \text{ as } p \to \infty. \tag{27}$$

The bound for $N(C)$ in the following lemma is well known; a proof, by induction on n, was given by S. H. Min [7] in 1947.

LEMMA 6. *Let $f(\mathbf{x})$ be a polynomial with coefficients in $[p]$, not identically zero. Then*

$$N(C) = O(p^{n-1}), \text{ as } p \to \infty. \tag{28}$$

A similar result can be deduced for a pair of polynomials†; to do this we use the fact that if $F_1(\mathbf{x}), \ldots, F_k(\mathbf{x})$ are k polynomials over $[p]$, at least one of which does not vanish identically, then there exist k polynomials $\Phi_1(\mathbf{x}), \ldots, \Phi_k(\mathbf{x})$ over $[p]$, such that

$$F_1\Phi_1 + \ldots + F_k\Phi_k = d\Omega,$$

where $d = d(\mathbf{x})$ is the highest common factor of $F_1, \ldots, F_k$ and Ω is a polynomial over $[p]$ which does not vanish identically and in which the variable x_1 does not appear (for a proof, see [**10**; p. 192, Satz 101]). Further, the degree of Ω is bounded in terms of the degrees of $F_1, \ldots, F_k$. Here, the special rôle played by the variable x_1 could equally well be taken by any of the other variables x_r $(2 \leqslant r \leqslant n)$. We also note that the greatest common divisor is unique, apart from units; in particular, the greatest common divisor of f and g over $[p]$ will be denoted by $(f, g)_p$. If either f or g is independent of some x_i, *i.e.* it is a polynomial in x_j $(j \neq i$: $j = 1, 2, \ldots, n)$, then so is $(f, g)_p$. Thus if, say f, is identically zero then $(f, g)_p = g$, apart from unit factors.

LEMMA‡ 7. *If $f(\mathbf{x})$ and $g(\mathbf{x})$ are polynomials in $\mathbf{x} = (x_1, \ldots, x_n)$, where $n \geqslant 2$, with coefficients in $[p]$, of degrees k_1 and k_2 respectively, such that $(f, g)_p = 1$, then the number of solutions of the pair of simultaneous equations*

$$f(\mathbf{x}) = g(\mathbf{x}) = 0, \quad [p],$$

† We are indebted to Professor H. A. Heilbronn, for a remark which suggested a lemma of this type.

‡ By elementary deductive arguments, it may be shown that this lemma is equivalent to Lemma 4. It would be of interest to know whether our elementary version of Lemma 7 is capable of extension to three or more polynomials.

is $O(p^{n-2})$, *where the constant implied in the O-symbol depends only on* n, k_1 *and* k_2.

Proof. We first prove the result for $n=2$. Since

$$\big(f(x_1, x_2), g(x_1, x_2)\big)_p = 1$$

we can find $a_1(x_1, x_2), a_2(x_1, x_2), b_1(x_1, x_2), b_2(x_1, x_2), \Omega_1(x_1) \neq 0$ and $\Omega_2(x_2) \neq 0$ such that

$$a_1 f + b_1 g = \Omega_1(x_1),$$

and

$$a_2 f + b_2 g = \Omega_2(x_2).$$

Thus $N(f=g=0) \leqslant N(\Omega_1 = \Omega_2 = 0) = O(1)$.

We now suppose that $n \geqslant 3$ and make the inductive hypothesis that the result is true for all polynomials in $(n-1)$ variables satisfying the conditions of the lemma. We consider three cases:

Case (i). Suppose that for some fixed i $(1 \leqslant i \leqslant n)$, f and g are polynomials in x_j $(j=1, 2, \ldots, n)$ with $j \neq i$. Then we can apply the inductive hypothesis to the pair f, g and obtain

$$N(f=g=0) = O(p \cdot p^{(n-1)-2}) = O(p^{n-2}),$$

since to each set $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ there corresponds at most p values for x_i.

Case (ii). We now show that it is sufficient to consider the case when at least one of f and g is a polynomial in at most $n-1$ of $x_1, \ldots, x_n$. For, if $(f, g)_p = 1$, we can find polynomials a_1 and b_1 and a polynomial $\Omega = \Omega(x_2, \ldots, x_n)$, independent of x_1, satisfying

$$a_1 f + b_1 g = \Omega(x_2, \ldots, x_n).$$

If $d_1 = (g, \Omega)_p$, then $d_1 = d_1(x_2, \ldots, x_n)$ and $(f, d_1)_p = 1$. Putting $g = d_1 g_1$, $\Omega = d_1 \Omega_1$, where $(g_1, \Omega_1)_p = 1$, we have

$$\begin{aligned} N(f=g=0) &= N(f=g=\Omega=0) \\ &= N(f=d_1 g_1 = d_1 \Omega_1 = 0) \\ &\leqslant N(g_1 = \Omega_1 = 0 : d_1 \neq 0) + N(f = d_1 = 0) \\ &\leqslant N(g_1 = \Omega_1 = 0) + N(f = d_1 = 0). \end{aligned}$$

Since Ω_1 and d_1 are independent of x_1 and

$$(g_1, \Omega_1)_p = (f, d_1)_p = 1$$

it suffices to consider the case described.

Case (iii). Suppose now that g, say, does not contain x_1. Proceed as in Case (ii), and define $a_1, b_1, \Omega, d_1, g_1, \Omega_1$. If $d_1=1$, then

$$N(f=g=0)\leqslant N(g_1=\Omega_1=0)$$

and Case (i) can be applied to give the required result. If $d_1\neq 1$, we get

$$N(f=g=0)\leqslant N(g_1=\Omega_1=0)+N(f=d_1=0)$$

just as for Case (ii). Since $g=d_1g_1$ is independent of x_1 so is g_1 and since $(g_1, \Omega_1)_p=1$, Case (i) applies to $N(g_1=\Omega_1=0)$. Also, for $N(f=d_1=0)$, we note that d_1 is independent of x_1 and $(f, d_1)_p=1$. Hence the pair f and d_1 satisfy the same hypotheses as the pair f and g. Moreover, d_1 is a non-unit divisor of g and therefore has lower degree than that of g. Hence the process can be repeated and after a certain number of steps, bounded in terms of the degree of g, we reach the condition $(d_r, \Omega_r)_p=1$ when the inductive hypothesis is applicable. Thus, writing $g=d_0$, we have

$$\begin{aligned}N(f=g=0)&=N(f=d_0=0)\\&\leqslant N(g_1=\Omega_1=0)+\ldots+N(g_{r-1}=\Omega_{r-1}=0)+N(f=d_r=0),\end{aligned}$$

where $$N(g_t=\Omega_t=0)=O(p^{n-2}),\quad (1\leqslant t\leqslant r-1)$$

by Case (i), and

$$N(f=d_r=0)\leqslant N(d_r=\Omega_r=0)=O(p^{n-2}),$$

by our induction hypothesis. Moreover, the constants implied in the O-symbols are, by our process, bounded in terms of n, k_1 and k_2. This proves the lemma. We can now prove

LEMMA 8. *Let $f(\mathbf{x})$ be a form of degree d in n variables, with coefficients in $[p]$, which does not vanish identically. Let s denote the number of absolutely irreducible factors over $[p]$ in the unique decomposition (apart from units and order) of $f=f_1^{\alpha_1}\ldots f_r^{\alpha_r}$ into powers of irreducible factors. Then*

$$N(C)=O(p^{n-2}),\ \text{as } p\to\infty,\ \text{if } s=0 \tag{29}$$

and

$$N(C)=sp^{n-1}+O(p^{n-3/2}),\ \text{as } p\to\infty,\ \text{if } s\geqslant 1. \tag{30}$$

Proof. Since

$$\begin{aligned}N(C)&=N\big(f(\mathbf{x})=0\big)\\&=N(f_1\ldots f_r=0)\\&=\sum_{1\leqslant i\leqslant r}N(f_i=0)-\sum_{1\leqslant i<j\leqslant r}N(f_i=f_j=0)+\ldots\\&\qquad\qquad+(-1)^{r-1}N(f_1=\ldots=f_r=0),\end{aligned}$$

we have

$$\Big|N(C)-\sum_{1\leqslant i\leqslant r}N(f_i=0)\Big|=O\Big\{\max_{1\leqslant i<j\leqslant r}N(f_i=f_j=0)\Big\}=O(p^{n-2}),$$

by Lemma 7. Thus if $f_1, \ldots, f_s$, say, are absolutely irreducible over $[p]$,

$$N(C) = \sum_{1 \leqslant i \leqslant s} \left(p^{n-1} + O(p^{n-3/2})\right) + \sum_{s+1 \leqslant i \leqslant r} O(p^{n-2}) + O(p^{n-2})$$

$$= sp^{n-1} + s \,.\, O(p^{n-3/2}) + O(p^{n-2}),$$

as required.

The next two lemmas are required for the proof of Theorems 2 and 3. They tell us, roughly, that if $f(\mathbf{x})$ is a non-singular form over $[p]$, then both $f(\mathbf{x})$ and $f(x_1, \ldots, x_{n-1}, 0)$ are absolutely irreducible over $[p]$, if n is large enough.

Lemma 9. *If $f(\mathbf{x})$ is a non-singular form over $[p]$ of degree d in $n \geqslant d+1$ variables, then $f(\mathbf{x})$ is absolutely irreducible over $[p]$.*

Proof. Suppose, if possible, that the conclusion is false for some such f. Then there are two possibilities; case (a), f is irreducible but not absolutely irreducible over $[p]$, case (b), f is reducible over $[p]$.

Case (a). Since $n \geqslant d+1$, Chevalley's theorem **[4]** implies the existence of at least one non-zero solution $\mathbf{x}$ of $f(\mathbf{x}) = 0$ $[p]$. By Lemma 3, this is a singular zero of f; a contradiction.

Case (b). Suppose $f = gh$, where $\deg g = d_1$, $\deg h = d_2$ and $d_1 + d_2 = d$. As $n \geqslant d+1$, (*i.e.* $n > d_1 + d_2$) Chevalley's theorem tells us that there is a non-zero solution of $g = h = 0$. But for such a solution we have

$$\frac{\partial f}{\partial x_i} = g\frac{\partial h}{\partial x_i} + h\frac{\partial g}{\partial x_i} = 0, \quad (i = 1, 2, \ldots, n),$$

whence it is a singular zero of f; a contradiction.

Remark. The following example shows that the converse is false, *i.e.* there exist absolutely irreducible forms of degree d in $n \geqslant d+1$ variables which are singular over $[p]$. Take

$$f(\mathbf{x}) = x_1 x_2^{d-1} - x_n^{d}, \tag{31}$$

where $n \geqslant d+1 > 3$; then f is absolutely irreducible over $[p]$ (see **[1**; Lemma 3]), but has a singular zero $(1, 0, \ldots, 0)$.

Lemma 10. *Let $f(\mathbf{x})$ be a non-singular form over $[p]$ in $n \geqslant 2d+1$ variables. Then $f(x_1, \ldots, x_{n-1}, 0)$ is absolutely irreducible over $[p]$.*

Proof. Put

$$f(x_1, \ldots, x_n) = a_d x_n^{d} + a_{d-1} x_n^{d-1} + \ldots + a_1 x_n + a_0,$$

where

$$a_i = a_i(x_1, \ldots, x_{n-1}), \quad i = 0, 1, 2, \ldots, d,$$

is a form of degree $d-i$, which possibly vanishes identically, and $a_0=f(x_1, \ldots, x_{n-1}, 0)$. By Lemma 9, $f(\mathbf{x})$ is absolutely irreducible over $[p]$ since $n \geqslant 2d+1 \geqslant d+1$. Hence it is irreducible over $[p]$ and a_0 cannot vanish identically. Now suppose a_0 is not absolutely irreducible over $[p]$. Then there are two possibilities; case (a), a_0 is irreducible over $[p]$ but is not absolutely irreducible over $[p]$, case (b), a_0 is reducible over $[p]$.

Case (a). By Chevalley's Theorem [4], there is a non-zero solution $(x_1^*, \ldots, x_{n-1}^*)$ satisfying $a_0=a_1=0$, since $n-1>d+(d-1)$, *i.e.* $n \geqslant 2d+1$. By Lemma 3, such a solution is a singular zero of a_0. Hence the partial derivatives $\dfrac{\partial a_0}{\partial x_i}$ $(i=1, 2, \ldots, n-1)$ vanish at $(x_1, \ldots, x_{n-1})=(x_1^*, \ldots, x_{n-1}^*)$. Put $\mathbf{x}^*=(x_1^*, \ldots, x_{n-1}^*, 0) \neq \mathbf{0}$. Since

$$\frac{\partial f}{\partial x_i}=\frac{\partial a_d}{\partial x_i}x_n{}^d+\ldots+\frac{\partial a_1}{\partial x_i}x_n+\frac{\partial a_0}{\partial x_i}, \quad (i=1, 2, \ldots, n-1)$$

the derivatives $\dfrac{\partial f}{\partial x_i}$ $(i=1, 2, \ldots, n-1)$ vanish at $\mathbf{x}=\mathbf{x}^*$, and since

$$\frac{\partial f}{\partial x_n}=a_d\, d x_n{}^{d-1}+\ldots+a_2\, 2x_n+a_1,$$

$\dfrac{\partial f}{\partial x_n}$ vanishes when $\mathbf{x}=\mathbf{x}^*$. Hence $\mathbf{x}^*$ is a singular zero of f, contradicting the hypothesis that f is non-singular over $[p]$.

Case (b). Suppose $a_0=hk$ $[p]$, where $\deg h=d_1$, $\deg k=d_2$ and $d_1+d_2=d$. By Chevalley's Theorem [4], there is a solution

$$(x_1^*, \ldots, x_{n-1}^*) \neq (0, \ldots, 0)$$

satisfying $h=k=a_1=0$ over $[p]$, since $n-1>d_1+d_2+(d-1)$, *i.e.* $n \geqslant 2d+1$. Then the argument of Case (a) is applicable and we can show, similarly, that $(x_1^*, \ldots, x_{n-1}^*, 0)$ is a singular zero of f, contradicting our hypothesis for f. Hence $a_0=f(x_1, \ldots, x_{n-1}, 0)$ is absolutely irreducible over $[p]$.

3. *Estimation of* $\mathscr{F}(\mathbf{y})$.

Definition. Let $a(u, \mathbf{y})=a(u, \mathbf{y}, p, f, C)$ denote the number of solutions $\mathbf{x} \in C$ of the pair of simultaneous equations

$$f(\mathbf{x})=\mathbf{x}.\mathbf{y}-u=0 \ [p]. \tag{32}$$

Firstly, we express $\mathscr{F}(\mathbf{y})$, as defined in (7), in terms of $a(u, \mathbf{y})$ in

LEMMA 11. $$\mathscr{F}(\mathbf{y})=p\sum_{u=0}^{p-1} e(-u)\,a(u, \mathbf{y}). \tag{33}$$

Proof. From (7) we have

$$\begin{aligned}\mathscr{F}(\mathbf{y}) &= \sum_{\mathbf{x}\in C}\sum_{t=0}^{p-1} e\big(tf(\mathbf{x})-\mathbf{x}.\mathbf{y}\big)\\ &= \sum_{\mathbf{x}\in C} e(-\mathbf{x}.\mathbf{y})\sum_{t=0}^{p-1} e\big(tf(\mathbf{x})\big)\\ &= \sum_{u=0}^{p-1}\sum_{\substack{\mathbf{x}\in C\\ \mathbf{x}.\mathbf{y}=u}} e(-\mathbf{x}.\mathbf{y})\sum_{t=0}^{p-1} e\big(tf(\mathbf{x})\big)\\ &= \sum_{u=0}^{p-1}\sum_{\substack{\mathbf{x}\in C\\ \mathbf{x}.\mathbf{y}=u}} e(-u)\sum_{t=0}^{p-1} e\big(tf(\mathbf{x})\big)\\ &= \sum_{u=0}^{p-1} e(-u)\sum_{\substack{\mathbf{x}\in C\\ \mathbf{x}.\mathbf{y}=u}}\sum_{t=0}^{p-1} e\big(tf(\mathbf{x})\big).\end{aligned}$$

From the definition of $a(u, \mathbf{y})$ we have

$$a(u,\mathbf{y}) = \frac{1}{p}\sum_{\substack{\mathbf{x}\in C\\ \mathbf{x}.\mathbf{y}=u}}\sum_{t=0}^{p-1} e\big(tf(\mathbf{x})\big) \tag{34}$$

and the lemma follows.

Next, we note the following two properties of $a(u, \mathbf{y})$ which lead to the interpretation of $\mathscr{F}(\mathbf{y})$ in Lemma 15.

LEMMA 12.
$$\sum_{u=0}^{p-1} a(u,\mathbf{y}) = N(C). \tag{35}$$

Proof. Trivial.

LEMMA 13. *If* $u \neq 0$ $[p]$, *then* $a(u, \mathbf{y}) = a(1, \mathbf{y})$. (36)

Proof. As $u\neq 0$ $[p]$, u^{-1} is uniquely defined by $uu^{-1}=1$. Then the substitution $\mathbf{x}=u\mathbf{z}$ maps C onto itself. Hence

$$\begin{aligned}a(u,\mathbf{y}) &= \frac{1}{p}\sum_{\substack{\mathbf{z}\in C\\ \mathbf{z}.\mathbf{y}=1}}\sum_{t=0}^{p-1} e\big(tf(u\mathbf{z})\big)\\ &= \frac{1}{p}\sum_{\substack{\mathbf{z}\in C\\ \mathbf{z}.\mathbf{y}=1}}\sum_{t=0}^{p-1} e\big(tu^d f(\mathbf{z})\big),\end{aligned}$$

since f is homogeneous of degree d. As $u\neq 0$ $[p]$, the substitution $v=tu^d$ permutes $[p]$. Thus

$$a(u,\mathbf{y}) = \frac{1}{p}\sum_{\substack{\mathbf{z}\in C\\ \mathbf{z}.\mathbf{y}=1}}\sum_{v=0}^{p-1} e\big(vf(\mathbf{z})\big) = a(1,\mathbf{y}).$$

LEMMA 14. *If* $u\neq 0$ $[p]$, *then*

$$a(u,\mathbf{y}) = (p-1)^{-1}\{N(C)-a(0,\mathbf{y})\}. \tag{37}$$

Proof. By Lemmas 12 and 13,

$$a(0, \mathbf{y}) + (p-1)\, a(u, \mathbf{y}) = N(C),$$

since $u \neq 0$ $[p]$.

LEMMA 15.
$$\mathscr{F}(\mathbf{y}) = \frac{p}{p-1}\{pa(0, \mathbf{y}) - N(C)\}. \tag{38}$$

Proof. By Lemma 11,

$$\mathscr{F}(\mathbf{y}) = p\sum_{u=0}^{p-1} e(-u)\, a(u, \mathbf{y})$$

$$= p\left\{a(0, \mathbf{y}) + \sum_{u=1}^{p-1} e(-u)\, a(u, \mathbf{y})\right\},$$

$$= p\left\{a(0, \mathbf{y}) + \sum_{u=1}^{p-1} e(-u)\left[\frac{N(C) - a(0, \mathbf{y})}{p-1}\right]\right\},$$

$$= p\left\{a(0, \mathbf{y}) - \frac{N(C) - a(0, \mathbf{y})}{p-1}\right\},$$

$$= \frac{p}{p-1}\{pa(0, \mathbf{y}) - N(C)\},$$

on using Lemma 14.

With this interpretation of $\mathscr{F}(\mathbf{y})$ the estimates available for $a(0, \mathbf{y})$ in Lemma 7 and for $N(C)$ in Lemma 8 are sufficient for our proof of Theorem 1. For Theorems 2, 3 we shall need a more precise estimate for $a(0, \mathbf{y})$:

LEMMA 16. *If $f(\mathbf{x})$ is a form of degree d, which is non-singular over $[p]$ and in $n \geqslant 2d+1$ variables then*

$$a(0, \mathbf{y}) = p^{n-2} + O(p^{n-5/2}) \tag{39}$$

uniformly in $0 \neq \mathbf{y} \in C$.

Proof. By definition $a(0, \mathbf{y})$ is the number of $\mathbf{x} \in C$ satisfying the pair of equations

$$f(\mathbf{x}) = \mathbf{x}.\mathbf{y} = 0, \quad [p].$$

Since $\mathbf{y} \neq \mathbf{0}$ $[p]$, we can transform $\mathbf{x}$ into $\mathbf{x}'$ by a non-singular, homogeneous, linear transformation so that the above pair becomes

$$f_1(\mathbf{x}') = x_n' = 0, \ [p].$$

This does not affect $a(0, \mathbf{y})$ nor the non-singularity of f, but the coefficients of f_1 will now depend on the y_i's. Thus $a(0, \mathbf{y})$ is just the number of solutions $(x_1', \ldots, x_{n-1}', 0)$ of

$$f_1(x_1', \ldots, x_{n-1}', 0) = 0.$$

By Lemma 10, $f_1(x_1', \ldots, x_{n-1}', 0)$ is absolutely irreducible over $[p]$ and so, by Lemma 2, we have

$$a(0, \mathbf{y}) = p^{n-2} + O(p^{n-5/2}), \text{ as } p \to \infty$$

uniformly in $\mathbf{0} \neq \mathbf{y} \in C$.

We give here an alternative interpretation of $\mathscr{F}(\mathbf{y})$ which is useful in special cases but not, however, effective for our general problem.

LEMMA 17. *Let $f(\mathbf{x})$ be a form in $x_1, \ldots, x_n$ of degree $d \geqslant 2$, with coefficients in $[p]$. Let k_{p-1} be the multiplicative group of $[p]$ and k_m the subgroup of k_{p-1} consisting of the $(d-1)$-th powers, where the order of k_m is $m = \frac{p-1}{l}$, $l = (d-1, p-1)$. Let $n_1, n_2, \ldots, n_l$ be elements of k_{p-1}, one from each coset of k_m relative to k_{p-1}. Then*

$$\mathscr{F}(\mathbf{y}) = \frac{p}{l} \sum_{i=1}^{l} N\Big(C, f(\mathbf{x}) - n_i \mathbf{x}.\mathbf{y}\Big) - p^n. \tag{40}$$

Proof. If the elements of k_m are denoted by $r_1, r_2, \ldots, r_m$, the cosets $\mathscr{C}_i$ can be represented by $\{n_i^{-1} r_1, \ldots, n_i^{-1} r_m\}$, $(i = 1, 2, \ldots, l)$. Then, for $\mathbf{y} \neq \mathbf{0}$ $[p]$,

$$\begin{aligned}
\mathscr{F}(\mathbf{y}) &= \sum_{t=1}^{p-1} \sum_{\mathbf{x} \in C} e\{tf(\mathbf{x}) - \mathbf{x}.\mathbf{y}\} \\
&= \sum_{i=1}^{l} \sum_{t \in \mathscr{C}_i} \sum_{\mathbf{x} \in C} e\{tf(\mathbf{x}) - \mathbf{x}.\mathbf{y}\} \\
&= \sum_{i=1}^{l} \sum_{\mathbf{x} \in C} \sum_{j=1}^{m} e\{n_i^{-1} r_j f(\mathbf{x}) - \mathbf{x}.\mathbf{y}\} \\
&= \frac{1}{l} \sum_{i=1}^{l} \sum_{\mathbf{x} \in C} \sum_{u=1}^{p-1} e\{n_i^{-1} u^{d-1} f(\mathbf{x}) - \mathbf{x}.\mathbf{y}\},
\end{aligned}$$

since $u^{d-1} = r_j$ $[p]$ has exactly l solutions u, for each $j = 1, 2, \ldots, m$. Put $\mathbf{x} = u^{-1}\mathbf{z}$ $[p]$, so that C is mapped onto itself over $[p]$ and note that

$$f(u^{-1}\mathbf{z}) = u^{-d} f(\mathbf{z}).$$

Then

$$\begin{aligned}
\mathscr{F}(\mathbf{y}) &= \frac{1}{l} \sum_{i=1}^{l} \sum_{\mathbf{z} \in C} \sum_{u=1}^{p-1} e\{u^{-1}[n_i^{-1} f(\mathbf{z}) - \mathbf{z}.\mathbf{y}]\} \\
&= \frac{1}{l} \sum_{i=1}^{l} \sum_{\mathbf{x} \in C} \sum_{u=1}^{p-1} e\{u[n_i^{-1} f(\mathbf{x}) - \mathbf{x}.\mathbf{y}]\}, \\
&= \frac{1}{l} \sum_{i=1}^{l} \sum_{\mathbf{x} \in C} \left[\left\{\sum_{u=0}^{p-1} e[u(n_i^{-1} f(\mathbf{x}) - \mathbf{x}.\mathbf{y})]\right\} - 1\right], \\
&= \frac{p}{l} \sum_{i=1}^{l} N\Big(C, n_i^{-1} f(\mathbf{x}) - \mathbf{x}.\mathbf{y}\Big) - p^n,
\end{aligned}$$

as required.

4. *Proof of Theorem* 1. By Lemmas 6 and 7,

$$N(C)=O(p^{n-1})$$

$$a(0,\mathbf{y})=O(p^{n-2}),\ \text{uniformly in } \mathbf{y}.$$

Hence, by Lemma 15,

$$\mathscr{F}(\mathbf{y})=O(p^{n-1}),$$

so we may take $\Phi=O(p^{n-1})$ in Lemma 1, obtaining the result.

Proof of Corollary 1. This is immediate on substituting the estimate for $N(C)$ given by Lemma 8 in the theorem.

Proof of Corollary 2. For arbitrary ϵ satisfying $0<\epsilon<n^{-1}$, take $h_i=[p^{1-n^{-1}+\epsilon}]$ and $\nu_i\geqslant 0$ (subject to $\nu_i+p^{1-n^{-1}+\epsilon}<p$) in Corollary 1; then

$$h_1\dots h_n p^{-n}\{sp^{n-1}+O(p^{n-3/2})\}=O(p^{n-2+n\epsilon})$$

exceeds the error term $O(p^{n-2}\log^n p)$ for $p\geqslant p_0=p_0(\epsilon,n,d)$, so $N(\mathfrak{B})>0$ and the result follows.

Proof of Theorem 2. By Lemma 9, $f(\mathbf{x})$ is absolutely irreducible over $[p]$ since $n\geqslant 2d+1\geqslant d+1$. Thus, by Lemma 2, $N(C)=p^{n-1}+O(p^{n-3/2})$. Also, by Lemma 16, $a(0,\mathbf{y})=p^{n-2}+O(p^{n-5/2})$ and so from Lemma 15 we have $\mathscr{F}(\mathbf{y})=O(p^{n-3/2})$ for $\mathbf{y}\neq\mathbf{0}$. The theorem then follows from Lemma 1 with $\Phi=O(p^{n-3/2})$.

Proof of Corollary 1. This is immediate on substituting the estimate for $N(C)$ from Lemma 8.

Proof of Theorem 3. Applying Theorem 2, with n replaced by $n+1$, to the box $\mathfrak{B}_0$ and the form F, we have

$$N(\mathfrak{B}_0,F)=h_1\dots h_n p^{-n-1}N(C_{n+1},F)+O(p^{n-3/2}\log^{n+1}p),$$

as $p\to\infty$. By Lemma 9, F is absolutely irreducible over $[p]$ and so, by Lemma 2,

$$N(C_{n+1},F)=p^n+O(p^{n-1/2}).$$

Since $N(\mathfrak{B}_0,F)=N(\mathfrak{B},f)$, the result follows.

The proofs of the corollaries to Theorems 2 and 3 are straightforward and follow the lines of that for Corollary 2 of Theorem 1.

5. *Extension to Galois Fields*. Let k_q denote the finite field of $q=p^m$ elements and write k_p for $[p]$. Select any fixed basis $\alpha_1,\dots,\alpha_m$ for k_q; then any $\alpha\in k_q$ may be expressed as

$$\alpha=c_1\alpha_1+\dots+c_m\alpha_m$$

with $c_i \in k_p$ $(i = 1, 2, \ldots, m)$. Denote the trace of α from k_q to k_p by $t(\alpha)$, so that

$$t(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{m-1}} \in k_p$$

and $t(\alpha+\beta) = t(\alpha) + t(\beta)$, for all α and β in k_q.

If we put

$$e(\alpha) = \exp\{2\pi i p^{-1} t(\alpha)\},$$

then it is easy to verify that the orthogonal property

$$\sum_{\alpha \in k_q} e(\lambda\alpha) = \begin{cases} q, & \text{if } \lambda = 0 \\ 0, & \text{otherwise,} \end{cases}$$

for the case $m = 1$, is preserved. We can now extend the definition of the box $\mathfrak{B}$ to the vector space V of points $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ over k_q, relative to our chosen basis, by

$$\mathfrak{B} = \{\mathbf{x} \mid \mathbf{x} \in V,\ x_i = c_{i1}\alpha_1 + \ldots + c_{im}\alpha_m,\ 0 \leqslant \nu_{ij} \leqslant c_{ij} < \nu_{ij} + h_{ij} \leqslant p\},$$

where $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$. It is now a routine matter to check that Lemma 1 goes through as it stands, but with p replaced by q and $[p]$ replaced by k_q, apart from the estimate for $\mathscr{E}(\mathfrak{B})$ in (11). With $\mathscr{E}(\mathfrak{B})$ defined as

$$\sum_{\mathbf{0} \neq \mathbf{y} \in V} \left| \sum_{\mathbf{z} \in \mathfrak{B}} e(\mathbf{y}.\mathbf{z}) \right|,$$

we shall repair this deficiency in Lemma 18. We note also that the estimates in §2 (see Lemmas 6, 7 and 8) which are used in the proof of Theorem 1 and its first corollary are readily extended to k_q. Then Theorem 1, for example, has the following generalization:

THEOREM 1′. *Let $f(\mathbf{x})$ denote a form over k_q, of degree $d \geqslant 2$, which admits no linear factors over k_q. If $N(V)$ denotes the number of zeros of $f(\mathbf{x})$ in V, then*

$$N(\mathfrak{B}) = \left(\prod_{i,j=1}^{n,m} h_{ij} \right) q^{-n} N(V) + O(q^{n-\frac{1}{2}} \log^{mn} p), \tag{41}$$

where the constant in the O-symbol depends at most on m and n.

Counterparts for the other theorems about $N(\mathfrak{B})$ may also be given, since the only new idea required is that in Lemma 18; the proof of which follows:

LEMMA 18. *There is an absolute constant p_0 such that*

$$\sum_{\mathbf{y} \in V} \left| \sum_{\mathbf{z} \in \mathfrak{B}} e(\mathbf{y}.\mathbf{z}) \right| < q^n (\log p)^{mn}, \tag{42}$$

for all $p \geqslant p_0$, $m \geqslant 1$, $n \geqslant 1$.

Proof. Since the given sum splits into a product of n sums of the type

$$\sum_{y_i \in k_q} \left| \sum_{z_i \in \mathfrak{B}_i} e(y_i z_i) \right|,$$

where

$$\mathfrak{B}_i = \{z_i | z_i \in k_q,\ z_i = c_{i1}\alpha_1 + \ldots + c_{im}\alpha_m,\ \nu_{ij} \leqslant c_{ij} < \nu_{ij} + h_{ij}\},$$

$1 \leqslant j \leqslant m$, it is sufficient to prove that this is less than $(p \log p)^m$, under the conditions stated. Dropping the subscripts i and writing

$$y = b_1\alpha_1 + \ldots + b_m\alpha_m$$

$$z = c_1\alpha_1 + \ldots + c_m\alpha_m$$

$$\nu_{ij} = \nu_j,\ h_{ij} = h_j$$

for convenience, this sum has the shape

$$\sum_{b_1=0}^{p-1} \cdots \sum_{b_m=0}^{p-1} \left| \sum_{c_1=\nu_1}^{\nu_1+h_1-1} \cdots \sum_{c_m=\nu_m}^{\nu_m+h_m-1} e\{(b_1\alpha_1 + \ldots + b_m\alpha_m)(c_1\alpha_1 + \ldots + c_m\alpha_m)\} \right|. \quad (43)$$

Now, the inner sums over $c_1, \ldots, c_m$ can be expressed as

$$\prod_{k=1}^{m} \sum_{c_k=\nu_k}^{\nu_k+h_k-1} \exp\{2\pi i p^{-1} \eta_k c_k\},$$

where

$$\eta_k = \sum_{j=1}^{m} b_j t(\alpha_j \alpha_k).$$

The $m \times m$ matrix

$$T = \{t(\alpha_j \alpha_k)\}$$

has determinant

$$[\det(\alpha_j^{p^{k-1}})]^2,$$

and, as is well known [see, *e.g.*, L. E. Dickson, *Linear Groups* (Dover, 1958), p. 52], this cannot vanish when $\alpha_1, \ldots, \alpha_m$ are linearly independent over k_p. Hence $\det T \not\equiv 0 \pmod p$ and so the m-dimensional vector space V_m of points $\mathbf{b} = (b_1, \ldots, b_m)$ is mapped onto itself by T. Thus $\sum_{\mathbf{b} \in V_m}$ can be replaced by $\sum_{\boldsymbol{\eta} \in V_m}$, where $\boldsymbol{\eta} = T\mathbf{b}$, and our sum (43) becomes

$$\prod_{k=1}^{m} \sum_{\eta_k=0}^{p-1} \left| \sum_{c_k=\nu_k}^{\nu_k+h_k-1} \exp\{2\pi i p^{-1} \eta_k c_k\} \right|.$$

Each of the m sums in this product is less than $p \log p$ (see, *e.g.*, [**11**; Ch. III, 11c]) for $p \geqslant 60$ and so (42) holds with $p_0 = 60$.

References

1. B. J. Birch and D. J. Lewis, "p-adic forms", *J. Indian Math. Soc.*, 23 (1959), 11–32.
2. B. J. Birch, "Forms in many variables", *Proc. Roy. Soc.* (A), 265 (1962), 245–263. (See [5] p. 652.)
3. J. H. H. Chalk, "The number of solutions of congruences in incomplete residue systems", *Canadian J. of Math.*, 15 (1963), 291–296.

4. C. Chevalley, " Démonstration d'une hypothèse de M. Artin ", *Abh. Math. Sem. Hamburg.*, 11 (1935), 73–75.
5. H. Davenport and D. J. Lewis, " Exponential sums in many variables ", *American J. of Math.*, 84 (1962), 649–665.
6. S. Lang and A. Weil, " Number of points of varieties in finite fields ", *American J. of Math.*, 76 (1954), 819–827.
7. S. H. Min, " On systems of algebraic equations and certain multiple exponential sums ". *Quart. J. of Math.*, (Oxford), 18 (1947), 133–142.
8. L. J. Mordell, " On the number of solutions in incomplete residue sets of quadratic congruences ", *Archiv der Math.*, 8 (1957), 153–157.
9. ———, " Incomplete exponential sums and incomplete residue systems for congruences ", Чехословацкий Математический Журнал (*Czech. Math. J.*), 14 (1964), 235–242.
10. O. Perron, *Algebra* I (2nd. ed. Berlin 1932).
11. I. M. Vinogradov, *Elements of number theory*, (Dover 1954), Chap. V, problem 12a, p. 102.
12. A. Weil, *Foundations of algebraic geometry* (New York), Amer. Math. Soc. Colloq. Pub., 29 (1946).

Department of Mathematics,
University of Toronto,
Toronto, Canada.

(*Received on the 25th of January, 1965.*)

Printed by C. F. Hodgson & Son, Ltd., Pakenham Street, London, W.C.1