NON-HOMOGENEOUS CUBIC EQUATIONS

H. DAVENPORT *and* D. J. LEWIS

1. *Introduction*

Let $\phi(x_1, \ldots, x_n) = \phi(\mathbf{x})$ be a cubic polynomial in n variables with integral coefficients, say

$$\phi = C(x_1, \ldots, x_n) + Q(x_1, \ldots, x_n) + L(x_1, \ldots, x_n) + N, \tag{1}$$

where C, Q, L are cubic, quadratic and linear forms respectively and N is an integer. We shall suppose that ϕ is not degenerate, that is, that ϕ cannot be transformed into a cubic polynomial in fewer than n variables by any integral unimodular linear substitution (not necessarily homogeneous) on the variables. This does not preclude the possibility that the cubic form C may degenerate, but we shall suppose that C does not vanish identically.

Our object is to prove that under certain conditions the equation

$$\phi(x_1, \ldots, x_n) = 0 \tag{2}$$

will have a solution in integers; and in fact our conditions will be such as to ensure that there are infinitely many solutions and to enable us to say something about their distribution.

It was proved recently† that a *homogeneous* cubic equation always has a non-trivial integral solution if $n \geqslant 16$. But it is easily seen that no condition on the size of n can suffice to ensure the solubility of non-homogeneous equations. In the first place, the following congruence condition is obviously necessary for solubility, and this condition need not be satisfied however large n is postulated to be.

Congruence condition. The congruence

$$\phi(x_1, \ldots, x_n) \equiv 0 \pmod{p^\nu} \tag{3}$$

is soluble‡ for every prime power p^ν.

For the analogous problem with a quadratic polynomial instead of a cubic polynomial, the congruence condition together with the supposition that the quadratic part of the polynomial is indefinite, is sufficient§ to

Received 3 August, 1963. This paper was completed during a period in which the authors received support from the National Science Foundation under Grant GP 88.

† H. Davenport, " Cubic forms in sixteen variables ", *Proc. Royal Soc.* (A), 272 (1963), 285–303. This paper was based in part on an earlier paper: " Cubic forms in 32 variables ", *Phil. Trans. Royal Soc.* (A), 251 (1959), 193–232. These papers will be referred to as C.F.16 and C.F.32, respectively.

‡ The zero solution is admissible, both in (3) and (2).

§ See G. L. Watson, " Indefinite quadratic Diophantine equations ", *Mathematika*, 8 (1961), 32–38 (Theorem 1).

[JOURNAL LONDON MATH. SOC., 39 (1964), 657–671]

ensure integral solubility provided $n \geqslant 5$. But a similar result cannot hold for cubic polynomials. This is illustrated by the following simple example (due to Dr. G. L. Watson):

$$\phi = (2x_1-1)(1+x_1^2+\ldots+x_n^2)+x_1x_2.$$

It is easily proved that the congruence condition is satisfied if $n \geqslant 5$, but the equation $\phi = 0$ is insoluble in integers since

$$|\phi| \geqslant 1+x_1^2+x_2^2-|x_1x_2| > 0.$$

A supplementary condition is therefore needed, and we shall give such a condition in terms of an invariant $h(C)$ of the cubic part C of ϕ, which we introduced recently[†] in a different context. We define $h = h(C)$ to be the least positive integer such that $C(x_1, \ldots, x_n)$ is expressible identically as

$$L_1(x_1, \ldots, x_n)\, Q_1(x_1, \ldots, x_n)+\ldots+L_h(x_1, \ldots, x_n)\, Q_h(x_1, \ldots, x_n), \tag{4}$$

where $L_1, \ldots, L_h$ and $Q_1, \ldots, Q_h$ are linear and quadratic forms respectively, with rational[‡] coefficients. Equivalently, we can define $n-h$ to be the greatest dimension of any rational linear space contained in the hypersurface $C = 0$; in the representation (4) such a linear space is given by

$$L_1 = L_2 = \ldots = L_h = 0.$$

Plainly $h(C) \leqslant n$, and since C does not vanish identically we have $h(C) \geqslant 1$.

By a combination of the methods used in C.F.16 and E.S., we shall prove

THEOREM 1. *Suppose that $h(C) \geqslant 17$ and that ϕ satisfies the congruence condition. Then the equation* (2) *has infinitely many solutions in integers.*

This will be a consequence of an asymptotic formula which we shall establish (in Lemma 8) for the number of integer solutions of $\phi = 0$ with $(x_1, \ldots, x_n)$ in a suitable box whose linear dimensions are proportional to P, as $P \to \infty$; the main term in the asymptotic formula being of order P^{n-3}.

The results apply in the special case when ϕ is homogeneous, *i.e.* when $\phi = C$, in which case the congruence condition is trivially satisfied. Thus, provided $h(C) \geqslant 17$, we get an asymptotic formula of the kind just described, for the solutions of $C(x_1, \ldots, x_n) = 0$. This formula supplements the results of C.F.16, where no such asymptotic formula was proved because the work of that paper presupposed that C did not represent zero.

[†] "Exponential sums in many variables", *American J. of Math.*, 84 (1962), 649–665. This will be referred to as E.S.

[‡] It is easily proved that $L_1, \ldots, L_h$ and $Q_1, \ldots, Q_h$ can in fact be taken to have integral coefficients.

Nor would such a formula be true without *some* condition on $h(C)$. For if, say, $h = 2$, we could express C identically as

$$L_1 Q_1 + L_2 Q_2,$$

and the solutions of $C = 0$ with $L_1 = L_2 = 0$ in a box of the kind described above are in number proportional to P^{n-2}.

The invariant h of $C(x)$ can also be regarded as an invariant of the polynomial $\phi(x)$, under integral unimodular substitutions (not necessarily homogeneous), since ϕ determines C uniquely. We can restate the significance of h in relation to ϕ, as follows. We consider any polynomial equivalent to ϕ, and ask what is the maximum number in a subset of variables which do not occur in this polynomial to the third power. The greatest number, for all equivalent polynomials, is $n-h$. This follows easily from the earlier definition of h, since the cubic part of ϕ in (4) is equivalent to

$$x_1 Q_1'(x_1, \ldots, x_n) + \ldots + x_h Q_h'(x_1, \ldots, x_n),$$

and here $x_{h+1}, \ldots, x_n$ do not occur to the third power. The argument is reversible.

It may be as well to remark that the value of h is not independent of the field of coefficients; it may diminish if the field is extended.

In a companion paper to this one, Dr. Watson establishes the solubility of $\phi = 0$, subject to the congruence condition, when $4 \leqslant h \leqslant n-4$ and $n \geqslant 20$. His work is based on the interpretation of h just given, which implies that an equivalent equation becomes quadratic (at most) in $n-h$ variables when h variables are given any constant values. Combining the results of both papers, we obtain

THEOREM 2. (Davenport, Lewis, Watson.) *If*

$$n \geqslant 20 \text{ and } h(C) \geqslant 4$$

and if ϕ satisfies the congruence condition, then (2) *is soluble in integers.*

Returning to the present paper, we remark that it is essential, in connection with the asymptotic formula of Lemma 8, to show that the sum of the *singular series* associated with the equation $\phi = 0$ is positive. The usual way of establishing this is to prove that for every prime p the equation $\phi = 0$ has a non-singular integral solution in the p-adic number field. This is equivalent to saying that for every ν there is a solution of the congruence (3) for which one at least of the partial derivatives

$$\partial\phi/\partial x_1, \ldots, \partial\phi/\partial x_n$$

is divisible only by a power of p which is bounded independently of ν. We shall deduce the truth of this from the simpler congruence condition stated earlier. We prove

THEOREM 3. *If $n \geqslant 15$ and if ϕ satisfies the congruence condition, then the equation $\phi = 0$ has a non-singular integral solution in every p-adic field.*

This result is used also in Dr. Watson's paper. The condition that $n \geqslant 15$ is best possible. For consider the example

$$\phi = x_1^2 - Nx_2^2 + p(x_3^2 - Nx_4^2)$$
$$+p^2\Big(x_5 x_1^2 + x_6 x_1 x_2 + x_7 x_1 x_3 + x_8 x_1 x_4 + x_9 x_2^2$$
$$+x_{10} x_2 x_3 + x_{11} x_2 x_4 + x_{12} x_3^2 + x_{13} x_3 x_4 + x_{14} x_4^2\Big)$$

in 14 variables, where p is a prime and N is a quadratic non-residue mod p. This polynomial is non-degenerate and satisfies the congruence condition trivially (with all the variables 0), but the only integral p-adic solutions are those with $x_1 = x_2 = x_3 = x_4 = 0$, and these are all singular.

2. *Proof of Theorem* 3

It will be convenient to prove a slightly more general result: we shall allow the coefficients of ϕ to be p-adic integers instead of restricting them to being rational integers. This generalization does not affect the meaning of the congruence condition, and it is immaterial in (3) whether $x_1, \ldots, x_n$ are rational integers or p-adic integers.

We suppose that ϕ does not degenerate in the p-adic field, that is, under linear substitutions with p-adic integral coefficients. It is easily seen that a polynomial with rational integral coefficients which does not degenerate in the rational field also does not degenerate in any extension of that field, and in particular in the p-adic field. For a polynomial ϕ can be transformed into a polynomial in $n-1$ variables by a non-singular linear substitution (not necessarily homogeneous) if and only if there exist numbers $t_1, \ldots, t_n$ such that

$$t_1 \partial\phi/\partial x_1 + \ldots + t_n \partial\phi/\partial x_n = 0$$

identically in $x_1, \ldots, x_n$. This identity is equivalent to a system of homogeneous linear equations in $t_1, \ldots, t_n$, and if this system is soluble at all it is soluble in the rational field.

We have to prove that the equation $\phi = 0$ has a non-singular p-adic integral solution. That is, we have to prove that for every ν there exist $x_1, \ldots, x_n$ satisfying (3) and such that the highest power of p dividing all of $\partial\phi/\partial x_j$ is bounded independently of ν. Here again it is immaterial whether $x_1, \ldots, x_n$ are rational integers or p-adic integers.

Let $\mathscr{A}(p^l)$ denote the condition that there exist $x_1, \ldots, x_n$ such that

$$\phi(x_1, \ldots, x_n) \equiv 0 \pmod{p^{2l-1}}$$

and

$$\partial\phi/\partial x_j \equiv 0 \pmod{p^{l-1}} \text{ for all } j,$$
$$\partial\phi/\partial x_j \not\equiv 0 \pmod{p^l} \text{ for some } j.$$

Then for the existence of a non-singular p-adic integral solution it is necessary and sufficient that the condition $\mathscr{A}(p^l)$ shall be satisfied for some l. The necessity is immediate, on taking p^{l-1} to be the highest power of p dividing all $\partial\phi/\partial x_j$ at the hypothetical non-singular solution. The sufficiency is proved by a well-known process ("Newton approximation" or "Hensel's lemma") which continues the solution $(\bmod p^{2l-1})$ to a solution $(\bmod p^{\nu})$ for every $\nu > 2l-1$.

The condition $\mathscr{A}(p^l)$ was used in C.F.32 (p. 197 *et seq.*), though in that paper only cubic forms were being considered.

We now proceed with the proof of Theorem 3. By hypothesis there is a solution $\mathbf{x}^{(\nu)}$ of

$$\phi(\mathbf{x}) \equiv 0 \pmod{p^{\nu}}$$

for every positive integer ν. The sequence $\mathbf{x}^{(\nu)}$ has at least one limit point in the p-adic sense as $\nu \to \infty$; if $\boldsymbol{\alpha}$ is such a limit point then $\boldsymbol{\alpha}$ is a p-adic integral point which satisfies $\phi(\boldsymbol{\alpha}) = 0$. By replacing $\mathbf{x}$ by $\mathbf{x}+\boldsymbol{\alpha}$, we can suppose without loss of generality that $\boldsymbol{\alpha} = 0$. Hence (1) becomes

$$\phi(\mathbf{x}) = C(\mathbf{x})+Q(\mathbf{x})+L(\mathbf{x}).$$

If $L(\mathbf{x})$ does not vanish identically the solution $\mathbf{x} = 0$ is non-singular, since the coefficients in $L(\mathbf{x})$ are the values of the partial derivatives $\partial\phi/\partial x_j$ at this point. Thus we can suppose that

$$\phi(\mathbf{x}) = C(\mathbf{x})+Q(\mathbf{x}). \tag{5}$$

Case 1. *Suppose* $Q(\mathbf{x}) = 0$ *identically.* Then $\phi(\mathbf{x}) = C(\mathbf{x})$ is a non-degenerate cubic form in n variables with p-adic integral coefficients. We can approximate to $C(\mathbf{x})$ arbitrarily precisely, in the p-adic sense, by a form $C_1(\mathbf{x})$ with rational integral coefficients. The arithmetical invariant† used in C.F.32, the vanishing of which expresses the degeneracy of the form, will be different from zero for $C_1(\mathbf{x})$, since it is different from zero for $C(\mathbf{x})$. By Lemma 2.8 of C.F.32, since $n \geqslant 10$, the form $C_1(\mathbf{x})$ satisfies the condition $\mathscr{A}(p^l)$ for some l, and from the proof of that lemma it will be seen that l is bounded in terms of the power to which p divides the arithmetical invariant of $C_1(\mathbf{x})$. If the approximation to $C(\mathbf{x})$ by $C_1(\mathbf{x})$ is sufficiently precise, this will be the same as the power to which p divides the arithmetical invariant of $C(\mathbf{x})$, and so will be bounded. Further, if the approximation is sufficiently precise, the fact that $C_1(\mathbf{x})$ has the property $\mathscr{A}(p^l)$ implies that $C(\mathbf{x})$ has the property $\mathscr{A}(p^l)$. Hence the result.

Case 2. *Suppose the quadratic form* $Q(\mathbf{x})$ *has rank* 5 *or more.* Then $Q(\mathbf{x})$ is equivalent to a non-degenerate quadratic form in 5 or more variables. It is well known that such a form represents zero non-trivially

† The invariant in question is denoted by $h(C)$ in C.F.32, but has no connection with the $h(C)$ of the present paper.

in the p-adic field, and the representation is necessarily non-singular. Hence there exists a p-adic integral point $\boldsymbol{\beta}$ at which

$$Q(\boldsymbol{\beta}) = 0, \quad Q^{(j)}(\boldsymbol{\beta}) \neq 0 \text{ for some } j,$$

where the superscript denotes a partial derivative.

Let p^{λ} be the highest power of p dividing all the numbers $Q^{(j)}(\boldsymbol{\beta})$, so that

$$Q^{(j)}(\boldsymbol{\beta}) \not\equiv 0 \pmod{p^{\lambda+1}} \text{ for some } j.$$

Choose $\nu > 2\lambda+1$ and take $\boldsymbol{\gamma} = p^{\nu}\boldsymbol{\beta}$. Then

$$\phi(\boldsymbol{\gamma}) = C(\boldsymbol{\gamma}) + Q(\boldsymbol{\gamma}) = p^{3\nu} C(\boldsymbol{\beta}) + 0 \equiv 0 \pmod{p^{3\nu}}.$$

Also, for some j,

$$C^{(j)}(\boldsymbol{\gamma}) = p^{2\nu} C^{(j)}(\boldsymbol{\beta}) \equiv 0 \pmod{p^{2\nu}},$$

$$Q^{(j)}(\boldsymbol{\gamma}) = p^{\nu} Q^{(j)}(\boldsymbol{\beta}) \not\equiv 0 \pmod{p^{\nu+\lambda+1}}.$$

Hence

$$\phi^{(j)}(\boldsymbol{\gamma}) \not\equiv 0 \pmod{p^{\nu+\lambda+1}}.$$

Since $3\nu \geqslant 2(\nu+\lambda+1)-1$, the polynomial $\phi(\mathbf{x})$ has the property $\mathscr{A}(p^{l})$ for some $l \leqslant \nu+\lambda+1$, and this proves the result.

Case 3. *Suppose* $Q(\mathbf{x})$ *has rank* $r = 1, 2, 3$ *or* 4. By a unimodular p-adic integral linear transformation from $\mathbf{x}$ to $\mathbf{y}$ we can express $Q(\mathbf{x})$ in (5) as $R(y_1, \ldots, y_r)$ where R is a non-singular quadratic form. By collecting together those terms in the transform of $C(\mathbf{x})$ which contain y_1, then those which contain y_2, and so on, we can write

$$\phi(\mathbf{x}) = \psi(\mathbf{y}) = y_1 R_1(y_1, \ldots, y_n) + \ldots + y_r R_r(y_1, \ldots, y_n) + \Gamma(y_{r+1}, \ldots, y_n) + R(y_1, \ldots, y_r), \qquad (6)$$

where $R_1, \ldots, R_r$ are quadratic forms and Γ is a cubic form.

Case 3*a*. *Suppose* $\Gamma(y_{r+1}, \ldots, y_n)$ *is not identically zero.* Choose p-adic integers $\delta_1, \ldots, \delta_r$ and $\delta_{r+1}, \ldots, \delta_n$ such that

$$R(\delta_1, \ldots, \delta_r) \neq 0, \quad \Gamma(\delta_{r+1}, \ldots, \delta_n) \neq 0.$$

Let p^{ρ} be the exact power of p dividing $\Gamma(\delta_{r+1}, \ldots, \delta_n)$. Define

$$\boldsymbol{\epsilon} = (p^{\rho+1}\delta_1, \ldots, p^{\rho+1}\delta_r, \delta_{r+1}, \ldots, \delta_n).$$

Write

$$\Gamma_0(\mathbf{y}) = y_1 R_1 + \ldots + y_r R_r + \Gamma(y_{r+1}, \ldots, y_n).$$

Then Γ_0 is a cubic form in $y_1, \ldots, y_n$, and

$$\Gamma_0(\boldsymbol{\epsilon}) \equiv 0 \pmod{p^{\rho}}, \quad \Gamma_0(\boldsymbol{\epsilon}) \not\equiv 0 \pmod{p^{\rho+1}}. \qquad (7)$$

Also

$$R(\epsilon_1, \ldots, \epsilon_r) = p^{2\rho+2} R(\delta_1, \ldots, \delta_r) \equiv 0 \pmod{p^{2\rho+2}}. \qquad (8)$$

Define a p-adic number μ by

$$\mu\Gamma_0(\epsilon)+R(\epsilon)=0.$$

Then $\mu\neq 0$ and μ is a p-adic integer by (7) and (8). We have

$$\psi(\mu\epsilon)=\mu^3\,\Gamma_0(\epsilon)+\mu^2\,R(\epsilon)=0.$$

Further, by Euler's theorem on homogeneous functions,

$$\begin{aligned}\sum_{j=1}^{n}\epsilon_j\,\psi^{(j)}(\mu\epsilon)&=\sum_{j=1}^{n}\epsilon_j\{\mu^2\,\Gamma_0^{(j)}(\epsilon)+\mu R^{(j)}(\epsilon)\}=3\mu^2\,\Gamma_0(\epsilon)+2\mu R(\epsilon)\\&=-\mu R(\epsilon)=-\mu p^{2\rho+2}\,R(\delta_1,\,\ldots,\,\delta_r)\neq 0.\end{aligned}$$

Hence the point $\mathbf{y}=\mu\epsilon$ provides a non-singular p-adic integral solution of $\psi(\mathbf{y})=0$.

Case 3b. Suppose $\Gamma(y_{r+1},\,\ldots,\,y_n)$ *in* (6) *vanishes identically.* We now have

$$\psi(\mathbf{y})=y_1\,R_1(y_1,\,\ldots,\,y_n)+\ldots+y_r\,R_r(y_1,\,\ldots,\,y_n)+R(y_1,\,\ldots,\,y_r).$$

Suppose first that there is some j $(1\leqslant j\leqslant r)$ for which the quadratic form

$$R_j(0,\,\ldots,\,0,\,y_{r+1},\,\ldots,\,y_n) \tag{9}$$

in $n-r$ variables does not vanish identically. Choose p-adic integers $y_{r+1},\,\ldots,\,y_n$ for which the value of this form is not zero. Then the point

$$(0,\,\ldots,\,0,\,y_{r+1},\,\ldots,\,y_n)$$

provides a non-singular p-adic integral solution of $\psi(\mathbf{y})=0$, since at this point the partial derivative of $\psi(\mathbf{y})$ with respect to y_j is the number (9).

Now suppose that the forms (9) are all identically zero. Then every term in each of the quadratic forms $R_j(y_1,\,\ldots,\,y_n)$ must contain at least one of the variables $y_1,\,\ldots,\,y_r$. Hence any term in $\psi(y)$ which contains any of $y_{r+1},\,\ldots,\,y_n$ is of the first degree in the latter set of variables. Thus we can write

$$\begin{aligned}\psi(\mathbf{y})=y_{r+1}\,S_{r+1}(y_1,\,\ldots,\,y_r)+\ldots+y_n\,S_n(y_1,\,\ldots,\,y_r)&\\+\Gamma_1(y_1,\,\ldots,\,y_r)+R(y_1,\,\ldots,\,y_r),&\end{aligned}$$

where $S_{r+1},\,\ldots,\,S_n$ are quadratic forms and Γ_1 is a cubic form.

The quadratic forms $S_{r+1},\,\ldots,\,S_n$ must be linearly independent, since otherwise we could express $\psi(\mathbf{y})$ as a polynomial in fewer than n variables, contrary to the hypothesis that $\phi(\mathbf{x})$ does not degenerate. The number of possible terms in a quadratic form in r variables is $\frac{1}{2}r(r+1)$; hence any set of linearly independent forms cannot number more than this. It follows that

$$n-r\leqslant\tfrac{1}{2}r(r+1),$$

and since $r\leqslant 4$, this implies that $n\leqslant 14$. This contradicts our hypothesis, and the proof is complete.

3. *The exponential sum*

Let $\mathscr{B}$ be a fixed box in n dimensional space, defined by inequalities of the type

$$x_j' \leqslant x_j \leqslant x_j'' \quad (1 \leqslant j \leqslant n), \tag{10}$$

and suppose (merely for convenience) that $0 < x_j'' - x_j' \leqslant 1$. Let P be a large positive integer and let α be a real number. Define

$$S(\alpha) = \sum_{\mathbf{x} \text{ in } P\mathscr{B}} e\Big(\alpha\phi(x_1, \ldots, x_n)\Big), \tag{11}$$

where $e(\lambda)$ denotes $e^{2\pi i\lambda}$.

We write the cubic part $C(x_1, \ldots, x_n)$ of ϕ as

$$C(\mathbf{x}) = \sum_{i,j,k} c_{ijk} x_i x_j x_k, \tag{12}$$

where the sums go from 1 to n, and the c_{ijk} are integers which are symmetrical functions[†] of i, j, k. We define the bilinear forms $B_j(\mathbf{x}|\mathbf{y})$ by

$$B_j(\mathbf{x}|\mathbf{y}) = \sum_{i,k} c_{ijk} x_i y_k. \tag{13}$$

LEMMA 1. *Let θ $(0 < \theta < 1)$ be independent of P, let κ be independent of P, and let ϵ be any fixed small positive number. Then either*

(A) *There are more than $P^{2n\theta - 4\kappa - \epsilon}$ pairs of integer points* $\mathbf{x}, \mathbf{y}$ *satisfying*[‡]

$$|\mathbf{x}| < P^{\theta}, \quad |\mathbf{y}| < P^{\theta}, \quad B_j(\mathbf{x}|\mathbf{y}) = 0 \quad (1 \leqslant j \leqslant n), \tag{14}$$

or (B) *if, for any* α,

$$|S(\alpha)| \geqslant P^{n-\kappa}, \tag{15}$$

then α has a rational approximation a/q satisfying

$$(a, q) = 1, \quad 1 \leqslant q \leqslant cP^{2\theta}, \quad |q\alpha - a| < P^{-3+2\theta}, \tag{16}$$

where c depends only on the coefficients of the form $C(\mathbf{x})$.

Proof. This is a simpler form of Lemma 9 of C.F.16, with only two alternatives instead of three, and is the result indicated at the end of §2 of C.F.16. The fact that the exponential sum $S(\alpha)$ of the present paper is defined with a cubic polynomial instead of a cubic form is of no significance, for the first step in the proof (see Lemma 3.1 of C.F.32) involves taking the second difference of $\phi(\mathbf{x})$, and in this the terms of degree less than 3 disappear, except to the extent of an additive constant (which is irrelevant). The bilinear forms $B_j(\mathbf{x}|\mathbf{y})$ in (13) arise as the coefficients in the second difference of ϕ; we have

$$\phi(\mathbf{z}+\mathbf{x}+\mathbf{y}) - \phi(\mathbf{z}+\mathbf{x}) - \phi(\mathbf{z}+\mathbf{y}) + \phi(\mathbf{z}) = 6\sum_j B_j(\mathbf{x}|\mathbf{y}) z_j + \psi,$$

where ψ is independent of $\mathbf{z}$.

[†] If necessary, we consider 6ϕ in place of ϕ.

[‡] $|\mathbf{x}| = \max(|x_1|, \ldots, |x_n|)$ if $\mathbf{x} = (x_1, \ldots, x_n)$.

Alternatively, reference may be made to Lemma 32 of Davenport's *Analytic methods for Diophantine equations and Diophantine inequalities* (Ann Arbor Publishers, 1963). This lemma is the same as Lemma 1 above, except that there κ has been given the particular value $\frac{1}{4}n\theta-\epsilon$.

Note that alternative (A) is independent of α. If κ is taken to be a particular multiple of θ (as it will be later) then alternative (A) is essentially independent of θ also, since it can be restated in terms of P^0 only.

LEMMA 2. *Let t and r be non-negative integers. Suppose there exist DR^{n-t} integer points $\mathbf{x}\neq 0$ with $|\mathbf{x}|<R$, for each of which the bilinear equations*

$$B_j(\mathbf{x}\,|\,\mathbf{y})=0 \quad (1\leqslant j\leqslant n)$$

have exactly r linearly independent solutions in $\mathbf{y}$. If D is greater than a certain function of n, and the preceding statement holds for some arbitrarily large values of R, then

$$h(C)\leqslant n-r+t-1.$$

Proof. This result is almost the same as Lemma 3 of E.S., but with integer points $\mathbf{x}$ in $|\mathbf{x}|<R$ replacing points $\mathbf{x}$ whose coordinates are integers (mod$p$). The proof given in E.S. applies with only verbal changes. The analogue of Lemma 2 of E.S., which is needed in the proof, is provided by Lemma 2 of C.F.16.

LEMMA 3. *The number of pairs of integer points $\mathbf{x}$, $\mathbf{y}$ satisfying*

$$|\mathbf{x}|<R,\quad |\mathbf{y}|<R,\quad B_j(\mathbf{x}\,|\,\mathbf{y})=0 \quad (j=1,\ldots,n) \tag{17}$$

is† $\ll R^{2n-h}$ *for large R, where $h=h(C)$.*

Proof. Suppose the contrary. Then for any fixed A there are arbitrarily large values of R for which there are more than AR^{2n-h} pairs $\mathbf{x}$, $\mathbf{y}$. Consider the set of those $\mathbf{x}\neq 0$ in $|\mathbf{x}|<R$ for which there are exactly r linearly independent solutions of the bilinear equations $B_j(\mathbf{x}\,|\,\mathbf{y})=0$ in $\mathbf{y}$. Then to each such $\mathbf{x}$ there correspond $\ll R^r$ solutions in $\mathbf{y}$ which satisfy $|\mathbf{y}|<R$. Hence for some r the number of $\mathbf{x}$ in the set is greater than $A'\,R^{2n-h-r}$, where A' is large with A. Plainly $h+r>n$.

Applying Lemma 2 with $t=h+r-n$ we obtain

$$h=h(C)\leqslant n-r+(h+r-n)-1=h-1,$$

a contradiction.

Note that if it is supposed that $C(\mathbf{x})$ does not represent 0 non-trivially, then $h(C)=n$ and the above lemma becomes the same as Lemma 4 of C.F.16.

† The symbol $\ll$ indicates an inequality with an unspecified constant factor.

Lemma 4. *Let $h = h(C)$. Let θ $(0 < \theta < 1)$ be independent of P. Then for any α either*

$$|S(\alpha)| < P^{n+\epsilon-h\theta/4} \tag{18}$$

or α has a rational approximation satisfying (16).

Proof. If we take $\kappa = (h\theta - 2\epsilon)/4$ in Lemma 1, then alternative (A) is excluded by Lemma 3, and the result follows from alternative (B).

Lemma 5. *For integers a, q with $q > 0$ and $(a, q) = 1$, let*

$$S(a, q) = \sum_{z \bmod q} e\left(\frac{a}{q}\phi(z)\right). \tag{19}$$

Then[†]

$$|S(a, q)| \ll q^{n+\epsilon-h/8}. \tag{20}$$

Proof. We regard $S(a, q)$ as an instance of $S(\alpha)$ with $\alpha = a/q$, with $P = q$, and with $0 \leqslant x_j < 1$ $(j = 1, \ldots, n)$ as the box $\mathscr{B}$. We take $\theta = \frac{1}{2} - \epsilon$ in Lemma 4. Then $\alpha (= a/q)$ does not have any rational approximation a'/q' satisfying (16), since this would require

$$1 \leqslant q' \ll P^{2\theta}, \text{ whence } 1 \leqslant q' < q,$$

and

$$|q'\alpha - a'| < P^{-3+2\theta},$$

whence

$$|q' a/q - a'| < q^{-2},$$

and this is impossible. Hence (18) applies, and gives

$$|S(a, q)| < P^{n - \frac{1}{4}h(\frac{1}{2}-\epsilon)+\epsilon} = q^{n+\epsilon'-h/8}.$$

4. *Major and minor arcs*

Let Δ be a fixed small positive number. Let $\mathfrak{M}_{a,q}$ denote the interval of values of α given by

$$|\alpha - a/q| < P^{-3+\Delta}, \tag{21}$$

where a, q are integers satisfying

$$1 \leqslant q \leqslant P^{\Delta}, \quad (a, q) = 1. \tag{22}$$

The intervals $\mathfrak{M}_{a,q}$ are obviously disjoint. Let $\mathfrak{M}$ denote the union of the intervals $\mathfrak{M}_{a,q}$ for $1 \leqslant a \leqslant q$, with the convention that the right-hand half of $\mathfrak{M}_{1,1}$ is replaced by the right-hand half of $\mathfrak{M}_{0,1}$. Then $\mathfrak{M}$ is contained in $0 \leqslant \alpha \leqslant 1$, and we denote its complement relative to this interval by $\mathfrak{m}$.

Lemma 6. *Suppose that $h = h(C) \geqslant 17$. Then*

$$\int_{\mathfrak{m}} |S(\alpha)| \, d\alpha \ll P^{n-3-\Delta/9}. \tag{23}$$

[†] It is to be understood that ϕ is a *fixed* cubic polynomial.

Proof. Let $\mathscr{E}(\theta)$ denote the set of those α in $0 \leqslant \alpha \leqslant 1$ which have a rational approximation a/q satisfying the conditions (16), which we now repeat for convenience of reference:

$$1 \leqslant q \leqslant cP^{2\theta}, \quad (a, q) = 1, \quad |q\alpha - a| < P^{-3+2\theta}. \tag{24}$$

Plainly $\mathscr{E}(\theta)$ increases with θ. Since every α has a rational approximation satisfying

$$1 \leqslant q \leqslant P^{3/2}, \quad (a, q) = 1, \quad |q\alpha - a| < P^{-3/2},$$

and these imply (24) when $\theta = \tfrac{3}{4} + \epsilon$, the whole interval $0 \leqslant \alpha \leqslant 1$ is contained in $\mathscr{E}(\tfrac{3}{4} + \epsilon)$. On the other hand, the set $\mathfrak{m}$ is contained in the complement of $\mathscr{E}(\tfrac{1}{2}\Delta - \epsilon)$, for the inequalities (24) with $\theta = \tfrac{1}{2}\Delta - \epsilon$ imply the inequalities (21) and (22).

We choose numbers $\theta_0, \theta_1, \ldots, \theta_g$ such that

$$\tfrac{1}{2}\Delta - \epsilon = \theta_0 < \theta_1 < \ldots < \theta_g = \tfrac{3}{4} + \epsilon. \tag{25}$$

Then $\mathfrak{m}$ is contained in the union of the sets

$$\mathscr{E}(\theta_f) - \mathscr{E}(\theta_{f-1}), f = 1, \ldots, g. \tag{26}$$

By Lemma 4 with $\theta = \theta_{f-1}$ we have

$$|S(\alpha)| < P^{n - \frac{1}{4}h\theta_{f-1} + \epsilon}$$

for all α in the set (26). Further, the set (26) is part of $\mathscr{E}(\theta_f)$, and by (24) the measure of $\mathscr{E}(\theta_f)$ is

$$\ll \sum_{q \leqslant cP^{2\theta_f}} \sum_{a=1}^{q} q^{-1} P^{-3+2\theta_f} \ll P^{-3+4\theta_f}.$$

Hence

$$\int_{(26)} |S(\alpha)|\, d\alpha \ll P^{n - \frac{1}{4}h\theta_{f-1} - 3 + 4\theta_f + \epsilon}$$

$$\ll P^{n-3-\frac{1}{4}\theta_{f-1} + 4(\theta_f - \theta_{f-1}) + \epsilon},$$

since $h \geqslant 17$.

Provided the numbers $\theta_0, \ldots, \theta_g$ in (25) are chosen sufficiently near together (but independent of P), the last exponent is less than

$$n - 3 - \frac{\Delta}{8} + 2\epsilon < n - 3 - \frac{\Delta}{9},$$

since ϵ is arbitrarily small. This proves Lemma 6.

LEMMA 7. *For α in $\mathfrak{M}_{a,q}$ we have*

$$S(\alpha) = q^{-n} S(a, q)\, I(\beta) + O(P^{n-1+2\Delta}), \tag{27}$$

where $\beta = \alpha - a/q$ and

$$I(\beta) = \int_{P\mathscr{B}} e\big(\beta\phi(\xi)\big)\, d\xi. \tag{28}$$

Proof. In the sum (11) defining $S(\alpha)$, put $x_j = qy_j + z_j$, where $0 \leqslant z_j < q$. Then

$$S(\alpha) = \sum_{\mathbf{z}} \sum_{\mathbf{y}} e\big(\alpha\phi(q\mathbf{y}+\mathbf{z})\big) = \sum_{\mathbf{z}} e\left(\frac{a}{q}\phi(\mathbf{z})\right) \sum_{\mathbf{y}} e\big(\beta\phi(q\mathbf{y}+\mathbf{z})\big).$$

The inner sum is over all $\mathbf{y}$ such that $q\mathbf{y}+\mathbf{z}$ is in the box $P\mathscr{B}$. Thus the variables $y_1, \dots, y_n$ run over independent intervals whose lengths are $\ll P/q$, since q is small compared with P.

For any integer point $\mathbf{y}$ and any differentiable function $F(\boldsymbol{\eta})$, we have

$$F(\mathbf{y}) = \int_{|\boldsymbol{\eta}-\mathbf{y}|<1/2} F(\boldsymbol{\eta})\, d\boldsymbol{\eta} + O(\max|\partial F/\partial \eta_j|), \tag{29}$$

the maximum being taken over j and over $\boldsymbol{\eta}$ in the cube of integration. When $F(\boldsymbol{\eta}) = e\big(\beta\phi(q\boldsymbol{\eta}+\mathbf{z})\big)$, we have

$$\max|\partial F/\partial \eta_j| \ll q|\beta|\,|q\boldsymbol{\eta}+\mathbf{z}|^2 \ll q|\beta|P^2.$$

Applying (29) to each integer point $\mathbf{y}$ in the inner sum above, we obtain an integral extended over a union of unit cubes, which differs from the box of summation by an amount at most 1 in each dimension. The discrepancy in volume is $\ll (P/q)^{n-1}$. Hence

$$\sum_{\mathbf{y}} e\big(\beta\phi(q\mathbf{y}+\mathbf{z})\big) = \int e\big(\beta\phi(q\boldsymbol{\eta}+\mathbf{z})\big)\, d\boldsymbol{\eta} + O\big(q|\beta|\, P^2(P/q)^n\big) + O\big((P/q)^{n-1}\big),$$

where the integration for $\boldsymbol{\eta}$ is over those $\boldsymbol{\eta}$ for which $q\boldsymbol{\eta}+\mathbf{z}$ lies in $P\mathscr{B}$.

Changing from the variable $\boldsymbol{\eta}$ to $\boldsymbol{\xi} = q\boldsymbol{\eta}+\mathbf{z}$, the last expression is

$$q^{-n}\int_{P\mathscr{B}} e\big(\beta\phi(\boldsymbol{\xi})\big)\, d\boldsymbol{\xi} + O(P^{n+2}q^{1-n}|\beta|) + O(P^{n-1}q^{1-n}).$$

Substituting in the double sum, we obtain

$$q^{-n}S(a,q)\,I(\beta) + O(P^{n+2}q|\beta|) + O(P^{n-1}q),$$

and now (27) follows from (21) and (22).

5. *The asymptotic formula*

LEMMA 8. *Suppose that $h = h(C) \geqslant 17$. Then the number $\mathscr{N}(P)$ of solutions of $\phi(\mathbf{x}) = 0$ with $\mathbf{x}$ in $P\mathscr{B}$ satisfies*

$$\mathscr{N}(P) = P^{n-3}J(P)\{\mathfrak{S} + O(P^{-\Delta/9})\} + O(P^{n-4+5\Delta}), \tag{30}$$

where

$$\mathfrak{S} = \sum_{q=1}^{\infty} \sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-n}S(a,q) \tag{31}$$

and

$$J(P) = \int_{-P^{\Delta}}^{P^{\Delta}} d\gamma \int_{\mathscr{B}} e\big(\gamma P^{-3}\phi(P\mathbf{x})\big)\, d\mathbf{x}. \tag{32}$$

Proof. The number of integer points $\mathbf{x}$ in $P\mathscr{B}$ with $\phi(\mathbf{x}) = 0$ is

$$\int_0^1 S(\alpha)\,d\alpha,$$

by the definition of $S(\alpha)$ in (11). We split the interval of integration into the various intervals $\mathfrak{M}_{a,q}$ and the set $\mathfrak{m}$. By Lemma 6 the contribution of $\mathfrak{m}$ is $O(P^{n-3-\Delta/9})$. By Lemma 7, the contribution of the intervals $\mathfrak{M}_{a,q}$ is

$$\sum_{q \leqslant P^\Delta} \sum_{\substack{a=1\\(a,q)=1}}^{q} \int_{\mathfrak{M}_{a,q}} S(\alpha)\,d\alpha$$

$$= \sum_{q \leqslant P^\Delta} \sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-n} S(a,q) \int_{|\beta|<P^{-3+\Delta}} I(\beta)\,d\beta + O\Big(\sum_{q \leqslant P^\Delta} qP^{n-1+2\Delta}\, P^{-3+\Delta}\Big).$$

The error term here is $O(P^{n-4+5\Delta})$.

The integral with respect to β, on putting $\beta = P^{-3}\gamma$, becomes

$$P^{-3} \int_{|\gamma|<P^\Delta} I(P^{-3}\gamma)\,d\gamma,$$

and by (28)

$$I(P^{-3}\gamma) = \int_{P\mathscr{B}} e\big(P^{-3}\gamma\phi(\boldsymbol{\xi})\big)\,d\boldsymbol{\xi} = P^n \int_{\mathscr{B}} e\big(P^{-3}\gamma\phi(P\mathbf{x})\big)\,d\mathbf{x}.$$

Thus the integral with respect to β becomes $P^{n-3}J(P)$.

It remains to consider

$$\sum_{q \leqslant P^\Delta} \sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-n} S(a,q).$$

This series, continued to infinity, is absolutely convergent by Lemma 5, since $h \geqslant 17$, and has sum $\mathfrak{S}$. The finite sum above differs from $\mathfrak{S}$ by an amount

$$\ll \sum_{q > P^\Delta} q \cdot q^{-n} . q^{n-h/8+\epsilon} \ll P^{-\Delta/9}.$$

This proves Lemma 8.

6. *The singular integral*

So far the box $\mathscr{B}$ has been arbitrary;. we now choose it in a particular manner which will ensure that

$$\lim_{P\to\infty} J(P) = J_0 > 0. \tag{33}$$

The choice will depend only on the cubic part $C(\mathbf{x})$ of $\phi(\mathbf{x})$. By Lemma 6.1 of C.F.32 there exists a real non-singular solution $(\xi_1^*, \ldots, \xi_n^*)$ of $C(\boldsymbol{\xi}) = 0$ with $\xi_j^* \neq 0$ for every j. We take $\mathscr{B}$ to be a cube

$$\xi_j^* - \rho < x_j < \xi_j^* + \rho, \tag{34}$$

with ρ a sufficiently small positive number.

LEMMA 9. *With $\mathscr{B}$ chosen as above,* (33) *holds.*

Proof. For $\mathbf{x}$ in the fixed box $\mathscr{B}$, we have

$$e\left(\gamma P^{-3}\phi(P\mathbf{x})\right)=e\left(\gamma C(\mathbf{x})+\gamma P^{-1}Q(\mathbf{x})+\gamma P^{-2}L(\mathbf{x})+\gamma P^{-3}N\right)$$
$$=e\left(\gamma C(\mathbf{x})\right)+O(P^{-1+\Delta}),$$

if $|\gamma|<P^{\Delta}$. Hence, by (32),

$$J(P)=\int_{-P^{\Delta}}^{P^{\Delta}}d\gamma\int_{\mathscr{B}}e\left(\gamma C(\mathbf{x})\right)d\mathbf{x}+O(P^{-1+2\Delta}).$$

By Lemma 6.2 of C.F.32, if ρ is chosen sufficiently small, the integral on the right has a limit $J_0>0$ as $P\to\infty$. Hence the result.

7. *The singular series*

LEMMA 10. *If $h=h(C)\geqslant 17$ and $\phi(\mathbf{X})$ satisfies the congruence condition then $\mathfrak{S}>0$.*

Proof. It is well known that

$$\mathfrak{S}=\prod_{p}\chi(p),$$

where

$$\chi(p)=1+\sum_{\nu=1}^{\infty}\sum_{\substack{a=1\\(a,p)=1}}^{p^{\nu}}(p^{\nu})^{-n}S(a,p^{\nu}).$$

It follows from Lemma 5 that

$$|S(a,p^{\nu})|\ll(p^{\nu})^{n-(1/8)h+\epsilon},$$

whence (since $h\geqslant 17$)

$$|\chi(p)-1|<p^{-9/8+2\epsilon}<p^{-10/9}.$$

Thus there exists p_0 such that

$$\prod_{p>p_0}\chi(p)>\tfrac{1}{2}.$$

It is also well known that

$$\chi(p)=\lim_{\nu\to\infty}M(p^{\nu})/p^{(n-1)\nu},\tag{35}$$

where $M(p^{\nu})$ denotes the number of solutions of the congruence

$$\phi(x_1,\ldots,x_n)\equiv 0\pmod{p^{\nu}}\tag{36}$$

with $0\leqslant x_j<p^{\nu}$ $(j=1,\ldots,n)$. We now prove that the limit on the right of (35) is positive provided the equation $\phi(\mathbf{x})=0$ has a non-singular p-adic integral solution.

Let $\boldsymbol{\alpha}$ be a non-singular p-adic solution of $\phi(\mathbf{x})=0$, and let p^{ρ} be the highest power of p dividing all the partial derivatives $\phi^{(j)}(\boldsymbol{\alpha})$. Let $M'(p^{\nu})$

denote the number of solutions of (36) which satisfy

$$\mathbf{x} \equiv \boldsymbol{\alpha} \pmod{p^{\rho+1}}, \tag{37}$$

and which are mutually incongruent to the modulus $p^{\nu-\rho}$. We prove that if $\nu \geqslant 2\rho+1$ then

$$M'(p^\nu) \geqslant p^{(n-1)(\nu-2\rho-1)}; \tag{38}$$

this will suffice for the result just stated. Plainly (38) holds if $\nu = 2\rho+1$, on taking an integer point $\mathbf{x} \equiv \boldsymbol{\alpha} \pmod{p^{2\rho+1}}$. Assuming the result (38) for a particular value of ν, we take $\mathbf{x}$ to be any one of the solutions of (36) and (37), and consider

$$\mathbf{y} = \mathbf{x} + p^{\nu-\rho}\mathbf{t}.$$

We have

$$\phi(\mathbf{y}) \equiv \phi(\mathbf{x}) + p^{\nu-\rho} \sum_{j=1}^{n} t_j \phi^{(j)}(\mathbf{x}) \pmod{p^{2(\nu-\rho)}}.$$

Here $\phi(\mathbf{x})$ is divisible by p^ν and all of $\phi^{(j)}(\mathbf{x})$ are divisible by p^ρ and one at least of them is not divisible by $p^{\rho+1}$. Hence, noting that $2(\nu-\rho) \geqslant \nu+1$, the congruence $\phi(\mathbf{y}) \equiv 0 \pmod{p^{\nu+1}}$ is satisfied if and only if $t_1, \ldots, t_n$ satisfy a linear congruence $(\bmod\, p)$ with the coefficients of $t_1, \ldots, t_n$ not all $\equiv 0 \pmod{p}$. This has p^{n-1} solutions, and for each solution we get a point $\mathbf{y}$ satisfying

$$\phi(\mathbf{y}) \equiv 0 \pmod{p^{\nu+1}}, \quad \mathbf{y} \equiv \mathbf{x} \pmod{p^{\nu-\rho}};$$

the points $\mathbf{y}$ arising from distinct $\mathbf{x}$ being distinct $\bmod\, p^{\nu-\rho+1}$. Hence

$$M'(p^{\nu+1}) \geqslant p^{n-1} M'(p^\nu),$$

and this proves (38) by induction on ν.

By Theorem 3, the fact that $\phi(\mathbf{x})$ satisfies the congruence condition implies the existence of a non-singular p-adic integral solution of $\phi(\mathbf{x}) = 0$, since $n \geqslant h \geqslant 17$. It follows from the preceding that $\chi(p) > 0$ for each $p \leqslant p_0$, whence $\mathfrak{S} > 0$.

8. *Proof of Theorem* 1

By Lemmas 8 and 9, if the box $\mathscr{B}$ is suitably chosen, the number $\mathscr{N}(P)$ of integer points $\mathbf{x}$ in $P\mathscr{B}$ with $\phi(\mathbf{x}) = 0$ satisfies

$$\mathscr{N}(P) = P^{n-3} J_0 \mathfrak{S} + o(P^{n-3})$$

as $P \to \infty$, where $J_0 > 0$. By Lemma 10 we have $\mathfrak{S} > 0$ under the hypotheses of Theorem 1. Hence there are infinitely many solutions.

We may further remark that the vectors from the origin to the solutions lie asymptotically everywhere dense on the cubic cone $C(\mathbf{x}) = 0$, since the vectors to the real points $(\xi_1^*, \ldots, \xi_n^*)$ which are admissible in §6 lie everywhere dense on the cone.

Trinity College,
Cambridge;

University of Michigan,
Ann Arbor, Michigan.