PROCEEDINGS OF THE
Cambridge Philosophical Society

VOL. 59 OCTOBER, 1963 PART 4

Proc. Camb. Phil. Soc. (1963), **59**, 683
Printed in Great Britain

Cubic forms over algebraic number fields

BY C. P. RAMANUJAM
Tata Institute of Fundamental Research, Bombay

Communicated by H. DAVENPORT

(*Received* 3 *September* 1962)

Davenport has proved (3) that any cubic form in 32 or more variables with rational coefficients has a non-trivial rational zero. He has also announced that he has subsequently been able to reduce the number of variables to 29. Following the method of (3), we shall prove that any cubic form over any algebraic number field has a non-trivial zero in that field, provided that the number of variables is at least 54. The following is the precise form of our result.

THEOREM. *Let K be any algebraic number field and let $C(X) = C(X_1, \ldots, X_m)$ be any homogeneous cubic form with coefficients in K. If the number m of variables is greater than* 53, *there exist $X_1^0, \ldots, X_m^0$ in K, not all zero, such that $C(X^0) = C(X_1^0, \ldots, X_m^0) = 0$.*

Throughout this paper, we shall use the following notations:

Γ, R and C denote the fields of rational, real and complex numbers respectively.

K is a finite algebraic extension of Γ of degree n.

Z and $\mathfrak{o}$ are the rings of integers of Γ and K respectively, and $\mathfrak{d}$ the different ideal of K over Γ.

$\omega_1, \ldots, \omega_n$ is a basis of $\mathfrak{o}$ over Z, and $\rho_1, \ldots, \rho_n$ the dual basis of $\mathfrak{d}^{-1}$ over Z, determined uniquely by the conditions $S(\omega_i \rho_j) = \delta_{ij}$, where S denotes the trace over Γ.

K_R is the n-dimensional commutative algebra $R \otimes_\Gamma K$ over R; we identify an element x of K with the element $1 \otimes x$ of K_R; then $\omega_1, \ldots, \omega_n$ form a basis of K_R over R, and for any y in K_R, we write $y = \Sigma y_i \omega_i$. For any $y \in K_R$, $S(y)$ and $N(y)$ will denote the trace and norm respectively of y over R. By a box $B = B(a_1, b_1, \ldots, a_n, b_n)$ in K_R, where the a_i, b_i are real numbers with $0 < b_i - a_i \leqslant 1$, we shall mean the set of y in K_R with $a_i \leqslant y_i < b_i$ $(i = 1, \ldots, n)$. B_0 will denote the set of y in K_R with $-1 \leqslant y_i < 1$.

$(K_R)^m$ will denote the mth Cartesian power of K_R, considered as an mn-dimensional vector space over R. A box $\mathscr{B}$ in $(K_R)^m$ is the Cartesian product $\prod_{i=1}^{m} B_i$ of boxes B_i

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

in K_R; similarly, $\mathscr{B}_0$ will denote $(B_0)^m$. Unless otherwise stated, all summations will be over 'integral' vectors $X = (X_1, \ldots, X_m)$ of $(K_R)^m$, $X_i \in \mathfrak{o}$, which are subject to the conditions stated either under the summation sign or immediately after.

For real values of x, $e(x)$ will denote $e^{2\pi i x}$ as usual and $\|x\|$ the distance of x from the nearest integer. We shall use the O, o, notation of Landau–Bachmann as well as the $\ll$ notation of Vinogradoff, whichever is more convenient. The parameters on which the constants involved in these notations depend will be explicitly mentioned, if not clear from the context.

1. *General cubic exponential sums.* Since the estimations of this and the next sections are straightforward extensions of those of the corresponding §§ 3 and 4 of (3), we shall only state the results or give brief sketches of the proofs, referring to (3) for details.

Let

$$\Gamma(X) = \sum_{i,j\,k=1}^{m} \gamma_{ijk} X_i X_j X_k$$

be a cubic form with coefficients in K_R which are symmetric in all three indices. We associate to this cubic form the bilinear forms $B_j(X, Y)$ $(j = 1, \ldots, m)$ on $(K_R)^m$ with values in K_R and the bilinear forms $\lambda_{jp}(X, Y)$ $(j = 1, \ldots, m;\ p = 1, \ldots, n)$ on $(K_R)^m$ with values in R by means of the equations

$$B_j(X, Y) = \sum_{i,k} \gamma_{ijk} X_i Y_k = \sum_{p=1}^{n} \lambda_{jp}(X, Y)\rho_p.$$

For a box $\mathscr{B}$ in $(K_R)^m$ and a real $P > 1$, we set

$$S = S(P, \mathscr{B}) = \sum_{X \in P\mathscr{B}} e(S(\Gamma(X))).$$

Throughout this section, the constant implied by the sign $\ll$ will depend only on m and n, and will in particular be independent of the coefficients of $\Gamma(X)$.

LEMMA 1·1.

$$|S|^4 \ll P^{mn} \sum_{X,\,Y \in P\mathscr{B}_0} \prod_{j=1}^{m} \prod_{p=1}^{n} \min\left(P, \|6\lambda_{j,p}(X, Y)\|^{-1}\right).$$

This is proved by following the first step of Weyl's method of estimating trigonometrical sums in one variable, exactly like Lemma 3·1 of (3).

The above lemma remains valid even if $\Gamma(X)$ contains quadratic and linear terms, as the proof of the lemma shows. This remark will be useful to us later.

We now find conditions under which the inequality

$$|S| > P^{(m-\kappa)n} \tag{1}$$

will be valid, where $0 < \kappa < m$.

LEMMA 1·2. *Suppose* (1) *holds and let N denote the number of distinct pairs of integral points X, Y satisfying*

$$X, Y \in P\mathscr{B}_0, \quad \|6\lambda_{jp}(X, Y)\| < P^{-1};$$

then

$$N \gg P^{(2m-4\kappa)n}(\log P)^{-mn}.$$

Proof. If $\{x\}$ denotes the fractional part of x for real x, and r_{jp} $(j = 1, \ldots, m;\ p = 1, \ldots, n)$ are integers satisfying $0 \leqslant r_{jp} \leqslant P$, the simultaneous inequalities

$$P^{-1}r_{jp} \leqslant \{6\lambda_{jp}(X, Y)\} < P^{-1}(r_{jp} + 1)$$

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

cannot hold for more than $N(X)$ integer points, Y lying in any fixed box with edges not exceeding P in length, where $N(X)$ denotes for any $X \in P\mathscr{B}_0$ the number of Y satisfying the inequalities stated in the lemma. Since $P\mathscr{B}_0$ can be subdivided into 2^{mn} such boxes, we obtain

$$\sum_{Y \in P\mathscr{B}_0} \prod_{j=1}^{m} \prod_{p=1}^{n} \min(P, \|6\lambda_{jp}(X, Y)\|^{-1}) \ll N(X) \prod_{j,p} \sum_{r_{j,p}=0}^{P-1} \min\left(P, \frac{P}{r_{jp}}, \frac{P}{P-r_{jp}-1}\right)$$
$$\ll N(X)(P \log P)^{mn};$$

summing over all $X \in P\mathscr{B}_0$ and applying Lemma 1·1, we get the estimate for N.

LEMMA 1·3. *Suppose* (1) *holds, and let* $0 < \theta < 1$. *Let* N_2 *denote the distinct pairs of integer points* X, Y *satisfying*

$$X, Y \in P^{\theta}\mathscr{B}_0, \quad \|6\lambda_{jp}(X, Y)\| < P^{-3+2\theta}.$$

Then

$$N_2 \gg (P^{2m\theta-4\kappa}(\log P)^{-m})^n.$$

Proof. For fixed X and $Y_i = \sum_{q=1}^{n} Y_{iq}\omega_q$, we have

$$6\lambda_{jp}(X, Y) = 6S(B_j(X, Y)\omega_p) = 6\sum_{k,q} S\Big(\sum_i \gamma_{ijk} X_i \omega_p \omega_q\Big) Y_{k,q},$$

which shows that the coefficient of $Y_{k,q}$ in $6\lambda_{jp}$ is equal to the coefficient of Y_{jp} in $6\lambda_{k,q}$. Thus we may apply Lemma 3·3 of (3) to the forms in Y obtained by substituting a fixed value of X in $6\lambda_{jp}(X, Y)$, and similarly also to the forms in X obtained by fixing Y.

Fixing X in $P\mathscr{B}_0$ and applying the aforementioned lemma to the forms $6\lambda_{jp}(X, Y)$ in Y with $A = P$, $Z_1 = P^{-1+\theta}$, $Z_2 = 1$, and summing over all integral X in $P\mathscr{B}_0$, we find that the number N_1 of distinct pairs of integral points X, Y satisfying

$$X \in P\mathscr{B}_0, \quad Y \in P^{\theta}\mathscr{B}_0, \quad \|6\lambda_{jp}(X, Y)\| < P^{-2+\theta}$$

is $\gg P^{(m+m\theta-4\kappa)n}(\log P)^{-mn}$, by Lemma 1·2. Another application of the lemma to the forms in X obtained by fixing $Y \in P^{\theta}\mathscr{B}_0$ with $A = P^{\frac{1}{2}(3-\theta)}$, $Z_1 = P^{-\frac{3}{2}(1-\theta)}$, $Z_2 = P^{-\frac{1}{2}(1-\theta)}$, and summation over Y, gives the result.

LEMMA 1·4. *Let* $\mathscr{Y}$ *be a set of at least* T *distinct integer points* Y *in* K^m, *with* $Y \in y\mathscr{B}_0$. *Suppose there are at most* r *points of* $\mathscr{Y}$ *linearly independent over* K. *Then*

$$T \leqslant Ay^{rn},$$

where A *depends only on* m *and* n.

Further, if W *is a positive integer with* $1 < W \leqslant T$, *there exist* W *distinct points* $Y^{(1)}, \ldots, Y^{(W)}$ *in* $\mathscr{Y}$ *such that*

$$Y^{(1)} - Y^{(w)} \in ByW^{1/rn}T^{-1/rn}\mathscr{B}_0 \quad (w = 1, \ldots, W),$$

where B *is again a constant depending only on* m *and* n.

Proof. Lemma 3·5 of (3) is our lemma in the special case $K = \Gamma$. Our lemma clearly reduces to this special case if we identify K^m with Γ^{mn} by means of the basis $\omega_1, \ldots, \omega_n$, and notice that if there are at most r independent points in $\mathscr{Y}$ over K, there are at most rn independent points over Γ.

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

Definition. Let m, n, r, κ, θ $(0 < \theta < 1)$, δ (> 0), be given with $m\theta > 4\kappa$. For $P > 1$, define r to be the greatest positive integer with the property that there exists a non-zero integer point X and r integer points $Y^{(1)}, \ldots, Y^{(r)}$ independent over K such that

$$X \in P^{\theta}\mathscr{B}_0, \quad Y^{(s)} \in P^{\theta}\mathscr{B}_0, \quad \|6\lambda_{jp}(X, Y^{(s)})\| < P^{-3+2\theta+\delta}$$

for $s = 1, \ldots, r$.

Note that under assumption (1) and for P large, $r \geqslant 1$ by Lemma 1·3.

LEMMA 1·5. *Suppose that*

$$0 < \xi \leqslant \theta, \quad 0 < \eta \leqslant \theta, \quad 0 < B \leqslant P^{-3+2\theta+\delta}$$

and that λ and ϵ are positive satisfying

$$\lambda > m\xi, \quad \lambda > r\eta.$$

Then there exists a $P_0 = P_0(m, n, \xi, \eta, \theta, \delta, \lambda, \epsilon)$, such that if $P > P_0$ and there are more than $P^{(\lambda+\epsilon)n}$ distinct pairs of integer points X, Y, neither zero, satisfying

$$X \in P^{\xi}\mathscr{B}_0, \quad Y \in P^{\eta}\mathscr{B}_0, \quad \|6\lambda_{jp}(X, Y)\| < B, \tag{2}$$

then

$$\lambda + \epsilon \leqslant m\xi + r\eta,$$

and there are more than $P^{mn\xi}$ distinct pairs of integer points X, Y, neither zero, with

$$X \in P^{\xi}\mathscr{B}_0, \quad Y \in P^{\eta-(\lambda-m\xi)/r}\mathscr{B}_0, \quad \|6\lambda_{jp}(X, Y)\| < 2B.$$

Proof. For each $X \neq 0$, let $T(X)$ denote the number of $Y \neq 0$ satisfying (2). Because of the assumptions on ξ, η and B, we can apply the first part of Lemma 1·4 to deduce that

$$T(X) \leqslant AP^{rn\eta};$$

since by assumption

$$\sum_{\substack{X \in P^{\xi}\mathscr{B}_0 \\ X \neq 0}} T(X) \geqslant P^{(\lambda+\epsilon)n}$$

we deduce that $P^{n(\lambda+\epsilon)-mn\xi-rn\eta} \leqslant A$, which shows that $\lambda + \epsilon \leqslant m\xi + r\eta$ unless P is small (the smallness as made precise in the statement of the lemma).

For $s = 0, 1, 2, \ldots$, let X_s denote the number of integer points $X \neq 0$, $X \in P^{\xi}\mathscr{B}_0$, for which

$$AP^{rn\eta}2^{-s-1} \leqslant T(X) < AP^{rn\eta}2^{-s}.$$

It is clearly sufficient to take $\ll \log P$ values of s to include all X for which $T(X) \neq 0$. Since we have

$$AP^{rn\eta} \sum_{s} 2^{-s}X_s > P^{(\lambda+\epsilon)n},$$

there exists at least one s for which

$$P^{rn\eta}2^{-s}X_s \geqslant A'P^{(\lambda+\epsilon)n}(\log P)^{-1},$$

A' being a constant dependent only on m and n. For this s, and ρ defined by the equation $P^{\rho} = P^{rn\eta-\frac{1}{2}\epsilon n}2^{-s}$, we have

$$X_s \geqslant A''(m, n, \epsilon)P^{\lambda n-\rho+\frac{1}{2}\epsilon n},$$

and since $X_s \ll P^{mn}$ trivially, it follows that $\rho > \lambda n - mn\xi + \frac{1}{4}\epsilon n$ unless P is small.

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

Assuming P large enough, we now have X_s integer points $X \neq 0$ to each of which there correspond $T(X)$ integer points $Y \neq 0$ such that (2) is satisfied. We apply to the set of points Y corresponding to a particular X the second part of Lemma 1·4 with

$$y = P^{\eta}, \quad T = T(X) \geqslant \tfrac{1}{2}AP^{\rho+\frac{1}{2}\epsilon n}, \quad W = [P^{\rho-\lambda n+mn\epsilon}]+1.$$

The condition $1 < W < T(X)$ is satisfied since $0 < n(\lambda - m\xi) < \rho$. We thus deduce that to each of the X_s points there correspond W distinct points $Y^{(1)}, \ldots, Y^{(W)}$ with

$$Y^{(1)} - Y^{(w)} \in B^1 P^{\eta} P^{(\rho-\lambda n+mn\xi)/rn} P^{-(\rho+\frac{1}{2}\epsilon n)/rn} \mathscr{B}_0 = B^1 P^{\eta-(\lambda-m\xi)/r-\frac{1}{2}\epsilon r} \mathscr{B}_0,$$

where B^1 is a constant depending only on m and n. Denoting $Y^{(1)} - Y^{(w)}$ by $Y'^{(w)}$, we see that to each of the X_s points there correspond $W-1$ distinct integer points $Y \neq 0$ satisfying

$$Y \in P^{\eta-\{(\lambda-m\xi)/r\}} \mathscr{B}_0, \quad \|6\lambda_{jp}(X, Y)\| < 2B,$$

if P is large enough. All the resulting pairs satisfy the condition of our lemma, and their number is

$$(W-1)X_s \geqslant \tfrac{1}{2}A'' P^{\rho-\lambda n+mn\xi} P^{\lambda n-\rho+\frac{1}{2}\epsilon n} \geqslant P^{mn\xi}$$

if P is large.

The lemma is thus proved.

LEMMA 1·6. *Let $m, \kappa, \theta\,(0 < \theta < 1)$ and $\delta\,(>0)$ be fixed independently of P and suppose that $m\theta > 4\kappa$ and that (1) holds. Then there exists a P_1 depending only on m, n, θ, κ and δ such that for $P \geqslant P_1$, we have*

$$r \geqslant m - 2\kappa/\theta.$$

Proof. The proof simply consists of repeated applications of the previous lemma, though the details are complicated.

We define several sequences of numbers depending on m, n, κ, θ and δ and on certain positive parameters $\epsilon_0, \epsilon_1, \ldots$, which will later be fixed in terms m, n, κ, θ and δ, as follows:

$$\left.\begin{aligned} \xi_0 = \theta, \quad \eta_0 = \theta, \quad B_0 = P^{-3+2\theta}, \quad \lambda_0 = 2m\theta - 4\kappa - 2\epsilon_0, \\ \xi_{q+1} = \eta_q - \frac{(\lambda_q - m\xi_q)}{r}, \quad \eta_{q+1} = \xi_q, \quad B_{q+1} = 2B_q, \quad \lambda_{q+1} = m\xi_q - \epsilon_{q+1}, \end{aligned}\right\} \tag{3}$$

for $q \geqslant 0$.

On substituting for η_q and λ_q in the expression for ξ_{q+1} when $q \geqslant 1$, we obtain

$$\xi_{q+1} = \xi_{q-1} - \frac{(m\xi_{q-1} - \epsilon_q - m\xi_q)}{r},$$

$$\xi_q - \xi_{q+1} = \omega(\xi_{q-1} - \xi_q) - \frac{1}{r}\epsilon_q,$$

where $\omega = m/r - 1$, and hence by induction,

$$\xi_q - \xi_{q+1} = \omega^q(\xi_0 - \xi_1) - \frac{1}{r}\sum_{t=1}^{q} \epsilon_t \omega^{q-t} \quad (q \geqslant 1).$$

Summation gives

$$\xi_0 - \xi_{q+1} = (\xi_0 - \xi_1)\sum_{s=0}^{q} \omega^q - \frac{1}{r}\sum_{s=0}^{q}\sum_{t=1}^{q} \epsilon_t \omega^{s-t}.$$

Now assume contrary to the required conclusion that $r < m - 2\kappa/\theta$. Since r is an integer, it follows that $m - 2\kappa/\theta - r$ must be greater than a positive number depending

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

only on m, κ and θ. We shall show that there exist $\phi(m,n,\theta,\kappa) > 0$ and an integer $Q = Q(m,n,\theta,\kappa)$ such that for $\epsilon_0 < \phi(m,n,\theta,\kappa)$ we have

$$\xi_0 - \xi_1 > \frac{m\theta - 4\kappa}{2m}$$

and

$$\xi_0 < (\xi_0 - \xi_1) \sum_{s=0}^{Q} \omega^s.$$

The first is clearly ensured if $\epsilon_0 < (m\theta - 4\kappa)/2m$. It follows that if $\omega \geqslant 1$, we can ensure the second by taking $Q+1 > 2m\theta/(m\theta - 4\kappa)$. Hence assume $\omega < 1$, that is,

$$\omega \leqslant 1 - 1/m.$$

Since $\xi_0 - \xi_1$ is bounded above by 2, it is clearly enough to show that if ϵ_0 is small enough,

$$\xi_0 < (\xi_0 - \xi_1) \sum_{s=0}^{\infty} \omega^s = (1-\omega)^{-1}(\xi_0 - \xi_1),$$

i.e.

$$\theta < \frac{r}{2r-m} \frac{(m\theta - 4\kappa - 2\epsilon_0)}{r} = \frac{m\theta - 4\kappa - 2\epsilon_0}{2r-m},$$

i.e.

$$2r < 2m - \frac{4\kappa}{\theta} - \frac{2\epsilon_0}{\theta},$$

which holds if ϵ_0 is less than $\theta(m - 2\kappa/\theta - r)$, and hence if ϵ_0 is less than $\phi'(m,n,\kappa,\theta)$. It follows easily that for $\epsilon_0 < \phi'(m,n,\kappa,\theta)$, we have

$$\xi_0 < (\xi_0 - \xi_1) \sum_{s=0}^{Q} \omega^s + \mu(m,n,\kappa,\theta),$$

where $\mu(m,n,\kappa,\theta) > 0$. Hence it follows that there exists a $\psi(m,n,\kappa,\theta) > 0$ such that if $\epsilon_i < \psi(m,n,\kappa,\theta)$ for $i = 0, \ldots, Q$ we have

$$\xi_0 < (\xi_0 - \xi_1) \sum_{s=0}^{Q} \omega^s - \frac{1}{r} \sum_{s=0}^{Q} \sum_{t=1}^{s} \epsilon_t \omega^{s-t} = \xi_0 - \xi_{Q+1},$$

$$\xi_{Q+1} < 0.$$

We shall now choose ϵ_i suitably depending only on m, n, θ, κ and δ to show that if the above inequality holds, P must be bounded above by a function of these parameters.

For every $q \leqslant Q$, we wish to choose $\epsilon_0, \ldots, \epsilon_q$ with $\epsilon_i < \psi(m,n,\kappa,\theta)$ and $P_q(m,n,\kappa,\theta,\delta)$ such that the following conditions hold:

$$\xi_s > 0, \quad \xi_s - \xi_{s+1} > 0, \quad \lambda_s > m\xi_s, \quad \lambda_s > r\eta_s \quad (s = 0, \ldots, q),$$

and if $P > P_q$, the inequalities

$$X \in P^{\xi_s}\mathscr{B}_0, \quad Y \in P^{\eta_s}\mathscr{B}_0, \quad \|6\lambda_{jp}(X,Y)\| < B_s$$

have at least $P^{n(\lambda_s+\epsilon_s)}$ pairs of solutions with $X, Y \neq 0$.

For $q = 0$, choose $\epsilon_0 = \frac{1}{2}\psi(m,n,\kappa,\theta)$. It follows from our previous considerations that the first set of conditions hold. Also by Lemma 1·3, the second set of inequalities

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

has $\geqslant (P^{2m\theta-4\kappa}(\log P)^{-m})^n$ solutions. Since the number of solutions with $X = 0$ or $Y = 0$ is $\ll P^{mn\theta}$ and $mn\theta < 2mn\theta - 4\kappa n$, we deduce that if $P > P_0(m, n, \kappa, \theta)$, the number of solutions with $X \neq 0$, $Y \neq 0$ is $\geqslant (P^{2m\theta-4\kappa-\epsilon_0})^n = P^{n(\lambda_0+\epsilon_0)}$.

Suppose we have now chosen $\epsilon_0, \ldots, \epsilon_q$ and P_q depending only on m, n, κ and θ satisfying our conditions. Applying Lemma 1·5 to the second set of inequalities with $s = q$, we deduce that if

$$P > \max(P_q, P_0(m, n, \xi_q, \eta_q, \theta, \delta, \lambda_q, \epsilon_q)) = P_{q+1}(m, n, \theta, \delta, \kappa)$$

we have
$$\lambda_q + \epsilon_q \leqslant m\xi_q + r\eta_q,$$

and that the number of pairs X, Y with $X \neq 0$, $Y \neq 0$ satisfying

$$X \in P^{\xi_q}\mathscr{B}_0, \quad Y \in P^{\eta_q-(\lambda_q-m\xi_q)/r}, \quad \|6\lambda_{jp}(X, Y)\| < B_{q+1}$$

is greater than $P^{mn\xi_q} = P^{n(\lambda_{q+1}+\epsilon_{q+1})}$. Since $\lambda_{jp}(X, Y) = \lambda_{jp}(Y, X)$ we may interchange X and Y in the above set of inequalities to deduce that the second set of conditions are satisfied for $s = q+1$. As to the first set, we have

$$\xi_{q+1} = \eta_q - \frac{(\lambda_q - m\xi_q)}{r} > 0, \quad \xi_{q+1} - \xi_{q+2} = \omega(\xi_q - \xi_{q+1}) - \frac{1}{r}\epsilon_{q+1} > 0,$$

if $\epsilon_{q+1} < \omega(\xi_q - \xi_{q+1})$, and since the right-hand side depends only on m, n, κ, θ, δ, if $\epsilon_{q+1} < \psi_{q+1}(m, n, \kappa, \theta, \delta)$. Also

$$\lambda_{q+1} - m\xi_{q+1} = m(\xi_q - \xi_{q+1}) - \epsilon_{q+1} > 0$$

again if $\epsilon_{q+1} < \psi'_{q+1}(m, n, \kappa, \theta, \delta)$; and finally,

$$\lambda_{q+1} - r\eta_{q+1} = (m-r)\xi_q - \epsilon_{q+1} > 0,$$

if $\epsilon_{q+1} < \psi''_{q+1}(m, n, \kappa, \theta, \delta)$. Thus if we choose $\epsilon_{q+1} = \frac{1}{2}\min(\psi_{q+1}, \psi'_{q+1}, \psi''_{q+1})$, all our conditions are satisfied and our induction is complete.

Thus we obtain for $s = Q+1$ that $\xi_{Q+1} > 0$ unless $P < P_{Q+1}(m, n, \kappa, \theta, \delta)$ and since we have already shown that $\xi_{Q+1} < 0$ (and since Q depends only on m, n, κ, θ, δ) we deduce that if $r < m - 2\kappa/\theta$, P must necessarily be bounded by a function of m, n, κ, θ and δ. The proof of the lemma is complete.

2. *Two particular types of exponential sums.* Let

$$C(X) = C(X_1, \ldots, X_m) = \sum_{i,j,k=1}^{m} c_{ijk} X_i X_j X_k$$

be a cubic form with coefficients which are integers of K, symmetric in all three indices. *We shall assume throughout this section that $C(X)$ does not represent zero non-trivially; that is, that $X = (0, \ldots, 0)$ is the only solution of $C(X) = 0$ in K.*

The cubic form $C(X)$ is said to *represent* the cubic form $C'(U) = C'(U_1, \ldots, U_s)$ in the s variables $U_1, \ldots, U_s$ if there exists a linear transformation

$$X_i = \sum_{t=1}^{s} p_{it} U_t, \quad p_{it} \in \mathfrak{o} \quad (i = 1, \ldots, m;\ t = 1, \ldots, s),$$

of rank s which transforms $C(X)$ into $C'(U)$. It follows that we must have $s \leqslant m$. We shall say that $C(X)$ *splits with remainder r* if it represents a form in $r+1$ variables of the type

$$a_0 U_0^3 + C_1(U_1, \ldots, U_r).$$

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

We define the following bilinear forms (not to be confused with the B_j defined in § 1) associated to $C(X)$:

$$B_j(X, Y) = \sum_{i,k} c_{ijk} X_i Y_k.$$

LEMMA 2·1. *Suppose there is a non-zero integral point Z and r linearly independent integral points $Y^{(1)}, \ldots, Y^{(r)}$ such that*

$$B_j(Z, Y^{(s)}) = 0 \quad (j = 1, \ldots, m;\ s = 1, \ldots, r).$$

Then $r \leqslant m-1$, and $C(X)$ splits with remainder r.

Proof. The linear transformation

$$X_i = Z_i U_0 + Y_i^{(1)} U_1 + \ldots + Y_i^{(r)} U_r$$

can be easily seen to be of rank precisely $r+1$, and transforms $C(X)$ into a form of the type $a_0 U_0^3 + C^1(U_1, \ldots, U_r)$, proving our assertion.

We will now apply Lemma 1·6 to two particular exponential sums which will arise in our later work.

Let $\mathscr{B}$ be a fixed box in $(K_R)^m$; for any $\alpha \in K_R$ and $P > 1$, we define

$$E(\alpha) = \sum_{X \in P\mathscr{B}} e(S(\alpha C(X))).$$

Let δ be any positive number. We then have

LEMMA 2·2. *Let κ and θ be fixed numbers satisfying*

$$0 < \theta < 1, \quad 0 < 4\kappa < m\theta.$$

Let $C(X)$ be any cubic form over K with integral coefficients which does not represent zero non-trivially and which does not split with remainder r, where r is the least integer satisfying

$$r \geqslant m - \frac{2\kappa}{\theta}.$$

Then there exists a P_0 (depending on K, C, θ, κ and δ) such that for $P \geqslant P_0$, either

$$|E(\alpha)| \leqslant P^{(m-\kappa)n} \tag{4}$$

or there exists an integer $\mu \in \mathfrak{o}$, $\mu \neq 0$, and $\mu \in P^{2\theta+\delta} B_0$, and a $\lambda \in \mathfrak{d}^{-1}$ such that

$$\mu\alpha - \lambda = \sum_{i-1}^{n} \epsilon_i P_i, \quad \epsilon_i \in R, \quad |\epsilon_i| < P^{-3+2\theta+\delta}. \tag{5}$$

Proof. We apply Lemma 1·6 with $\Gamma(X) = \alpha C(X)$. It follows that for large P, either (4) holds or there exists an integral point X and $r \geqslant m - 2\kappa/\theta$ integral points $Y^{(1)}, \ldots, Y^{(r)}$, in $P^\theta \mathscr{B}_0$, linearly independent over K, such that the following conditions hold:

$$6\alpha B_j(X, Y^{(s)}) = \lambda_{j,s} + \sum_i \epsilon_i(j, s)\rho_i,$$

$$\lambda_{j,s} \in \mathfrak{d}^{-1}, \quad \epsilon_i(j, s) \in R, \quad |\epsilon_i(j, s)| < P^{-3+2\theta+\delta} \quad (i, j = 1, \ldots, n;\ s = 1, \ldots, r).$$

All the $B_j(X, Y^{(s)})$ cannot be zero, since it would then follow from Lemma 2·1 that $C(X)$ splits with remainder r. Also since X, $Y^{(s)} \in P^\theta \mathscr{B}_0$, it follows that

$$6B_j(X, Y^{(s)}) \in AP^{2\theta} \mathscr{B}_0,$$

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

where A is a constant depending only on K and C. Our lemma therefore follows if we take $\mu = 6B_j(X, Y^{(s)})$ with j and s so chosen that $B_j(X, Y^{(s)}) \neq 0$.

We note that in view of the remark made at the end of Lemma 1·1, the above lemma holds without change even if we replace the sum $E(\alpha)$ by the sum

$$\sum_{X \in P\mathscr{B}} e(S(\alpha C(X)) + L(X)),$$

where $L(X)$ is a real linear form in the X_{ij}.

Now let γ be any non-zero element of K. We associate with γ the integral ideal $\mathfrak{a}_\gamma$ which is the denominator of $(\gamma)\mathfrak{d}$, that is to say $\mathfrak{a}_\gamma = (\text{g.c.d.}(\mathfrak{o}, \gamma\mathfrak{d}))^{-1}$. Let $l = (l_{ij})$ $(1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n)$ be any system of rational integers. We define

$$S_1(l, \gamma) = \sum_{X \bmod N\mathfrak{a}_\gamma} e\left(S(\gamma C(X)) + \sum_{i,j} \frac{l_{ij}}{N\mathfrak{a}_\gamma} X_{ij}\right),$$

where $X = (X_1, \ldots, X_m)$, $X_i = \sum_j X_{ij}\omega_j$, and each X_{ij} runs through a complete system of residues modulo $N\mathfrak{a}_\gamma$. We also put

$$S_1((0), \gamma) = (N\mathfrak{a}_\gamma)^{m(n-1)} \sum_{X \bmod N\mathfrak{a}_\gamma} e(S(\gamma C(X))) = (N\mathfrak{a}_\gamma)^{m(n-1)} S_\gamma.$$

LEMMA 2·3. *Let $C(X)$ be a fixed cubic form in m variables which does not represent zero non-trivially, and κ a fixed number satisfying*

$$0 < \kappa < \tfrac{1}{8}m.$$

Suppose $C(X)$ does not split with remainder r, where r is the least integer satisfying

$$r \geqslant m - 4\kappa.$$

Then, for any $\gamma \in K$ and any system of rational integers $l = (l_{ij})$, we have

$$|S_1(l, \gamma)| < (N\mathfrak{a}_\gamma)^{mn-\kappa} \tag{6}$$

unless $N\mathfrak{a}_\gamma$ is bounded above by a constant depending only on κ, the field K and the form C. In particular, if $N\mathfrak{a}_\gamma$ is large, we obtain

$$|S_\gamma| < (N\mathfrak{a}_\gamma)^{m-\kappa}. \tag{7}$$

Proof. We apply Lemma 2·2 (and the remark made at the end of that lemma) with the box $\mathscr{B} = \{X: 0 \leqslant X_{ij} < 1\}$, γ instead of α, $N\mathfrak{a}_\gamma$ instead of P, $(1/2n) - \delta$ instead of θ, and κ/n instead of κ. The conditions of that lemma are verified if δ is small enough. Hence if $N\mathfrak{a}_\gamma$ is large enough and (6) does not hold, there is a non-zero integer μ in $(N\mathfrak{a}_\gamma)^{1/n-\delta} B_0$ and a $\lambda \in \mathfrak{d}^{-1}$ such that

$$\mu\gamma - \lambda = \sum_{i=1}^{n} \epsilon_i \rho_i, \quad |\epsilon_i| < (N\mathfrak{a}_\gamma)^{-3-\delta+1/n}.$$

But since $\mathfrak{a}_\gamma(\mu\gamma - \lambda) \subset \mathfrak{d}^{-1}$, $N\mathfrak{a}_\gamma \epsilon_i$ must be a rational integer, and since

$$|N\mathfrak{a}_\gamma \epsilon_i| < (N\mathfrak{a}_\gamma)^{-2+1/n-\delta} < 1$$

for $N\mathfrak{a}_\gamma$ large, it follows that $\epsilon_i = 0$ for $1 \leqslant i \leqslant n$, and $\mu\gamma \in \mathfrak{d}^{-1}$. By the definition of $\mathfrak{a}_\gamma$, we must have $\mu \in \mathfrak{a}_\gamma$, and $N\mathfrak{a}_\gamma$ divides $N\mu$. But since

$$\mu \in (N\mathfrak{a}_\gamma)^{1/n-\delta} \mathscr{B}_0, \quad |N\mu| \leqslant A(N\mathfrak{a}_\gamma)^{1-n\delta},$$

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

where A depends only on K, which implies that for large $N\mathfrak{a}_\gamma$, we must have $|N\mu| < N\mathfrak{a}_\gamma$, and therefore $\mu = 0$, which is a contradiction. This proves the inequality (6). The inequality (7) follows from (6) since we have $S_1((0), \gamma) = (N\mathfrak{a}_\gamma)^{m(n-1)} S_\gamma$.

3. *The contribution of the major arcs.* We shall continue to use the notations of the previous section. Further, we define $\mathscr{R}$ to be the parallelepiped in K_R defined by

$$\mathscr{R} = \left\{ x = \sum_{i=1}^{n} x_i \rho_i \middle| 0 \leqslant x_i < 1 \right\}.$$

For any $\gamma \in K$, we define the 'major arc' B_γ to be the set of $\alpha \in K_R$ such that if

$$\beta = \alpha - \gamma = \sum_{i=1}^{n} \beta_i \rho_i,$$

we have $|\beta_i| < P^{-2-\delta}(N\mathfrak{a}_\gamma)^{-1}$. We assert that if $\gamma \neq \gamma'$ and $N\mathfrak{a}_\gamma \leqslant P^{1-2\delta}$, $N\mathfrak{a}_{\gamma'} \leqslant P^{1-2\delta}$, B_γ and $B_{\gamma'}$ cannot intersect. In fact, if they did intersect, we must have

$$\gamma - \gamma' = \Sigma \gamma_i \rho_i, \quad |\gamma_i| < P^{-2-\delta}((N\mathfrak{a}_\gamma)^{-1} + (N\mathfrak{a}_{\gamma'})^{-1}).$$

But since $\mathfrak{a}_\gamma \mathfrak{a}_{\gamma'}(\gamma - \gamma') \subset \mathfrak{d}^{-1}$, $N\mathfrak{a}_\gamma N\mathfrak{a}_{\gamma'} \gamma_i$ must be a rational integer for all i. Since $|N\mathfrak{a}_\gamma N\mathfrak{a}_{\gamma'} \gamma_i| < P^{-2-\delta}(N\mathfrak{a}_\gamma + N\mathfrak{a}_{\gamma'}) < 2P^{1-2\delta}P^{-2-\delta} = 2P^{-1-3\delta} < 1$, we must have $\gamma_i = 0$ and $\gamma = \gamma'$.

Now let $C(X)$ be a cubic form in m variables with coefficients integers in K and symmetric in all three indices. Our ultimate goal is to find, under suitable conditions on C and for a suitable choice of the box $\mathscr{B}$, an asymptotic formula for the number $\mathscr{N}(P)$ of solutions of the equation $C(X) = 0$ with X integral and $X \in P\mathscr{B}$. If $\alpha = \Sigma \alpha_i \rho_i$ denotes a general point of $\mathscr{R}$ and $d\alpha$ denotes the measure $d\alpha_1, \ldots, d\alpha_n$, we have the following integral representation for $\mathscr{N}(P)$:

$$\mathscr{N}(P) = \int_{\mathscr{R}} E(\alpha)\, d\alpha. \tag{8}$$

In this section, we shall establish under certain conditions on C, and the box $\mathscr{B}$ being suitably chosen, an asymptotic formula for the contribution to the integral on the right of (8) of the major arcs B_γ with $N\mathfrak{a}_\gamma \leqslant P^{1-2\delta}$. Because of the definition of $\mathscr{R}$ and the periodicity of $E(\alpha)$ in the variables α_i, the contribution of these major arcs is given by

$$\sum_{N\mathfrak{a} \leqslant P^{1-2\delta}} \sum_{\substack{\gamma \bmod \mathfrak{d}^{-1} \\ \mathfrak{a}_\gamma = \mathfrak{a}}} \int_{B_\gamma} E(\alpha)\, d\alpha.$$

The main result of this section is the following:

LEMMA 3·1. *Let $C(X)$ be any cubic form in more than nine variables with integral coefficients in K which does not represent zero non-trivially. Assume that (in the notation of § 2) we have a uniform estimate of the form*

$$|S_1(l, \gamma)| \ll (N\mathfrak{a}_\gamma)^{mn-\omega}$$

with $\omega > 2$. Then for P tending to infinity suitably, and with a suitable choice of the box $\mathscr{B}$, we have the following asymptotic formula

$$\sum_{N\mathfrak{a} \leqslant P^{1-2\delta}} \sum_{\substack{\gamma \bmod \mathfrak{d}^{-1} \\ \mathfrak{a}_\gamma = \mathfrak{a}}} \int_{B_\gamma} E(\alpha)\, d\alpha = AP^{(m-3)n} + o(P^{(m-3)n}) \quad (0 < A < \infty).$$

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

The whole of this section is devoted to the proof of this lemma, which will be carried out in several steps.

Let $g(t_1, \ldots, t_p)$ be a function of p variables defined in a parallelepiped $A_i^1 \leqslant t_i \leqslant A_i^2$, and let Q be a subset $(r_1 < \ldots < r_q)$ of the set of integers $\{1, 2, \ldots, p\}$. We shall adopt the following conventions: h_Q will denote an element of Z^Q, that is, a set of integers $(h_{r_1}, \ldots, h_{r_q})$, and $|h_Q|$ the sum $\sum_{i=1}^{q} h_{r_i}$. If s is a fixed integer, we shall denote the set $(s, \ldots, s)$ by $(s)_Q$. We shall write $\partial_Q^{h_Q} g$ in place of

$$\frac{\partial^{|h_Q|} g}{(\partial t_{r_1})^{h_{r_1}} \ldots (\partial t_{r_q})^{h_{r_q}}}.$$

If a and b are two integers, the symbol $\sum_{h_Q=a}^{b}$ will imply summation over all the h_Q with $a \leqslant h_{r_i} \leqslant b$ $(1 \leqslant i \leqslant q)$. An integral of the form $\int_{A_Q^1}^{A_Q^2} g\, dt_Q$ will stand for the multiple integral

$$\int_{A_{r_1}^1}^{A_{r_1}^2} \ldots \int_{A_{r_q}^1}^{A_{r_q}^2} g\, dt_{r_1} \ldots dt_{r_q}.$$

Finally, we shall mean by the symbol $[g(t_1, \ldots, t_p)]\,\Delta_Q$ the multiple difference expression

$$\sum_{\lambda_i = 1 \text{ or } 2} (-1)^{\sum \lambda_i} g(t_1, \ldots, A_{r_1}^{\lambda_1}, \ldots, A_{r_2}^{\lambda_2}, \ldots, A_{r_q}^{q}, \ldots).$$

With these notations, we can state

LEMMA 3·2. *Let $f(x) = f(x_1, \ldots, x_k)$ be a function of k variables defined and continuous with all its partial derivatives up to order s in an open set containing the parallelepiped $A_i \leqslant x_i \leqslant B_i$ $(i = 1, \ldots, k)$, where we assume the A_i and B_i to be non-integral. Let $z = (z_1, \ldots, z_k)$ be a set of k integers and let q be any integer $\geqslant 1$. Then we have*

$$\sum_{\substack{A_i < x < B_i \\ x_i \equiv z_i (q)}} f(x_1, \ldots, x_k) = \sum_{\Phi} (-1)^{\mu} q^{\nu(s-1)-\lambda} \times \left[\sum_{h_J = 0}^{s-1} q^{|h_J|} \prod_{j \in J} \psi_{h_j}\left(\frac{\xi_j - z_j}{q}\right) \int_{A_I}^{B_I} \int_{A_K}^{B_K} \prod_{k \in K} \psi_{s-1}\left(\frac{\xi_k - z_k}{q}\right) \partial_J^{h_J} \partial_K^{(s)_K} f\, d\xi_I\, d\xi_K \right]_{\Delta_J},$$

where Φ runs through all partitions of $[1, k]$ into three disjoint sets of integers

$$I = \{i_1 < \ldots < i_\lambda\}, \quad J = \{j_1 < \ldots < j_\mu\} \quad \text{and} \quad K = \{k_1 < \ldots < k_\nu\},$$

and for any integer $h \geqslant 0$, we write

$$\psi_h(x) = (-1)^{h+1} \sum_{\substack{l = -\infty \\ l \neq 0}}^{\infty} \frac{e(lx)}{(2\pi i l)^{h+1}}.$$

This lemma can be proved by induction on the number of variables, starting from Lemma 5·2 of (3). We omit the details.

Note that ψ_h is bounded, being continuous and periodic.

LEMMA 3·3. *Let $\xi_i = \sum_{j=1}^{n} \xi_{ij} \omega_j$ $(i = 1, \ldots, m)$ and $\beta = \sum_{1}^{n} \beta_j \rho_j$ be elements of K_R, and*

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

let h_{ij} $(1 \leqslant i \leqslant m;\ 1 \leqslant j \leqslant n)$ be non-negative integers. Considering $e(S(\beta C(\xi)))$ as a function of the real variables ξ_{ij} and β_k, we have identically

$$\frac{\partial^h}{\partial\xi_{11}^{h_{11}} \dots \partial\xi_{m,n}^{h_{m,n}}}(e(S(\beta C(\xi))) = e(S(\beta C(\xi))) \sum_{\frac{1}{3}h \leqslant |\alpha| \leqslant h} \beta^\alpha \Phi_\alpha(\xi_{11}, \dots, \xi_{mn})),$$

where α runs through all multi-indices $(\alpha_1, \dots, \alpha_n)$, $\alpha_i \geqslant 0$, such that $|\alpha| = \Sigma\alpha_i$ lies between $\frac{1}{3}h$ and h (h stands for $\sum_{i,j} h_{i,j}$) and Φ_α is a homogeneous real polynomial in the ξ_{ij} of degree $3|\alpha| - h$.

In particular, if $|\xi_{ij}| \leqslant BP$ and $|\beta_i| \leqslant \mu$, with $P^3\mu > 1$, then the left side of the above identity is $\leqslant B'(P^2\mu)^h$, where B' depends only on B, h_{ij}, the coefficients of C and the field K.

Proof. The first part can be proved easily by induction on $h = \sum_{i,j} h_{ij}$. It follows that if $|\xi_{ij}| \leqslant BP$ and $|\beta_i| \leqslant \mu$, and $P^3\mu > 1$, the left side is bounded in absolute value by a constant multiple of

$$\sum_{\frac{1}{3}h \leqslant \nu \leqslant h} \mu^\nu P^{3\nu - h} = P^{3\nu_0 - h}\mu^{\nu_0}\{(P^3\mu)^{h-\nu_0+1} - 1\}/(P^3\mu - 1) \ll P^{3\nu_0-h}\mu^{\nu_0}(P^3\mu)^{h-\nu_0} = (P^2\mu)^h,$$

where ν_0 denotes the least integer $\geqslant h/3$.

The lemma is proved.

We shall now start on the proof of Lemma 3·1. Let $I = I(P)$ denote the expression on the left in Lemma 3·1, and $I_\gamma = \int_{B_\gamma} E(\alpha)\,d\alpha$, so that we have

$$I = \sum_{N\mathfrak{a} \leqslant P^{1-s\delta}} \sum_{\gamma \bmod \mathfrak{b}-1} I_\gamma.$$

For α in B_γ, we write $\alpha = \beta + \gamma$, so that we have

$$\beta = \sum_i \beta_i \rho_i, \quad |\beta_i| < P^{-2-\delta}(N\mathfrak{a}_\gamma)^{-1}.$$

Suppose the box $P\mathscr{B}$ is defined by the inequalities $A_{ij} < X_{ij} < B_{ij}$, where we assume that the A_{ij} and B_{ij} are non-integral. We then have for α in B_γ,

$$E(\alpha) = \sum_{Z_{ij}=1}^{N\mathfrak{a}_\gamma} e(S(\gamma C(Z))) \sum_{\substack{X_{ij} \equiv Z_{ij} (N\mathfrak{a}_\gamma) \\ A_{ij} < X_{ij} < B_{ij}}} e(S(\beta C(X))), \tag{9}$$

where Z stands for $(Z_1, \dots, Z_m)$, $Z_i = \sum_{j=1}^{n} Z_{ij}\omega_j$. Let s be a fixed positive integer such that $s\delta > n + 1$. We substitute for the inner sum in the above expression from Lemma 3·2.

Still retaining the notations of Lemma 3·2, let $\Phi = I \cup J \cup K$ be any partition of the set of double indices (i, j), $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, with K non-empty, that is $\nu > 0$, and let h_J be a fixed element of $[0, s-1]^J$. By Lemma 3·3, and using the fact that the A_{ij} and B_{ij} are $O(P)$, we deduce that the term arising from Lemma 3·2 corresponding to such a Φ and h_J is

$$\ll (N\mathfrak{a}_\gamma)^{\nu(s-1)-\lambda+|h_J|}(P^{-\delta}(N\mathfrak{a}_\gamma)^{-1})^{|h_J|+s\nu}P^{\lambda+\nu} = P^{-\delta(s\nu+|h_J|)}(PN\mathfrak{a}_\gamma^{-1})^{\lambda+\nu},$$

and since $PN\mathfrak{a}_\gamma^{-1} \geqslant P^{2\delta} > 1$, and $\nu \geqslant 1$, the above expression is $\ll P^{-\delta s}(P(N\mathfrak{a}_\gamma)^{-1})^{mn}$. Summation over the Z_{ij} and integration over B_γ gives the contribution of the terms

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

corresponding to a fixed Φ and h_J to I_γ to be $\ll P^{mn-\delta s}(P^{-2+\delta}N\mathfrak{a}_\gamma)^{-n}$, and hence the contribution to I is

$$P^{(m-2-\delta)n-s\delta}\sum_{N\mathfrak{a}\leqslant P^{1-\delta}}(N\mathfrak{a})^{1-n} \ll P^{(m-2-\delta)n-(s+2)\delta+1} \ll P^{mn-3n-\delta}$$

since $s\delta > n+1$. This takes care of the terms arising from Lemma 3·2 corresponding to the partitions Φ for which K is non-empty. For the estimation of the remaining terms, we have to make a proper choice of the box $\mathscr{B}$. The possibility of this choice is given by the next

LEMMA 3·4. *Let* $C(\xi) = \sum_{i=1}^{n} C_i(\xi_{11}, \ldots, \xi_{mn})\,\omega_i$, *where each* C_i *is a cubic form with rational integral coefficients in the variables* ξ_{ij}. *We assume that* $m > 1$ *and that* $C(\xi)$ *does not represent zero non-trivially. Then there exists a box*

$$\mathscr{B} = \{\xi \in (K_R)^m \mid a_{ij} < \xi_{ij} < b_{ij}\}$$

in $(K_R)^m$ *such that the following conditions hold*:

(*a*) $a_{ij} = m_{ij}/2N$, $b_{ij} = n_{ij}/2N$, *where* m_{ij} *and* n_{ij} *are odd integers, and* N *a positive integer. We have* $b_{ij} - a_{ij} < 1$;

(*b*) *there is a point* $\xi^0 = (\xi^0_{ij})$ *in* $\mathscr{B}$ *and a set* R *of* n *couples* (p_j, q_j) $(j = 1, \ldots, n)$ *such that we have*

$$C_i(\xi^0) = 0 \quad (i = 1, \ldots, n),$$

$$\det\left|\frac{\partial C_i}{\partial \xi_{(p_j, q_j)}}(\xi^0)\right| \neq 0.$$

Let T *denote the set of couples* (i, j) $(1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n)$ *not belonging to* R;

(*c*) *for any subset* S *of* R, *there is a subset* S' *of* $\{1, 2, \ldots, n\}$ *such that for any fixed values of* ξ_{ij} *for* $(i, j) \in R - S$ *satisfying* $a_{ij} < \xi_{ij} < b_{ij}$, *the mapping* $(\xi_T, \xi_S) \to (\xi_T, \eta_{S'})$ *defined by* $\eta_i = C_i(\xi)$ *is an analytic isomorphism of the domain defined by* $a_T < \xi_T < b_T$, $a_S < \xi_S < b_S$ *onto a domain in the* $(\xi_T, \eta_{S'})$ *space containing the domain defined by* $a_T < \xi_T < b_T$, $|\eta_{S'}| < \epsilon$ (ξ_T, ξ_S, *etc., stand for the set of variables* ξ_{ij} *with* $(i, j) \in T, S$, *etc., respectively*; ϵ *is some fixed positive quantity*).

In order not to interrupt our discussion, we shall postpone the proof of this lemma to the end of this section.

Let us now turn to the estimation of those terms arising from the substitution from Lemma 3·2 in (9), corresponding to a fixed partition Φ of the double-indices into two sets I and J (in the notations of the same lemma) with J non-empty, and to a fixed h_J. Let $I = \{(i_1, j_1), \ldots, (i_p, j_p)\}$ and $J = \{(i'_1, j'_1), \ldots, (i'_q, j'_q)\}$, with $q > 0$, and let $h_J = (h_{(i'_1, j'_1)}, \ldots, h_{(i'_q, j'_q)})$. Such a term when summed over the Z_{ij} and integrated over B_γ gives

$$\pm (N\mathfrak{a}_\gamma)^{-p+h}T\sum_{\frac{1}{2}h\leqslant|\alpha|\leqslant h}\int_{A_I}^{B_I}\Phi_\alpha(\xi)\left\{\int_{|\beta|<\mu}\beta^\alpha\, e(S(\beta C(\xi)))\,d\beta\right\}d\xi_I, \tag{10}$$

where the Φ_α are as in Lemma 3·3, each one of the variables $\xi_{(i'_1, j'_1)}, \ldots, \xi_{(i'_q, j'_q)}$ is fixed at a corresponding A_{ij} or B_{ij}, μ stands for the expression $P^{-2-\delta}(N\mathfrak{a}_\gamma)^{-1}$, and T is defined by the equation

$$T = \sum_{Z_{ij}=1}^{N\mathfrak{a}_\gamma} e(S(\gamma C(Z)))\,\psi_{h_{(i'_1, j'_1)}}\left(\frac{\xi_{(i'_1, j'_1)} - Z_{(i'_1, j'_1)}}{N\mathfrak{a}_\gamma}\right)\cdots\psi_{h_{(i'_q, j'_q)}}\left(\frac{\xi_{(i'_q, j'_q)} - Z_{(i'_q, j'_q)}}{N\mathfrak{a}_\gamma}\right).$$

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

Let us put

$$S_r(x) = \int_{-x}^{x} t^r e(t)\,dt.$$

Then (10) becomes

$$\pm (N\mathfrak{a}_\gamma)^{-p+h} T \sum_{\frac{1}{2}h \leqslant |\alpha| \leqslant h} \int_{A_I}^{B_I} \Phi_\alpha(\xi) \prod_{r=1}^{n} \frac{S_{\alpha_r}(\mu C_r(\xi))}{(C_r(\xi))^{\alpha_r+1}}\,d\xi_I.$$

If we change ξ (including the fixed ξ_J) to $P\xi$, and use the fact that Φ_α is homogeneous of degree $3|\alpha| - h$, the above expression becomes

$$\pm (N\mathfrak{a}_\gamma)^{-p+h} T \sum_{\frac{1}{2}h \leqslant |\alpha| \leqslant h} P^{p-3n-h} \int_{a_I}^{b_I} \Phi_\alpha(\xi) \prod_{r=1}^{n} \frac{S_{\alpha_r}(P^3\mu C_r(\xi))}{(C_r(\xi))^{\alpha_r+1}}\,d\xi_I.$$

Now let $S = R \cap I$ and S' the subset of $\{1, 2, \ldots, n\}$ corresponding to S by Lemma 3·4(c); let $T' = I - R \cap I = T \cap I$. For any fixed values of ξ_{R-I} in the respective intervals, the mapping $\xi_I = (\xi_S, \xi_{T'}) \to (\eta_{S'}, \xi_{T'})$ defined by $\eta_i = C_i(\xi)$ is an analytic isomorphism of the parallelepiped $a_I < \xi_I < b_I$ onto a domain in the $(\eta_{S'}, \xi_{T'})$ space, whose Jacobian we shall denote by $J(\xi_{T'}, \eta_{S'})$. Writing ϕ for $P^3\mu$, the above expression then transforms into

$$\pm (N\mathfrak{a}_\gamma)^{-p+h} T \sum_{\frac{1}{2}h \leqslant |\alpha| \leqslant h} P^{p-3n-h}$$
$$\times \int \prod_{r \in S'} \frac{S_{\alpha_r}(\phi\eta_r)}{\eta_r^{\alpha_r+1}} \left\{ \int_{\mathscr{D}(\eta_{s'})} \prod_{r \notin S'} \frac{S_{\alpha_r}(\phi C_r(\xi))}{(C_r(\xi))^{\alpha_r+1}} \Phi_\alpha(\xi)\,|J(\xi_{T'}, \eta_{S'})|\,d\xi_{T'} \right\} d\eta_{S'},$$

where the integration with respect to $\eta_{S'}$ is over a certain bounded domain and for every $\eta_{S'}$ in this domain, $\mathscr{D}(\eta_{S'})$ is a uniformly bounded domain in the $\xi_{T'}$-space. It is easy to see (by direct evaluation, or otherwise), that we have $S_p(x) \ll x^p$ for all x and $S_p(x) \ll x^{p+1}$ for $x \leqslant 1$. Since $\Phi_\alpha(\xi)$ and J are absolutely and uniformly bounded on any bounded domain, the above integral is

$$\ll \phi^{\sum_{r \notin S'} (\alpha_r+1)} \prod_{r \in S} \left\{ \int_{-A}^{A} \left| \frac{S_{\alpha_r}(\phi\eta_r)}{\eta_r^{\alpha_r+1}} \right| d\eta_r \right\} \ll \phi^{|\alpha|+n_0} \log^n \phi \ll \phi^{|\alpha|+n_0} \log^n P,$$

where n_0 denotes the number (n – number of elements in S). Hence (10) is bounded by

$$|T|\,(P(N\mathfrak{a}_\gamma)^{-1})^{p-h} P^{-3n} (P^3\mu)^{n_0+|\alpha|} \log^n P = |T|\,(P(N\mathfrak{a}_\gamma)^{-1})^{p-h+n_0+|\alpha|} P^{-3n-\delta(n_0+|\alpha|)} \log^n P$$
$$\ll |T|\,(P(N\mathfrak{a}_\gamma)^{-1})^{p+n_0} P^{-3n-\delta n_0}.$$

We shall now estimate $|T|$. We have for any integer $k \geqslant 0$ and any integer $Q \geqslant 0$,

$$\psi_k(x) = (-1)^{k+1} \sum_{l=-Q}^{Q}{}' \frac{e(lx)}{(2\pi i l)^{k+1}} + R_Q,$$

where the $'$ over the summation sign means that there is no term corresponding to $l = 0$, and

$$|R_Q| \ll \frac{1}{Q^{k+1}\|x\|}.$$

We shall now assume that P varies through odd multiples of the integer denoted by N in Lemma 3·4(a). It follows that for Z_{ij} integral and $\xi_{ij} = Pa_{ij}$ or Pb_{ij},

$$\left\| \frac{\xi_{ij} - Z_{ij}}{N\mathfrak{a}_\gamma} \right\| \gg \frac{1}{N\mathfrak{a}_\gamma},$$

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

and on substituting from the above expression for $\psi_k(x)$ into T, with $Q = (N\mathfrak{a}_\gamma)^{mn+1}$, we obtain

$$|T| \leqslant \left(\frac{1}{2\pi}\right)^{h+q} \sum_{l_1,\ldots,l_q=-(N\mathfrak{a}_\gamma)^{mn+1}}^{(N\mathfrak{a}_\gamma)^{mn+1}\prime} |l_1|^{-h_{(i_1',j_1')}-1} \ldots |l_q|^{-h_{(i_q',j_q')}-1} \times \left| \sum_{Z_{ij}=1}^{N\mathfrak{a}_\gamma} e(S(\gamma C(Z))) + \frac{l_1 Z_{(i_1',j_1')} + \ldots + l_q Z_{(i_q',j_q')}}{N\mathfrak{a}_\gamma} \right|$$

and by our assumption in Lemma 3·1, we get

$$|T| \ll (N\mathfrak{a}_\gamma)^{mn-\omega} (\log N\mathfrak{a}_\gamma)^{mn} \ll (N\mathfrak{a}_\gamma)^{mn-\omega'}$$

for any fixed $\omega' < \omega$. Substituting in our earlier estimate for (10), summing over all $\gamma \bmod \mathfrak{d}^{-1}$ with $\mathfrak{a}_\gamma = \mathfrak{a}$ and finally summing over all $\mathfrak{a}$ with $N\mathfrak{a} \leqslant P^{1-2\delta}$ we deduce that the total contribution to I of the terms arising from a partition Φ for which J is non-empty is

$$\ll P^{p+n_0-3n-\delta n_0} \log^n P \sum_{N\mathfrak{a} < P^{1-2\delta}} (N\mathfrak{a})^{mn-p-n_0-\omega'+1}$$

$$\ll P^{p+n_0-3n-\delta n_0} \log^{n+1} P (1 + P^{mn-p-n_0-\omega'+2}).$$

Since by definition $n_0 \leqslant q$, we must have $p + n_0 \leqslant p + q = mn$, and if $p + n_0 = mn$, we must have $n_0 = q \geqslant 1$. Hence if we put $\rho = \min(\delta, \omega' - 2)$, the above expression is $O(P^{mn-3n-\rho} \log^{n+1} P)$ which is $o(P^{(m-3)n})$.

To complete the proof of Lemma 3·1, it only remains to estimate the main term which arises from the partition Φ for which J and K are empty, so that I is the set of all couples (i, j), $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$. A calculation exactly similar to the one made above shows that the contribution of this term to I_γ is

$$(N\mathfrak{a}_\gamma)^{-mn} S_1((0), \gamma) \int_{P\mathscr{B}} \left\{ \int_{-\mu}^{\mu} e(S(\beta C(\xi)))\, d\beta \right\} d\xi = P^{(m-3)n} (N\mathfrak{a}_\gamma)^{-1} S_\gamma \int_{\mathscr{B}} \left(\prod_{r=1}^{n} \frac{\sin \phi C_r(\xi)}{C_r(\xi)} \right) d\xi$$

with the notations of the previous paragraph. Changing from (ξ_R, ξ_T) to (η, ξ_T), the above becomes

$$P^{(m-3)n} (N\mathfrak{a}_\gamma)^{-m} S_\gamma \int_{a_T}^{b_T} d\xi_T \left\{ \int_{\mathscr{D}(\xi_T)} \prod_{r=1}^{n} \frac{\sin \phi\eta_r}{\eta_r} |J(\xi_T, \eta)|\, d\eta \right\},$$

where $J(\xi_T, \eta)$ denotes the Jacobian of the above transformation and $\mathscr{D}(\xi_T)$ is a certain uniformly bounded domain in the η-space which always contains the domain $|\eta| < \epsilon$, by Lemma 3·4(*c*).

Now split the domain $\mathscr{D}(\xi_T)$ into 2^n parts in each of which a certain subset of the variables η remain $> \epsilon$, while the others remain $< \epsilon$. We shall show that on any of these subdomains on which at least one η_i remains $> \epsilon$, the integral over this subdomain of $\prod_{r=1}^{n} \eta_r^{-1} \sin \phi\eta_r J(\xi_T, \eta)$ tends to zero uniformly with respect to ξ_T as ϕ tends to ∞. Assume for instance that $\eta_n > \epsilon$ in such a subdomain. We rewrite the integral of the above function as a repeated integral

$$\int \frac{\sin \phi\eta_1}{\eta_1} d\eta_1 \int \frac{\sin \phi\eta_2}{\eta_2} d\eta_2 \ldots \int \frac{\sin \phi\eta_n}{\eta_n} d\eta_n.$$

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

Now, since the boundary of $\mathscr{D}(\xi_T)$ consists of algebraic hypersurfaces, it is easy to see that the line through any point $(\eta_1, \ldots, \eta_n)$ in $\mathscr{D}(\xi_T)$ parallel to the η_n-axis meets the boundary of $\mathscr{D}(\xi_T)$ in a uniformly bounded number of points. Hence the last integral with respect to η_n is over a uniformly bounded number of intervals in η_n on all of which intervals we have $|\eta_n| > \epsilon$. Since $|J(\xi_T, \eta)|/\eta_n$ is uniformly bounded and of uniformly bounded variation with respect to η_n in any bounded interval on which $|\eta_n| > \epsilon$, we deduce that the above repeated integral is

$$\ll \frac{1}{\phi}\left\{\int_{-A}^{A}\left|\frac{\sin\phi\eta}{\eta}\right|d\eta\right\}^{n-1} \ll \frac{\log^{n-1}\phi}{\phi}$$

$\to 0$ uniformly as $\phi \to \infty$, and since $\phi = P^3\mu = P^{1-\delta}(N\mathfrak{a}_\gamma)^{-1} \geqslant P^\delta$, also as $P \to \infty$. Hence the 'main term' of I_γ is

$$P^{mn-3n}(N\mathfrak{a}_\gamma)^{-m} S_\gamma\left[\int_{a_T}^{b_T} d\xi_T\left\{\int_{|\eta|<\epsilon}\prod_r \frac{\sin\phi\eta_r}{\eta_r}|J(\xi_T,\eta)|\,d\eta\right\} + o(1)\right].$$

Now since $|J(\xi_T, \eta)|$ (being always equal to $J(\xi_T, \eta)$ or to $-J(\xi_T, \eta)$ in $\mathscr{D}(\xi_T)$) is analytic in η, we may write

$$|J(\xi_T, \eta)| = |J(\xi_T, 0)| + \sum_i \eta_i \psi_i(\xi_T, \eta),$$

where the ψ_i are again analytic. It can be shown by an argument similar to the one used above that

$$\int_{|\eta|<\epsilon}\prod_r \frac{\sin\phi\eta_r}{\eta_r}\eta_i\psi_i(\xi_T,\eta)\,d\eta$$

$\to 0$ as $P \to \infty$ for all i uniformly. Hence the main term reduces to

$$P^{(m-3)n}(N\mathfrak{a}_\gamma)^{-m} S_\gamma\left\{\int_{a_T}^{b_T}|J(\xi_T,0)|\,d\xi_T\left(\int_{-\epsilon}^{\epsilon}\frac{\sin\phi x}{x}dx\right)^n + o(1)\right\}$$
$$= P^{(m-3)n}(N\mathfrak{a}_\gamma)^{-m} S_\gamma(A + o(1)),$$

where
$$A = \pi^n\int_{a_T}^{b_T}|J(\xi_T,0)|\,d\xi_T > 0$$

and $o(1)$ tends to zero uniformly as $P \to \infty$.

On summing over the γ for which $\mathfrak{a}_\gamma = \mathfrak{a}$ and summing over all $\mathfrak{a}$ with $N\mathfrak{a} \leqslant P^{1-2\delta}$, we see that the main term in I is

$$AP^{(m-3)n}\sum_{\substack{\gamma \bmod \mathfrak{b}^{-1}\\ N\mathfrak{a}_\gamma \leqslant P^{1-2\delta}}}(N\mathfrak{a}_\gamma)^{-m} S_\gamma + o\Big(P^{(m-3)n}\sum_{\substack{\gamma \bmod \mathfrak{b}^{-1}\\ N\mathfrak{a}_\gamma \leqslant P^{1-2\delta}}}(N\mathfrak{a}_\gamma)^{-m}|S_\gamma|\Big).$$

Since $(N\mathfrak{a}_\gamma)^{m(n-1)} S_\gamma = S_1((0), \gamma)$, the assumption of Lemma 4·1 implies that

$$S_\gamma = O((N\mathfrak{a}_\gamma)^{m-\omega}),$$

with $\omega > 2$, and hence the series

$$\mathfrak{r} = \sum_{\gamma \bmod \mathfrak{b}^{-1}}(N\mathfrak{a}_\gamma)^{-m} S_\gamma$$

converges absolutely.

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

Hence we obtain finally that

$$I = A\mathfrak{r}P^{(m-3)n} + o(P^{(m-3)n}),$$

and Lemma 3·1 will be proved completely if we can show that $\mathfrak{r} > 0$. This will be our next task.

LEMMA 3·5. *Under the assumptions of Lemma* 3·1, *we have*

$$\mathfrak{r} > 0.$$

Proof. It can be shown by standard arguments that if γ_1 and γ_2 are elements of K different from zero such that $\mathfrak{a}_{\gamma_1}$ and $\mathfrak{a}_{\gamma_2}$ are coprime, we have $S_{\gamma_1} S_{\gamma_2} = S_{\gamma_1+\gamma_2}$. For any prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, we define

$$\chi(\mathfrak{p}) = 1 + \sum_{p \geqslant 1} (N\mathfrak{p})^{-mp} \sum_{\substack{\gamma \bmod \mathfrak{d}^{-1} \\ \mathfrak{a}_\gamma = \mathfrak{p}^p}} S_\gamma;$$

this series is absolutely convergent, since it is majorized by the absolute values of the terms of the series for $\mathfrak{r}$, and we deduce easily that

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

the product being absolutely convergent. To prove the lemma, it is therefore sufficient to show that $\chi(\mathfrak{p}) > 0$ for all $\mathfrak{p}$.

Now, let $M(\mathfrak{p}^N)$ denote for any integer N the number of solutions of the congruence

$$C(X) \equiv O(\mathfrak{p}^N),$$

when the X_i run through a complete system of residues modulo $\mathfrak{p}^N$. Then it can be shown easily that

$$\sum_{p=0}^{N} (N\mathfrak{p})^{-mp} \sum_{\substack{\gamma \bmod \mathfrak{d}^{-1} \\ \mathfrak{a}_\gamma = \mathfrak{p}^p}} S_\gamma = (N\mathfrak{p})^{-(m-1)N} M(\mathfrak{p}^N),$$

and therefore

$$\chi(\mathfrak{p}) = \lim_{N \to \infty} (N\mathfrak{p})^{-N(m-1)} M(\mathfrak{p}^N).$$

Let $K_\mathfrak{p}$ denote the $\mathfrak{p}$-adic completion of the field K. Then it is well known (and is easily established) that if the form $C(X)$ has a non-trivial *non-singular* zero in $K_\mathfrak{p}$, then

$$\lim_{N \to \infty} (N\mathfrak{p})^{-N(m-1)} M(\mathfrak{p}^N) > 0.$$

From the fact that $C(X)$ does not represent zero non-trivially it follows that it is non-degenerate, i.e. we cannot reduce it to a form in a fewer number of variables by making a non-singular linear change of variable in $C(X)$. But for a non-degenerate cubic form over a $\mathfrak{p}$-adic field in more than 9 variables, the existence of a non-singular zero has been proved by several authors (see, for instance, (2)).

This finishes the proof of Lemma 3·5.

Lemma 3·1 is therefore completely proved, except for the proof of Lemma 3·4, which we shall now give.

Proof of Lemma 3·4. It is enough to prove the existence of a point ξ^0 in $(K_R)^m$, $\xi^0 \neq 0$, such that

$$C_i(\xi^0) = 0 \quad (i = 1, \ldots, n), \quad \operatorname{Rank} \left\| \frac{\partial C_i}{\partial \xi_{(j,k)}} (\xi^0) \right\| = n.$$

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

For, once we have found such a ξ^0, we can find a box $\mathscr{B}$ satisfying the conditions (a), (b) and (c) by the implicit function theorem (to get (a), we use the fact that the rational numbers of the form $a/2N$, where a is an odd integer and N a positive integer, are dense in R). We are therefore reduced to proving the existence of a real non-trivial, non-singular zero of the variety defined by the equations $C^i(\xi) = 0$ $(1 \leqslant i \leqslant n)$.

Let $\chi^{(1)}, \ldots, \chi^{(r_1)}$ denote the distinct isomorphisms of K into R, and $\chi^{(r_1+1)}, \ldots, \chi^{(n)}$ the distinct isomorphisms of K into C such that $\chi^{(r_1+r_2+p)} = \overline{\chi}^{(r_1+p)}$ $(1 \leqslant p \leqslant r_2)$. For any $x \in K$, we shall put $x^{(i)} = \chi^{(i)}(x)$, and $C^{(i)}(X)$ will denote the form deduced from $C(X)$ by applying $\chi^{(i)}$ to its coefficients. For $1 \leqslant p \leqslant r_2$, we put

$$C^{(r_1+p)}(X + iY) = C_1^{(r_1+p)}(X, Y) + iC_2^{(r_1+p)}(X, Y),$$

where $C_1^{(r_1+p)}$ and $C_2^{(r_1+p)}$ are forms in the variables $X = (X_{ij})$ and $Y = (Y_{ij})$ with real coefficients.

If we now make the following real non-singular transformation of the variables ξ_{ij},

$$\eta_i^{(p)} = \sum_j \xi_{ij}\omega_j(p) \qquad (1 \leqslant p \leqslant r_1),$$

$$\left.\begin{aligned} \eta_i'^{(r_1+p)} &= \sum_j \xi_{ij}\omega_j'^{(r_1+p)} \\ \eta_i''^{(r_1+p)} &= \sum_j \xi_{ij}\omega_j''^{(r_1+p)} \end{aligned}\right\} \quad (1 \leqslant p \leqslant r_2),$$

where $\omega_j'^{(r_1+p)}$ and $\omega_j''^{(r_1+p)}$ stand for the real and imaginary parts of $\omega_j^{(r_1+p)}$, the variety in the ξ-space defined by $C_i(\xi) = 0$ $(i = 1, \ldots, n)$ gets transformed into the variety in the η-space defined by the equations

$$C^{(p)}(\eta_1^{(p)}, \ldots, \eta_m^{(p)}) = 0 \quad (1 \leqslant p \leqslant r_1),$$

$$\left.\begin{aligned} C_1^{(r_1+p)}(\eta_1'^{(r_1+p)}, \ldots, \eta_m'^{(r_1+p)}, \eta_1''^{(r_1+p)}, \ldots, \eta_m''^{(r_1+p)}) &= 0 \\ C_2^{(r_1+p)}(\eta_1'^{(r_1+p)}, \ldots, \eta_m'^{(r_1+p)}, \eta_1''^{(r_1+p)}, \ldots, \eta_m''^{(r_1+p)}) &= 0 \end{aligned}\right\} \quad (1 \leqslant p \leqslant r_2),$$

and is therefore the product of the varieties V_p defined by $C^{(p)}(X) = 0$ $(1 \leqslant p \leqslant r_1)$ and the varieties W_q defined by $C_1^{(r_1+q)}(X, Y) = 0$, $C_2^{(r_1+q)}(X, Y) = 0$ $(1 \leqslant q \leqslant r_2)$. Hence it is enough to find a real non-trivial, non-singular point on each of the varieties V_p, W_q. It is shown in (3), Lemma 6·1 that such a point exists on each V_p. As for W_q, it is easy to see that if $Z = X + iY$ is a non-singular zero of $C^{(r_1+q)}(Z) = 0$, where X and Y are real, (X, Y) is a real non-singular zero of W_q. This concludes the proof of Lemma 3·4.

We make a final remark concerning the exponential sum $S_1(l, \gamma)$. Suppose $C(X)$ and $C'(Y)$ are two cubic forms in the disjoint sets of variables X and Y, and $S_1(l, \gamma)$ and $S_1'(l', \gamma)$ are the corresponding sums. Then if $S_1''((l, l'), \gamma)$ denotes the sum corresponding to the form $C(X) + C'(Y)$ in the variables X and Y, we have clearly

$$S_1''((l, l'), \gamma) = S_1'(l, \gamma)\, S_1'(l', \gamma)$$

and therefore the uniform estimates $|S_1(l, \gamma)| \ll (N\mathfrak{a}_\gamma)^{mn-\omega}$, $|S_1'(l', \gamma)| \ll (N\mathfrak{a}_\gamma)^{m'n-\omega'}$ imply the uniform estimate $|S_1''((l, l'), \gamma)| \ll (N\mathfrak{a}_\gamma)^{(m+m')n-(\omega+\omega')}$, where m and m' are the number of variables X, and Y respectively. We shall make use of this remark later.

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

4. *Proof of the theorem.* We preserve the notations of §§ 2, 3.

We shall denote by $\mathfrak{m}$ the set of points of $\mathscr{R}$ which do not belong to the major arcs, i.e. $\mathfrak{m} = \mathscr{R} - \bigcup_{N\mathfrak{a}_\gamma \leqslant P^{1-2\delta}} B_\gamma$. For any θ with $0 < \theta < 1$, we shall denote by $\mathfrak{m}_\theta$ the set of points $\alpha \in \mathfrak{m}$ for which there does not exist an integer $\lambda \in P^{2\theta+\delta}B_0$, $\lambda \neq 0$, and a $\mu \in \mathfrak{d}^{-1}$ such that we have

$$\lambda\alpha - \mu = \Sigma\epsilon_i\rho_i, \quad |\epsilon_i| < P^{-3+2\theta+\delta}.$$

We shall show that if $\theta < \{1-\delta(n+2)\}/2n$ and P is large enough, $\mathfrak{m}_\theta = \mathfrak{m}$. Suppose on the contrary that there exists an integer λ and an element $\mu \in \mathfrak{d}^{-1}$ satisfying the above conditions. Putting $\gamma = \mu/\lambda$, we have clearly $\lambda \in \mathfrak{a}_\gamma$ and therefore

$$N\mathfrak{a}_\gamma \leqslant N\lambda \ll P^{n(2\theta+\delta)},$$

and by our assumption on θ, it follows that if P is large enough, $N\mathfrak{a}_\gamma \leqslant P^{1-2\delta}$. Moreover, we have

$$\alpha - \gamma = \alpha - \mu/\lambda = \lambda^{-1}\Sigma\epsilon_i\rho_i = \sum_{i=1}^{n}\epsilon_i\left(\sum_{j=1}^{n}\alpha_{ij}\rho_j\right) = \sum_{j=1}^{n}(\Sigma\alpha_{ij}\epsilon_i)\rho_j = \sum_{j=1}^{n}\beta_j\rho_j,$$

where (a_{ij}) is the regular representation matrix of λ^{-1} with respect to the basis $\rho_1, \ldots, \rho_n$ of K over Γ. Hence it follows that (a_{ij}) is the inverse of the regular representation matrix of λ with respect to the same basis. Hence for any i, j $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$, we have

$$a_{ij} \ll P^{(n-1)(2\theta+\delta)}(N\lambda)^{-1}, \quad |\beta_j| \ll P^{-3+2\theta+\delta+(n-1)(2\theta+\delta)}(N\lambda)^{-1} \ll P^{-3+n(2\theta+\delta)}(N\mathfrak{a}_\gamma)^{-1},$$

and therefore for P large, $|\beta_j| \leqslant P^{-2-2\delta}(N\mathfrak{a}_\gamma)^{-1}$, which shows that α lies on the 'major arc' B_γ, and hence cannot be in $\mathfrak{m}$. Our contention is proved.

For any θ with $0 < \theta < 1$, we shall denote by $\mathscr{E}(\theta)$ the set of points $\alpha \in \mathscr{R}$ for which there exists an integer $\lambda \in P^{2\theta+\delta}B_0$, $\lambda \neq 0$, and a $\mu \in \mathfrak{d}^{-1}$, such that

$$\lambda\alpha - \mu = \Sigma\epsilon_i\rho_i, \quad |\epsilon_i| < P^{-3+2\theta+\delta}.$$

We have $$\mathfrak{m} - \mathfrak{m}_\theta = \mathfrak{m} \cap \mathscr{E}(\theta) \subset \mathscr{E}(\theta).$$

We want to estimate the measure of $\mathscr{E}(\theta)$. For a fixed λ and μ, the set of α having the above property is equal to $(P^{-3+2\theta+\delta})^n(N\lambda)^{-1}$, since multiplication by λ multiplies the n-dimensional measures of sets by $N\lambda$. Since for any fixed integer λ, there correspond at most $O(N\lambda)$ elements $\mu \in \mathfrak{d}^{-1}$ for which there exists an $\alpha \in \mathscr{R}$ satisfying the above inequalities with respect to this λ and μ, we obtain

$$|\mathscr{E}(\theta)| \ll \sum_{\lambda \in P^{2\theta+\delta}B_0} (P^{-3+2\theta+\delta})^n (N\lambda)^{-1} N\lambda \ll (P^{-3+4\theta+2\delta})^n.$$

We need two lemmas which give estimates for exponential sums involving a single cube.

LEMMA 4·1. *For $\alpha \in \mathscr{R}$, B a fixed box in K_R, d an integer in K and $P > 1$, we define*

$$T_d(\alpha) = \sum_{X \in PB} e(S(\alpha d X^3)).$$

Then for $\alpha \in \mathfrak{m}_\theta$ and P large, we have

$$|T_d(\alpha)| < P^{(1-\frac{1}{2}\theta)n}.$$

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

Proof. We apply Lemma 1·3 of § 1 to $\Gamma(X) = \alpha dX^3$, with $\theta + \frac{1}{3}\delta$ instead of θ and $\kappa = \frac{1}{4}\theta$; we have $B_1(X, Y) = 6\alpha dXY$. We conclude that if the above estimate for $|T_d(\alpha)|$ is not valid, and P large enough, there exist $X \in P^{\theta+\frac{1}{3}\delta}B_0$, $Y \in P^{\theta+\frac{1}{3}\delta}B_0$, neither zero, and $\mu \in \mathfrak{b}^{-1}$ such that

$$6\alpha dXY - \mu = \sum_1^n \epsilon_i \rho_i,$$

$$|\epsilon_i| < P^{-3+2\theta+\frac{2}{3}\delta} < P^{-3+2\theta+\delta}.$$

For, the number of solutions of these inequalities is, by Lemma 1·3, $\geqslant \{P^{\theta+\frac{2}{3}\delta}(\log P)^{-1}\}^n$ and the number of solutions with X or Y zero is $\ll P^{n\theta}$.

But now, $6dXY$ is a non-zero integer and is in $P^{2\theta+\delta}B_0$ for P large. This contradicts the fact that $\alpha \in \mathfrak{m}_\theta$, proving the lemma.

LEMMA 4·2. *Let $\gamma \in K$ and let $l_1, \ldots, l_n$ be any set of rational integers. Then if*

$$X = \sum_1^n X_i \omega_i$$

runs through a complete system of residues mod $N\mathfrak{a}_\gamma$, *we have for any $\epsilon > 0$,*

$$\left| \sum_{X \bmod N\mathfrak{a}_\gamma} e\left(S(\gamma dX^3) + \frac{l_1 X_1 + \ldots + l_n X_n}{N\mathfrak{a}_\gamma}\right)\right| \ll (N\mathfrak{a}_\gamma)^{n-\frac{1}{3}+\epsilon}.$$

Proof. Let $\mathfrak{a} = \text{g.c.d.}\left(\gamma, \frac{\Sigma l_i' \rho_i}{N\mathfrak{a}_\gamma}\right)$ and $\mathfrak{b} = (1, \mathfrak{a}\mathfrak{d})^{-1}$.

It is clear that $\mathfrak{a}_\gamma$ divides $\mathfrak{b}$, which in turn divides $N\mathfrak{a}_\gamma$. The above sum can be rewritten as

$$\sum_{X \bmod N\mathfrak{a}_\gamma} e\left(S\left(\gamma dX^3 + \frac{\Sigma l_i \rho_i}{N\mathfrak{a}_\gamma} X\right)\right) = \frac{(N\mathfrak{a}_\gamma)^n}{N\mathfrak{b}} \sum_{X \bmod \mathfrak{b}} e\left(S\left(\gamma dX^3 + \frac{\Sigma l_i \rho_i}{N\mathfrak{a}_\gamma} X\right)\right).$$

By Hua (4), the latter sum is $\ll (N\mathfrak{b})^{\frac{2}{3}+\epsilon}$, and therefore for the sum we started with, we obtain

$$|\Sigma| \ll (N\mathfrak{a}_\gamma)^n (N\mathfrak{b})^{\frac{1}{3}+\epsilon} \ll (N\mathfrak{a}_\gamma)^{n-\frac{1}{3}+\epsilon}$$

since $N\mathfrak{b} \geqslant N\mathfrak{a}_\gamma$. Lemma 4·2 is proved.

LEMMA 4·3. *Let*

$$C(X, Y) = C^{(1)}(X_1, \ldots, X_{m_1}) + d_1 Y_1^3 + \ldots + d_t Y_t^3$$

be a cubic form with symmetric integral coefficients in K which does not represent zero. We assume moreover that

(i) $0 \leqslant t \leqslant 8$;

(ii) *if r is the least integer $> 7 - \frac{1}{2}t$, then $m_1 \geqslant 2(r+1)$.*

Then $C^{(1)}(X)$ splits with remainder $m_1 - r$.

Proof. Assuming that $C^{(1)}(X)$ does not split with remainder $m_1 - r$, we shall show that $C(X, Y)$ represents zero non-trivially.

For any $\gamma \in K$, and any sets of rational integers

$$l = (l_{ij}) \quad (1 \leqslant i \leqslant m_1,\ 1 \leqslant j \leqslant n) \quad \text{and} \quad l' = (l'_{kj}) \quad (1 \leqslant k \leqslant t,\ 1 \leqslant j \leqslant n),$$

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

let $S_1^{(1)}(l,\gamma)$ and $S_1(l,l',\gamma)$ be the exponential sums associated to the forms $C^{(1)}$ and C respectively. We may apply Lemma 2·3 to the form $C^{(1)}$ with $\kappa = \frac{1}{4}(r+1)-\delta$, since

$$0 < 8\kappa = 2(r+1)-8\delta < m_1$$

and $C^{(1)}(x)$ does not split with remainder $m_1 - r$ which is the least integer

$$\geqslant m_1 - 4\kappa = m_1 - r - 1 + 4\delta.$$

Hence we obtain $$|S_1^{(1)}(l,\gamma)| \ll (N\mathfrak{a}_\gamma)^{m_1 n - \frac{1}{4}(r+1)+\delta}.$$

This, coupled with Lemma 4·2 and the remark made at the end of § 3, gives

$$|S_1(l,l',\gamma)| \ll (N\mathfrak{a}_\gamma)^{(m_1+t)n-\frac{1}{4}(r+1)-\frac{1}{8}t+2\delta}$$

and $$\tfrac{1}{4}(r+1)+\tfrac{1}{8}t-2\delta \geqslant \tfrac{1}{4}(r+1)+\tfrac{1}{8}t-2\delta = \tfrac{1}{4}(r+1+\tfrac{1}{2}t)-2\delta > 2$$

if δ is small enough, by our assumption (ii). Hence by Lemma 3·1, there is a box $\mathscr{B}$ in $(K_R)^{m_1+t}$ such that if $E(\alpha)$ denotes the exponential sum attached to $C(X,Y)$, the contribution of the major arcs to the integral of $E(\alpha)$ is

$$AP^{(m_1+t-3)n} + o(P^{(m_1+t-3)n}) \quad (A > 0).$$

We shall now show that the contribution of the 'minor arcs' $\mathfrak{m}$ is $o(P^{(m_1+t-3)n})$. Let $\mathscr{B}^{(1)}$ denote the projection of the box $\mathscr{B}$ in $(K_R)^{m_1+t}$ onto the product of the first m_1 components and B_i the projection into the (m_1+i)th component for $i = 1,\ldots,t$. Let $E^{(1)}(\alpha)$ denote the exponential sum associated to $C^{(1)}$ and the box $\mathscr{B}^{(1)}$, and $T_{d_i}(\alpha)$ the exponential sum associated to $d_i Y_i^3$ and the box B_i, for $i = 1,\ldots,t$. We then have

$$E(\alpha) = E^{(1)}(\alpha) \prod_{i=1}^{t} T_{d_i}(\alpha).$$

The conditions of Lemma 2·2 are fulfilled by the form $C^{(1)}(X)$ with $\kappa = \frac{1}{2}(r+1)\theta(1-\delta)$, and we obtain the estimate

$$|E^{(1)}(\alpha)| < P^{(m_1 - \frac{1}{2}(r+1)\theta(1-\delta))n}$$

for P large and $\alpha \in \mathfrak{m}_\theta$. Hence by Lemma 4·1, we get for $\alpha \in \mathfrak{m}_\theta$

$$|E(\alpha)| < P^{(m_1 - \frac{1}{2}(r+1)\theta(1-\delta)+t-\frac{1}{4}t\theta)n}.$$

Applying this with $\theta = \frac{7}{8}$, we get

$$\int_{\mathfrak{m}_{\frac{7}{8}}} |E(\alpha)|\, d\alpha = o(P^{(m_1+t-3)n}),$$

since

$$m_1 - \tfrac{1}{2}(r+1)\tfrac{7}{8}(1-\delta) + t - \frac{7t}{32} < m_1 + t - \tfrac{1}{2}(8-\tfrac{1}{2}t)\tfrac{7}{8}(1-\delta) - \frac{7t}{32}$$

$$= m_1 + t - \frac{7}{2} + \frac{7\delta}{32}(16-t) < m_1 + t - 3$$

if δ is small.

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

Now let $\frac{7}{8} = \theta_0 > \theta_1 > \theta_2 > \ldots > 0$ be a decreasing sequence of positive real numbers, to be chosen suitably later. We shall estimate the integral of $E(\alpha)$ on the set $\mathfrak{m}_{\theta_{g+1}} - \mathfrak{m}_{\theta_g}$. Since $\mathfrak{m}_{\theta_{g+1}} - \mathfrak{m}_{\theta_g} \subset \mathscr{E}(\theta_g)$, we obtain by the above estimate for $E(\alpha)$,

$$\int_{\mathfrak{m}_{\theta_{g+1}} - \mathfrak{m}_{\theta_g}} |E(\alpha)|\, d\alpha \ll |\mathscr{E}(\theta_g)|\, P^{Un} \ll P^{Vn},$$

where $$U = m_1 - \tfrac{1}{2}(r+1)\,\theta_{g+1}(1-\delta) + t - \tfrac{1}{4}t\theta_{g+1},$$

and $$V = m_1 + t - 3 + 4\theta_g + 2\delta - \tfrac{1}{2}(r+1)\,\theta_{g+1}(1-\delta) - \tfrac{1}{4}t\theta_{g+1}.$$

Hence $$\int_{\mathfrak{m}_{\theta_{g+1}} - \mathfrak{m}_{\theta_g}} |E(\alpha)|\, d\alpha = o(P^{(m_1+t-3)n})$$

if $$4\theta_g - \tfrac{1}{2}(r+1)\,\theta_{g+1} - \tfrac{1}{4}t\theta_{g+1} + \delta(2 + \tfrac{7}{16}(r+1)) < \theta,$$

i.e. $$4(\theta_g - \theta_{g+1}) + \theta_{g+1}\{4 - \tfrac{1}{2}(r+1) - \tfrac{1}{4}t\} < -\{2 + \tfrac{7}{16}(r+1)\}\delta.$$

This inequality clearly holds if θ_{g+1} remains greater than a fixed positive quantity (independent of δ), δ is small enough and the jumps $\theta_g - \theta_{g+1}$ are less than a positive quantity. Hence we can find a finite sequence

$$\tfrac{7}{8} = \theta_0 > \theta_1 > \ldots > \theta_G \quad \text{with} \quad \frac{1}{4n} < \theta_G < \frac{1-\delta(n+2)}{2n},$$

such that $$\int_{\mathfrak{m}_{\theta_{g+1}} - \mathfrak{m}_{\theta_g}} |E(\alpha)|\, d\alpha = o(P^{(m_1+t-3)n}).$$

Since $\mathfrak{m}_{\theta_G} = \mathfrak{m}$, we finally reach the conclusion that the number $\mathscr{N}(P)$ of integral points (X, Y) in $P\mathscr{B}$ for which $C(X, Y) = 0$ satisfies

$$\mathscr{N}(P) = \int_{\mathscr{R}} E(\alpha)\, d\alpha = AP^{(m_1+t-3)n} + o(P^{(m_1+t-3)n}) \quad (A > 0).$$

Since this is positive for P large, it follows that $C(X, Y)$ represents zero non-trivially, which is a contradiction, proving Lemma 4·3.

We have tabulated below for $0 \leqslant t \leqslant 8$ the associated values of r and the minimum permissible value of m_1 for the validity of Lemma 4·3.

t	r	Minimum permissible value of m_1
0	8	18
1	7	16
2	7	16
3	6	14
4	6	14
5	5	12
6	5	12
7	4	10

The main theorem stated at the beginning of this paper can be easily deduced from the above lemma.

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press

Let $C(X)$ be a form with symmetric integral coefficients in K in at least 54 variables. If it does not represent zero, the above lemma says that it must represent a form of the type $C_1(X') + d_1 Y_1^3$, where C_1 is a form in at least 46 variables. The form $C_1(X') + d^1 Y_1^3$ cannot represent zero either, and another application of the lemma shows that C_1 represents a form of the type $C_2(X'') + d_2 Y_2^3$, where C_2 is a form in at least 39 variables. Hence $C(X)$ represents the form $C_2(X'') + d_1 Y_1^3 + d_2 Y_2^3$. Continuing in this way, we get finally that $C(X)$ represents a form of the type

$$C_8(Z) + d_1 Y_1^3 + \ldots + d_8 Y_8^3,$$

which therefore cannot represent zero non-trivially. Let d_0 be any value taken by $C_8(Z)$ with $Z \neq (0)$; then $C(X)$ represents $d_0 Y_0^3 + d_1 Y_1^3 + \ldots + d_8 Y_8^3$ and hence this form cannot have a non-trivial zero. But by a theorem of Birch ((1), p. 458), we know that any diagonal cubic form in at least 9 variables represents zero non-trivially. Hence there exist $Y_0^0, \ldots, Y_8^0$, not all zero, such that $Y_i = Y_i^0$ is a zero of the form written above. This is a contradiction.

The theorem is therefore proved.

The author wishes to thank Prof. K. G. Ramanathan for suggesting the problem to him and for being of great help in the preparation of this paper, and Prof. K. Chandrasekharan for constant advice and encouragement.

REFERENCES

(1) Birch, B. J. Waring's problem over algebraic number fields. *Proc. Cambridge Philos. Soc.* **57** (1961), 449–459.

(2) Birch, B. J. and Lewis, D. J. P-adic forms. *J. Indian Math. Soc.* **23** (1959), 11–33.

(3) Davenport, H. Cubic forms in thirty-two variables. *Philos. Trans. Roy. Soc. London Ser. A*, **251** (1958–59), 193–232.

(4) Hua, L. K. On exponential sums over an algebraic number field. *Canadian J. Math.* **3** (1951), 44–51.

https://doi.org/10.1017/S0305004100003698 Published online by Cambridge University Press