Canad. Math. Bull. Vol. **28** (3), 1985

SMALL SOLUTIONS OF CONGRUENCES IN A LARGE NUMBER OF VARIABLES[1]

BY

WOLFGANG M. SCHMIDT

Dedicated to the memory of R. A. Smith

ABSTRACT. It is shown that a system of congruences

$$\mathfrak{F}_1(\boldsymbol{x}) \equiv \ldots \equiv \mathfrak{F}_r(\boldsymbol{x}) \equiv 0 \pmod{m}$$

where each $\mathfrak{F}_i(\boldsymbol{x}) = \mathfrak{F}_i(x_1, \ldots, x_s)$ is a form of degree at most k has a nontrivial solution $\boldsymbol{x}$ satisfying

$$|x_i| \leqq cm^{(1/2)+\epsilon} \qquad (i = 1, \ldots, s)$$

with $c = c(k, r, \epsilon)$, provided that $\epsilon > 0$ and that $s > s_1(k, r, \epsilon)$.

1. **Introduction**. Our goal is the proof of the assertion enunciated in the Abstract:

THEOREM. *Given natural k, r and given $\epsilon > 0$, there is a number $s_1 = s_1(k, r, \epsilon)$ such that a system of congruences*

$$\mathfrak{F}_1(x_1, \ldots, x_s) \equiv \ldots \equiv \mathfrak{F}_r(x_1, \ldots, x_s) \equiv 0 \pmod{m} \tag{1.1}$$

with $s > s_1$ and each $\mathfrak{F}_i$ a form (i.e., a homogeneous polynomial) of degree between 1 and k, has a solution $\boldsymbol{x} = (x_1, \ldots, x_s)$ with

$$0 < |\boldsymbol{x}| \ll m^{(1/2)+\epsilon}. \tag{1.2}$$

Here $|\boldsymbol{x}| := \max(|x_1|, \ldots, |x_s|)$, and the constant in $\ll$ depends only on k, r, ϵ.

The Theorem clearly remains true with the forms $\mathfrak{F}_i$ replaced by polynomials with constant term zero. Another seemingly more general formulation is that when $\mathfrak{F}_1, \ldots, \mathfrak{F}_r$ are any polynomials of degree $\leqq k$ and if $\boldsymbol{x}_0$ is a solution of (1.1), then there is another solution $\boldsymbol{x}$ with $|\boldsymbol{x} - \boldsymbol{x}_0| \ll m^{(1/2)+\epsilon}$.

The case when m is a prime had been established in [9], but considerable extra complications arise for general m. On the other hand when all our forms are of degree > 1, we may restrict ourselves to m square free. For when $m = m_1^2 m_2$ with m_2 square free, set $\boldsymbol{x} = m_1 \boldsymbol{y}$ where $\boldsymbol{y}$ is a small solution of the congruences modulo m_2. Then $|\boldsymbol{x}| = m_1|\boldsymbol{y}| \ll m_1 m_2^{(1/2)+\epsilon} \ll m^{(1/2)+\epsilon}$. This argument shows in particular that the case when m is a square is of little interest. It is likely that the Theorem remains true

Received by the editors February 20, 1984 and, in revised form, May 9, 1984.

[1]Written with partial support from NSF-MCS-8211461.

AMS Subject Classification (1980): 10B30, 10C10.

with the extra condition imposed on $\boldsymbol{x}$ that $gcd(m, x_1, \ldots, x_s) = 1$; such a stronger version would retain its interest when m is a square.

When k is even and $\mathfrak{F} = (x_1^2 + \ldots + x_s^2)^{k/2}$, each solution $\boldsymbol{x} \neq \mathbf{0}$ of $\mathfrak{F}(\boldsymbol{x}) = 0 \pmod m$ has $|\boldsymbol{x}| \gg m^{1/2}$, which shows that the $1/2$ in the exponent in (1.2) is best possible. It remains open whether the ϵ could be removed. On the other hand when all the forms are of odd degree, the estimate (1.2) could be replaced by $0 < |\boldsymbol{x}| \ll m^{\epsilon}$, as had been shown by the author in [8]. Thus the interesting case is when the forms are of even degree. Schinzel, Schlickewei and Schmidt [7] had shown the theorem for a single quadratic form, and R. C. Baker [1] for a system of quadratic forms.

Very recently R. C. Baker [2] has shown that fairly strong assertions about small solutions of congruences can be derived from work of Deligne if the forms in question are nonsingular. Much of the difficulty in the general case arises from forms which are "degenerate" in some sense. Our proof will depend on estimates for exponential sums recently derived by the author [9].

The number $s_1 = s_1(k, r, \epsilon)$ could in principle be estimated by the present method, but any bound so derived would be extremely large. Our Theorem thus belongs to a group of "many variable results" which include the work of R. Brauer [5] on the solubility of homogeneous equations in p-adic fields and the work of B. Birch [4] on the solubility of odd degree homogeneous equations in the rational field. In all these cases, good estimates for the required number of variables would be of considerable interest.

2. **A conjecture on fractional parts**. Denote by $\|\alpha\|$ the distance from a real number α to the nearest integer.

CONJECTURE. *Given natural k, r and given $\epsilon > 0$, there is a number $s_2 = s_2(k, r, \epsilon)$ as follows. Let $\mathfrak{F}_1, \ldots, \mathfrak{F}_r$ be forms with real coefficients in $s > s_2$ variables with degrees between 1 and k. Then given $N > 1$, there is a nonzero integer point $\boldsymbol{x}$ with $|\boldsymbol{x}| \leqq N$ and*

$$\|\mathfrak{F}_i(\boldsymbol{x})\| \ll N^{-(2/r)+\epsilon} \qquad (i = 1, \ldots, r), \tag{2.1}$$

with a constant in $\ll$ which depends only on k, r, ϵ.

The case $r = 1$ of the Conjecture implies the case $r = 1$ of our Theorem, as we now proceed to show. For let $\mathfrak{F}(\boldsymbol{x})$ be a form of degree k with integer coefficients, and put $\mathfrak{G}(\boldsymbol{x}) = m^{-1}\mathfrak{F}(\boldsymbol{x})$. Set $N = am^{(1/2)+\epsilon}$, with a constant a to be specified in a moment, and apply the Conjecture to $\mathfrak{G}$: there is an integer point $\boldsymbol{x}$ with $0 < |\boldsymbol{x}| \leqq am^{(1/2)+\epsilon}$ and with $\|\mathfrak{G}(\boldsymbol{x})\| \ll N^{-2+\epsilon} \ll a^{-2+\epsilon}m^{-1}$. Thus when a is sufficiently large, say when $a > a_1(k, \epsilon)$, we have $\|\mathfrak{G}(\boldsymbol{x})\| < m^{-1}$ and therefore $\mathfrak{F}(\boldsymbol{x}) \equiv 0 \pmod m$. But the general case of the Theorem does not seem to follow from the general case of the Conjecture.

The exponent in (2.1) is essentially best possible. This may be seen as follows. Using the Borel-Cantelli Lemma one finds that for given $h \geqq 1$, almost all r-tuples $(\alpha_1, \ldots, \alpha_r)$ (in the sense of Lebesgue measure) have

$$\max(\|\alpha_1 x^h\|, \ldots, \|\alpha_r x^h\|) \gg x^{-1/r} (\log 2x)^{-2}$$

for each natural x. Setting $k = 2h$ and $\mathfrak{F}_i(\boldsymbol{x}) = \alpha_i(x_1^2 + \ldots + x_s^2)^h$, we have for $0 < |\boldsymbol{x}| \leqq N$ that

$$\max(\|\mathfrak{F}_1(\boldsymbol{x})\|, \ldots, \|\mathfrak{F}_r(\boldsymbol{x})\|) \gg |\boldsymbol{x}|^{-2/r} (\log 2|\boldsymbol{x}|)^{-2} \gg N^{-2/r}(\log 2N)^{-2}.$$

On the other hand, a much stronger result than (2.1) is true when all the forms are of odd degree, as was shown in [9]: In this case (2.1) may be replaced by $\|\mathfrak{F}_i(\boldsymbol{x})\| \ll N^{-E}$ $(i = 1, \ldots, r)$, for any given E, provided that $s > s_3(k, r, E)$.

The Conjecture is known only for $k = 1$ (which is an immediate consequence of a theorem of Dirichlet) and for $k = 2$. It had been shown for a single quadratic form by Schinzel, Schlickewei and Schmidt [7], then for a system of quadratic forms by Baker and Harman [3].

3. **The number of solutions in small cubes**. Let $2 \leqq \ell \leqq k$, and let $\underline{\mathfrak{F}} = (\underline{\mathfrak{F}}^{(k)}, \underline{\mathfrak{F}}^{(k-1)}, \ldots, \underline{\mathfrak{F}}^{(\ell)})$ be a system of $r = r_k + r_{k-1} + \ldots + r_\ell$ forms with integer coefficients, where the subsystem $\underline{\mathfrak{F}}^{(d)}$ consists of $r_d \geqq 0$ forms of degree d. When $r_d > 0$ write $\underline{\mathfrak{F}}^{(d)} = (\mathfrak{F}_1^{(d)}, \ldots, \mathfrak{F}_{r_d}^{(d)})$. Further let $\boldsymbol{m} = (\boldsymbol{m}^{(k)}, \boldsymbol{m}^{(k-1)}, \ldots, \boldsymbol{m}^{(\ell)})$, where $\boldsymbol{m}^{(d)}$ for $\ell \leqq d \leqq k$ is an r_d-tuple of positive integers, say $\boldsymbol{m}^{(d)} = (m_1^{(d)}, \ldots, m_{r_d}^{(d)})$ when $r_d > 0$. We are interested in solutions $\boldsymbol{x} = (x_1, \ldots, x_s)$ of the system of congruences

$$\mathfrak{F}_i^{(d)}(\boldsymbol{x}) \equiv 0 \pmod{m_i^{(d)}} \qquad (1 \leqq i \leqq r_d, \ell \leqq d \leqq k). \tag{3.1}$$

(These conditions should be interpreted as empty for d with $r_d = 0$.) Now given $P > 1$, write N_P for the number of solutions of these congruences with $\boldsymbol{x}$ in the cube $\mathfrak{C}_P$ given by $1 \leqq x_j \leqq P$ $(j = 1, \ldots, s)$. Heuristically one should expect that

$$N_P \approx P^s/M, \tag{3.2}$$

where M is the product of the components of $\boldsymbol{m}$.

For each d with $r_d > 0$ put $m^{(d)} = \ell cm(m_1^{(d)}, \ldots, m_{r_d}^{(d)})$, and let m be a common multiple of the numbers $m^{(d)}$ so obtained; thus m is a common multiple of the components of $\boldsymbol{m}$. Given a prime factor p of $m^{(d)}$, let $\underline{\mathfrak{F}}_p^{(d)}$ consist of the reductions modulo p of those forms $\mathfrak{F}_i^{(d)}$ of $\underline{\mathfrak{F}}^{(d)}$ for which $p | m_i^{(d)}$. Thus $\underline{\mathfrak{F}}_p^{(d)}$ is a nonempty tuple with at most r_d components. (In general, the p in $\mathfrak{F}_p$ or $\underline{\mathfrak{F}}_p$ will always refer to reduction modulo p, and a confusion with components $\mathfrak{F}_i$ of $\underline{\mathfrak{F}}$ should not arise.)

Now if $\mathfrak{G}$ is a form of degree $d \geqq 2$ with coefficients in the finite field $\mathbb{F}_p$, write $h(\mathfrak{G})$ for the least integer h such that $\mathfrak{G}$ may be written as

$$\mathfrak{G} = \mathfrak{A}_1\mathfrak{B}_1 + \ldots + \mathfrak{A}_h\mathfrak{B}_h,$$

with forms $\mathfrak{A}_i$, $\mathfrak{B}_i$ of positive degrees with coefficients in $\mathbb{F}_p$. When $\underline{\mathfrak{G}}$ is a t-tuple $(\mathfrak{G}_1, \ldots, \mathfrak{G}_t)$ of forms of equal degree d, define $h(\underline{\mathfrak{G}})$ as the minimum of $h(\mathfrak{G})$ over forms $\mathfrak{G}$ in the pencil, i.e., forms $\mathfrak{G} = \boldsymbol{a}\underline{\mathfrak{G}} = a_1\mathfrak{G}_1 + \ldots + a_t\mathfrak{G}_t$ with $\boldsymbol{a} = (a_1, \ldots, a_t) \in \mathbb{F}_p \setminus \boldsymbol{0}$.

Then $h(\underline{\mathfrak{F}}_p^{(d)})$ (with $\underline{\mathfrak{F}}_p^{(d)}$ as above) is defined for each d with $r_d > 0$ and each prime p dividing $m^{(d)}$. We now set

$$h(\underline{\mathfrak{F}}, \boldsymbol{m}) = \min_{\substack{\ell \leqq d \leqq k \\ r_d > 0}} \min_{p \mid m^{(d)}} h(\underline{\mathfrak{F}}_p^{(d)}). \tag{3.3}$$

PROPOSITION. *Suppose that* $P = m^{(1/\ell)+\epsilon}$ *with* $\epsilon > 0$ *and that* $h(\underline{\mathfrak{F}}, \boldsymbol{m}) \geqq h_1(k, \ell; r_k, \ldots, r_\ell; \epsilon)$. *Then if* m *is square free with each prime divisor* $\geqq p_1(s; k, \ell; r_k, \ldots, r_\ell; \epsilon)$, *we have*

$$|N_P - P^s/M| < \frac{1}{2} P^s/M. \tag{3.4}$$

We will employ vectors $(\boldsymbol{a}^{(k)}, \ldots, \boldsymbol{a}^{(\ell)})$ where $\boldsymbol{a}^{(d)}$ has r_d components; say $\boldsymbol{a}^{(d)} = (a_1^{(d)}, \ldots, a_{r_d}^{(d)})$ when $r_d > 0$ and $\boldsymbol{a}^{(d)} = 0$ when $r_d = 0$. Given $\boldsymbol{a}^{(d)}$, put

$$\boldsymbol{A}^{(d)} = (a_1^{(d)}/m_1^{(d)}, \ldots, a_{r_d}^{(d)}/m_{r_d}^{(d)}).$$

The notation

$$\sum_{\boldsymbol{a}^{(d)}}$$

will stand for the r_d-fold sum where $a_i^{(d)}$ ranges from 1 to $m_i^{(d)}$ $(1 \leqq i \leqq r_d)$. With these conventions, and with $e(z) = e^{2\pi i z}$, we have

$$\sum_{\boldsymbol{a}^{(k)}} \cdots \sum_{\boldsymbol{a}^{(\ell)}} e(\boldsymbol{A}^{(k)} \underline{\mathfrak{F}}^{(k)}(\boldsymbol{x}) + \ldots + \boldsymbol{A}^{(\ell)} \underline{\mathfrak{F}}^{(\ell)}(\boldsymbol{x})) = \begin{cases} M & \text{when (3.1) holds,} \\ 0 & \text{otherwise.} \end{cases}$$

Here $\boldsymbol{A}^{(d)} \underline{\mathfrak{F}}^{(d)}$ is the inner product $A_1^{(d)} \mathfrak{F}_1^{(d)} + \ldots A_{r_d}^{(d)} \mathfrak{F}_{r_d}^{(d)}$. It follows that

$$N_P = M^{-1} \sum_{\boldsymbol{a}^{(k)}} \cdots \sum_{\boldsymbol{a}^{(\ell)}} S(\boldsymbol{a}^{(k)}, \ldots, \boldsymbol{a}^{(\ell)}) \tag{3.5}$$

with

$$S(\boldsymbol{a}^{(k)}, \ldots, \boldsymbol{a}^{(\ell)}) = \sum_{\boldsymbol{x} \in \mathfrak{S}_P} e(\boldsymbol{A}^{(k)} \underline{\mathfrak{F}}^{(k)}(\boldsymbol{x}) + \ldots + \boldsymbol{A}^{(\ell)} \underline{\mathfrak{F}}^{(\ell)}(\boldsymbol{x})). \tag{3.6}$$

Given $\boldsymbol{a}^{(k)}, \ldots, \boldsymbol{a}^{(\ell)}$, write Δ_k for the denominator of $\boldsymbol{A}^{(k)}$ in case $r_k > 0$, and $\Delta_k = 1$ if $r_k = 0$. Let Δ_{k-1} be the positive integer such that $\Delta_k \Delta_{k-1}$ is the least denominator of the point $(\boldsymbol{A}^{(k)}, \boldsymbol{A}^{(k-1)})$ when $r_{k-1} > 0$, and set $\Delta_{k-1} = 1$ when $r_{k-1} = 0$. In general, choose $\Delta_k, \Delta_{k-1}, \ldots, \Delta_\ell$ such that $\Delta_k \Delta_{k-1} \ldots \Delta_d$ for $\ell \leqq d \leqq k$ is the denominator of $(\boldsymbol{A}^{(k)}, \ldots, \boldsymbol{A}^{(d)})$. Finally set $\Delta = \Delta_k \Delta_{k-1} \ldots \Delta_\ell$. In the sum in (3.5) there is precisely one summand with $\Delta = 1$, namely the summand with $a_i^{(d)} = m_i^{(d)}$ throughout. This summand has $S(a^{(k)}, \ldots, a^{(\ell)}) = |\mathfrak{S}_P| = P^s + O(P^{s-1})$ where $|\mathfrak{S}_P|$ is the cardinality of $\mathfrak{S}_P$, and hence contributes

$$P^s M^{-1} + O(P^{s-1} M^{-1}) \tag{3.7}$$

to (3.5). It remains for us to estimate the contribution of summands with $\Delta > 1$.

4. **Estimation of exponential sums**. Before proceeding further it will be convenient

to state some auxiliary results. We will need boxes of the type $a_j \leqq x_j < b_j$ with integers a_j, b_j. Such a box will be said to be of side $\leqq R$ if $b_j - a_j \leqq R$ $(j = 1, \ldots, s)$.

LEMMA 1. *Let $\mathfrak{P} = \mathfrak{F}^{(d)} + \mathfrak{F}^{(d-1)} + \ldots + \mathfrak{F}^{(0)}$ be a polynomial of degree d, with the typical summand $\mathfrak{F}^{(j)}$ homogeneous of degree j and with coefficients in the ring $\mathbb{Z}/n\mathbb{Z}$ where n is square free. Let $\mathfrak{B}$ be a box of side $\leqq R = n^{\delta}$ where $d^{-1} < \delta \leqq 1$, and let $S_{\mathfrak{B}}$ be the sum*

$$S_{\mathfrak{B}} = \sum_{x \in \mathfrak{B}} e(n^{-1}\mathfrak{P}(x)). \tag{4.1}$$

Suppose that $K \geqq 1$, and that $\Gamma > 1$ is an integer. Suppose further that $n \geqq n_1(s, d, \delta, \Gamma)$. Then either

$$|S_{\mathfrak{B}}| < R^{s-K}, \tag{4.2}$$

or there is a factorization $n = ab$ with $b \leqq R^{1/\Gamma}$ and with

$$h(\mathfrak{F}_p^{(d)}) \leqq (d - \delta^{-1})^{-1} d^2 2^{d-1} \Phi(d) K\Gamma, \tag{4.3}$$

for every prime factor p of a, where $\mathfrak{F}_p^{(d)}$ is the reduction of $\mathfrak{F}^{(d)}$ modulo p, and where $\Phi(d)$ depends only on d.

PROOF. This is Theorem 5 of [9].

LEMMA 2. *Let n be square free, and $\mathfrak{P}$ as in Lemma 1. Let $d^{-1} < \delta \leqq 1$ and let $\mathfrak{B}$ be a box of side $\leqq R$ where*

$$R \geqq n^{\delta}.$$

Given $K \geqq 1$ and $\Gamma > 1$ as above, we either have

$$S_{\mathfrak{B}} \ll R^s n^{-\delta K}, \tag{4.4}$$

or there is a factorization $n = ab$ with $b \leqq n^{1/\Gamma}$ and with (4.3) for each prime factor p of a. The constant in $\ll$ depends only on s, d, δ, Γ.

PROOF. We will assume that n has no factorization as indicated, and we will derive (4.4). The box $\mathfrak{B}$ is the union of boxes $\mathfrak{B}^*$ of side $\leqq n^{\delta} = R_1$ say. It is the union of $\ll (R/R_1)$ such boxes $\mathfrak{B}^*$. By Lemma 1, a sum $S_{\mathfrak{B}^*}$ has $|S_{\mathfrak{B}^*}| < R_1^{s-K} = R_1^s n^{-\delta K}$ when n is large, hence has $S_{\mathfrak{B}^*} \ll R_1^s n^{-\delta K}$ in general. (For since $h(\mathfrak{F}_p^{(d)}) \leqq s$ always, the nonexistence of a factorization of n as above is possible only if the right hand side of (4.3) is $< s$, hence if K is bounded.) Taking the sum over the boxes $\mathfrak{B}^*$ making up $\mathfrak{B}$ we get

$$S_{\mathfrak{B}} \ll (R/R_1)^s R_1^s n^{-\delta K} = R^s n^{-\delta K}.$$

5. **Proof of the proposition**. We now return to the situation described at the end of §3.

LEMMA 3. *Make the hypotheses of the Proposition, and let $\mathbf{a}^{(k)}, \ldots, \mathbf{a}^{(\ell)}$ with $\Delta > 1$ be given. Then*

$$S(\boldsymbol{a}^{(k)}, \dots, \boldsymbol{a}^{(\ell)}) \ll P^s \Delta^{-hc_1},$$

where $h = h(\underline{\mathfrak{F}}, \boldsymbol{m})$, *where* $c_1 = c_1(k, \ell; r_k, \dots, r_\ell; \epsilon)$, *and where the constant in* $\ll$ *again depends only on* $s; k, \ell; r_k, \dots, r_\ell; \epsilon$.

PROOF. Instead of just for the cube $\mathfrak{C}_P$, we will prove the lemma for any box $\mathfrak{B}$ of side $\leqq P$ where $P \geqq m^{(1/\ell)+\epsilon}$. We clearly may suppose that $0 < \epsilon < 1$. Set

$$\Phi = 2^k/\epsilon, \qquad \Gamma = \Phi + 1. \tag{5.1}$$

Set

$$V_d = \Delta_k \Delta_{k-1} \dots \Delta_{d+1} \quad \text{when} \quad \ell \leqq d < k, \quad \text{but} \quad V_k = 1.$$

Put

$$W_d = \Delta_d \Delta_{d-1} \dots \Delta_\ell \quad \text{when} \quad \ell \leqq d \leqq k, \quad \text{but} \quad W_{\ell-1} = 1.$$

Then

$$\Delta = V_d W_d \qquad (\ell \leqq d \leqq k).$$

It may not happen that

$$\Delta_j^\Phi < W_{j-1} \tag{5.2}$$

for each j in $\ell \leqq j \leqq k$. For if this were the case, we had $\Delta_\ell^\Phi \leqq W_{\ell-1} = 1$, whence $\Delta_\ell = 1$. Next, $\Delta_{\ell+1}^\Phi \leqq W_\ell = \Delta_\ell = 1$, so that $\Delta_{\ell+1} = 1$, etc. We would obtain $\Delta = 1$, against our hypothesis. From now on, let d be the largest number in $\ell \leqq d \leqq k$ for which (5.2) fails for $j = d$. Thus

$$\Delta_d^\Phi > W_{d-1}, \tag{5.3}$$

but (5.2) is true for $d < j \leqq k$. In the case when $d < k$ it follows that $\Delta_{d+1}^\Phi \leqq W_d$, next that $\Delta_{d+2}^\Phi \leqq W_{d+1} = \Delta_{d+1} W_d \leqq W_d^2$, next that $\Delta_{d+3}^\Phi \leqq W_{d+2} = \Delta_{d+2} W_{d+1} < W_d^{2^2}$, and so on, finally that $\Delta_k^\Phi < W_d^{2^{k-d-1}}$. Therefore $V_d^\Phi < W_d^{2^{k-d}}$, and by our choice of Φ this yields $V_d < W_d^{\epsilon/2}$. This relation is true also in the case $d = k$. We may infer on the one hand that

$$W_d > \Delta^{1/2}, \tag{5.4}$$

and on the other hand that

$$P \geqq m^{(1/\ell)+\epsilon} \geqq W_d^{(1/\ell)+\epsilon} \geqq W_d^{(1/d)+\epsilon} \geqq V_d W_d^{(1/d)+(\epsilon/2)}. \tag{5.5}$$

We have $\boldsymbol{A}^{(d)} = (V_d \Delta_d)^{-1} \boldsymbol{b}$ where $\boldsymbol{b}$ is an integer point with $gcd(\Delta_d, b_1, \dots, b_{r_d}) = 1$. Thus

$$\boldsymbol{A}^{(d)} \underline{\mathfrak{F}}^{(d)} = (V_d \Delta_d)^{-1} \mathfrak{F} \quad \text{with} \quad \mathfrak{F} = \boldsymbol{b} \underline{\mathfrak{F}}^{(d)}. \tag{5.6}$$

Every prime factor p of Δ_d also divides $m^{(d)}$, and hence $h(\underline{\mathfrak{F}}^{(d)}) \geqq h$ by the definition (3.3) of $h = h(\underline{\mathfrak{F}}, \boldsymbol{m})$. Now if i is a subscript with $p \nmid m_i^{(d)}$, then p is not in the denominator of $A_i^{(d)} = a_i^{(d)}/m_i^{(d)}$, and we must have $p | b_i$. On the other hand since p does

occur in the denominator of $\boldsymbol{A}^{(d)}$, there must be some subscripts i with $p|m_i^{(d)}$ and $p \nmid b_i$. The components of $\underline{\mathfrak{F}}_p^{(d)}$ stem from forms $\mathfrak{F}_i^{(d)}$ with $p|m_i^{(d)}$, and $\mathfrak{F}_p$ (i.e., the reduction of $\mathfrak{F}$ modulo p) belongs to the pencil of $\underline{\mathfrak{F}}_p^{(d)}$, so that

$$h(\mathfrak{F}_p) \geqq h. \tag{5.7}$$

Points $\boldsymbol{x}$ in the given box $\mathfrak{B}$ will be written as $\boldsymbol{x} = V_d \boldsymbol{y} + \boldsymbol{z}$ with $0 \leqq z_j < V_d$. For given $\boldsymbol{z}$, for $\boldsymbol{x}$ to be in the box $\mathfrak{B}$ of side $\leqq P$ the point $\boldsymbol{y}$ will be in a box $\mathfrak{B}(\boldsymbol{z})$ of side $\leqq 2P/V_d$. (Note that $V_d \leqq P$ by (5.5)). For given $\boldsymbol{z}$ we have modulo 1

$$\begin{aligned} \boldsymbol{A}^{(k)}\underline{\mathfrak{F}}^{(k)}(\boldsymbol{x}) + \ldots + \boldsymbol{A}^{(\ell)}\underline{\mathfrak{F}}^{(\ell)}(\boldsymbol{x}) &\equiv \boldsymbol{A}^{(d)}\underline{\mathfrak{F}}^{(d)}(V_d \boldsymbol{y}) \\ &+ W_d^{-1}\mathfrak{F}^{(d-1)}(\boldsymbol{y}) + \ldots + W_d^{-1}\mathfrak{F}^{(1)}(\boldsymbol{y}) + \Delta^{-1}\mathfrak{F}^{(0)}, \end{aligned} \tag{5.8}$$

where $\mathfrak{F}^{(d-1)}, \ldots, \mathfrak{F}^{(0)}$ are forms of respective degrees $d-1, \ldots, 0$ with integer coefficients. In view of (5.6) we have

$$\boldsymbol{A}^{(d)}\underline{\mathfrak{F}}^{(d)}(V_d \boldsymbol{y}) = \Delta_d^{-1} V_d^{d-1}\mathfrak{F}(\boldsymbol{y}) = W_d^{-1}\mathfrak{F}^{(d)}(\boldsymbol{y}) \tag{5.9}$$

with $\mathfrak{F}^{(d)} = W_{d-1}V_d^{d-1}\mathfrak{F}$. Since m is square free, Δ_d is coprime to W_{d-1} and to V_d, and hence (5.7) yields

$$h(\mathfrak{F}_p^{(d)}) \geqq h \tag{5.10}$$

for every prime factor p of Δ_d.

We are going to apply Lemma 2 to the polynomial $\mathfrak{P} = \mathfrak{F}^{(d)} + \mathfrak{F}^{(d-1)} + \ldots + \mathfrak{F}^{(1)}$ with the forms $\mathfrak{F}^{(j)}$ coming from (5.8), (5.9), and to a box $\mathfrak{B}(\boldsymbol{z})$. Such a box has side $\leqq 2P/V_d = R$, say. Setting $n = W_d$, $\delta = (1/d) + (\epsilon/2)$, we have $R \geqq n^{\delta}$ by (5.5). Let Γ be given by (5.1) and put

$$K = (d - \delta^{-1})d^{-2}2^{-d}\Phi(d)^{-1}\Gamma^{-1}h, \tag{5.11}$$

so that $K \geqq 1$ when $h \geqq h_1$. One alternative of Lemma 2 gives a factorization $W_d = ab$. By (4.3), (5.10) and our choice of K, a prime factor p of Δ_d cannot divide a, so that $\Delta_d|b$, and hence $\Delta_d \leqq n^{1/\Gamma}$, or $\Delta_d^{\Gamma} \leqq n = W_d = \Delta_d W_{d-1}$, or $\Delta_d^{\Phi} \leqq W_{d-1}$, contradicting (5.3). Thus the other alternative must hold. This means in view of (5.8) and (5.9) that the part $S(\boldsymbol{z})$ of the sum $S(\boldsymbol{a}^{(k)}, \ldots, \boldsymbol{a}^{(\ell)})$ with $\boldsymbol{x} = V_d \boldsymbol{y} + \boldsymbol{z}$ and given $\boldsymbol{z}$ has

$$S(\boldsymbol{z}) \ll R^s n^{-\delta K} \ll (P/V_d)^s W_d^{-\delta K}.$$

Taking the sum over $\boldsymbol{z}$ we obtain

$$S(\boldsymbol{a}^{(k)}, \ldots, \boldsymbol{a}^{(\ell)}) \ll P^s W_d^{-\delta K} \ll P^s \Delta^{-(\delta/2)K} \ll P^s \Delta^{-c_1 h}$$

by virtue of (5.4) and (5.11).

Now that Lemma 3 has been established, the proof of the Proposition is easily completed. Given Δ, there are not more than Δ^r vectors $(\boldsymbol{a}^{(k)}, \ldots, \boldsymbol{a}^{(\ell)})$. Thus all the sums $S(\boldsymbol{a}^{(k)}, \ldots, \boldsymbol{a}^{(\ell)})$ with given Δ contribute together not more than $\ll P^s \Delta^{r-c_1 h}$, and this is $\ll P^s \Delta^{-2}$ when $h \geqq h_1$. Since the least prime factor of m is $\geqq p_1$, the sum over

all the $S(\boldsymbol{a}^{(k)}, \ldots, \boldsymbol{a}^{(1)})$ with $\Delta > 1$ is $\ll P^s p_1^{-1}$. In view of (3.5), and the contribution (3.7) from $\Delta = 1$, we obtain

$$N_P = P^s M^{-1}(1 + 0(P^{-1} + p_1^{-1})).$$

Thus (3.4) is certainly true when p_1, and hence P, is large.

Incidentally, when m is arbitrary, i.e., possibly with small prime divisors or not square free, one should aim not for (3.2), but for

$$N_p \approx P^s(\nu(m)/m^s),$$

where $\nu(m)$ is the number of solutions $\boldsymbol{x} \pmod m$ of (3.1). But this is not needed for our present purpose.

6. **An inductive argument**. Throughout this and the next section, $\delta > 0$ will be fixed. With a given $\boldsymbol{r} = (r_k, \ldots, r_1)$ we will associate a set of vectors $\boldsymbol{u}$, as follows. Given r_d put

$$t_d = [\delta^{-1} 2^d r_d] + 1. \tag{6.1}$$

The symbol $\boldsymbol{u}^{(d)}$ will denote the zero vector when $r_d = 0$, but when $r_d > 0$ it will denote vectors $\boldsymbol{u}^{(d)} = (u_1^{(d)}, \ldots, u_{r_d}^{(d)})$ with integer components in $1 \leqq u_i^{(d)} \leqq t_d$. Given d and r_d, let $\prec$ be an ordering of the vectors $\boldsymbol{u}^{(d)}$ such that $\boldsymbol{u}'^{(d)} \neq \boldsymbol{u}^{(d)}$ and $u_i'^{(d)} \leq u_i^{(d)}$ $(i = 1, \ldots, r_d)$ implies $\boldsymbol{u}'^{(d)} \prec \boldsymbol{u}^{(d)}$. We now consider tuples

$$(r_k, \boldsymbol{u}^{(k)}, \ldots, r_2, \boldsymbol{u}^{(2)}, r_1, \boldsymbol{u}^{(1)}) = (\boldsymbol{r}, \boldsymbol{u}), \tag{6.2}$$

say, where $r_k > 0$, where each $r_d \geqq 0$ and each $\boldsymbol{u}^{(d)}$ is of the type described. We order these tuples by the convention that $(\boldsymbol{r}', \boldsymbol{u}') \prec (\boldsymbol{r}, \boldsymbol{u})$ if either $\boldsymbol{r}' = (r_\ell', \ldots, r_1')$, $\boldsymbol{r} = (r_k, \ldots, r_1)$ with $\ell < k$, or if $\ell = k$ and there is a d in $1 \leqq d \leqq k$ such that $r_j' = r_j$, $\boldsymbol{u}'^{(j)} = \boldsymbol{u}^{(j)}$ for $d < j \leqq k$, and either $r_d' < r_d$, or $r_d' = r_d$ and $\boldsymbol{u}'^{(d)} \prec \boldsymbol{u}^{(d)}$. The tuples $(\boldsymbol{r}, \boldsymbol{u})$ are then well ordered.

In proving the Theorem we will initially suppose m to be square free. Given $\underline{\mathfrak{F}} = (\underline{\mathfrak{F}}^{(k)}, \ldots, \underline{\mathfrak{F}}^{(1)})$ where $\underline{\mathfrak{F}}^{(d)}$ consists of $r_d \geq 0$ forms of degree d, and given divisors $m_i^{(d)}$ of m $(1 \leq i \leq r_d$ with $1 \leq d \leq k$ and $r_d > 0)$ it will suffice to show that the system

$$\mathfrak{F}_i^{(d)}(\boldsymbol{x}) \equiv 0 \pmod{m_i^{(d)}} \qquad (1 \leq i \leq r_d,\ 1 \leqq d \leqq k) \tag{6.3}$$

has a solution $\boldsymbol{x}$ satisfying (1.2), with the constant in $\ll$ depending only on $\boldsymbol{r}, \epsilon$ where $\boldsymbol{r} = (r_k, \ldots, r_1)$, provided that the number s of variables exceeds some $s_1 = s_1(\boldsymbol{r}, \epsilon)$.

Given $\delta > 0$ and given $(\boldsymbol{r}, \boldsymbol{u})$, we now formulate the following

ASSERTION $(\boldsymbol{r}, \boldsymbol{u})_\delta$. *Let $\underline{\mathfrak{F}} = (\underline{\mathfrak{F}}^{(k)}, \ldots, \underline{\mathfrak{F}}^{(1)})$ be a system of forms as above, let m be square free, and let $m_i^{(d)}$ be divisors of m with*

$$m_i^{(d)} \leqq m^{u_i^{(d)}/t_d} \qquad (1 \leqq i \leqq r_d,\ 1 \leqq d \leqq k). \tag{6.4}$$

Then if $\epsilon > \delta$ and if $s > s_1(\boldsymbol{r}, \boldsymbol{u}, \epsilon)$, the system (6.3) *has a solution $\boldsymbol{x}$ with* (1.2) *and with the constant in $\ll$ depending only on $(\boldsymbol{r}, \boldsymbol{u})$ and ϵ.*

The truth of the Assertion for every $\delta > 0$ and every $(\boldsymbol{r}, \boldsymbol{u})$ will give the truth of the

https://doi.org/10.4153/CMB-1985-035-9 Published online by Cambridge University Press

Theorem, since for given ϵ we may set $\delta = \epsilon/2$, and since we may take $u_i^{(d)} = t_d$ throughout, in which case (6.4) is automatically satisfied. The Assertion itself will for given $\delta > 0$ be proved by induction with respect to$\prec$. The following lemma gets us off the ground.

LEMMA 4. *The assertion is true for every tuple* $(r_1, \boldsymbol{u}^{(1)})$. *Moreover, when it is true for some particular*

$$(r_k, \boldsymbol{u}^{(k)}, \ldots, r_2, \boldsymbol{u}^{(2)}, 0, \mathbf{0}) = (\boldsymbol{r}, \boldsymbol{u}), \tag{6.5}$$

say, then it is true for every tuple of the form

$$(r_k, \boldsymbol{u}^{(k)}, \ldots, r_2, \boldsymbol{u}^{(2)}, r_1, \boldsymbol{u}^{(1)}).$$

PROOF. (See [9]). We will restrict ourselves to the second claim. Let $\underline{\mathfrak{F}} = (\underline{\mathfrak{F}}^{(k)}, \ldots, \underline{\mathfrak{F}}^{(1)})$ be given. We may suppose the coefficients of our forms to have absolute values less than m. Then $\underline{\mathfrak{F}}^{(1)}$ has a common integer zero $\boldsymbol{y}$ with $0 < |\boldsymbol{y}| < (sm)^{r_1/(s-r_1)}$ by Siegel's Lemma (see Cassels [5], §IV.3, Lemma 3). Now when $\epsilon > \delta$, set $\eta = (\epsilon - \delta)/2$. Thus when $s > \eta^{-1}(1+\eta)r_1$, there is a nontrivial zero of $\underline{\mathfrak{F}}^{(1)}$ with $|\boldsymbol{y}| < (sm)^{\eta}$, and when $s > \ell(\eta^{-1}(1+\eta)r_1 + 1)$, there are ℓ linearly independent such zeros $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_\ell$. With each form $\mathfrak{F}$ of $\underline{\mathfrak{F}}$ we associate a new form $\underline{\mathfrak{F}}^*(\boldsymbol{Z}) = \mathfrak{F}(Z_1\boldsymbol{y}_1 + \ldots + Z_\ell\boldsymbol{y}_\ell)$ in $\boldsymbol{Z} = (Z_1, \ldots, Z_\ell)$. Since the r_1 linear forms $\mathfrak{F}_i^{(1)*}$ vanish identically, it remains to deal with the congruences

$$\mathfrak{F}_i^{(d)*}(\boldsymbol{z}) \equiv 0 \pmod{m_i^{(d)}} \tag{6.6}$$

where $1 \leqq i \leqq r_d$ and $2 \leqq d \leqq k$. By the Assertion $(\boldsymbol{r}, \boldsymbol{u})_\delta$ with $(\boldsymbol{r}, \boldsymbol{u})$ given in (6.5), we see that when $\ell > s_1(\boldsymbol{r}, \boldsymbol{u}, \delta + \eta)$, there is a nontrivial solution $\boldsymbol{z}$ of (6.6) with $|\boldsymbol{z}| \ll m^{(1/2)+\delta+\eta}$. But then $\boldsymbol{x} = z_1\boldsymbol{y}_1 + \ldots + z_\ell\boldsymbol{y}_\ell$ solves all the congruences (6.3), and $0 < |\boldsymbol{x}| \ll |\boldsymbol{y}||\boldsymbol{z}| \ll m^{(1/2)+\delta+2\eta} = m^{(1/2)+\epsilon}$. The way we derived it, the constant in $\ll$ here may depend on s, but it is clear a priori that the correct constant in the assertion (1.2) cannot increase with s.

It therefore will be enough to prove the Assertion for $(\boldsymbol{r}, \boldsymbol{u})$ of the type (6.5), assuming its truth for each $(\boldsymbol{r}', \boldsymbol{u}') \prec (\boldsymbol{r}, \boldsymbol{u})$. So let $(\underline{\mathfrak{F}}^{(k)}, \ldots, \underline{\mathfrak{F}}^{(2)})$ be given, let m be square free and let $m_i^{(d)}$ be divisors of m with (6.4).

7. **Proof of the Theorem**. In what follows, let

$$h_1 = h_1(k, 2; r_k, \ldots, r_2; \delta/2)$$

be as in the Proposition. As before we write $m^{(d)}$ for the least common multiple of $m_1^{(d)}, \ldots, m_{r_d}^{(d)}$ where $r_d > 0$, but $m^{(d)} = 1$ when $r_d = 0$. For each prime factor p of $m^{(d)}$ we define $\underline{\mathfrak{F}}_p^{(d)}$ and $h(\underline{\mathfrak{F}}_p^{(d)})$ as in §3. We factor $m^{(d)} = a^{(d)}b^{(d)}$ such that $a^{(d)}$ is the product of exactly those prime factors p of $m^{(d)}$ for which

$$h(\underline{\mathfrak{F}}_p^{(d)}) \geqq h_1. \tag{7.1}$$

We now distinguish two cases.

(I) *There is an* e *in* $2 \leqq e \leqq k$ *with* $b^{(e)} \geqq m^{r_e/t_e}$.

Let such an e be fixed. For each prime factor p of $b^{(e)}$, by the negation of (7.1) for $d = e$, some form

$$\mathfrak{F}_p = a_{p1}\mathfrak{F}_1^{(e)} + \ldots + a_{pr_e}\mathfrak{F}_{r_e}^{(e)}$$

has $h(\mathfrak{F}_p) < h_1$, where $a_{pi} \equiv 0 \pmod p$ for subscripts i with $p \nmid m_i^{(e)}$, but where there is at least one i with $p | m_i^{(e)}$ and $a_{pi} \not\equiv 0 \pmod p$. There is an i_0 in $1 \leqq i_0 \leqq r_e$ and a divisor b' of $b^{(e)}$ with $b' \geqq (b^{(e)})^{1/r_e} \geqq m^{1/t_e}$ such that for each prime factor p of b' we have $p | m_{i_0}^{(e)}$ and $a_{pi} \not\equiv 0 \pmod p$. Say $i_0 = 1$.

The congruences

$$\mathfrak{F}_i^{(e)}(\boldsymbol{x}) \equiv 0 \pmod{m_i^{(e)}} \qquad (1 \leqq i \leqq r_e)$$

then have the same solution set as the congruences

$$\mathfrak{F}_i^{(e)}(\boldsymbol{x}) \equiv 0 \pmod{m_i^{(e)}} \qquad (2 \leqq i \leqq r_e) \tag{7.2a}$$

$$\mathfrak{F}_1^{(e)}(\boldsymbol{x}) \equiv 0 \pmod{m_1^{(e)}/b'}, \tag{7.2b}$$

$$\mathfrak{F}_p(\boldsymbol{x}) \equiv 0 \pmod p \text{ for each prime factor } p \text{ of } b'. \tag{7.2c}$$

Now since $h(\mathfrak{F}_p) < h_1$, each $\mathfrak{F}_p$ can be written as

$$\mathfrak{F}_p = \sum_{j=1}^{h_1 - 1} \mathfrak{A}_{pj}\mathfrak{B}_{pj},$$

where $\mathfrak{A}_{pj}$, $\mathfrak{B}_{pj}$ are forms with degrees between 1 and $e - 1$. By the Chinese Remainder Theorem, there are forms $\mathfrak{A}_j$ such that (coefficient-wise) $\mathfrak{A}_j \equiv \mathfrak{A}_{pj} \pmod p$ for each prime factor p of b'. The $\mathfrak{A}_j$ have degrees less than e. The condition (7.2c) is certainly satisfied of $\mathfrak{A}_j(\boldsymbol{x}) \equiv 0 \pmod{b'}$ for $1 \leqq j < h_1$. The original system (6.3) of congruences is therefore satisfied whenever the following new system is satisfied

$$\mathfrak{F}_i^{(d)}(\boldsymbol{x}) \equiv 0 \pmod{m_i^{(d)}} \quad (1 \leqq i \leqq r_d,\ 2 \leqq d \leqq k, \text{ but excluding } i = 1,\ d = e), \tag{7.3α}$$

$$\mathfrak{F}_1^{(e)}(\boldsymbol{x}) \equiv 0 \pmod{m_1'^{(e)}} \quad \text{where } m_1'^{(e)} = m_1^{(e)}/b', \tag{7.3β}$$

$$\mathfrak{A}_j(\boldsymbol{x}) \equiv 0 \pmod{b'} \qquad (1 \leqq j < h_1). \tag{7.3γ}$$

Note that

$$m_1'^{(e)} = m_1^{(e)}/b' \leqq m^{(u_1^{(e)} - 1)/t_e}. \tag{7.4}$$

Now (7.3) is of the type

$$(\boldsymbol{r}', \boldsymbol{u}') = (r_k, \boldsymbol{u}^{(k)}, \ldots, r_{e+1}, \boldsymbol{u}^{(e+1)}, r_e', \boldsymbol{u}'^{(e)}, \ldots, r_2', \boldsymbol{u}'^{(2)}, r_1', \boldsymbol{u}'^{(1)}),$$

for the congruences of degree $> e$ have not been changed. But when $u_1^{(e)} > 1$, we may take $r_e' = r_e$ *and* $\boldsymbol{u}'^{(e)} = (u_1^{(e)} - 1, u_2^{(e)}, \ldots, u_{r_e}^{(e)})$ by (7.4), while when $u_1^{(e)} = 1$, we may take $r_e' = r_e - 1$. Since the components of $\boldsymbol{r}'$ are bounded in terms of $\boldsymbol{r}$ and δ, our

inductive assumption yields for $\epsilon > \delta$ and $s > s_1(\boldsymbol{r}, \boldsymbol{u}, \epsilon)$ a solution $\boldsymbol{x}$ of (7.3) with (1.2).

This leaves us with the case

(II) $b^{(d)} < m^{r_d/t_d}$ *for* $2 \leqq d \leqq k$.

Let g be the product of the primes $\leqq p_1$ where $p_1 = p_1(s; k, 2; r_k, \ldots, r_2; \delta/2)$ is the quantity of the Proposition. Consider the congruences

$$\Im_i^{(d)}(\boldsymbol{y}) \equiv 0 \pmod{m_i^{*(d)}} \qquad (1 \leqq i \leqq r_d,\ 2 \leqq d \leqq k) \tag{7.5}$$

where $m_i^{*(d)} = m_i^{(d)}/(m_i^{(d)}, gb^{(d)})$. Then $m^{*(d)}$ (defined in the obvious way) is coprime to $b^{(d)}$ and by (7.1) we have $h(\Im_p^{(d)}) \geqq h_1$ for each prime factor p of $m^{*(d)}$. The least common multiple m^* of the numbers $m^{*(d)}$ is square free and its prime factors exceed p_1. Thus by the Proposition, (7.5) has a solution $\boldsymbol{y} \neq \boldsymbol{0}$ with $|\boldsymbol{y}| \ll m^{*(1/2)+(\delta/2)} \leqq m^{(1/2)+(\delta/2)}$. We now set

$$\boldsymbol{x} = gb^{(2)}b^{(3)} \ldots b^{(k)}\boldsymbol{y}.$$

Then $\boldsymbol{x}$ is a solution of the original congruences, and

$$|\boldsymbol{x}| \ll m^{(r_2/t_2)+\ldots+(r_k/t_k)} m^{(1/2)+(\delta/2)} \leqq m^{(1/2)+\epsilon}$$

by our choice of $t_2, \ldots, t_k$ in (6.1).

This finishes the proof of the Theorem for m square free. By the argument of the Introduction, the Theorem is therefore true for arbitrary m and for systems of forms of the type $r = (r_k, \ldots, r_2, 0)$. An application of Siegel's Lemma such as in the proof of Lemma 4 leads from this to systems of forms of arbitrary type $(r_k, \ldots, r_2, r_1)$.

References

1. R. C. Baker, *Small solutions of quadratic and quartic congruences*, Mathematika **27** (1980), pp. 30–45.
2. R. C. Baker, *Small solutions of congruences*, Mathematika **30** (1983), pp. 164–188.
3. R. C. Baker and G. Harman, *Small fractional parts of quadratic and additive forms*, Math. Proc. Camb. Phil. Soc. **90** (1981), pp. 5–12.
4. B. Birch, *Homogeneous forms of odd degree in a large number of variables*, Mathematika **4** (1957), pp. 102–105.
5. R. Brauer, *A note on systems of homogeneous algebraic equations*, Bull. A.M.S. **51** (1945), pp. 749–755.
6. J. W. S. Cassels, *An introduction to diophantine approximation*, Cambridge Tracts in Math. and Math. Physics, **45** (1957).
7. A. Schinzel, H. P. Schlickewei and W. M. Schmidt, *Small solutions of quadratic congruences and small fractional parts of quadratic forms*, Acta Arith. **37** (1980), pp. 241–248.
8. W. M. Schmidt, *Diophantine inequalities for forms of odd degree*, Advances in Math. **38** (1980), pp. 128–151.
9. W. M. Schmidt, *Bounds for exponential sums*, Acta Arith. (to appear).

University of Colorado
Boulder, Colorado
U.S.A.