Functiones et Approximatio
XXVIII (2000), 19–34

To Professor Włodzimierz Staś on his 75th birthday

SMALL SOLUTIONS OF CONGRUENCES. II

R. C. Baker

1. Introduction

Let p be prime and denote by $\mathbb{F}_p$ the field with p elements, $\mathbb{F}_p^*$ the multiplicative group of nonzero elements of $\mathbb{F}_p$ and $(\mathbb{F}_p^*)^k$ the subgroup $\{x^k : x \in \mathbb{F}_p^*\}$. Let $Q(X_1, \ldots, X_s)$ be a quadratic form with coefficients in $\mathbb{F}_p$. It was shown by Schinzel, Schlickewei and Schmidt [12] that, for odd s, there is a subspace of $\mathbb{F}_p^s$ of dimension $(s-1)/2$ on which Q is zero. This result is, in fact, best possible.

Theorem 1.1.

(i) *A quadratic form Q in $\mathbb{F}_p[X_1, \ldots, X_s]$ with* $\det Q \neq 0$ *cannot vanish on a subspace of $\mathbb{F}_p^s$ of dimension greater than $[s/2]$.*

(ii) *If, further, s is even and $(-1)^{s/2} \det Q \notin (\mathbb{F}_p^*)^2$, then Q cannot vanish on a subspace of dimension $s/2$.*

In [12] the 'subspace theorem' cited above is applied to show that for a quadratic form Q in $\mathbb{Z}[X_1, \ldots, X_s]$ (s odd), any congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{m}$$

has a solution satisfying

$$0 < |\mathbf{x}| = \max(|x_1|, \ldots, |x_s|) \leq m^{1/2+1/(2s)}.$$

This has been improved for $s \geq 4$ by Heath-Brown [9]. Finally in [12] the above result on small solutions of congruences is used to prove

$$\min_{0<|\mathbf{x}|\leq N} \|Q(x_1, \ldots, x_s)\| < C(s, \epsilon) N^{-2+\eta_s+\epsilon}. \tag{1.1}$$

Here Q is a quadratic form, $Q \in \mathbb{R}[X_1, \ldots, X_s], \epsilon > 0, \eta_s$ is explicitly given and $s\eta_s$ is bounded; and $\| \ldots \|$ denotes distance from the nearest integer. For improvements of (1.1) see Baker and Harman [4], Heath-Brown [9] and (for $s = 2$) Dyke [8].

Acknowledgment. Research supported in part by a grant from the National Science Foundation.

Analogous results for forms of higher degree are known in the additive case. Throughout the paper let

$$A_k(X_1, \ldots, X_s) = a_1 X_1^k + \cdots + a_s X_s^k.$$

If A_k has coefficients in $\mathbb{F}_p$, then A_k vanishes on a subspace of $\mathbb{F}_p^s$ having dimension $[s/3]$, provided $p > C_1(k)$. This follows from the fact that a ternary additive form over $\mathbb{F}_p$ with $p > C_1(k)$ has a nontrivial zero [2, page 167]. Using the geometry of numbers as in [12] (or Theorem 2.1, below), one can then solve any congruence

$$A_k(x_1, \ldots, x_s) \equiv 0 \pmod{m} \tag{1.2}$$

(where $A_k \in \mathbb{Z}[X_1, \ldots, X_s]$) with

$$0 < |\mathbf{x}| \leq C_2(k) m^{1-[s/3]/s}. \tag{1.3}$$

For $s = 3$, the exponent $2/3$ in (1.3) is best possible [2, §2]. For $s \geq 5$, a different method provides solutions smaller than in (1.3); the exponent in (1.3) would be $1/2 + 1/(2s-2) + \epsilon$.

Theorem 1.2. *Let $s \geq 4, m \geq C_3(s, k, \epsilon)$. Let $B_1, \ldots, B_s$ be positive numbers with*

$$B_1 \ldots B_s \geq m^{s/2+s/(2s-2)+\epsilon}. \tag{1.4}$$

The congruence (1.2) has a solution $\mathbf{x} \neq \mathbf{0}$ with

$$|x_i| \leq B_i \quad (i = 1, \ldots, s). \tag{1.5}$$

This is Theorem 1A of [2]. Recently Dietmann [7] pointed out that if $A_3 \in \mathbb{F}_p[X_1, \ldots, X_s]$ (s odd), then A_3 vanishes on a subspace of $\mathbb{F}_p^s$ of dimension $(s-1)/2$. This enabled him to replace the exponent in (1.3) by $1/2 + 1/(2s)$ for odd s.

If Dietmann's method is generalized to degree k, the following result ensues.

Theorem 1.3. *Let k be odd, $k \geq 3$. Let s be odd, $s \geq k$. Then for $p > C_1(k)$, a form $A_k(X_1, \ldots, X_s)$ over $\mathbb{F}_p$ vanishes on a subspace of $\mathbb{F}_p^s$ having dimension $(s-k)/2 + [k/3]$.*

We also note a simple extension of Dietmann's congruence result.

Theorem 1.4. *Let s be odd, let $m \geq 1$, and let $B_1, \ldots, B_s$ be positive numbers,*

$$B_1 \ldots B_s \geq m^{s/2+1/2}. \tag{1.6}$$

Given $A_3 \in \mathbb{Z}[X_1, \ldots, X_s]$, the congruence

$$A_3(x_1, \ldots, x_s) \equiv 0 \pmod{m} \tag{1.7}$$

has a solution $\mathbf{x} \neq \mathbf{0}$ satisfying (1.5).

Since Theorem 1.3 yields no improvement of Theorem 1.2 for $k > 3$, it is of interest to obtain complementary results.

Theorem 1.5.

(i) *Let $k \geq 3$ and $1 \leq s \leq k+1$. Let $p > s$. Suppose that a form A_k in $\mathbb{F}_p[X_1, \ldots, X_s]$ with $a_1 \ldots a_s \neq 0$ vanishes on a subspace V of $\mathbb{F}_p^s$ having dimension d. Then $\{1, \ldots, s\}$ can be partitioned into subsets $\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_d$ such that $(v_i)_{i \in \mathcal{B}_0}$ is the zero vector for all $\mathbf{v}$ in V, while*

$$\sum_{i \in \mathcal{B}_j} a_i u_i^k = 0 \tag{1.8}$$

for $j = 1, \ldots, d$; the vector $(u_i)_{i \in \mathcal{B}_j}$ is nonzero $(j = 1, \ldots, d)$.

(ii) *Let $k \geq 3, 1 \leq s \leq k$. If $p > s$ and $k|(p-1)$ there is a form A_k in $\mathbb{F}_p[X_1, \ldots, X_s]$ that does not vanish on any subspace of dimension greater than $[s/3]$.*

It is easy to see that for $s > k$, the integer $[s/3]$ in (ii) could be replaced by

$$[k/3] + s - k.$$

However, the following result is stronger for large s.

Theorem 1.6.

(i) *Let s be odd and let $p > \max(k, s)$. A form A_k in $\mathbb{F}_p[X_1, \ldots, X_s]$ with $a_1 \ldots a_s \neq 0$ cannot vanish on a subspace of $\mathbb{F}_p^s$ of dimension greater than $(s-1)/2$.*

(ii) *Let s be even and $p > \max(k, s)$. Suppose A_k is a form in $\mathbb{F}_p[X_1, \ldots, X_s]$ with $a_1 \ldots a_s \neq 0$ that vanishes on a subspace of $\mathbb{F}_p^s$ of dimension $s/2$. If k is even, then $(-1)^{s/2} a_1 \ldots a_s \in (\mathbb{F}_p^*)^2$. If k is odd and $p > \max(k, s!)$, then after renumbering the variables we have*

$$a_{2i-1} a_{2i}^{-1} \in (\mathbb{F}_p^*)^k \quad (i = 1, \ldots, s/2). \tag{1.9}$$

(iii) *Suppose that $(p-1, k) > 1$. Let s be even, and suppose $p > \max(k, s!)$. There is a form A_k in $\mathbb{F}_p[X_1, \ldots, X_s]$ that does not vanish on any subspace of $\mathbb{F}_p^s$ having dimension $s/2$.*

We note a result for a 'general' form

$$G(X_1, \ldots, X_s) = \sum_{\substack{i_1 \geq 0, \ldots, i_s \geq 0 \\ i_1 + \cdots + i_s = k}} a(i_1, \ldots, i_s) X_1^{i_1} \ldots X_s^{i_s}.$$

over $\mathbb{Z}$.

Theorem 1.7. *For G as above, and $s \geq k+1$, any congruence*

$$G(\mathbf{x}) \equiv 0 \pmod{m} \tag{1.10}$$

has a solution satisfying

$$0 < |\mathbf{x}| \leq m^{k/(k+1)}. \tag{1.11}$$

In contrast, for $s = k$ the congruence (1.10) may have only the trivial solution, as explained in [2].

We now turn to additive forms over $\mathbb{R}$. It was shown by Cook [6] that, for real $\lambda_1, \ldots, \lambda_s$,

$$\min_{0<|\mathbf{x}|\leq N} \|\lambda_1 x_1^k + \cdots + \lambda_s x_s^k\| < C_4(k, \epsilon) N^{-s/K+\epsilon};$$

K denotes 2^{k-1}. Assuming that k is relatively small, this is still the best result known, except that the case $k = 2, s = 1$ (a theorem of Heilbronn [10]) has been improved by Zaharescu [14]; the exponent $-1/2+\epsilon$ is replaced by $-4/7+\epsilon$. The ideas in [12] enable one to go beyond the exponent $-1+\epsilon$ for $s > K$; see [2], [9], [7]. In the present paper we refine the approach in [2] and obtain the following result, which sharpens those in [2] and [7].

Theorem 1.8. *Let $k \geq 3$ and let $s > K$. Let*

$$\sigma_{s,3} = \min\left(\frac{s}{4}, \max_{\substack{5\leq h\leq s\\ h \text{ odd}}} \min\left(\frac{2h(s-3)+4h}{(h+1)(s-3)+4h}, \frac{s-h+5}{4}\right)\right)$$

and let

$$\sigma_{s,k} = \min\left(\frac{s}{K}, \max_{K+1\leq h\leq s} \min\left(\frac{(2h-2)(s-k)+4h-4}{h(s-k)+4h-4}, \frac{s-h+K+1}{K}\right)\right)$$

for $k \geq 4$. Then for real $\lambda_1, \ldots, \lambda_s$,

$$\min_{0<|\mathbf{x}|\leq N} \|\lambda_1 x_1^k + \cdots + \lambda_s x_s^k\| < C_5(k, \epsilon) N^{-\sigma_{s,k}+\epsilon}.$$

In particular, we have $\sigma_{5,3} = 5/4$ and $\sigma_{s,4} = s/8$ for $9 \leq s \leq 12$.

2. From subspaces to small solutions

Theorem 2.1. *Let s and d be natural numbers, $s \geq 2d$. Suppose that for $p > C_6 = C_6(k, s)$, every form A_k in $\mathbb{F}_p[X_1, \ldots, X_s]$ vanishes on a subspace of $\mathbb{F}_p^s$ of dimension d. Let $B_1, \ldots, B_s$ be positive numbers,*

$$B_1 \ldots B_s \geq C_7 m^{s-d}, \tag{2.1}$$

where

$$C_7 = \prod_{p\leq C_6} p^s.$$

Then for every modulus m, and every form A_k in $\mathbb{Z}[X_1, \ldots, X_s]$, the congruence (1.2) has a solution $\mathbf{x} \neq \mathbf{0}$ satisfying (1.5)

Proof. Let $u = \prod_{p \le C_6} p$. Suppose first that m is squarefree, $(m, u) = 1$. By hypothesis, for each prime p dividing m there is a set of linear forms $K_1, \ldots, K_{s-d}$ in $\mathbb{Z}[X_1, \ldots, X_s]$ with the property that

$$K_i(\mathbf{x}) \equiv 0 \pmod{p} \quad (1 \le i \le s-d)$$

implies $A_k(\mathbf{x}) \equiv 0 \pmod{p}$. By an application of the Chinese remainder theorem we obtain $s-d$ linear forms $L_1, \ldots, L_{s-d}$ in $\mathbb{Z}[X_1, \ldots, X_s]$ such that

$$A_k(\mathbf{x}) \equiv 0 \pmod{m}$$

whenever

$$L_i(\mathbf{x}) \equiv 0 \pmod{m} \quad (1 \le i \le s-d).$$

Minkowski's linear forms theorem yields a nonzero $(x_1, \ldots, x_{2s-d})$ in $\mathbb{Z}^{2s-d}$ such that

$$|x_i| \le B_i \quad (i = 1, \ldots, s),$$
$$|L_i(x_1, \ldots, x_s) - m x_{s+i}| < 1 \quad (i = 1, \ldots, s-d).$$

For the determinant of the $2s-d$ linear forms in question is m^{s-d}, which is $\le B_1 \ldots B_s$. Clearly $(x_1, \ldots, x_s) \neq \mathbf{0}$ and

$$A_k(x_1, \ldots, x_s) \equiv 0 \pmod{m}.$$

For a general modulus m, write $m = \ell^2 v n$ where v and n are squarefree, $v | u$ and $(n, u) = 1$. Given B_i satisfying (2.1) there is a $\mathbf{y} \neq \mathbf{0}$ with

$$A_k(\mathbf{y}) \equiv 0 \pmod{n},$$
$$|y_i| \le B_i/(\ell v).$$

For

$$\begin{aligned} B_1 \ldots B_s/(\ell v)^s &\ge u^s m^{s-d} \ell^{-s} v^{-s} \\ &\ge m^{s-d} \ell^{-s} \ge n^{s-d} \end{aligned}$$

since

$$\ell^s n^{s-d} \le (\ell^2 n)^{s-d} \le m^{s-d}.$$

Now

$$A_k(\ell v \mathbf{y}) = \ell^k v^k A_k(\mathbf{y}) \equiv 0 \pmod{m}$$

while $\ell v \mathbf{y} \neq \mathbf{0}$,

$$|\ell v y_i| \le B_i.$$

This completes the proof of Theorem 2.1. ∎

3. Subspaces on which $\mathbf{A_k}$ vanishes

We now prove Theorem 1.3 by induction on s. The case $s = k$ is covered in the introduction. Let $s > k$, s odd, and suppose the theorem already known for $s-2$. If any a_i, say a_1, is 0, then the form $a_1X_1^k + a_2X_2^k$ in (X_1, X_2) vanishes on a subspace of dimension 1. Since $A_k(0, 0, X_3, \ldots, X_s)$ vanishes on a subspace of dimension

$$\frac{s-2-k}{2} + \left[\frac{k}{3}\right],$$

we obtain in an obvious way a subspace of dimension

$$1 + \frac{s-2-k}{2} + \left[\frac{k}{3}\right] = \frac{s-k}{3} + \left[\frac{k}{3}\right]$$

on which A_k vanishes. Hence we may assume that no a_i is 0. Now $(\mathbb{F}_p^*)^k$ has $(p-1, k)$ cosets in $\mathbb{F}_p^*$. Since $s > k$, there must be two a_i (say a_1, a_2) in the same coset, so that $a_1 = u^k a_2, u \in \mathbb{F}_p^*$. Now $(t, -ut)(t \in \mathbb{F}_p)$ gives a 1-dimensional subspace on which $a_1X_1^k + a_2X_2^k$ vanishes. We now complete the induction step as before, and Theorem 1.3 is proved.

Proof of Theorem 1.4. By a result of Lewis [11], the congruence

$$a_1x_1^3 + a_2x_2^3 + a_3x_3^3 \equiv 0 \pmod p$$

is solvable nontrivially for every p, and thus we may take $C_1(3) = 1$ in Theorem 1.3. Applying Theorem 2.1 with $C_6 = C_7 = 1, d = (s-3)/2 + 1 = (s-1)/2$, we obtain the desired result. ■

We conclude this section by proving Theorem 1.7. According to the Chevalley-Warning theorem [13, page 136] for given p there is $\mathbf{a} \in \mathbb{F}_p^{k+1}\backslash\{\mathbf{0}\}$, such that $G(\mathbf{a}) = 0$. The multiples of $\mathbf{a}$ form a 1-dimensional subspace on which G vanishes. Arguing as in the proof of Theorem 2.1 with $d = 1, s = k+1$ and $B_1 = \ldots = B_{k+1} = m^{k/(k+1)}$, we obtain a solution of (1.10) satisfying (1.11).

4. Forms that do not vanish on any large subspace

Proof of Theorem 1.1. We observe that if R is a quadratic form in $\mathbb{F}_p[X_1, \ldots, X_s]$ and

$$R(0, \ldots, 0, w_{t+1}, \ldots, w_s) = 0 \quad \text{identically}$$

for some $t < s$, we may write R in the form

$$R(w_1, \ldots, w_s) = w_1M_1(w_1, \ldots, w_s) + \cdots + w_tM_t(w_t, \ldots, w_s)$$

where $M_1, \ldots, M_t$ are linear forms. To see this, we may proceed by induction on t. The case $t = 1$ follows from the Remainder Theorem. In the induction step, choose $M_1(\mathbf{w})$ so that

$$R' = R(w_1, \ldots, w_s) - w_1M_1(\mathbf{w})$$

does not contain w_1 explicitly. Then $R' = R'(w_2, \dots, w_s)$ vanishes when $w_2, \dots, w_t$ are zero. Accordingly,

$$R' = w_2 M_2(w_2, \dots, w_s) + \cdots + w_t M_t(w_t, \dots, w_s)$$

and the induction step is complete.

Now let s be even and take a quadratic form Q in $\mathbb{F}_p(X_1, \dots, X_{2s})$ that vanishes on a subspace of $\mathbb{F}_p^{2s}$ of dimension $s-t$. There are linearly independent linear forms $L_1(\mathbf{X}), \dots, L_t(\mathbf{X})$ such that $Q(\mathbf{x}) = 0$ whenever $L_1(\mathbf{x}) = \dots = L_t(\mathbf{x}) = 0$. Choose linear forms $L_{t+1}, \dots, L_{2s}$ such that $\det(L_1, \dots, L_{2s}) \neq 0$ and make the change of variables $y_j = L_j(\mathbf{x})$ $(1 \le j \le 2s)$. We write

$$Q'(y_1, \dots, y_{2s}) = Q(x_1, \dots, x_{2s}).$$

Since $Q'(0, \dots, 0, w_{t+1}, \dots, w_{2s}) = 0$ identically, we have

$$Q'(y_1, \dots, y_{2s}) = y_1 M_1(\mathbf{y}) + \cdots + y_t M_t(\mathbf{y}).$$

Since there are no terms $y_i y_j$ with $i > t, j > t$, the matrix of Q' may be written

$$\left[\begin{array}{c|c} A & B \\ \hline B^{tr} & 0 \end{array}\right]$$

where A is $t \times t$ and B is $t \times (s-t)$. If $t = s/2$, $\det Q' = (-1)^{s/2}(\det B)^2$. Since $\det Q = r \det Q'$ for some $r \in (\mathbb{F}_p^*)^2$, we have $(-1)^{s/2} \det Q \in (\mathbb{F}_p^*)^2$, which proves Theorem 1.1 (ii). If $t < s/2$, it is easy to see that any product occurring in $\det Q'$ has a factor 0, so that $\det Q' = 0$ and $\det Q = 0$. This completes the proof of Theorem 1.1. ■

Proof of Theorem 1.6. Suppose that A_k vanishes on a subspace V of $\mathbb{F}_p^s$ having dimension d, when $d = s/2$ (s even), $d = (s+1)/2$ (s odd). Let $\mathbf{u}, \mathbf{x}$ be in V. Then

$$0 = \sum_{j=1}^{s} a_j(z_1 u_j + z_2 x_j)^k = \sum_{j=1}^{s} a_j \sum_{h=0}^{k} \binom{k}{h} u_j^h x_j^{k-h} z_1^h z_2^{k-h} \tag{4.1}$$

for any z_1, z_2 in $\mathbb{F}_p$. Since $p > k$, the coefficient of $z_1^h z_2^{k-h}$ must be 0 for $h = 0, \dots, k$. In particular,

$$Q_{\mathbf{u}}(\mathbf{x}) := \sum_{j=1}^{s} a_j u_j^{k-2} x_j^2 = 0 \quad (\mathbf{x} \in V). \tag{4.2}$$

By Theorem 1.1, if s is even we may assert that

$$(-1)^{s/2} a_1 \dots a_s (u_1 \dots u_s)^{k-2} \in (\mathbb{F}_p^*)^2, \tag{4.3}$$

for arbitrary $\mathbf{u}$ in V with $u_1 \dots u_s \neq 0$.

Let U be a matrix whose rows are a basis of V. There are two cases to consider.

Case 1. U has zero columns, let us say columns $1, \dots, r$.

In this case $Q_{\mathbf{u}}$ can be considered as a quadratic form in $s - r$ variables, which vanishes on a subspace having dimension d. Moreover, $d > (s-r)/2$. The number of elements of V having a zero coordinate in a given position $j, j > r$, is p^{d-1}, since these are the elements of a $(d-1)$-dimensional subspace of V. So there are at least $p^d - (s-r)p^{d-1}$ elements $\mathbf{u}$ of V with $u_{r+1} \dots u_s \neq 0$. Now for each such $\mathbf{u}, Q_{\mathbf{u}}$ has nonzero determinant, and since $p > s$, we obtain a contradiction by comparing (4.2) with Theorem 1.1.

Case 2. U has no zero column. By the argument in the preceding paragraph, there is $\mathbf{u}$ in U with $u_1 \dots u_s \neq 0$. If s is odd, (4.2) contradicts Theorem 1.1. This proves Theorem 1.6 (i).

Suppose now that s is even. If k is even, then (4.3) shows that $(-1)^{s/2} a_1 \dots a_s \in (\mathbb{F}_p^*)^2$, proving Theorem 1.6 (ii) in this case. Thus we may suppose that k is odd; (4.3) now yields a conclusion for any element $\mathbf{v}$ of V:

$$(-1)^{s/2} a_1 \dots a_s (tu_1 + v_1) \dots (tu_s + v_s) \in (\mathbb{F}_p^*)^2$$

for every choice of t in $\mathbb{F}_p$ except $t = -v_1/u_1, \dots, t = -v_s/u_s$. In terms of the character

$$\chi(x) = \left(\frac{x}{p}\right).$$

we have the inequality

$$\sum_{t \in \mathbb{F}_p} \chi\left((-1)^{s/2} \prod_{j=1}^{s} a_j(tu_j + v_j)\right) \geq p - s > p/2. \tag{4.4}$$

Now the character sum in (4.4) has modulus at most

$$(s-1)p^{1/2}$$

unless the polynomial

$$f(t) = (-1)^{s/2} \prod_{j=1}^{s} a_j(tu_j + v_j)$$

is a perfect square [13, Theorem 2C′]. Since $p/2 > (s-1)p^{1/2}$, we conclude that $f(t)$ is a perfect square. The zeros of f occur in pairs, say

$$\frac{v_1}{u_1} - \frac{v_2}{u_2} = 0, \dots, \frac{v_{s-1}}{u_{s-1}} - \frac{v_s}{u_s} = 0. \tag{4.5}$$

Since $\mathbf{v}$ is an arbitrary point in V, and since $p^{s/2} > s! p^{s/2-1}$, it is clear that one of the $s/2$-dimensional subspaces, defined by (4.5) or an analogous pairing, coincides with V.

Consider the point $(u_1, u_2, 0, \ldots, 0)$ of V. We have

$$a_1 u_1^k + a_2 u_2^k = 0,$$

giving (1.9) for $i = 1$; and clearly (1.9) holds for $2 \le i \le s/2$ in the same way. This establishes Theorem 1.6 (ii).

Part (iii) of the theorem is now obvious. For instance, if k is odd, choose $a_1 = \ldots = a_{s-1}$ and a_s in a different coset of $(\mathbb{F}_p^*)^k$ from a_1, so that no numbering could allow (1.9). ■

Proof of Theorem 1.5 (i). We proceed by induction on s. The case $s = 1$ is obvious. In the induction step, let A_k be a form in $\mathbb{F}_p(X_1, \ldots, X_s)$ with $s \le k+1, a_1 \ldots a_s \ne 0$ and suppose that A_k vanishes on a subspace V of $\mathbb{F}_p^s$ having dimension d. Let U be a $d \times s$ matrix whose rows are a basis of V. If U has zero columns, we form a block $\mathcal{B}_0$ consisting of the numbers of these columns and get the desired result by applying the inductive hypothesis to the form in the remaining variables. Thus we may exclude this case, and as in the proof of Theorem 1.6 there are at most sp^{d-1} elements $\mathbf{u}$ of V with $u_1 \ldots u_s = 0$.

Fix $\mathbf{u}$ in V with $u_1 \ldots u_s \ne 0$. We relabel the variables so that the first d columns of U are linearly independent, and let $h_1, \ldots, h_d$ be any d elements of $\mathbb{F}_p$ with

$$\frac{h_1}{u_1}, \ldots, \frac{h_d}{u_d} \quad \text{distinct.}$$

Since the reduced echelon form of U has standard basis vectors as its first d columns, we can find $\mathbf{v}$ in V of the form

$$\mathbf{v} = (h_1, \ldots, h_d, v_{d+1}, \ldots, v_s).$$

We now apply (4.1) with $\mathbf{v}$ in place of $\mathbf{x}$. Thus

$$\sum_{j=1}^{s} a_j u_j^{k-h} v_j^h = 0 \quad (h = 0, 1, \ldots, k);$$

rewrite this in the form

$$\sum_{j=1}^{s} a_j u_j^k r_j^h = 0 \quad (h = 0, 1, \ldots, k) \tag{4.6}$$

where $r_i = v_i / u_i$.

Let $R_1 = r_1, \ldots, R_d = r_d, \ldots, R_m$ be the distinct ones among $r_1, \ldots, r_s$. We rewrite (4.6) in the form

$$\sum_{n=1}^{m} b_n R_n^h = 0 \quad (h = 0, 1, \ldots, k) \tag{4.7}$$

where

$$b_n = \sum_{j \in \mathcal{B}_n} a_j u_j^k;$$

$\mathcal{B}_n$ is the set of j in $\{1, \dots, s\}$ with $r_j = R_n$.

The first m equations (4.7), those with $0 \le h \le m-1$, form a system of linear equations whose determinant is the Vandermonde determinant $\det(R_i^j)$ $(i = 1, \dots, m; j = 0, 1, \dots, m-1)$ which is not zero. We conclude that $b_1 = \cdots = b_m = 0$, that is,

$$\sum_{j \in \mathcal{B}_n} a_j u_j^k = 0 \quad (n = 1, \dots, m).$$

We may reduce the number of blocks $\mathcal{B}_n$ to d by uniting blocks, and Theorem 1.5 (i) follows.

(ii) Choose $a_1, \dots, a_s$ from distinct cosets of $(\mathbb{F}_p^*)^k$. If A_k vanishes on a subspace of dimension d, and if $u_1, \dots, u_s$ are chosen as in (1.8), then no $\mathcal{B}_j$ can have fewer than three elements. Thus $3d \le s$ as required. ■

5. Small fractional parts of additive forms

We assemble some lemmata needed for the proof of Theorem 1.8. We assume, as we may, that ϵ is sufficiently small and $N > C_8(s, k, \epsilon)$; and write $\eta = \epsilon^2$, $L = [N^{\sigma_{n,k} - \epsilon + \eta}]$, and

$$S_j(m) = \sum_{x=1}^{N} e(m\lambda_j x^k)$$

where $e(\theta) = e^{2\pi i\theta}$. Implied constants depend at most on s, k and ϵ.

Lemma 5.1. *Suppose that for some $\lambda_1, \dots, \lambda_s$ with $s > K$, $K = 2^{k-1}$, $k \ge 3$, the inequality*

$$\|\lambda_1 y_1^k + \cdots + \lambda_s y_s^k\| < N^{-\sigma_{s,k}+\epsilon} \tag{5.1}$$

has no solution with

$$0 < \max(|y_1|, \dots, |y_s|) \le N. \tag{5.2}$$

Then after relabelling $\lambda_1, \dots, \lambda_s$, there is a set $\mathcal{B}$ of natural numbers, $\mathcal{B} \subset [1, L]$, and there are positive numbers $B_1 \ge \dots \ge B_s$ such that, for $m \in \mathcal{B}$,

$$B_i < |S_i(m)| \le 2B_i \quad (i = 1, \dots, s). \tag{5.3}$$

Moreover,

$$B_1 \dots B_s |\mathcal{B}| \gg N^{s-\eta}. \tag{5.4}$$

Proof. This may be shown by a slight variant of the argument on p. 184 of [2]. ■

Lemma 5.2. *Suppose that for some j, $1 \le j \le n$ and some m, $1 \le m \le L$ we have*

$$|S_j(m)| > B_j \ge N^{1-1/K+\eta}. \tag{5.5}$$

Then there is a natural number q_j and an integer v_j with

$$q_j \le N^{k+\eta} B_j^{-k}, \tag{5.6}$$

$$|m\lambda_j q_j - v_j| \le N^{\eta} B_j^{-k}; \tag{5.7}$$

and there is a natural number r_j and an integer b_j with

$$r_j \le N^{2+\eta} B_j^{-2}, \tag{5.8}$$

$$|m\lambda_j r_j^k - b_j| \le N^{k+\eta} B_j^{-2k}. \tag{5.9}$$

Proof. For the existence of q_j and v_j, see the case $M = 1$ of [1], Theorem 1. We now apply [3], Lemma 8.6, noting that (5.5), (5.6) together yield

$$\begin{aligned} q_j &\le (N/B_j)^k N^{\eta} \le N^{k/K} \le N^{1-\eta}, \\ |m\lambda_j q_j - v_j| &\le N^{-k+k/K} < N^{1-k-\eta}, \\ B_j &\ge N^{k-1+2\eta} B_j^{-(k-1)} \ge q_j^{(k-1)/k} N^{\eta}. \end{aligned}$$

Thus the conditions (8.68), (8.69) in [3] are satisfied, and the existence of r_j and b_j follows. ■

Lemma 5.3. *Suppose that θ is real and that there exist R distinct integer pairs x, z satisfying*

$$|\theta x - z| < \zeta, \tag{5.10}$$

$$0 < |x| < X \tag{5.11}$$

where $R \ge 24\zeta X > 0$. Then all integer pairs x, z satisfying (5.10), (5.11) have the same ratio z/x.

Proof. This is a lemma of Birch and Davenport [5]; see also [3], Lemma 5.2. ■

Lemma 5.4. *Under the hypotheses of Lemma 5.1, the set $\mathcal{B}$ has cardinality*

$$|\mathcal{B}| \ll L N^{k-1+2\eta} B_1^{-k} \ll (LN^{-1})^{s/(s-k)} N^{3s\eta}. \tag{5.12}$$

Proof. From (5.4),

$$B_1 > (N^{s-2\eta} L^{-1})^{1/s} > N^{1-1/K+\eta},$$

since $\sigma_{s,k} \le s/K$. Thus Lemma 5.2 is applicable for $j = 1$ and each m in $\mathcal{B}$. We write $q_1 = q_1(m), v_1 = v_1(m)$ for the integers satisfying (5.6), (5.7). The number R of distinct products $mq_1(m)$ $(m \in \mathcal{B})$ for which $m \sim M, q(m) \sim Q$ satisfies

$$R \ge |\mathcal{B}| N^{-\eta}, \tag{5.13}$$

for some choice of $M, 1 \le M \le L$ and $Q, 1 \le Q \le N^{k+\eta}B_1^{-k}$. This follows from a simple divisor argument. Let

$$X = LN^{k+\eta}B_1^{-k},$$
$$\zeta = N^{\eta}B_1^{-k}.$$

In order to apply Lemma 5.3 with $\theta = \lambda_1$ we need to verify that $R \ge 24\zeta X$. Now

$$\begin{aligned}\zeta X R^{-1} &\ll LN^{k+3\eta}B_1^{-2k}|\mathcal{B}|^{-1}\\ &\ll LN^{k+3\eta}(|\mathcal{B}|N^{-s+\eta})^{2k/s}|\mathcal{B}|^{-1}\end{aligned}$$

from (5.4). If $2k < s$ this is $\ll LN^{-k+\epsilon}$ and so $R \ge 24\zeta X$. If $s \le 2k$, we obtain instead the bound

$$\ll N^{-k+\epsilon}L^{2k/s} \ll N^{-\epsilon}$$

and again $R \ge 24\zeta X$. We conclude that there are integers $s \ge 1$ and t such that

$$\frac{v_1(m)}{mq_1(m)} = \frac{t}{s}$$

for all m in $\mathcal{B}$.

We observe that, since each $mq_1(m)$ is a multiple of s,

$$\begin{aligned}Rs &\ll MQ,\\ s &\ll MQ|\mathcal{B}|^{-1}N^{\eta}\\ &\ll LN^{k+2\eta}B_1^{-k}|\mathcal{B}|^{-1}\end{aligned} \tag{5.14}$$

from (5.13), (5.6). Moreover, for any m in $\mathcal{B}$,

$$\begin{aligned}|\lambda_1 s - t| &= \frac{s}{mq(m)}\,|\lambda_1 mq(m) - v_1(m)|\\ &\ll \frac{s}{MQ}\,N^{\eta}B_1^{-k}\end{aligned}$$

from (5.7), so that

$$\begin{aligned}\|\lambda_1 s^k\| &\ll \frac{s^k}{MQ}\,N^{\eta}B_1^{-k}\\ &\ll (MQ)^{k-1}N^{(k+1)\eta}|\mathcal{B}|^{-k}B_1^{-k}\\ &\ll L^{k-1}N^{k(k-1)+2k\eta}|\mathcal{B}|^{-k}B_1^{-k^2}\end{aligned}$$

from (5.14), (5.6).

Now by hypothesis, either

$$s > N \tag{5.15}$$

or

$$\|\lambda_1 s^k\| > L^{-1}. \tag{5.16}$$

If (5.15) holds, then

$$LN^{k+2\eta}B_1^{-k}|\mathcal{B}|^{-1} \gg N,$$

which yields the first inequality of (5.12). If (5.16) holds, then

$$L^{k-1}N^{k(k-1)+2k\eta}|\mathcal{B}|^{-k}B_1^{-k^2} \gg L^{-1},$$

which leads to the same conclusion and completes the proof of the first inequality in (5.12). To get the second inequality, we insert the bound $B_1^s|\mathcal{B}| \gg N^{s-\eta}$ which follows from (5.4), to obtain

$$|\mathcal{B}| \ll LN^{k-1+2\eta}|\mathcal{B}|^{k/s}N^{-k+k\eta/s};$$
$$|\mathcal{B}| \ll (LN^{-1})^{\frac{s}{s-k}}N^{c\eta},$$

where $c = (2s+k)/(s-k) < 3s$. ∎

Proof of Theorem 1.8. We suppose that (5.1) has no solution satisfying (5.2) and obtain a contradiction. We select an integer h for which, in case $k=3$,

$$h \text{ is odd, } 5 \le h \le s, \text{ and } \min\left(\frac{2h(s-3)+4h}{(h+1)(s-3)+4h}, \frac{s-h+5}{4}\right)$$

attains its largest value over odd h in $[5,s]$. In case $k>3$ we drop the restriction to odd h and require that

$$\min\left(\frac{(2h-2)(s-k)+4h-4}{h(s-k)+4h-4}, \frac{s-h+K+1}{K}\right)$$

attains its largest value subject to $K+1 \le h \le s$.

We select any m in $\mathcal{B}$. We need to verify that

$$B_h > N^{(K-1)/K+\eta}. \tag{5.17}$$

If (5.17) does not hold, then

$$\begin{aligned} N^{s-\eta} &\ll B_1 \dots B_s|\mathcal{B}| \\ &\ll B_1^{h-1}B_h^{s-h+1}|\mathcal{B}| \\ &\ll |\mathcal{B}|B_1^{h-1}N^{((K-1)/K+\eta)(s-h+1)}. \end{aligned}$$

We now apply (5.12) to obtain

$$\begin{aligned} N^{s-\eta} &\ll LN^{k-1+2\eta}B_1^{h-k-1}N^{((K-1)/K+\eta)(s-h+1)} \\ &\ll LN^{h-2+2\eta+((K-1)/K+\eta)(s-h+1)}, \\ L &\gg N^{(s-h+K+1)/K-s\eta}, \end{aligned}$$

contrary to the definition of L. This establishes (5.17)

For $j = 1, \ldots, h$, let r_j, b_j be the integers provided by Lemma 5.2. We now apply Theorem 1.4, if $k = 3$, or Theorem 1.2, if $k > 3$, to obtain integers $x_1, \ldots, x_h$, not all zero,

$$|x_j| \leq N^{-1-\eta} B_j^2 (m/L)^{1/k} \quad (1 \leq j \leq h) \tag{5.18}$$

such that

$$b_1 x_1^k + \cdots + b_h x_h^k \equiv 0 \pmod{m}. \tag{5.19}$$

For

$$\begin{aligned} \prod_{j=1}^{h} N^{-1-\eta} B_j^2 (mL^{-1})^{1/k} &= (B_1 \ldots B_h)^2 N^{-h-h\eta} (mL^{-1})^{h/k} \\ &\gg (N^{s-\eta} |\mathcal{B}|^{-1})^{2h/s} N^{-h-h\eta} (mL^{-1})^{h/k} \\ &\gg N^{h-2h\eta} |\mathcal{B}|^{-2h/s} (mL^{-1})^{h/k}. \end{aligned} \tag{5.20}$$

Using the bound (5.12), we arrive at the lower bound

$$\gg N^{h-2h\eta} (LN^{-1})^{-2h/(s-k)} N^{-6h\eta} (mL^{-1})^{h/k}.$$

We have to show that the last expression is at least

$$m^{(h+1)/2}$$

in case $k = 3$, and at least

$$m^{h^2/(2h-2)} N^{\eta}$$

in case $k \geq 4$, so that we can apply Theorem 1.4 or Theorem 1.2.

(i) $\mathbf{k = 3}$.

$$\begin{aligned} N^{h-8h\eta} &(LN^{-1})^{-2h/(s-3)} (mL^{-1})^{h/3} m^{-(h+1)/2} \\ &\geq N^{h-8h\eta} (LN^{-1})^{-2h/(s-3)} L^{-(h+1)/2} \\ &\geq 1 \end{aligned}$$

since $m \leq L$ and

$$L^{2h/(s-3)+(h+1)/2} \leq N^{h+2h/(s-3)-\epsilon}.$$

(ii) $\mathbf{k \geq 4}$.

$$\begin{aligned} N^{h-9h\eta} &(LN^{-1})^{-2h/(s-k)} (mL^{-1})^{h/k} m^{-h^2/(2h-2)} \\ &\geq N^{h-9h\eta} (LN^{-1})^{-2h/(s-k)} L^{-h^2/(2h-2)} \geq 1 \end{aligned}$$

since $m \leq L$ and

$$L^{h^2/(2h-2)+2h/(s-k)} \leq N^{h+2h/(s-k)-\epsilon}.$$

This establishes the solvability of (5.19) subject to (5.18).

We now observe that $y_j = x_j r_j$ satisfies

$$0 < \max(|y_1|, \ldots, |y_h|) \le N$$

from (5.8), (5.18). Moreover,

$$\begin{aligned}&\lambda_1 y_1^k + \cdots + \lambda_h y_h^k \\ &\quad = (m\lambda_1 r_1^k - b_1)\,\frac{x_1^k}{m} + \cdots + (m\lambda_h r_h^k - b_h)\,\frac{x_h^k}{m} + \frac{b_1 x_1^k + \cdots + b_h x_h^k}{m}.\end{aligned}$$

In view of (5.19),

$$\begin{aligned}\|\lambda_1 y_1^k + \cdots + \lambda_h y_h^k\| &\le m^{-1} \sum_{j=1}^{h} |x_j|^k |m\lambda_j r_j^k - b_j| \\ &\le m^{-1} \sum_{j=1}^{h} N^{-k-k\eta} B_j^{2k}\,\frac{m}{L}\,N^{k+\eta} B_j^{-2k} \\ &< L^{-1}.\end{aligned}$$

This contradicts our initial hypothesis. We conclude that there is a solution of (5.1), (5.2).

For the final remark of the theorem, we first take $k = 3, s = 5$ and thus $h = 5$. Then

$$\frac{2h(s-3)+4h}{(h+1)(s-3)+4h} = \frac{40}{32} = \frac{5}{4} = \frac{s-h+5}{4} = \frac{s}{4}.$$

Next, take $k = 4, 9 \le s \le 12$ and $h = 9$. Then $(s-h+9)/8 = s/8$, while the inequality

$$\frac{(2h-2)(s-4)+4h-4}{h(s-4)+4h-4} = \frac{16s-32}{9s-4} \ge \frac{s}{8}$$

is equivalent to

$$9s^2 - 132s + 256 \le 0,$$

which is easily verified; the left-hand side is increasing with s and negative for $s = 12$. ■

References

[1] R. C. Baker, *Weyl sums and Diophantine approximation*, J. London Math. Soc. (2) **25** (1982), 25–34. Correction, ibid. **46** (1992), 202–204.

[2] R. C. Baker, *Small solutions of congruences*, Mathematika **20** (1983), 164–188.

[3] R. C. Baker, *Diophantine inequalities*, Oxford University Press, Oxford 1986.

[4] R. C. Baker and G. Harman, *Small fractional parts of quadratic forms*, Proc. Edinburgh Math. Soc. **25** (1982), 269–277.

[5] B. J. Birch and H. Davenport, *On a theorem of Davenport and Heilbronn*, Acta Math. **100** (1958), 259–279.

[6] R. J. Cook, *The fractional parts of an additive form*, Proc. Camb. Phil. Soc **72** (1972), 209–212.

[7] R. Dietmann, *Small solutions of additive cubic congruences*, preprint 1999.

[8] S. Dyke, D. Phil. Thesis, Oxford 1992.

[9] D. R. Heath-Brown, *Small solutions of quadratic congruences. II*, Mathematika **38** (1991), 264–284.

[10] H. Heilbronn, *On the distribution of the sequence* $\theta n^2 (\mathrm{mod}\, 1)$, Quart. J. of Math. Oxford (2) (1948), 249–256.

[11] D. J. Lewis, *Cubic congruences*, Mich. Math. J. **4** (1957), 85–95.

[12] 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), 241–248.

[13] W. M. Schmidt, *Equations over finite fields: an elementary approach*, Lect. Notes Math. **536**, Springer; Berlin-Heidelberg-New York 1976.

[14] A. Zaharescu, *Small values of* $n^2\alpha \pmod 1$, Invent. Math. **121** (1995), 379–388.

Address: Department of Mathematics, Brigham Young University, Provo, UT 84602
E-mail: baker@math.byu.edu
Received: 10 November 1999