JOURNAL OF NUMBER THEORY 3, 19–32 (1971)

A Distribution Property of the Solutions of a Congruence Modulo a Large Prime

KENNETH S. WILLIAMS*

Department of Mathematics, Carleton University, Ottawa 1, Canada

Communicated by H. Zassenhaus

Received March 21, 1969

A regularity in the distribution of the solutions of the congruence

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$$

is shown.

1. INTRODUCTION

Let Z denote the domain of integers of the real number field R and let p denote a prime. For any integer $n \geqslant 1$, we define the *fundamental cube* of $R^n = R \times \cdots \times R$ (with respect to p) to be the set

$$R^n(p) = \{\mathbf{x} = (x_1, \ldots, x_n) \in R^n \mid 0 \leqslant x_i < p,\ i = 1, 2, \ldots, n\} \quad (1.1)$$

and the *fundamental lattice* of R^n (with respect to p) to be

$$Z^n(p) = \{\mathbf{x} = (x_1, \ldots, x_n) \in Z^n \mid 0 \leqslant x_i < p,\ i = 1, 2, \ldots, n\}. \quad (1.2)$$

Clearly $Z^n(p) = Z^n \cap R^n(p)$. A *subcube* of $R^n(p)$ is a set S of the form

$$S = \{\mathbf{x} \in R^n(p) \mid a_i \leqslant x_i < a_i + b,\ i = 1, 2, \ldots, n\}, \quad (1.3)$$

where $a_i (i = 1, 2, \ldots, n)$, $b \in R$ are such that

$$0 \leqslant a_i < a_i + b \leqslant p,\ i = 1, 2, \ldots, n. \quad (1.4)$$

The length of each side of S is clearly b. We write this symbolically as $\| S \| = b$. A finite family of subcubes $\{S_i\} (i = 1, 2, \ldots, k)$ of $R^n(p)$ will be called a *subcube division* of $R^n(p)$ if

(i) $\| S_i \|$ is the same for $i = 1, 2, \ldots, k$,

(ii) $S_i \cap S_j = \varnothing$, for $i \neq j$, $i, j = 1, 2, \ldots, k$, $\quad$ (1.5)

(iii) $\bigcup_{i=1}^{k} S_i = R^n(p)$.

* This research was supported by the National Research Council of Canada under Grant No. A-7233.

These conditions require the S_i to be congruent, pairwise disjoint and exhaustive.

Now let $f(X_1, \ldots, X_n)$ be a polynomial of degree $d \geqslant 2$ in the $n \geqslant 2$ indeterminates $X_1, \ldots, X_n$, with integral coefficients which does not vanish $(\bmod\, p)$. A number of authors, Vinogradov [9], Mordell [5], Chalk [2], Mordell [6], Chalk and Williams [3], Tietäväinen [8], Smith [7], and Williams [10], have considered the distribution of the solutions $\mathbf{x} \in Z^n$ of the congruence

$$f(\mathbf{x}) \equiv 0 \pmod{p}, \tag{1.6}$$

within the fundamental cube $R^n(p)$, particularly when p is large in comparison with n and d. We denote the number of solutions of (1.6) in $R^n(p)$ by $N_p(f)$. A study of the results of the above authors suggests a distribution result for the solutions of (1.6) of the following type:

If p is large in comparison with n and d, $\{S_i\}$ is a subcube division of $R^n(p)$ with $\| S_i \| \gg p^{1-(1/n)}$, and $N_p(f) \gg p^{n-1}$ then each S_i contains a solution $\mathbf{x}$ of (1.6).

It is the purpose of this paper to obtain a precise result along these lines. The method employed is based on that of Tietäväinen [8]. The modifications necessary require the estimation of a certain exponential sum $\mathscr{F}(f, \mathbf{y})$ (see Section 4). This sum has been considered by Chalk and the author in [3]. It was estimated effectively only when f is homogeneous and free from linear factors modulo p. Therefore, in view of the type of distribution property we are considering, we restrict ourselves to the case of *homogeneous* polynomials f of degree $d \geqslant 2$, which are *irreducible* $(\bmod\, p)$. To guarantee $N_p(f) \gg p^{n-1}$, we further assume that f is *absolutely irreducible* $(\bmod\, p)$, for if not, by a result of Birch and Lewis [1] $N_p(f) \ll p^{n-2}$. With these assumptions, we know from the deep work of Lang and Weil [4] that

$$N_p(f) = p^{n-1} + O(p^{n-3/2}), \tag{1.7}$$

where the constant implied by the O-symbol depends only on n and d. Hence we know that

$$N_p(f) \geqslant \tfrac{1}{2} p^{n-1}, \tag{1.8}$$

for p large enough compared with n and d and it is convenient to assume that this occurs for

$$p \geqslant (20d)^n. \tag{1.9}$$

(See the remark in [1] concerning the implied constant in (1.7)). We prove:

THEOREM. *Let $f(X_1, \dots, X_n) \in Z[X_1, \dots, X_n]$ be a homogeneous polynomial of degree $d \geqslant 2$ in the $n \geqslant 2$ indeterminates $X_1, X_2, \dots, X_n$ and let p be a prime satisfying* (1.9). *If f is absolutely irreducible* (mod p) *and $N_p(f) \geqslant \frac{1}{2}p^{n-1}$ then every subcube*

$$S(i_1, \dots, i_n) = \{\mathbf{x} \in R^n(p) \mid i_j\mu \leqslant x_j < (i_j + 1)\mu, j = 1, 2, \dots, n\}$$
$$i_1, \dots, i_n = 0, 1, 2, \dots, \lambda - 1, \tag{1.10}$$

where

$$\lambda \equiv \lambda(p, n, d) = \left[\frac{p^{1/n}}{10d}\right] \in Z \tag{1.11}$$

$$\mu \equiv \mu(p, n, d) = \frac{p}{\lambda} \in R, \tag{1.12}$$

contains a solution $\mathbf{x} \in Z^n$ of (1.6).

We note that $\lambda \geqslant 2$, $\lambda\mu = p$, and the family $\{S(i_1, \dots, i_n)\}$ is a subcube division of $R^n(p)$, with $\| S(i_1, \dots, i_n)\| = \mu \approx p^{1-1/n}$.

2. NOTATION

It is convenient to let

$$e(t) = \exp\{2\pi it/p\}, \; t \in R. \tag{2.1}$$

It is well-known that for $b \in Z$,

$$\sum_{t=0}^{p-1} e(bt) = \begin{cases} p, & b \equiv 0 \pmod p \\ 0, & b \not\equiv 0 \pmod p \end{cases}, \tag{2.2}$$

and, more generally, for $\mathbf{x} \in Z^n$

$$\sum_{\mathbf{y} \in Z^n(p)} e(\mathbf{x} \cdot \mathbf{y}) = \begin{cases} p^n, & \mathbf{x} \equiv \mathbf{0} \pmod p, \\ 0, & \mathbf{x} \not\equiv \mathbf{0} \pmod p. \end{cases} \tag{2.3}$$

We also let

$$\mathscr{F}(f, \mathbf{y}) = \sum_{\mathbf{z} \in Z^n(p)} \sum_{t=0}^{p-1} e(tf(\mathbf{z}) - \mathbf{y} \cdot \mathbf{z}). \tag{2.4}$$

Taking $\mathbf{y} \equiv \mathbf{0} \pmod p$, we have

$$\mathscr{F}(f, \mathbf{0}) = \sum_{\mathbf{z} \in Z^n(p)} \sum_{t=0}^{p-1} e(tf(\mathbf{z})) = pN_p(f), \tag{2.5}$$

by (2.2), and for $\mathbf{y} \not\equiv \mathbf{0} \pmod{p}$, we have

$$\mathscr{F}(f, \mathbf{y}) = \sum_{\mathbf{z} \in Z^n(p)} \left\{ e(-\mathbf{y} \cdot \mathbf{z}) + \sum_{t=1}^{p-1} e(tf(\mathbf{z}) - \mathbf{y} \cdot \mathbf{z}) \right\} \tag{2.6}$$

$$= \sum_{\mathbf{z} \in Z^n(p)} \sum_{t=1}^{p-1} e(tf(\mathbf{z}) - \mathbf{y} \cdot \mathbf{z}),$$

by (2.3).

Finally we let

$$R(i, \mu) = \{x \in R \mid \tfrac{1}{2} i\mu \leqslant x < \tfrac{1}{2}(i+1)\mu\}, \quad i = 0, 1, 2, \ldots, \lambda - 1, \tag{2.7}$$
$$= [\tfrac{1}{2} i\mu, \tfrac{1}{2}(i+1)\mu),$$

$$Z(i, \mu) = R(i, \mu) \cap Z, \quad i = 0, 1, 2, \ldots, \lambda - 1, \tag{2.8}$$

$$A(t, i, \mu) = \sum_{w \in Z(i, \mu)} e(tw), \quad t \in Z, i = 0, 1, 2, \ldots, \lambda - 1, \tag{2.9}$$

and if X denotes a set with only a finite number of elements, then we write $| X |$ for the number of elements in X.

3. Some Lemmas

The six lemmas proved in this section are all of an elementary computational nature. Lemmas 3.1 and 3.2 are required in the proof of Lemma 3.4. Lemmas 3.1 and 3.3 are required in the proof of Lemma 3.5. Lemmas 3.4–3.6 are used in the proof of the theorem.

Lemma 3.1. *If $a, b \in R$ with $a < b$, then*

$$b - a - 2 < | Z \cap [a, b)| < b - a + 2.$$

Proof. The half-closed, half-open interval $[a, b)$ contains the integers $[a] + 1, \ldots, [b] - 1$, so

$$\begin{aligned} | Z \cap [a, b)| &\geqslant ([b] - 1) - ([a] + 1) + 1 \\ &= [b] - [a] - 1 \\ &> b - a - 2. \end{aligned}$$

As $Z \cap [a, b) \subseteq Z \cap [[a], [b]]$, we have

$$\begin{aligned} | Z \cap [a, b)| &\leqslant | Z \cap [[a], [b]]| \\ &= [b] - [a] + 1 \\ &< b - a + 2. \end{aligned}$$

LEMMA 3.2.

$$\frac{1}{2}\mu - 2 \geqslant \frac{199}{40}\, dp^{1-1/n}.$$

Proof. $\mu = p/\lambda = p/[p^{1/n}/10d] > p/(p^{1/n}/10d) = 10dp^{1-1/n}$.
Now

$$\begin{aligned}\left(5 - \frac{199}{40}\right) dp^{1-(1/n)} &= \frac{1}{40}\, dp^{1-1/n}\\ &\geqslant \frac{1}{20}\, p^{1/2} \qquad\qquad (n, d \geqslant 2)\\ &\geqslant \frac{20d}{20} \qquad\qquad (p \geqslant (20d)^n \geqslant (20d)^2)\\ &\geqslant 2,\end{aligned}$$

so that

$$\frac{1}{2}\mu - 2 \geqslant 5dp^{1-1/n} - 2 \geqslant \frac{199}{40}\, dp^{1-1/n}.$$

LEMMA 3.3.

$$\frac{1}{2}\mu + 2 < \frac{401}{40}\, dp^{1-1/n}.$$

Proof.

$$\mu = p/\lambda = p/[p^{1/n}/10d] < p/((p^{1/n}/10d) - 1) \leqslant p/(p^{1/n}/20d) = 20dp^{1-1/n},$$

as

$$\left(\frac{1}{10} - \frac{1}{20}\right)\frac{p^{1/n}}{d} = \frac{p^{1/n}}{20d} \geqslant 1, \text{ recalling } p \geqslant (20d)^n.$$

Now

$$\left(\frac{401}{40} - 10\right) dp^{1-1/n} = \frac{1}{40}\, dp^{1-1/n} \geqslant 2, \text{ as in Lemma 3.2, giving}$$

$$\frac{1}{2}\mu + 2 \leqslant 10dp^{1-1/n} + 2 \leqslant \frac{401}{40}\, dp^{1-1/n}.$$

LEMMA 3.4.

$$\prod_{j=1}^{n} A(0, i_j, \mu)^2 > \frac{199^{2n}}{40^{2n}}\, d^{2n} p^{2n-2}.$$

Proof.

$$\begin{aligned} A(0, i_j, \mu) &= \sum_{w \in Z(i_j,\mu)} 1 \\ &= |Z(i_j, \mu)| \\ &= \left| Z \cap \left[\frac{i_j\mu}{2}, \frac{(i_j+1)\mu}{2}\right]\right| \\ &> \frac{1}{2}\mu - 2, \quad \text{by} \quad \text{Lemma 3.1}, \\ &\geqslant \frac{199}{40} dp^{1-1/n}, \quad \text{by} \quad \text{Lemma 3.2}, \end{aligned}$$

which gives

$$\prod_{j=1}^{n} A(0, i_j, \mu)^2 > \frac{199^{2n}}{40^{2n}} d^{2n} p^{2n-2}.$$

LEMMA 3.5.

$$\prod_{j=1}^{n} \sum_{t_j=0}^{p-1} | A(t_j, i_j, \mu)|^2 < \frac{401^n}{40^n} d^n p^{2n-1}.$$

Proof.

$$\begin{aligned} &\sum_{t_j=0}^{p-1} | A(t_j, i_j, \mu)|^2 \\ &\quad= \sum_{t_j=0}^{p-1} A(t_j, i_j, \mu) \overline{A(t_j, i_j, \mu)} \\ &\quad= \sum_{t_j=0} \sum_{w \in Z(i_j,\mu)} \sum_{v \in Z(i_j,\mu)} e(t_j(w-v)) \\ &\quad= \sum_{w,v \in Z(i_j,\mu)} \sum_{t_j=0}^{p-1} e(t_j(w-v)) \\ &\quad= p\, | Z(i_j, \mu)| \\ &\quad= p\, | Z \cap [\tfrac{1}{2}i_j\mu, \tfrac{1}{2}(i_j+1)\mu)| \\ &\quad< p(\tfrac{1}{2}\mu + 2), \quad \text{by} \quad \text{Lemma 3.1}, \\ &\quad< \frac{401}{40} dp^{2-1/n}, \quad \text{by} \quad \text{Lemma 3.3}. \end{aligned}$$

Hence

$$\prod_{j=1}^{n} \sum_{t_j=0}^{p-1} | A(t_j, i_j, \mu)|^2 < \frac{401^n}{40^n} d^n p^{2n-1}.$$

LEMMA 3.6. $199^{2n} \cdot 2^{n-2} - 4 \cdot 40^n \cdot 401^n > 0$, for $n \geqslant 2$.

Proof. As $39601 > 2 \cdot 16040$, we have, as $n \geqslant 2$,

$$199^{2n} = (39601)^n > 2^n \cdot (16040)^n \geqslant 4 \cdot (16040)^n = 4.40^n \cdot 401^n.$$

Hence

$$\begin{aligned} &199^{2n} \cdot 2^{n-2} - 4.40^n \cdot 401^n \\ &\quad > 2^n \cdot 40^n \cdot 401^n - 4.40^n \cdot 401^n \\ &\quad = (2^n - 4)\, 40^n \cdot 401^n \\ &\quad \geqslant 0. \end{aligned}$$

4. ESTIMATION OF $\mathscr{F}(f, \mathbf{y})$

LEMMA 4.1. *If $f(X_1, ..., X_n) \in Z[X_1, ..., X_n]$ is of total degree $d \geqslant 0$ and does not vanish identically* (mod p), *then the number of solutions $(x_1, ..., x_n) \in Z^n(p)$ of the congruence*

$$f(x_1, ..., x_n) \equiv 0 \pmod p \tag{4.1}$$

is at most dp^{n-1}.

Proof. We prove the result by induction on the number of variables n. The result is clearly true when $n = 1$. We assume the estimate is valid for polynomials of any degree, which do not vanish (mod p), in at most k variables. Suppose $F(X_1, ..., X_{k+1}) \in Z[X_1, ..., X_{k+1}]$ is of total degree d_1 and does not vanish identically (mod p). Then

$$F(X_1, ..., X_{k+1}) = \sum_{i=0}^{d_1} F_i(X_1, ..., X_k)\, X_{k+1}^i, \tag{4.2}$$

where each $F_i(X_1, ..., X_k) \in Z[X_1, ..., X_k]$, degree $F_i + i \leqslant d_1$ and not all the F_i vanish (mod p) as F does not vanish (mod p). Let d_2 denote the largest value of $i (0 \leqslant i \leqslant d_1)$ for which $F_i(X_1, ..., X_k)$ does not vanish (mod p). We consider two cases according as $d_2 = 0$ or $d_2 \neq 0$. If $d_2 = 0$,

$$F(X_1, ..., X_{k+1}) = F_0(X_1, ..., X_k) \tag{4.3}$$

and the number of solutions $(x_1, ..., x_{k+1}) \in Z^{k+1}(p)$ of $F(x_1, ..., x_{k+1}) \equiv 0$ (mod p) is p times the number of solutions $(x_1, ..., x_k) \in Z^k(p)$ of $F_0(x_1, ..., x_k) \equiv 0$ (mod p). By the inductive hypothesis this number is less than $p \cdot d_1 p^{k-1} = d_1 p^k$. If $d_2 \neq 0$,

$$F(X_1, ..., X_{k+1}) = \sum_{i=0}^{d_2} F_i(X_1, ..., X_k)\, X_{k+1}^i, \tag{4.4}$$

where $F_{d_2}(X_1, ..., X_k)$ does not vanish identically $(\text{mod } p)$. The solutions $(x_1, ..., x_{k+1}) \in Z^{k+1}(p)$ of $F(x_1, ..., x_{k+1}) \equiv 0 \pmod p$ are of 2 kinds, those which also satisfy $F_{d_2}(x_1, ..., x_k) \equiv 0 \pmod p$ and those which do not. The number of the former type is at most $p \cdot (d_1 - d_2) p^{k-1}$ and the number of the latter type is at most $d_2 p^k$. Thus, the required number is less than or equal to $(d_1 - d_2) p^k + d_2 p^k = d_1 p^k$. The result now follows by mathematical induction.

LEMMA 4.2. *Suppose* $f(X_1, ..., X_n) \in Z[X_1, ..., X_n]$ *is of total degree* $d \geqslant 2$ *in* $n \geqslant 2$ *indeterminates* $X_1, ..., X_n$, *does not vanish* $(\text{mod } p)$ *and is irreducible* $(\text{mod } p)$. *Then, if not all of* $a_1, ..., a_n \in Z$ *vanish* $(\text{mod } p)$, *the number of solutions* $(x_1, ..., x_n) \in Z^n(p)$ *of the pair of simultaneous congruences*

$$\begin{aligned} f(x_1, ..., x_n) &\equiv 0 \pmod p, \\ a_1 x_1 + \cdots + a_n x_n &\equiv 0 \pmod p, \end{aligned} \tag{4.5}$$

is at most dp^{n-2}.

Proof. As not all of $a_1, ..., a_n$ vanish $(\text{mod } p)$, we can assume without any loss of generality that $a_1 \not\equiv 0 \pmod p$. The linear congruence becomes

$$x_1 \equiv -a_1^{-1}(a_2 x_2 + \cdots + a_n x_n) \pmod p. \tag{4.6}$$

Set

$$g(x_2, ..., x_n) = f(-a_1^{-1}(a_2 x_2 + \cdots + a_n x_n), x_2, ..., x_n). \tag{4.7}$$

The number of solutions $(x_1, ..., x_n) \in Z^n(p)$ of (4.5) is just the number of solutions $(x_2, ..., x_n) \in Z^{n-1}(p)$ of $g(x_2, ..., x_n) \equiv 0 \pmod p$. By Lemma 4.1 this is at most dp^{n-2}, unless g vanishes $(\text{mod } p)$. g cannot vanish $(\text{mod } p)$ however, for if so every solution $(x_1, ..., x_n)$ of $a_1 x_1 + \cdots + a_n x_n \equiv 0 \pmod p$ would satisfy $f(x_1, ..., x_n) \equiv 0 \pmod p$ and so by Hilbert's Nullstellensatz there exists an integer k and a polynomial

$$h(x_1, ..., x_n) \in Z[x_1, ..., x_n]$$

such that

$$\{f(x_1, ..., x_n\}^k \equiv (a_1 x_1 + \cdots + a_n x_n)\, h(x_1, ..., x_n) \pmod p. \tag{4.8}$$

Hence

$$a_1 x_1 + \cdots + a_n x_n \mid f(x_1, ..., x_n), \tag{4.9}$$

which contradicts the fact that f is irreducible $(\text{mod } p)$ and of degree $d \geqslant 2$.

LEMMA 4.3. *If* $f(X_1, ..., X_n) \in Z[X_1, ..., X_n]$ *is homogeneous of degree* $d \geqslant 2$, *does not vanish* (mod p) *and is irreducible* (mod p), *then for* $\mathbf{y}(\not\equiv \mathbf{0}) \in Z^n(p)$ *we have*

$$|\mathscr{F}(f, \mathbf{y})| \leqslant 4dp^{n-1}. \tag{4.10}$$

Proof. For $l \in Z$:

$$\mathscr{F}(f, l\mathbf{y}) = \sum_{\mathbf{x} \in Z^n(p)} \sum_{t=0}^{p-1} e(tf(\mathbf{x}) - l\mathbf{x} \cdot \mathbf{y}). \tag{4.11}$$

If $l \not\equiv 0 \pmod p$, m is uniquely defined $(\operatorname{mod} p)$ by $lm \equiv 1 \pmod p$. The mapping $\mathbf{x} \to m\mathbf{x}$ is a bijection on $Z^n(p)$. Hence

$$\begin{aligned}\mathscr{F}(f, l\mathbf{y}) &= \sum_{\mathbf{x} \in Z^n(p)} \sum_{t=0}^{p-1} e(tf(m\mathbf{x}) - \mathbf{x} \cdot \mathbf{y}) \\ &= \sum_{\mathbf{x} \in Z^n(p)} \sum_{t=0}^{p-1} e(tm^d f(\mathbf{x}) - \mathbf{x} \cdot \mathbf{y}),\end{aligned}$$

as f is homogeneous of degree d. As $m \not\equiv 0 \pmod p$, the mapping $t \to tm^d$ is a bijection on $Z(p)$, so that

$$\begin{aligned}\mathscr{F}(f, l\mathbf{y}) &= \sum_{\mathbf{x} \in Z^n(p)} \sum_{t=0}^{p-1} e(tf(\mathbf{x}) - \mathbf{x} \cdot \mathbf{y}) \\ &= \mathscr{F}(f, \mathbf{y}).\end{aligned}$$

Hence

$$\sum_{l=0}^{p-1} \mathscr{F}(f, l\mathbf{y}) = \mathscr{F}(f, \mathbf{0}) + (p-1)\,\mathscr{F}(f, \mathbf{y}). \tag{4.12}$$

On the other hand

$$\begin{aligned}\sum_{l=0}^{p-1} \mathscr{F}(f, l\mathbf{y}) &= \sum_{l=0}^{p-1} \sum_{\mathbf{x} \in Z^n(p)} \sum_{t=0}^{p-1} e(tf(\mathbf{x}) - l\mathbf{x} \cdot \mathbf{y}) \\ &= \sum_{\mathbf{x} \in Z^n(p)} \sum_{t=0}^{p-1} e(tf(\mathbf{x})) \sum_{l=0}^{p-1} e(-l\mathbf{x} \cdot \mathbf{y}) \\ &= p \sum_{\substack{\mathbf{x} \in Z^n(p) \\ \mathbf{x} \cdot \mathbf{y} \equiv 0}} \sum_{t=0}^{p-1} e(tf(\mathbf{x})) \\ &= p^2 \sum_{\substack{\mathbf{x} \in Z^n(p) \\ \mathbf{x} \cdot \mathbf{y} \equiv 0 \\ f(\mathbf{x}) \equiv 0}} 1 \\ &= p^2 N,\end{aligned}$$

where N denotes the number of solutions $\mathbf{x} \in Z^n(p)$ of

$$f(\mathbf{x}) \equiv \mathbf{x} \cdot \mathbf{y} \equiv 0 \pmod{p}.$$

Thus

$$\mathscr{F}(f, \mathbf{y}) = \frac{p}{p-1} \{pN - N_p(f)\} \tag{4.13}$$

and so by Lemmas 4.1 and 4.2

$$\begin{aligned} |\mathscr{F}(f, \mathbf{y})| &\leqslant \frac{p}{p-1} \{pN + N_p(f)\} \\ &\leqslant 2\{p \cdot dp^{n-2} + dp^{n-1}\} \\ &= 4dp^{n-1}, \end{aligned}$$

as required.

5. Proof of Theorem

We let a denote any integer and set

$$\begin{aligned} N(a, i, \mu) = {} & \text{Number of } (u, v) \in Z(i, \mu) \times Z(i, \mu) \text{ such that} \\ & u + v \equiv a \pmod{p}. \end{aligned} \tag{5.1}$$

We have

$$\begin{aligned} N(a, i, \mu) &= \frac{1}{p} \sum_{u,v \in Z(i,\mu)} \sum_{t=0}^{p-1} e((u + v - a)\, t) \\ &= \sum_{t=0}^{p-1} e(-at) \sum_{u \in Z(i,\mu)} e(tu) \sum_{v \in Z(i,\mu)} e(tv), \end{aligned}$$

giving

$$N(a, i, \mu) = \frac{1}{p} \sum_{t=0}^{p-1} e(-at)\{A(t, i, \mu)\}^2. \tag{5.2}$$

For $0 \leqslant i_1, \ldots, i_n \leqslant \lambda - 1$, we let $N(i_1, \ldots, i_n, \mu)$ denote the number of solutions $(\mathbf{x}, \mathbf{y}) \in Z(i_1, \mu) \times \cdots \times Z(i_n, \mu) \times Z(i_1, \mu) \times \cdots \times Z(i_n, \mu)$ of

$$f(\mathbf{x} + \mathbf{y}) \equiv 0 \pmod{p}. \tag{5.3}$$

We have

$$N(i_1, \ldots, i_n, \mu) = \frac{1}{p} \sum_{\mathbf{x},\mathbf{y}}{}' \sum_{t=0}^{p-1} e(tf(\mathbf{x} + \mathbf{y})), \tag{5.4}$$

where the prime (′) denotes that the summation is taken over $\mathbf{x}, \mathbf{y} \in Z(i_1, \mu) \times \cdots \times Z(i_n, \mu)$.

Hence

$$\begin{aligned}
N(i_1, \ldots, i_n, \mu) &= \frac{1}{p} \sum_{t=0}^{p-1} \sum_{\mathbf{x}}{}' \sum_{\mathbf{y}}{}' e(tf(\mathbf{x}+\mathbf{y})) \\
&= \frac{1}{p} \sum_{t=0}^{p-1} \sum_{\mathbf{z} \in Z^n(p)} \sum_{\substack{\mathbf{x} \quad \mathbf{y} \\ \mathbf{x}+\mathbf{y} \equiv \mathbf{z}}}{}' \sum{}' e(tf(\mathbf{z})) \\
&= \frac{1}{p} \sum_{t=0}^{p-1} \sum_{\mathbf{z} \in Z^n(p)} e(tf(\mathbf{z})) \sum_{\substack{\mathbf{x} \quad \mathbf{y} \\ \mathbf{x}+\mathbf{y} \equiv \mathbf{z}}}{}' \sum{}' 1 \\
&= \frac{1}{p} \sum_{t=0}^{p-1} \sum_{\mathbf{z} \in Z^n(p)} e(tf(\mathbf{z})) \prod_{j=1}^{n} N(z_j, i_j, \mu) \\
&= \frac{1}{p^{n+1}} \sum_{t=0}^{p-1} \sum_{\mathbf{z} \in Z^n(p)} e(tf(z)) \sum_{\mathbf{t} \in Z^n(p)} e(-\mathbf{z} \cdot \mathbf{t}) \prod_{j=1}^{n} A(t_j, i_j, \mu)^2,
\end{aligned}$$

from (5.2). Picking out the term with $t = 0$, we obtain

$$\begin{aligned}
&p^{n+1} N(i_1, \ldots, i_n, \mu) \\
&\quad = \sum_{\mathbf{z} \in Z^n(p)} \sum_{\mathbf{t} \in Z^n(p)} e(-\mathbf{z} \cdot \mathbf{t}) \prod_{j=1}^{n} A(t_j, i_j, \mu)^2 \\
&\quad\quad + \sum_{t=1}^{p-1} \sum_{\mathbf{z} \in Z^n(p)} e(tf(\mathbf{z})) \sum_{\mathbf{t} \in Z^n(p)} e(-\mathbf{z} \cdot \mathbf{t}) \prod_{j=1}^{n} A(t_j, i_j, \mu)^2.
\end{aligned}$$

As

$$\sum_{\mathbf{z} \in Z^n(p)} e(-\mathbf{z} \cdot \mathbf{t}) = \begin{cases} p^n, & \mathbf{t} \equiv \mathbf{0}, \\ 0, & \text{otherwise}, \end{cases} \tag{5.5}$$

the first of these sums is

$$p^n \prod_{j=1}^{n} A(0, i_j, \mu)^2. \tag{5.6}$$

The second of these can be written

$$\sum_{\mathbf{t} \in Z^n(p)} \prod_{j=1}^{n} A(t_j, i_j, \mu)^2 \sum_{t=1}^{p-1} \sum_{\mathbf{z} \in Z^n(p)} e(tf(\mathbf{z}) - \mathbf{t} \cdot \mathbf{z}). \tag{5.7}$$

The terms in (5.7), with $\mathbf{t} = \mathbf{0}$, give

$$\prod_{j=1}^{n} A(0, i_j, \mu)^2 \sum_{t=1}^{p-1} \sum_{\mathbf{z} \in Z^n(p)} e(tf(\mathbf{z}))$$

$$= \prod_{j=1}^{n} A(0, i_j, \mu)^2 \left\{ \sum_{\mathbf{z} \in Z^n(p)} \sum_{t=0}^{p-1} e(tf(\mathbf{z}) - p^n \right\}$$

$$= \prod_{j=1}^{n} A(0, i_j, \mu)^2 \{pN_p(f) - p^n\}.$$

Hence,

$$\left| p^{n+1} N(i_1, \dots, i_n, \mu) - pN_p(f) \prod_{j=1}^{n} A(0, i_j, \mu)^2 \right|$$

$$= \left| \sum_{0 \neq \mathbf{t} \in Z^n(p)} \prod_{j=1}^{n} A(t_j, i_j, \mu)^2 \mathscr{F}(f, \mathbf{t}) \right|$$

$$\leqslant \sum_{0 \neq \mathbf{t} \in Z^n(p)} \prod_{j=1}^{n} | A(t_j, i_j, \mu)|^2 \, | \mathscr{F}(f, t)|$$

$$\leqslant 4dp^{n-1} \prod_{j=1}^{n} \sum_{t_j=0}^{p-1} | A(t_j, i_j, \mu)|^2, \quad \text{by Lemma 4.3,}$$

$$\leqslant 4 \cdot \frac{401^n}{40^n} \cdot d^{n+1} p^{3n-2}, \quad \text{by Lemma 3.5.}$$

Thus,

$$N(i_1, \dots, i_n, \mu)$$

$$\geqslant \frac{N_p(f)}{p^n} \prod_{j=1}^{n} A(0, i_j, \mu)^2 - 4 \cdot \frac{401^n}{40^n} \cdot d^{n+1} p^{2n-3}$$

$$\geqslant \frac{199^{2n}}{2 \cdot 40^{2n}} d^{2n} p^{2n-3} - 4 \cdot \frac{401^n}{40^n} d^{n+1} p^{2n-3}, \quad \text{by Lemma 3.4,}$$

$$= \frac{d^{n+1} p^{2n-3}}{40^{2n}} \left(\frac{d^{n-1} 199^{2n}}{2} - 4 \cdot 40^n \cdot 401^n \right)$$

$$\geqslant \frac{d^{n+1} p^{2n-3}}{40^{2n}} (2^{n-2} \cdot 199^{2n} - 4 \cdot 40^n \cdot 401^n)$$

$$> 0, \quad \text{by Lemma 3.6.}$$

Thus for *any* selection $i_1, ..., i_n \in Z$ satisfying $0 \leqslant i_1, ..., i_n \leqslant \lambda - 1$, we have proved the existence of $\mathbf{x}$ and $\mathbf{y} \in Z(i_1, \mu) \times \cdots \times Z(i_n, \mu)$ such that $f(\mathbf{x} + \mathbf{y}) \equiv 0 \pmod{p}$; that is, of $\mathbf{z} \in S(i_1, ..., i_n)$ such that $f(\mathbf{z}) \equiv 0 \pmod{p}$, so that every such subcube contains a solution of (1.6), as required.

6. Conclusion

We illustrate the theorem by a simple numerical example. We choose $n = 3$, $d = 2$ (the choice $n = d = 2$ is excluded as f must be both absolutely irreducible (mod p) and homogeneous),

$$f(X_1, X_2, X_3) = X_1^2 + X_2^2 - X_2X_3, \tag{6.1}$$

TABLE I

$S(i_1, i_2, i_3)$					
i_1	i_2	i_3	x_1	x_2	x_3
0	0	0	0	0	0
0	0	1	50 000	50 000	100 000
0	0	2	74 000	37 000	185 000
0	1	0	80 761	100 000	70 158
0	1	1	0	92 000	92 000
0	1	2	90 000	180 000	225 000
0	2	0	90 000	270 000	25 823
0	2	1	50 000	224 177	174 177
0	2	2	0	200 000	200 000
1	0	0	108 000	58 177	4 177
1	0	1	180 000	90 000	175 823
1	0	2	120 000	30 000	235 823
1	1	0	180 000	180 000	85 823
1	1	1	170 000	99 138	99 139
1	1	2	92 000	92 000	184 000
1	2	0	120 000	244 177	38 354
1	2	1	125 823	200 000	177 469
1	2	2	108 000	216 000	270 000
2	0	0	274 176	1	2
2	0	1	224 177	50 000	100 000
2	0	2	200 177	37 000	185 000
2	1	0	184 177	94 177	49 177
2	1	1	248 354	100 000	177 469
2	1	2	184 177	180 000	225 000
2	2	0	184 177	270 000	25 823
2	2	1	200 000	200 000	125 823
2	2	2	270 000	270 000	265 823

and $p = 274\,177$ ($\geqslant (20d)^n = 64\,000$). (274 177 is the smaller of the two *prime* factors of $F_6 = 2^{2^6} + 1$). As f is linear in X_3, f is absolutely irreducible (mod p) and $N_p(f) = p^2 (\geqslant \frac{1}{2}p^2)$. Finally,

$$\lambda = [274\,177^{1/3}/20] = [3.2...] = 3 \tag{6.2}$$

and

$$\mu = 91{,}392\tfrac{1}{3}. \tag{6.3}$$

In view of the special form of f, it is easy to check that each of the 27 subcubes

$$S(i_1, i_2, i_3) = \{(x_1, x_2, x_3) \in R^3 \mid 91{,}392\tfrac{1}{3}\, i_j \leqslant x_j < 91{,}392\tfrac{1}{3}\, (i_j + 1),$$
$$j = 1, 2, 3\},\ i_1, i_2, i_3 = 0, 1, 2, \tag{6.4}$$

contains a solution of (1.6). The table gives a solution in each case.

We close with the question—does a similar result hold for nonhomogeneous polynomials?

References

1. B. J. Birch and D. J. Lewis, p-adic forms, *J. Indian Math. Soc.*, **23** (1959), 11–32.
2. J. H. H. Chalk, The number of solutions of congruences in incomplete residue systems, *Canad. J. Math.*, **15** (1963), 291–296.
3. J. H. H. Chalk and K. S. Williams, The distribution of solutions of congruences, *Mathematika* **12** (1965), 176–192.
4. S. Lang and A. Weil, Number of points of varieties in finite fields, *Amer. J. Math.*, **76** (1954), 819–827.
5. L. J. Mordell, On the number of solutions in incomplete residue sets of quadratic congruences, *Arch. Math.*, **8** (1957), 153–157.
6. L. J. Mordell, Incomplete exponential sums and incomplete residue systems for congruences, *Czechoslovak Math. J.*, **14** (1964), 235–242.
7. R. A. Smith, The circle problem in an arithmetic progression, *Canad. Math. Bull.*, **11** (1968), 175–184.
8. A. Tietäväninen, On the solvability of equations in incomplete finite fields, *Ann. Univ. Turku. Ser. A1*, **102** (1967), 3–13.
9. I. M. Vinogradov, "Elements of number theory," Chap. 5, p. 103, problem 12(b)(ϵ), Dover, New York, 1954.
10. K. S. Williams, Small solutions of the congruence $ax^2 + by^2 \equiv c(\text{mod } k)$, *Canad. Math. Bull.*, **21** (1969), 311–320.