This dissertation has been
microfilmed exactly as received 67-15,685

RYAVEC, Charles Albert, 1941-
PROBLEMS IN DIOPHANTINE ANALYSIS.

The University of Michigan, Ph.D., 1967
Mathematics

University Microfilms, Inc., Ann Arbor, Michigan

PROBLEMS IN DIOPHANTINE ANALYSIS

by

Charles Albert Ryavec

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy in the
University of Michigan
1967

Doctoral Committee;

Professor Donald J. Lewis, Chairman
Professor A. Bruce Clarke
Professor Abraham Kaplan
Professor William J. LeVeque
Professor Maxwell O. Reade

PROBLEMS IN DIOPHANTINE ANALYSIS

by Charles A. Ryavec

The purpose of this study is to answer certain questions in Diophantine analysis. The study is divided into three parts, and the first part is further divided into two sections.

In the first part two theorems are proved:

Theorem 1. Let $a_1, \ldots, a_m$ be m distinct, non-zero residues modulo n, where n is any natural number and where

$$m \geq 3\sqrt{6n}\, \exp\left\{ c\frac{\sqrt{\log n}}{\log \log n} \right\} ,$$

where c is some large, positive constant. Then the congruence $\varepsilon_1 a_1 + \ldots + \varepsilon_m a_m \equiv 0 \pmod{n}$ is solvable with $\varepsilon_i = 0$ or 1 and not all $\varepsilon_i = 0$.

This result answers a question posed by Erdős at the 1966 Midwestern Conference of Group Theory and Number Theory.

Theorem 2. Let $a_1, \ldots, a_m$ be m distinct, non-zero residues modulo n, where n is a natural number belonging to one of the types:

(1) $n = p$, p a prime ,

(2) $n = p_1 p_2$, $p_2 \geq p_1$ primes: $p_1^2 > c\, p_2$

(3) $n = p_1 p_2 p_3$, $p_3 \geq p_2 \geq p_1$ primes: $p_1^2 > c\, p_2 p_3$,

where c is an arbitrary, but fixed, positive constant. Then if $F(N)$ denotes the number of solutions of the congruence

$\varepsilon_1 a_1 + \ldots + \varepsilon_m a_m \equiv 0 \pmod{n}$ with $\varepsilon_i \equiv 0$ or 1, and if $m^3 n^{-2} \to \infty$ as $n \to \infty$, we have $F(N) \equiv \frac{2^m}{n}(1 + o(1))$ for all residues N modulo n.

The proof of this theorem is based on techniques involving exponential sums which are developed in a paper by Erdős and Heilbronn ("On the Addition of Residue Classes mod p," Acta Arithmetika, (IX), (1964), 149-159).

In the second part, the following result is proved:

Theorem. Let $\lambda_1, \ldots, \lambda_s$ be non-zero, real numbers not all of the same sign, and let β be any real number. Let $\tau > 12$ and τ not an integer. Then there is an absolute constant $c > 0$ such that if $s > c\tau \log \tau$, the inequality $|\lambda_1 k_1^{\tau} + \ldots + \lambda_s k_s^{\tau} + \beta| < \varepsilon$ has infinitely many solutions in positive integers k_i for all $\varepsilon > 0$.

The proof of this theorem uses a variation of the Hardy-Littlewood method which is developed by Davenport and Roth for the same theorem as above when τ is an integer. (See "The Solubility of Certain Diophantine Inequalities," Mathematika, (4), 81-96). The case when τ is not an integer employs estimates for exponential sums obtained by van der Corput and I. M. Vinogradov.

In the last part of the thesis, the following result is proved:

Theorem. Let K be an algebraic number field and $\mathcal{O}_K$ its ring of integers. Let C(X) be a homogeneous, cubic form in not less than 17 variables, with coefficients in $\mathcal{O}_K$. Then C(X) represents 0 non-trivially in $\mathcal{O}_K$.

This theorem is an extension of, and is based on the ideas of, a result of Davenport concerning cubic forms with rational coefficients (See "Proceedings of the Royal Society, Ser. A, (272), (1963), 285-303). The proof of this result is based on the Hardy-Littlewood method.

PREFACE

The purpose of this study is to answer certain questions in Diophantine analysis. The study is divided into three parts, and the first part is divided into two sections.

In the first part the following two theorems are proved:

Theorem. Let $a_1, \ldots, a_m$ be m distinct, non-zero residues modulo n, where n is any natural number and where $m \geq 3\sqrt{6n}\, \exp\left\{ c \frac{\sqrt{\log n}}{\log \log n} \right\}$, where c is some large, positive constant. Then the congruence

$$\varepsilon_1 a_1 + \ldots + \varepsilon_m a_m \equiv 0 \pmod{n}$$

is solvable with $\varepsilon_i = 0$ or 1 and not all $\varepsilon_i = 0$.

This result answers a question posed by Erdős at the 1966 Midwestern Conference of Group Theory and Number Theory.

Theorem. Let $a_1, \ldots, a_m$ be m distinct, non-zero residues modulo n, where n is a natural number belonging to one of the types:

(1) $n = p$, p a prime,

(2) $n = p_1 p_2$, $p_2 \geq p_1$ primes: $p_1^2 > c\, p_2$,

(3) $n = p_1p_2p_3$, $p_3 \geq p_2 \geq p_1$ primes: $p_1^2 > c\,p_2p_3$,

where c is an arbitrary, but fixed, positive constant.

Then if $F(N)$ denotes the number of solutions of the congruence

$$\varepsilon_1 a_1 + \ldots + \varepsilon_m a_m \equiv N \pmod{n}$$

with $\varepsilon_i = 0$ or 1, and if $m^3 n^{-2} \to \infty$ as $n \to \infty$, we have $F(N) = \frac{2^m}{n}(1 + o(1))$ for all residues N modulo n.

In the second part of the thesis, the following result is obtained:

Theorem. Let $\lambda_1, \ldots, \lambda_s$ be non-zero, real numbers not all of the same sign, and let β be any real number. Let $\tau > 12$ and τ not an integer. Then there is an absolute constant $c > 0$ such that if $s > c\,\tau \log \tau$, the inequality

$$|\lambda_1 k_1^\tau + \ldots + \lambda_s k_s^\tau + \beta| < \varepsilon$$

has infinitely many solutions in positive integers k_i for all $\varepsilon > 0$.

This extends the result of Davenport and Roth [5] when τ is an integer ≥ 12.

In the third part of the thesis, the following result is proved:

Theorem. Let K be an algebraic number field and $\mathcal{O}_K$ its ring of integers. Let $C(X)$ be a homogeneous, cubic

form in not less than 17 variables, with coefficients in $\mathcal{O}_K$. Then C(X) represents 0 non-trivially in $\mathcal{O}_K$.

In the introduction to each part of the thesis, a brief history of the problem and the relationship of the problem to earlier literature are given.

I wish to extend my special thanks to Professor Donald Lewis for his many valuable suggestions and his constant encouragement during the research and preparation of this thesis. I also wish to thank Professor William LeVeque for his reading of the thesis and for his helpful comments.

While the research for this work was being done, I received financial support from the National Science Foundation, for which I am very grateful.

This work is dedicated to my wife.

TABLE OF CONTENTS

	Page
PREFACE	ii
PART I. SECTION 1	1
PART I.. SECTION 2	11
PART II	21
PART III	43
1. Notation	46
2. General Cubic Exponential Sums	47
3. Special Cubic Exponential Sums	50
4. Alternative (A)	52
5. Alternative (B)	58
BIBLIOGRAPHY	83

PART I

SECTION 1

In a recent paper by Erdős and Heilbronn (See [6]) the following question is investigated. Let p be a prime and $a_1, \ldots, a_m$ distinct, non-zero residue classes modulo p, and N any residue class modulo p. Let $F(N) = F(N; p; a_1, \ldots, a_m)$ denote the number of solutions of the congruence

$$\varepsilon_1 a_1 + \ldots + \varepsilon_m a_m \equiv N \pmod{p} \quad , \tag{1}$$

where the ε_i are restricted to the values 0 or 1. What can be said about the function $F(N)$? The authors prove the following result:

Theorem I. $F(N) > 0$ if $m \geq 3\sqrt{6p}$.

They conjecture that the bound $3\sqrt{6p}$ in Theorem I is not best possible: $3\sqrt{6p}$ can probably be replaced by $2\sqrt{p}$. On the other hand, they show that the constant 2 cannot be replaced by any smaller constant, as shown by the example

$$a_1 = 1 \ , \quad a_2 = -1, \ldots, \quad a_m = (-1)^{m-1}\left[\frac{m+1}{2}\right] \quad .$$

Note that if $m < 2 \quad (\sqrt{p} - 2)$, then $F(\frac{1}{2}(p-1)) = 0$.

The question which now arises is what can be said about $F(N)$ if the prime p is replaced by a composite integer n? Theorem I is

clearly false for composite n. In fact, even the bound $m \geq -1 + n/2$ will not guarantee that $F(N) > 0$ for all N when n is composite. The difficulty is that all of the a_i may have a prime factor in common with n, in which case $N = 1$ could not be represented in the form (1). However, this predicament does not arise when we try to represent 0 in the form (1). Therefore, it is natural to ask what condition on m will guarantee $F(0) > 0$ for all n. Erdős and Heilbronn conjectured that $F(0) > 0$ provided $m > 2\sqrt{n}$; * and at a conference at Ohio State University Erdős raised the question whether $F(0) > 0$ could be proved if one assumed the stronger hypothesis that $m > n^{\frac{1}{2}+\varepsilon}$, where ε is any positive number.

In the present paper, the following is proved:

Theorem. Let $a_1, \ldots, a_m$ be m distinct, non-zero residues modulo n, where n is any natural number and where $m \geq 3\sqrt{6n}\ \exp\left\{c\ \frac{\sqrt{\log n}}{\log\log n}\right\}$, where $c > 0$ is some large constant. Then the congruence

$$\varepsilon_1 a_1 + \ldots + \varepsilon_m a_m \equiv 0 \pmod{n}$$

is solvable with $\varepsilon_i = 0$ or 1 and not all $\varepsilon_i = 0$.

Note that the expression $\exp\left\{c\ \frac{\sqrt{\log n}}{\log\log n}\right\}$ is $O(n^{\varepsilon})$ for any $\varepsilon > 0$. Hence, the above theorem answers Erdős' question.

---

*Relative to this conjecture, we mention an unpublished result of Mann and Olson (See [11]. They have shown that if G is a group of type (p,p) and $a_1, \ldots, a_m$ are distinct elements of G, then $F(g) > 0$ for every $g \in G$ if $m \geq 2p = 2\sqrt{|G|}$.

In order to prove the theorem, we shall need a number of lemmas which are rather straightforward modifications of the argument given by Erdős and Heilbronn.

Lemma 1. Let $b_1, \ldots, b_\ell$ be ℓ distinct residues modulo n; and let $B(x)$ denote the number of solutions of

$$x \equiv b_i - b_j \pmod{n}$$

with $1 \leq i, j \leq \ell$. Then $B(x + y) \geq -\ell + B(x) + B(y)$; i.e., $\ell - B(x + y) \leq (\ell - B(x)) + (\ell - B(y))$.

Proof. See [6], page 150.

Lemma 2. Let $1 \leq k \leq \ell \leq n/2$ and let $d_1, \ldots, d_k$ be k distinct residues modulo n such that $(d_i, n) = 1$. Let $b_1, \ldots, b_\ell$ be ℓ distinct residues modulo n. Then there is an i, $1 \leq i \leq k$, such that

$$B(d_i) < \ell - k/6 \quad ,$$

where $B(d_i)$ is the number of solutions of

$$d_i \equiv b_s - b_t \pmod{n} \quad .$$

Proof. Let G denote the cyclic group of residues modulo n, and let $A = \{0, d_1, \ldots, d_k\}$. Put $r = 1 + [\frac{2\ell}{k}]$. By I. Chowla's theorem on the addition of residues modulo n (See [10], Corollary 1.2.4 (p. 3)), we have

$$\begin{aligned} |2A| &\geq |A| + |A| - 1 = 2k + 1 \\ &\vdots \\ |rA| &\geq r\ k + 1 \quad , \end{aligned}$$

provided $jA \neq G$ for $1 \leq j \leq r$. Hence, we obtain $t \geq \min(n-1, r\ k)$ distinct, non-zero residues $c_1, \ldots, c_t$ modulo n which can be expressed as sums of not more than r of the d_j; and the summands need not be distinct.

Since $\sum_{1 \leq s \leq t} B(c_s) \leq B(0) + \ldots + B(n-1) = \ell(\ell-1)$, there is an s such that

$$B(c_s) \leq \frac{\ell(\ell-1)}{t}$$

$$\leq \ell(\ell-1) \max\left\{\frac{1}{n-1}, \frac{1}{r\ k}\right\}$$

$$\leq \frac{\ell(\ell-1)}{2\ell-1} = \frac{\ell}{2} \cdot \frac{\ell-1}{\ell-\frac{1}{2}} < \frac{\ell}{2} \quad ;$$

i.e., $\ell - B(c_s) > \frac{\ell}{2}$.

By using induction on the conclusion of Lemma 1, we obtain

$$\ell - B(x_1 + \ldots + x_t) \leq \sum_{i=1}^{t} (\ell - B(x_i)) \quad . \tag{2}$$

By construction, $c_s \equiv \sum_{i=1}^{r} \varepsilon_i d_{j_i} \pmod n$ is solvable with not all $\varepsilon_i = 0$. Rewrite the above expression as $c_s \equiv \sum_{i=1}^{r_1} d_{j_i} \pmod n$, where we have suppressed those terms in the sum for which $\varepsilon_i = 0$. Applying (2) we obtain

$$\frac{\ell}{2} < \ell - B(c_s) \leq \sum_{i=1}^{r} (\ell - B(d_{j_i})) \quad .$$

Therefore, we obtain a d_i such that

$$\ell - B(d_i) > \frac{\ell}{2r_1} \geq \frac{\ell}{2r} \geq \frac{\ell k}{2(k+2\ell)} \geq \frac{k}{6} \quad ,$$

since $1 \leq r_1 \leq r$.

Q.E.D.

We now let $1 \leq d_1 < d_2 < \ldots < d_\nu \leq n-1$ be ν distinct residues modulo n such that $(d_i, n) = 1$. For $1 \leq u \leq \nu/2$, we consider all possible subsets, S_u, of u elements from the set $\{d_1, \ldots, d_{2u}\}$. For each subset S_u, let $L(S_u)$ denote the number of distinct residue classes modulo n which can be obtained in the form $\varepsilon_1 d_1 + \ldots + \varepsilon_{2u} d_{2u}$, where not all $\varepsilon_i = 0$ and where $\varepsilon_i = 0$ or 1 and $\varepsilon_i = 0$ if d_i is not in S_u. Note that in determining $L(S_u)$, we do not include the residue class 0 unless it can be expressed as the sum of $\leq u$ distinct elements of S_u.

Finally, put $L(u) = \text{Max}(L(S_u))$, where the maximum is taken over all subsets, S_u, of u elements from the set $\{d_1, \ldots, d_{2u}\}$.

Lemma 3. Let $d_1, \ldots, d_\nu$ satisfy the properties in the above definition. If

$$\varepsilon_1 d_1 + \ldots + \varepsilon_\nu d_\nu \equiv 0 \pmod{n}$$

implies that all $\varepsilon_i = 0$, then we have

(3) $$L(u+1) \geq L(u) \quad \text{when} \quad u \geq 1$$

(4) $$L(u) \geq u + 2 \quad \text{when} \quad u \geq 3 \quad .$$

Proof. (3) is obvious. In order to prove (2), we may assume without loss of generality that the maximum, $L(u)$, is obtained from $d_1, \ldots, d_u$, which are distinct modulo n by assumption. Also, $d_1 + \ldots + d_u$ is distinct from them by the assumption that $\varepsilon_1 d_1 + \ldots + \varepsilon_\nu d_\nu \equiv 0(n)$ is impossible unless all $\varepsilon_i = 0$. Now let $T = \{ d_1 + d_i \mid 2 \leq i \leq u \}$. Each element of T is distinct from $d_1 + \ldots + d_u$, when $u \geq 3$, and from d_1. It will be shown that at least one element of T is distinct from all of $d_1, \ldots, d_u$. This element, in addition to the $u + 1$ elements $d_1, \ldots, d_u$, $d_1 + \ldots + d_u$ will give $u + 2$ distinct residues modulo n, which proves (4), provided $u \geq 3$.

So assume that no element of T is distinct from $d_1, \ldots, d_u$, and let $d_1 + d_i = d_j$, where j is a function of i. It is clear that $\{ d_j \mid 2 \leq j \leq u \} = \{ d_2, \ldots, d_u \}$, since no two d_j are congruent modulo n and none are congruent to d_1. Consequently,

$$\sum_{i=2}^{u} (d_1 + d_i) \equiv \sum_{j=2}^{u} d_j \pmod{n} .$$

Therefore, $(u-1)d_1 \equiv 0 \pmod{n}$, which contradicts $(d_1, n) = 1$, as

$$2 \leq u - 1 < \nu - 1 \leq n - 2 .$$

Q.E.D.

Lemma 4. Let $d_1, \ldots, d_u, \ldots, d_\nu$ satisfy the same conditions as in Lemma 3. For $3 \leq u \leq -1 + \nu/2$, either $L(u) > n/2$ or $L(u + 1) > L(u) + \frac{u + 2}{6}$.

Proof. If $L(u) > n/2$ we are finished. So assume that $L(u) \leq n/2$. Now let S_u be a set for which $L(u) = L(S_u)$. So we have $L(u)$ distinct residue classes $b_1, \ldots, b_{L(u)}$ modulo n which are representable as sums of distinct elements from S_u. We have $\nu - u \geq 1 + \nu/2 \geq u + 2$ other elements d_i which are not in S_u. Select $u + 2$ of these and, if necessary, relabel them as $d_1, \ldots, d_{u+2}$. Since $1 \leq u + 2 \leq L(u) \leq n/2$, we can apply Lemma 2 to the sets $\{b_1, \ldots, b_{L(u)}\}$ and $\{d_1, \ldots, d_{u+2}\}$, where $k = u + 2$, $\ell = L(u)$. Hence, we obtain an i, $1 \leq i \leq u + 2$ for which $B(d_i) < L(u) - \frac{u+2}{6}$, where $B(d_i)$ is the number of representations of d_i in the form

$$d_i \equiv b_j - b_h \pmod{n} \quad .$$

Putting $S_{u+1} = S_u \cup \{d_i\}$, we have

$$L(u + 1) \geq L(S_{u+1}) = L(u) + (L(u) - B(d_i))$$

$$> L(u) + \frac{u+2}{6} \quad ,$$

Q.E.D.

Lemma 5. As before, let $1 \leq d_1 < \ldots < d_\nu \leq n - 1$ be ν distinct residues modulo n such that $(d_i, n) = 1$. Then if $\nu \geq 3\sqrt{6n}$, the congruence

$$\varepsilon_1 d_1 + \ldots + \varepsilon_\nu d_\nu \equiv 0 \pmod{n}$$

is solvable with not all $\varepsilon_i = 0$.

Proof. Assume that $\varepsilon_1 d_1 + \ldots + \varepsilon_\nu d_\nu$, with $\varepsilon_i = 0$ or 1, implies that all $\varepsilon_i = 0$. We will then obtain a contradiction. By Lemma 4, either

$L(u) > n/2$ or $L(u) > \sum_{\lambda=3}^{u-1} (\frac{\lambda+2}{6}) + L(3) \geq \frac{u^2 + 3u + 42}{12}$, which is larger than $n/2$ provided $u \geq \sqrt{6n}$. Therefore, with $u \geq \sqrt{6n}$, we have $L(u) > n/2$ in either case. But we have $\nu \geq 3\sqrt{6n}$ distinct residues. Applying the preceding analysis to the more than $2\sqrt{6n}$ remaining residues, we obtain $L(u) > n/2$ for this set also.

Therefore, we have two, not necessarily disjoint, sets each with more than $n/2$ residues modulo n. Call these two sets A, B. By a well-known argument, either $A + B = G$ or $|G| \geq |A| + |B| > n/2 + n/2 = n$. Therefore, $A + B = G$; and we conclude that 0 is representable as the sum of distinct elements from $\{d_1, \ldots, d_\nu\}$. This contradicts our original assumption that 0 is not so represented. Therefore,

$$\varepsilon_1 d_1 + \ldots + \varepsilon_\nu d_\nu \equiv 0 \pmod{n}$$

is solvable non-trivially.

Q.E.D.

Proof of theorem.

For each divisor d of n, let $\Phi(d) = \{a_i \mid d = (a_i, n)\}$. Put $\Phi(d) = \{c_1, \ldots, c_h\}$, where h and the c_j depend on d, although this dependence is suppressed without loss of clarity.

For each $c_j \in \Phi(d)$, we have $c_j = d c_j'$, where $(\frac{n}{d}, c_j') = 1$. Furthermore, since the c_j are distinct modulo n, the c_j' are distinct modulo n/d, and they satisfy

$$1 \le c_1' < \ldots < c_h' \le [\frac{n-1}{d}] = \frac{n}{d} - 1 \quad .$$

Therefore, by Lemma 5, if $h \ge 3\sqrt{6n/d}$, the congruence $\varepsilon_1 c_1' + \ldots + \varepsilon_h c_h' \equiv 0 \pmod{n/d}$ is solvable non-trivially, in which case the congruence $\varepsilon_1 c_1 + \ldots + \varepsilon_h c_h \equiv 0 \pmod{n}$ is solvable non-trivially.

So if $m = \sum_{d/n} |\Phi(d)| \ge \sum_{d/n} 3\sqrt{6n/d}$, then for some d, $\Phi(d)$ will contain more than $3\sqrt{6n/d}$ distinct elements modulo n such that $(\frac{a_i}{d}, \frac{n}{d}) = 1$. Thus, the congruence $\varepsilon_1 a_1 + \ldots + \varepsilon_m a_m \equiv 0 \pmod{n}$ will be solvable non-trivially.

We now obtain an upper bound for $\sum_{d/n} 3\sqrt{6n/d}$ in terms of n. Suppose $p^{e_p} \,||\, n$. Then we have

$$\sum_{d/n} 3\sqrt{6n/d} = 3\sqrt{6n} \sum_{d/n} d^{-\frac{1}{2}}$$

$$= 3\sqrt{6n} \prod_{p/n} (1 + p^{-\frac{1}{2}} + \ldots + (p^{e_p})^{-\frac{1}{2}})$$

$$< 3\sqrt{6n} \prod_{p/n} (1 - p^{-\frac{1}{2}})^{-1} \quad .$$

Put $f(n) = \prod_{p/n} (1 - p^{-\frac{1}{2}})^{-1}$ and choose the prime $q = q(n)$ such that $\eta = \prod_{p \le q} p \le n < q' \prod_{p \le q} p$, where q' is the smallest prime greater than q. Clearly $f(\eta) \ge f(n)$. Now

$$\log(f(\eta)) = -\sum_{p \le q} \log(1 - p^{-\frac{1}{2}}) = \sum_{p \le q} p^{-\frac{1}{2}} + O(1)$$

$$= O\Big(\sum_{p \le q} p^{-\frac{1}{2}}\Big) = O\Big(\frac{\sqrt{q}}{\log q}\Big) \quad .$$

But $\log \eta = \sum_{p \le q} \log p = \delta(q) \le \log n$. It is well known that there exist positive constants α and β such that

$$\alpha q \le \delta(q) \le \beta q$$

for all primes q. Hence, we conclude that $\log n \ge \alpha \cdot q$. Also, $\eta' = \eta \cdot q' > n$, which implies that $\log \eta' > \log n$. But $\log \eta' = \delta(q') \le \beta q' = \beta\, q(q'/q) \le \gamma q$, for some constant $\gamma > 0$. Therefore, $\log q \ge \gamma_1 \cdot \log \log n$; and so $f(n) \le f(\eta) \le \exp\Big\{ c \ \frac{\sqrt{\log n}}{\log \log n} \Big\}$, where $c > 0$ is some positive constant.

Q.E.D.

PART I

SECTION 2

Let p be a prime and $a_1, \ldots, a_m$ distinct, non-zero residues modulo p. Let N be a residue modulo p and let $F(N) = F(N ; p ; a_1, \ldots, a_m)$ denote the number of solutions of the congruence

$$\varepsilon_1 a_1 + \ldots + \varepsilon_m a_m \equiv 0 \pmod{n} \quad , \tag{1}$$

where $\varepsilon_i = 0$ or 1. In the second part of their paper (See [4]), Erdős and Heilbronn proved the following result:

Theorem II $\quad F(N) = \frac{2^m}{p}(1 + o(1))$ if $m^3 p^{-2} \to \infty$ as $p \to \infty$.

The essential part in the proof of their theorem is the validation for each r, $1 \leq r \leq p - 1$, that $\sum_{k=1}^{m} \sin^2(\frac{\pi r a_k}{p})$ is sufficiently large; i.e., that

$$\sum_{r=1}^{p-1} \exp\{-\frac{1}{2} \sum_{k=1}^{m} \sin^2(\frac{\pi r a_k}{p})\} = o(1) \tag{2}$$

as $p \to \infty$. To see the relevance of (2) to $F(N)$, note that

$$F(N) = \frac{1}{p} \sum_{r=0}^{p-1} e(-\frac{rN}{p}) \prod_{k=1}^{m} (1 + e(\frac{ra_k}{p})) \quad ,$$

where we have

$$F(N) = \frac{1}{p}\sum_{r=0}^{p-1} e\left(\frac{r(A-2N)}{2p}\right) \prod_{k=1}^{m} \left(e\left(\frac{ra_k}{p}\right) + e\left(-\frac{ra_k}{p}\right)\right)$$

$$= \frac{2^m}{p}\sum_{r=0}^{p-1} e\left(\frac{r(A-2N)}{2p}\right) \quad \beta r \quad ,$$

where $\beta r = \prod_{k=1}^{m} \cos\left(\frac{\pi r a_k}{p}\right)$ and $A = \sum_{k=1}^{m} a_k$.

Hence $\left|F(N) - \frac{2^m}{p}\right| \leq \frac{2^m}{p}\sum_{r=1}^{p-1} |\beta r|$. Now

$$|\beta r| = \left(\prod_{k=1}^{m} \left(1 - \sin^2\left(\frac{\pi r a_k}{p}\right)\right)\right)^{\frac{1}{2}}$$

$$\leq \left(\prod_{k=1}^{m} \exp\left(-\sin^2\left(\frac{\pi r a_k}{p}\right)\right)\right)^{\frac{1}{2}}$$

$$= \exp\left\{-\frac{1}{2}\sum_{k=1}^{m} \sin^2\left(\frac{\pi r a_k}{p}\right)\right\} \quad ;$$

and so the relation (2) implies that $\sum_{r=1}^{p-1} |\beta r| = o(1)$ as $p \to \infty$.

Hence, their result.

It is natural to ask if Theorem II can be extended to sequences of natural numbers other than a sequence of primes, without changing the hypotheses of their theorem; i.e., assuming that $a_1, \ldots, a_m$ are distinct, non-zero residues modulo n, and N is any residue modulo n, does $F(N) = \frac{2^m}{n}(1 + o(1))$ when $m^3 n^{-2} \to \infty$ as $n \to \infty$? The answer is, in general, no, as shown by the following example:

Let

$$n = p^4 \quad , \qquad p \text{ a prime}$$

$$a_k = p\ k \quad , \qquad 1 \leq k \leq [p^{8/3} \log p] = m$$

$$N = 1 \quad .$$

Clearly, $m^3 n^{-2} \to \infty$ as $n \to \infty$ and the a_k are distinct modulo n and non-zero. But $F(1) = 0$.

A partial generalization of Theorem II can be obtained, however, without weakening the hypotheses of the theorem: We prove

Theorem. Let $a_1, \ldots, a_m$ be distinct, non-zero residues modulo n, where the n are natural numbers belonging to one of the types

(3) $n = p$, p a prime

(4) $n = p_1\ p_2$, $p_2 \geq p_1$ primes such that $p_1^2 > c\, p_2$

(5) $n = p_1\ p_2\ p_3$, $p_3 \geq p_2 \geq p_1$ primes such that $p_1^2 > c\, p_2\ p_3$ where $c > 0$ is an arbitrary, but fixed, constant.

If $m^3 n^{-2} \to \infty$ as $n \to \infty$, then $F(N) = \frac{2^m}{n}(1 + o(1))$ for all residues $N \pmod n$. And this conclusion does not hold for numbers not of type (3), (4), (5).

Proof. Write

$$F(N) = \frac{1}{n} \sum_{r=0}^{n-1} e(-\frac{rN}{n}) \prod_{k=1}^{m} (1 + e(\frac{ra_k}{n}))$$

$$= \frac{2^m}{n} \sum_{r=0}^{n-1} e(\frac{r(A-2N)}{2n}) \beta r \quad ,$$

where $\beta r = \prod_{k=1}^{m} \cos(\frac{\pi r a_k}{n})$, $A = \sum_{k=1}^{m} a_k$. Then

$|F(N) - \frac{2^m}{n}| \leq \frac{2^m}{n} \sum_{r=1}^{n-1} |\beta r|$. Now assume that n is of type (5). The easier case (4) follows similarly. For each divisor d of n, $d \neq n$, put $T(d) = \{ r \mid 1 \leq r \leq n-1 ; d = (r,n) \}$. Thus, $\{ r \mid 1 \leq r \leq n-1 \} = \bigcup_{\substack{d/n \\ d \neq n}} T(d)$. We will show for each divisor d of n, $d \neq n$, that

$$(6) \qquad \sum_{r \in T(d)} \exp\{ -\frac{1}{2} \sum_{k=1}^{m} \sin^2(\frac{\pi r a_k}{n}) \} = o(1) \quad \text{as} \quad n \to \infty \quad .$$

Consequently, we will be able to conclude that

$$\sum_{r=1}^{n-1} \exp\{ -\frac{1}{2} \sum_{k=1}^{m} \sin^2(\frac{\pi r a_k}{n}) \}$$

$$= \sum_{\substack{d/n \\ d \neq n}} \sum_{r \in T(d)} \exp\{ -\frac{1}{2} \sum_{k=1}^{m} \sin^2(\frac{\pi r a_k}{n}) \} = o(1)$$

as $n \to \infty$.

Hence, we have $F(N) = \frac{2^m}{n}(1 + o(1))$ as $n \to \infty$. Following the format of the Erdős-Heilbronn proof, it is a relatively straightforward matter to

check that (6) holds for each divisor d of n, $d \neq n$. One verifies that each step in their proof for the case n = prime is valid in the case (5), where we are given that

(7) $$m > f(n)\ n^{2/3} = f(n)\ (p_1\ p_2\ p_3)^{2/3}\ ,\ \lim_{n\to\infty} f(n) = \infty\ .$$

Two facts used in the Erdős-Heilbronn proof which are not immediately verifiable in case (5) are

(8) $$(m^3 n^{-2})^{-1} \sum_{k=1}^{m} \sin^2\left(\frac{\pi r a_k}{n}\right) \geq \gamma\ ,$$ an absolute positive constant.

(9) For each r, $1 \leq r \leq n-1$, the congruence $vr \equiv u(n)$ is solvable with $1 \leq v \leq \log n$, $1 \leq |u| \leq n/\log n$, $(u,v) = 1$.

To show (8), put $S = S_r = \sum_{k=1}^{m} \sin^2\left(\frac{\pi r a_k}{n}\right)$, and let $r = \rho \cdot d$, $n = \eta \cdot d$, $(\rho, \eta) = 1$, $1 \leq \rho \leq \eta - 1$. Then we have

$$S = \sum_{k=1}^{m} \sin^2\left(\frac{\pi r a_k}{n}\right) = \sum_{k=1}^{m} \sin^2\left(\pi \left\| \frac{\rho a_k}{\eta} \right\|\right),$$ where $\|y\|$ is the distance of y to the nearest integer. Let $\lambda_\rho(j)$ denote the number of a_k such that $\rho a_k \equiv j \pmod{\eta}$. Then we have

$$S = \sum_{j=0}^{\eta-1} \lambda_\rho(j) \sin^2\left(\pi \left\|\frac{j}{\eta}\right\|\right) \geq 4 \sum_{j=0}^{\eta-1} \lambda_\rho(j) \left\|\frac{j}{\eta}\right\|^2\ ,$$ since $\sin \pi x \geq 2x$ for $0 \leq x \leq \frac{1}{2}$. Because $\sum_{j=0}^{\eta-1} \lambda_\rho(j) = m$, then either

$$\sum_{0 \leq j \leq \frac{1}{2}(\eta-1)} \lambda_\rho(j) \geq m/2 \quad \text{or} \quad \sum_{\frac{1}{2}(\eta-1) < j \leq \eta-1} \lambda_\rho(j) \geq m/2\ .$$

We can assume that the former inequality holds. Now, since $a_1, \ldots, a_m$ are distinct modulo n, there are at most $d = n/\eta$ of them which satisfy $\rho a_k \equiv j \pmod{\eta}$ for any j modulo η. Therefore,

$$S \geq 4\ \eta^{-2}\ d \sum_{j=0}^{[\frac{m}{2d}]} j^2 >> \eta^{-2}\ d\ (\frac{m}{d})^3 = m^3 n^{-2} \quad ,$$

provided $m/2d \geq 1$. Otherwise, we could only conclude that $\sum_{j=0}^{[\frac{m}{2d}]} j^2 \geq 0$. But we have

$$[\frac{m}{2d}] \geq \frac{m}{2\ p_2\ p_3} - 1 \geq \frac{(p_1 p_2 p_3)^{2/3} f(n)}{2\, p_2 p_3} - 1$$

by (7). Thus,

$$[\frac{m}{2d}] \geq \frac{1}{2} c^{2/3}\ f(n) - 1 \quad ,$$

since $p_1^2 > c\ p_2 p_3$. But $\lim_{n\to\infty} f(n) = \infty$; so for all sufficiently large n, we have $\frac{1}{2} c^{2/3}\ f(n) - 1 > 1$. Therefore, $(m^3 n^{-2})^{-1}\ S \geq \gamma > 0$, where γ is an absolute constant. This proves (8). To prove (9), consider the residues $v\ r - u \pmod{n}$, where $1 \leq r \leq n - 1$, r is fixed, and $0 \leq v \leq \log n$, $0 \leq u \leq n/\log n$. The number of residues considered is $(1 + [\log n])\ (1 + [n/\log n]) > n$. Hence, there are two residues which are congruent modulo n, say

(10) $$v_1 r - u_1 \quad , \quad v_2 r - u_2 \quad .$$

If $v_1 = v_2$, then $u_1 - u_2 \equiv 0 \pmod{n}$; hence $u_1 = u_2$. If $u_1 = u_2$, then we have $(v_1 - v_2)r \equiv 0 \pmod{n}$. But the smallest proper divisor of n is $p_1 > \sqrt[3]{cn}$, and $0 \leq |v_1 - v_2| \leq \log n$. Hence $v_1 = v_2$. Therefore, we can suppose $v_2 > v_1$ and $u_1 \neq u_2$; and we obtain $vr \equiv u \pmod{n}$, with $0 < v \leq \log n$ and $0 < |u| \leq n/\log n$. We can write $vr - u = q\,n$. If $(u,v) > 1$, then $(u,v) \mid q$, since $(v,n) = 1$. Hence, we can divide v, u, q by (u,v) and obtain the result. This proves (9).

With these two results we can now mimic the proof of the Erdős-Heilbronn theorem to obtain $F(N) = \frac{2^m}{n}(1 + o(1))$ in case (5). The proof of case (4) is similar.

It still remains to be shown that, subject to the hypotheses of the theorem, only numbers of type (3), (4), (5) satisfy $F(N) = \frac{2^m}{n}(1 + o(1))$ as $n \to \infty$.

Suppose $m > n^{2/3} f(n)$, where $f(n)$ is any positive function such that $\lim_{n\to\infty} f(n) = \infty$. In order that $F(N) > 0$ for all residues N modulo n, it is necessary that $(a_1, \ldots, a_m, n) = 1$. Suppose $n = p_1^{e_1} \cdots p_t^{e_t}$, where $p_t > p_{t-1} > \ldots > p_1$ are primes with $e_1 \geq 1$, $e_i \geq 0$ $(2 \leq i \leq t)$. For each divisor d of n, $d \neq n$, there can be as many as $-1 + n/d$ of the a_k divisible by d. So in order to guarantee that not all of the a_k are divisible by a proper divisor d of n, $d \neq n$, we require that $n^{2/3} f(n) = m > n/d > -1 + n/d$. If the above inequality is satisfied for $d = p_1$, then it is satisfied for all proper divisors of n, since p_1 is

the smallest such. Thus we require

$$(11) \qquad (p_1^{e_1} \dots p_t^{e_t})^{2/3} \, f(n) > p_1^{e_1 - 1} \, p_2^{e_2} \dots p_t^{e_t} ,$$

which implies $f(n) > p_1^{e_1 - 3} \, p_2^{e_2} \dots p_t^{e_t}$. Now, if either $e_1 > 3$ or $e_2 + \dots + e_t > 3 - e_1$, we would have a contradiction to (11); for we could choose an increasing sequence of natural numbers n and a function $f(n)$ to grow so slowly that for all sufficiently large n,

$$f^3(n) < p_1^{e_1 - 3} \, p_2^{e_2} \dots p_t^{e_t} ,$$

which would contradict (11); and, hence, would allow $(a_1, \dots, a_m, n) > 1$. Therefore, we must have $e_1 \leq 3$ and $e_2 + \dots + e_t \leq 3 - e$. The only natural numbers $n \neq$ prime which satisfy these two conditions are those such that $n = p_1 \, p_2$ and $n = p_1 \, p_2 \, p_3$ (where p_1 and p_2 could be equal in the first case and p_1, p_2, p_3 could be equal in the second case). In these two cases we need $f^3(p_1 p_2) \, p_1^2 > p_2$ and $f^3(p_1 \, p_2 \, p_3) p_1^2 > p_2 \, p_3$, respectively, where f is any positive function such that $\lim_{n \to \infty} f(n) = \infty$. Therefore, we must have $\dfrac{p_1^2}{p_2} > c$ and $\dfrac{p_1^2}{p_2 p_3} > c$, respectively, where c is some positive constant. Thus n is of type (3), (4), (5).

Erdős and Heilbronn have shown that the bound $m \geq n^{2/3} f(n)$, where $\lim_{n \to \infty} f(n) = \infty$, is sharp; i.e., if $n =$ prime and $m = O(n^{2/3})$, then $\lim_{n \to \infty} \dfrac{n}{2^m} F(0) > 1$, where

$$F(0) = F(0\ ;\ p\ ;\ 1,\ -1,\ \ldots,\ (-1)^{m-1}\ [\tfrac{m+1}{2}]\ ) \quad .$$

Therefore, the hypothesis $m^3 n^{-2} \to \infty$ as $n \to \infty$ cannot be strengthened without correspondingly weakening the qualitative hypotheses concerning $a_1, \ldots, a_m$ and still obtain

$$F(N) = \frac{2^m}{n}\,(1 + o(1)) \quad \text{as} \quad n \to \infty \quad . \tag{12}$$

One could obtain (12) for a wider class of integers than (3), (4), (5) by requiring that $m^a n^{-b} \to \infty$ as $n \to \infty$, where $1 > a/b > 2/3$. In such cases, one obtains (12) for those integers $n = p_1^{e_1} \ldots p_t^{e_t}$ which satisfy

$$(b - a)e_1 \leq b \quad , \qquad e_1 \geq 1 \quad , \tag{13}$$

$$(b - a)(e_2 + \ldots + e_t) \leq b - (b - a)e_1 \quad , \tag{14}$$

$$p_1^{b-(b-a)e_1} > c\,(p_2^{e_2} \ldots p_t^{e_t})^{b-a} \tag{15}$$

for some $c > 0$; and (13), (14), (15) are obtained in the same way as the corresponding conditions in the case $a/b = 2/3$.

Finally, there is still the possibility that if m is chosen large enough, yet still satisfying $m\, n^{-1} \to 0$ as $n \to \infty$ (say $m \geq n/\log n$, for example), then the conclusion of our theorem would hold for all n. The following example shows that this is not possible, however:

Let

$$n = 2\lambda$$

$$a_j = 2^j , \quad 1 \leq j \leq \lambda - 1$$

$$N = 1 \quad .$$

Clearly, the a_j are non-zero and distinct modulo n. But $F(1) = 0$, while $m = n/2 - 1$.

PART II

Employing estimates due to Vinogradov, Davenport and Roth* have proved the following:

> Let $\lambda_1, \ldots, \lambda_s$ be non-zero, real numbers not all of the same sign and not all in rational ratios, and let β be any real number. Let m be an integer such that $m \geq 12$. Then there is an absolute constant $c > 0$ such that if $s > cm \log m$, the inequality

(1)
$$|\lambda_1 k_1^m + \ldots + \lambda_s k_s^m + \beta| < \varepsilon$$

> has infinitely many solutions in positive integers k_i, where $\varepsilon > 0$ is an arbitrary real number.

In this section we will show that their methods can be adapted to prove a similar result when the exponent m is not an integer. In this case it no longer needs to be assumed that some ratio λ_i/λ_j is irrational. When m is an integer this assumption is necessary, since then the values of $\lambda_1 k_1^m + \ldots + \lambda_s k_s^m$ are discrete--and so (1) could not be solvable for all β and all $\varepsilon > 0$. It is clearly necessary to assume that not all of the λ_i have the same sign in order to solve (1) for all

---

*See [5].

real β. This condition is also necessary when m is not an integer. Finally, it will be assumed that $m \geq 12$ so that Vinogradov's strong estimates for certain exponential sums can be used.

We prove

Theorem. Let $\lambda_1, \ldots, \lambda_s$ be non-zero, real numbers not all of the same sign, and let β be any real number. Let $\tau > 12$ and τ not an integer. Then there is an absolute constant $c > 0$ such that if $s > c\,\tau \log \tau$, the inequality

$$|\lambda_1 k_1^{\tau} + \ldots + \lambda_s k_s^{\tau} + \beta| < \varepsilon \tag{2}$$

has infinitely many solutions in positive integers k_i for all $\varepsilon > 0$.

The proof of the above theorem follows that of Davenport and Roth, where the main divergence from their proof is in Lemma 10. The proof of this lemma requires a more complicated analysis than the proof of the corresponding lemma in the case where τ is an integer, and it requires different types of exponential sums.

Note that it suffices to prove (2) in the special case when $\varepsilon = 1$, as the proof of the general case follows by replacing $\lambda_1, \ldots, \lambda_s, \beta$ with $\lambda_1/\varepsilon, \ldots, \lambda_s/\varepsilon, \beta/\varepsilon$. Without loss of generality, it may be assumed that $\lambda_1, \lambda_2 > 0$ and $\lambda_3 < 0$, since we have assumed that not all of the λ_i are of the same sign. Finally, (2) will be proved for the case when $\beta = 0$, since the proof of the general case is, with

minor changes, identical to the proof of the case $\beta = 0$.

For convenience it will be assumed that s is an odd integer, say $s = 2r + 1$.

We have the following notation:

$$a = |\lambda_3|/4(\lambda_1 + \lambda_2) \quad , \tag{3}$$

$$\theta = 1/\tau \quad , \tag{4}$$

$$\theta(\ell) = (1 - \theta)^{\ell}, \qquad 1 \leq \ell \leq r - 1 \quad . \tag{5}$$

We now divide the $s = 2r + 1$ numbers $\lambda_1, \ldots, \lambda_s$ into three sets:

$$\{\lambda_1, \lambda_2, \lambda_3\} \quad , \tag{6}$$

$$\{\mu_1, \ldots, \mu_{r-1}\} = \{\lambda_4, \ldots, \lambda_{r+2}\} \quad , \tag{7}$$

$$\{\nu_1, \ldots, \nu_{r-1}\} = \{\lambda_{r+3}, \ldots, \lambda_{2r+1}\} \quad . \tag{8}$$

Let α be a real number which will later be treated as a variable of integration, and let x be a large, positive number. Then we define

$$S(\lambda_j \alpha) = \sum_{ax < k^{\tau} \leq 8ax} e(\lambda_j \alpha k^{\tau}) \quad , \qquad j = 1, 2 \quad , \tag{9}$$

$$T(\lambda_3 \alpha) = \sum_{x/2 < k^{\tau} \leq 2x} e(\lambda_2 \alpha k^{\tau}) \quad , \tag{10}$$

$$U(\mu_{\ell} \alpha) = \sum_{x^{\theta(\ell)} < k^{\tau} \leq 2x^{\theta(\ell)}} e(\mu_{\ell} \alpha k^{\tau}) \quad , \qquad 1 \leq \ell \leq r - 1 \quad , \tag{11}$$

(12) $$U(\nu_\ell \alpha) = \sum_{x^{\theta(\ell)} < k^\tau \leq 2x^{\theta(\ell)}} e(\nu_\ell \alpha k^\tau) \quad , \quad 1 \leq \ell \leq r-1 \ ,$$

(13) $$P(\alpha) = S(\lambda_1 \alpha) S(\lambda_2 \alpha) T(\lambda_3 \alpha) \quad ,$$

(14) $$Q(\alpha) = \prod_{1 \leq \ell \leq r-1} U(\mu_\ell \alpha) \quad ,$$

(15) $$R(\alpha) = \prod_{1 \leq \ell \leq r-1} U(\nu_\ell \alpha) \quad ,$$

(16) $$F(x, \alpha) = F(\alpha) = P(\alpha) Q(\alpha) R(\alpha) \quad .$$

Lemma 1. For any real number t, we have

$$\int_{-\infty}^{\infty} e(t\alpha) \left(\frac{\sin \pi \alpha}{\pi \alpha}\right)^2 d\alpha = \begin{cases} 1 - |t| \ , & |t| \leq 1 \\ 0 \ , & |t| > 1 \end{cases} \ .$$

Proof. See [5], page 158.

Henceforth, we will denote $\left(\frac{\sin \pi \alpha}{\pi \alpha}\right)^2$ by $D(\alpha)$. Then, by Lemma 1 and (16), we obtain

(17) $$\Delta(x) = \int_{-\infty}^{\infty} F(\alpha) D(\alpha) d\alpha = \sum_{|K| < 1} (1 - |K|) \quad ,$$

where

(18) $$K = \lambda_1 h_1^\tau + \ldots + \lambda_3 h_3^\tau + \mu_1 g_1^\tau + \ldots + \mu_{r-1} g_{r-1}^\tau + \nu_1 k_1^\tau + \ldots + \nu_{r-1} k_{r-1}^\tau$$

and where the positive integers h_1, h_2, h_3, g_ℓ, k_ℓ $(1 \leq \ell \leq r-1)$ are summed over

(19) $$ax < h_1^{\tau},\ h_2^{\tau} \leq 8ax \quad ,$$

(20) $$x/2 < h_3^{\tau} \leq 8ax \quad ,$$

(21) $$x^{\theta(\ell)} < g_{\ell}^{\tau},\ k_{\ell}^{\tau} \leq 2x^{\theta(\ell)} \quad .$$

The proof of the theorem depends on showing that $\Delta(x)$ tends to infinity as x tends to infinity; for if the integral in (17) is unbounded, then there must be infinitely many values of K with $|K| < 1$.

In order to show this, the interval $(-\infty, \infty)$ is divided into three disjoint sets J_1, J_2, J_3. It will be shown that the contribution to (17) from those α in J_1 is $>>^{*} x(1 + \theta - 2(1 - \theta)^r)$, where we have put

(22) $$x^y = x(y) \quad .^{**}$$

Also, it will be shown that the contribution to (17) from the α in $J_2 \cup J_3$ is $<< x(1 + \theta - 2(1 - \theta)^r - \delta)$ for some small, but fixed, $\delta > 0$. This will show that (17) is unbounded.

---

*If $g(x) \geq 0$ for all $x > 0$, the notations $f(x) = O(g(x))$ and $f(x) << g(x)$ both mean that there is a positive constant c such that $|f(x)| \leq cg(x)$ for all sufficiently large x.

**This notation will be used mainly for complicated expressions which appear as exponents of the variable x.

We define

(23) $$J_1 = \{ \alpha : |\alpha| \leq x(-1 + \theta - \theta^2) \} \quad ,$$

(24) $$J_2 = \{ \alpha : x(-1 + \theta - \theta^2) < |\alpha| \leq x \} \quad ,$$

(25) $$J_3 = \{ \alpha : |\alpha| > x \} \quad ,$$

(26) $$L(\lambda_j \alpha) = \theta \int_{ax}^{8ax} e(\alpha \lambda_j \xi) \xi^{\theta - 1} d\xi \quad , \qquad j = 1, 2 \quad ,$$

(27) $$M(\lambda_3 \alpha) = \theta \int_{x/2}^{2x} e(\alpha \lambda_3 \xi) \xi^{\theta - 1} d\xi \quad .$$

Lemma 2. Let $f(t)$ be a real-valued, differentiable function on the interval (t_1, t_2) such that $f'(t)$ is monotonic and $|f'(t)| \leq d < 1$. Then

$$\sum_{t_1 < n \leq t_2} e(f(n)) = \int_{t_1}^{t_2} e(f(t)) + O(1) .$$

Proof. See [7], Hilfssatz 2, Section 8.

Lemma 3. For α in J_1, we have $S(\lambda_j \alpha) = L(\lambda_j \alpha) + O(1)$, $j = 1, 2$, $T(\lambda_3 \alpha) = M(\lambda_3 \alpha) + O(1)$, for all sufficiently large x.

Proof. The lemma will be proved for $S(\lambda_1 \alpha)$. The proofs of the other two cases are similar. From (9), we have

$$(28) \qquad S(\lambda_1 \alpha) = \sum_{(ax)^\theta < k \le (8ax)^\theta} e(\lambda_1 \alpha k^\tau) \quad .$$

We now apply Lemma 2 to the right hand side of (28) with $f(t) = \lambda_1 \alpha t^\tau$. For $\alpha \in J_1$, $\alpha \ge 0$, we have

$$(29) \qquad f''(t) = \lambda_1 \alpha \ \tau(\tau - 1) t^{\tau - 2} \ge 0$$

$$(30) \qquad \left| \frac{d}{dt}(\lambda_1 \alpha t^\tau) \right| \le |\lambda_1 \tau \ x(-1 + \theta - \theta^2) \ (8ax)^{1-\theta}| << x(-\theta^2) \quad ,$$

since $(ax)^\theta < t \le (8ax)^\theta$. So, for all sufficiently large x, $\left| \frac{d}{dt}(\lambda_1 \alpha t^\tau) \right| \le \frac{1}{2}$. The conditions of Lemma 2 are satisfied by (29) and (30), so we have

$$S(\lambda_1 \alpha) = \int_{(ax)^\theta}^{(8ax)^\theta} e(\lambda_1 \alpha t^\tau) dt + O(1)$$

$$= \theta \int_{ax}^{8ax} e(\lambda_1 \alpha \xi) \xi^{\theta - 1} d\xi + O(1) \quad ,$$

where we have made the change of variable $\xi = t^\tau$. This proves the result for $\alpha \in J_1$, $\alpha \ge 0$. The proof for $\alpha \in J_1$, $\alpha < 0$ is similar.

Lemma 4. $L(\lambda_j \alpha) << \min(x^\theta, x^{\theta - 1} / |\alpha|)$, $j = 1, 2$,

$M(\lambda_3 \alpha) << \min(x^\theta, x^{\theta - 1} / |\alpha|)$, for all α.

Proof. Clearly, $|L(\lambda_1\alpha)| << \int_{ax}^{8ax} \xi^{\theta-1}\,d\xi << x^{\theta}$. By the Second Mean Value Theorem, there is a ξ_1 such that $ax < \xi_1 < 8ax$ and

$$L(\lambda_1\alpha) = (ax)^{\theta-1}\int_{ax}^{\xi_1} e(\alpha\lambda_1\xi)d\xi + (8ax)^{\theta-1}\int_{\xi_1}^{8ax} e(\alpha\lambda_1\xi)d\xi$$

$$<< x^{\theta-1}/|\alpha| \quad .$$

This proves the lemma for $L(\lambda_1\alpha)$. The proofs for $L(\lambda_2\alpha)$ and $M(\lambda_3\alpha)$ are similar.

Lemma 5. $$\int_{\alpha \notin J_1} F(\alpha)D(\alpha)d\alpha >> x(1 + \theta - 2(1-\theta)^r) \quad .$$

Proof. The proof of Lemma 5 will proceed in steps. We will prove the following three inequalities:

(31) $$H_1 = \int_{-\infty}^{\infty} Q(\alpha)R(\alpha)L(\lambda_1\alpha)L(\lambda_2\alpha)M(\lambda_3\alpha)D(\alpha)d\alpha$$

$$>> x(1 + \theta - 2(1-\theta)^r) \quad ,$$

(32) $$H_2 = \int_{\alpha \notin J_1} Q(\alpha)R(\alpha)L(\lambda_1\alpha)L(\lambda_2\alpha)M(\lambda_3\alpha)D(\alpha)d\alpha$$

$$<< x(1 - \theta - 2(1-\theta)^r + 2\theta^2) \quad ,$$

$$H_3 = \int_{\alpha \in J_1} Q(\alpha)R(\alpha)(P(\alpha) - L(\lambda_1\alpha)L(\lambda_2\alpha)M(\lambda_3\alpha))D(\alpha)d\alpha \tag{33}$$

$$<< x(1 - 2(1 - \theta)^r) \quad .$$

This suffices for the proof of the lemma, since

$$\int_{\alpha \in J_1} F(\alpha)D(\alpha)d\alpha = H_3 + H_1 - H_2 \quad .$$

In (31) interchange the order of integration and summation and integrate with respect to α. By Lemma 1, we obtain

$$H_1 = \Sigma \int A \; d\xi_1 \, d\xi_2 \, d\xi_3 \quad , \tag{34}$$

where

$$A = A(g_1, \ldots, g_{r-1}; k_1, \ldots, k_{r-1}; \xi_1, \xi_2, \xi_3)$$

$$= \begin{cases} (1 - |B|)(\xi_1\xi_2\xi_3)^{\theta-1} & \text{if} \quad |B| \leq 1 \\ 0 & \text{if} \quad |B| > 1 \end{cases} ,$$

and

$$B = \mu_1 g_1^\tau + \ldots + \mu_{r-1} g_{r-1}^\tau + \nu_1 k_1^\tau + \ldots + \nu_{r-1} k_{r-1}^\tau$$

$$+ \lambda_1\xi_1 + \lambda_2\xi_2 + \lambda_3\xi_3 \quad ,$$

and where the summation in (34) is over positive integers g_ℓ, k_ℓ satisfying (21) and (22), and the integration in (34) is over the range

$$ax < \xi_1, \xi_2 \leq 8ax \quad , \tag{35}$$

$$x/2 < \xi_3 \leq 2x \quad . \tag{36}$$

For $3ax \le \xi_1, \xi_2 \le 6ax$, we have

$$3|\lambda_3|x/4 = 3ax(\lambda_1 + \lambda_2) \le \lambda_1\xi_1 + \lambda_2\xi_2 \le 6ax(\lambda_1 + \lambda_2) = 3|\lambda_3|x/2 \quad . \tag{37}$$

We also have

$$|B - (\lambda_1\xi_1 + \lambda_2\xi_2 + \lambda_3\xi_3)| << x^{1-\theta} \quad , \tag{38}$$

since $g_\ell^\tau, k_\ell^\tau << x^{\theta(\ell)}$ for $1 \le \ell \le r-1$. Hence, for $3ax \le \xi_1, \xi_2 \le 6ax$ and for all sufficiently large x, we have

$$(3/4 - \eta)|\lambda_3|x \le M - \lambda_3\xi_3 \le (3/2 + \eta)|\lambda_3|x$$

by (37) and (38), where η is a very small positive number. Since the range of integration for ξ_3 is $(x/2, 2x]$, there is an interval of length $1/2$, say $\mathcal{I} = \mathcal{I}(g_1, \ldots, g_{r-1}; k_1, \ldots, k_{r-1}; \xi_1, \xi_2)$ for ξ_3, lying completely within $(x/2, 2x]$, such that $|M| \le 1/2$ on this interval; and this holds for all ξ_1, ξ_2 such that $3ax \le \xi_1, \xi_2 \le 6ax$ and all g_ℓ, k_ℓ satisfying (21) and (22). Hence, for ξ_1, ξ_2, ξ_3 in the region

$$\mathcal{R} = [3ax, 6ax] \times [3ax, 6ax] \times \mathcal{I} \quad ,$$

we have $A \ge (\xi_1\xi_2\xi_3)^{\theta-1}/2$, uniformly for all g_ℓ, k_ℓ satisfying (21) and (22). So for any choice of g_ℓ, k_ℓ, $1 \le \ell \le r-1$, we have

$$\int_{\mathcal{R}} A \, d\xi_1 \, d\xi_2 \, d\xi_3 >> x^2 x^{-3(1-\theta)} = x^{-1+3\theta} \quad . \tag{39}$$

The number of terms in the sum in (34) is

$$>> x(2\theta \sum_{1 \le \ell \le r-1} (1-\theta)^r) = x(2(1-\theta) - 2(1-\theta)^r)$$

by (21) and (22). Therefore,

$$H_1 >> x(-1 + 3\theta + 2(1-\theta) - 2(1-\theta)^r)$$

$$= x(1 + \theta - 2(1-\theta)^r) \quad ,$$

which proves (31).

Turning to the proof of (32), we have the estimates

$$L(\lambda_j \alpha) << x^{\theta-1}/|\alpha| \qquad \text{for } j = 1, 2,$$

and

$$M(\lambda_3 \alpha) << x^{\theta-1}/|\alpha| \qquad \text{by Lemma 4.}$$

Therefore,

$$L(\lambda_1 \alpha)L(\lambda_2 \alpha)M(\lambda_3 \alpha) << x^{3(\theta-1)}/|\alpha|^3 \quad . \tag{40}$$

Now if $Q(\alpha)R(\alpha)$ is multiplied out, the number of terms obtained is $<< x(2\theta \sum_{1 \le \ell \le r-1} (1-\theta)^\ell = x(2(1-\theta) - 2(1-\theta)^r)$, and each term is in ≤ 1 in absolute value. Therefore,

$$|Q(\alpha)R(\alpha)| << x(2(1-\theta) - 2(1-\theta)^r) \quad .$$

Since $|D(\alpha)| << 1$, we have by (40)

$$|H_2| << x(2(1-\theta) - 2(1-\theta)^r) \int x^{3(\theta-1)}/|\alpha|^3 \, d\alpha \quad ,$$

where the integration is over those α not in J_1. Therefore,

$$|H_2| << x(2(1-\theta) - 2(1-\theta)^r + 3(\theta-1) + 2(1+\theta^2-\theta))$$

$$= x(1 - \theta - 2(1-\theta)^r + 2\theta^2) \quad ,$$

which proves (32). To prove (33), we use Lemma 3 for α in J_1 to obtain

$$S(\lambda_j\alpha) = L(\lambda_j\alpha) + O(1) \quad , \qquad j = 1, 2 \quad ,$$

and

$$T(\lambda_3\alpha) = M(\lambda_3\alpha) + O(1) \quad .$$

So by Lemma 4,

$$|P(\alpha) - L(\lambda_1\alpha)L(\lambda_2\alpha)M(\lambda_3\alpha)| << \min(x^{2\theta}, x^{2(\theta-1)}/|\alpha|^2) \quad .$$

Estimating H_3 by the methods used in estimating H_2, we have

$$|H_3| << x(2(1-\theta) - 2(1-\theta)^r) \times$$

$$\left(\int x^{2\theta}\,d\alpha + \int x^{2(\theta-1)}/|\alpha|^2 d\alpha\right) \quad ,$$

where the first integral is over $|\alpha| \leq 1/x$, and the second is over $1/x < |\alpha| \leq x(-1+\theta-\theta^2)$. So

$$|H_3| << x(2(1-\theta) - 2(1-\theta)^r + 2\theta - 1)$$

$$= x(1 - 2(1-\theta)^r) \quad ,$$

which proves (33) and hence the lemma.

Lemma 6. $$\int_{-\infty}^{\infty} |S(\lambda_1\alpha)Q(\alpha)|^2 D(\alpha)\,d\alpha << x(1-(1-\theta)^r) \quad ,$$

$$\int_{-\infty}^{\infty} |T(\lambda_3\alpha)R(\alpha)|^2 D(\alpha)\,d\alpha << x(1-(1-\theta)^r) \quad .$$

Proof. The integral appearing in the first line of the lemma is the number of solutions of the inequality

$$|\lambda_1(h^\tau - m^\tau) + \mu_1(g_1^\tau - m_1^\tau) + \ldots + \mu_{r-1}(g_{r-1}^\tau - m_{r-1}^\tau)| < 1 \tag{41}$$

in integers h, m, g_ℓ, m_ℓ satisfying

$$ax < h^\tau, m^\tau \leq 8ax \tag{42}$$

$$x^{\theta(\ell)} < g_\ell^\tau, m_\ell^\tau \leq 2x^{\theta(\ell)} \quad , \quad 1 \leq \ell \leq r-1 \quad . \tag{43}$$

Now for a particular value of h satisfying (42), the inequality (41) determines m^τ with an error which is $<< x(\tau-1)$; and hence determines m^τ to within a bounded number of possibilities, i.e., to within O(1). Similarly, given particular values of h^τ, m^τ, g_1^τ satisfying (42) and (43), m_1^τ is determined within O(1) possibilities, etc. Therefore, the number of solutions of (41) in integers h, m, g_ℓ, m_ℓ satisfying (42) and (43) is

$$<< x(\theta + \theta \sum_{1 \leq \ell \leq r-1} (1-\theta)^\ell) = x(1 - (1-\theta)^r) \quad ,$$

which proves the lemma for the first integral. The second inequality is proved similarly.

Lemma 7. Let $G(\alpha) = \Sigma\, e(\alpha f(x_1, \ldots, x_m))$, where the sum is over a finite set of integer values of $x_1, \ldots, x_m$ and f is real. Then for $W > 4$, we have

$$\int_{|\alpha|>W} |G(\alpha)|^2 D(\alpha)d\alpha \leq \frac{16}{W} \int_{-\infty}^{\infty} |G(\alpha)|^2 D(\alpha)d\alpha \, .$$

Proof. See [5], page 82.

Lemma 8. $$\int_{\alpha \in J_3} F(\alpha)D(\alpha)d\alpha << x(\theta - (1 - \theta)^r) \quad .$$

Proof. Since the number of terms in the sum defining $T(\lambda_3 \alpha)$ is $<<x^{\theta}$ and since each such term is ≤ 1 in absolute value, we have $|T(\lambda_3 \alpha)| << x^{\theta}$. Applying this estimate and the Cauchy-Schwarz inequality to the integral

$$\int_{\alpha \in J_3} |Q(\alpha)R(\alpha)S(\lambda_1 \alpha)T(\lambda_3 \alpha)| D(\alpha)d\alpha \quad ,$$

we have

$$\int_{\alpha \in J_3} F(\alpha)D(\alpha)d\alpha << x^{\theta} F_1 F_2 \quad ,$$

where

$$F_1 = \Big(\int_{|\alpha| > x} |S(\lambda_1 \alpha)Q(\alpha)|^2 D(\alpha)d\alpha \Big)^{\frac{1}{2}} \quad ,$$

$$F_2 = \Big(\int_{|\alpha| > x} |T(\lambda_3 \alpha)R(\alpha)|^2 D(\alpha)d\alpha \Big)^{\frac{1}{2}} \quad .$$

The result follows by Lemmas 6 and 7.

Lemma 9. Let N and P be integers, P being large and positive. Let f(u) be a real-valued function on $N \leq u \leq N + P$, and having in this interval a continuous (n+1)-st derivative satisfying

$1/z \leq |f^{(n+1)}(u)/(n+1)!| \leq c'/z$,

where $n \geq 11$ and $P << z << P^{2+2/n}$. Let

$S = \sum_{N \leq k \leq N+P} e(f(k))$. Then we have $|S| << P^{1-\Phi'}$,

where

$$\Phi' = 1/3n^2 \log(125\, n) \quad .$$

Proof. See [15], Theorem 2a, page 109.

Lemma 10. Let $f(u)$ be a real-valued function defined on $b + 1 \leq u \leq b + p$. For $n \geq 2$, suppose $f^{(n)}(u) \geq \gamma > 0$ (or $f^{(n)}(u) \leq \gamma < 0$) for all u in $[b + 1, b + p]$. Then

$$\left| \sum_{b+1 \leq k \leq b+p} e(f(k)) \right| \quad \text{is}$$

$$<< p[(\gamma/\Gamma^2)^{-1/(2^n-2)} + (\gamma p^n)^{-1/(2^n-1)} + (\gamma p/\Gamma)^{-1/2^{(n-1)}}] \quad ,$$

where $\Gamma = (1/p)[f^{(n-1)}(b + p) - f^{(n-1)}(b + 1)]$.

Proof. See [7], Satz 3, Section 8.

Lemma 11. For α in J_2, $S(\lambda_1 \alpha) << x(\theta(1 - \Phi))$, where $\Phi = \min((1 - \theta)/2^{11} - 2),\ 1/3\phi^2 \log(125\phi))$, and $\phi = 1 + [2\tau]$.

Proof. We will prove the lemma for $\alpha \in J_2$, $\alpha > 0$. The proof for negative α in J_2 is similar. So, for $\alpha > 0$, α in J_2, put $\alpha = x(\theta y)$. Hence,

$$y = \tau \log \alpha / \log x ;$$

and since

$$x(-1 + \theta - \theta^2) < \alpha \leq x \quad ,$$

we have

$$\tau(-1 + \theta - \theta^2) < y \leq \tau \quad . \tag{44}$$

Now divide the positive values of α in J_2 into two disjoint sets J_{21} and J_{22}, where

$$J_{21} = \{\alpha \in J_2 : \alpha > 0 \; ; \; [\tau + y] \geq 10\} \quad ,$$

$$J_{22} = \{\alpha \in J_2 : \alpha > 0\} - J_{21} \quad .$$

For a specific value of α in J_{21} apply Lemma 9 to $S(\lambda_1 \alpha)$ with $f(u) = \lambda_1 \alpha u^{\tau}$ and $n = 1 + [\tau + y]$. For this value of n, letting $E = |\lambda_1 \tau(\tau-1) \ldots (\tau-n)/(n+1)!|$, we have for all u in (ax, 8ax], the inequalities

$$E\, a^{\theta(\tau-n+1)} x^{\theta(y+\tau-n-1)} \leq |f^{(n+1)}(u)/(n+1)!| \leq E(8a)^{\theta(\tau-n+1)} x^{\theta(y+\tau-n-1)} \quad .$$

If we put

$$1/z = E\, a^{\theta(\tau-n-1)} x^{\theta(y+\tau-n-1)} \tag{45}$$

$$c' = 8^{\theta(\tau-n-1)} \quad ,$$

then we have

(46) $$1/z \leq |f^{(n+1)}(u)/(n+1)!| \leq c'/z$$

for all u in $(ax, 8ax]$. From (45), we have

$$z = x(\theta(n + 1 - y - \tau))/E a^{\theta(\tau-n-1)}$$

$$>> x(\theta(n + 1 - y - \tau)) >> x^{\theta} ,$$

since $n + 1 - y - \tau = [\tau + y] + 2 - (\tau + y) \geq 1$. Also, $2 + 2/n > 2 \geq [\tau + y] + 2 - (\tau + y)$. Putting $P = x^{\theta}$, we obtain

(47) $$P^{2+2/n} >> z >> P .$$

So by (46) and (47), and since $n \geq 11$, we see that the hypotheses of Lemma 9 are satisfied. Therefore,

$$|S(\lambda_1 \alpha)| << P^{1-\Phi'} = x(\theta(1 - \Phi'))$$

holds for $\alpha \in J_{21}$ with $n = [\tau + y] + 1$, where

$$\Phi' = 1/3n^2 \log(125\, n) .$$

Note that as α varies over J_{21}, $y = \tau \log \alpha/\log x$ also changes. Consequently, $n = 1 + [\tau + y]$ will also change. So in order to obtain a uniform estimate for $S(\lambda_1 \alpha)$ for all α in J_{21}, we must choose the value of n which is greatest. From (44), this is seen to be $1 + [2\tau]$. Therefore, for all α in J_{21},

(48) $$|S(\lambda_1 \alpha)| << x(\theta(1 - \Phi''))$$

where

$$\Phi'' = 1/3([2\tau] + 1)^2 \log(125([2\tau] + 1)) .$$

For α in J_{22} we cannot apply the estimate of Lemma 9 to $S(\lambda_1\alpha)$, since in this case $n \leq 10$. We can apply Lemma 10, however. To do this, put $\alpha = x(\theta y)$ as before. Since α is in J_{22}, we have $[\tau + y] \leq 9$; i.e., $y < 10 - \tau$. From (44) we also have $\tau(\theta - 1 - \theta^2) < y$. So

$$1 - \tau - \theta < y < 10 - \tau \quad , \tag{49}$$

since $\theta\tau = 1$.

We apply Lemma 10 to $S(\lambda_1\alpha)$ with $n = [\tau + y] + 2$ and $f(u) = \lambda_1\alpha u^{\tau}$, and $b = [(ax)^{\theta}]$, $p = [(8ax)^{\theta}] - [(ax)^{\theta}]$.

Note that $x^{\theta}/p \asymp 1$ * for $x \geq 1$. Also, for all u in $(ax, 8ax]$, we have

$$|f^{(n)}(u)| = |\lambda_1\alpha\ \tau(\tau - 1)\ldots(\tau - n + 1)u^{\tau - n}|$$

$$\geq |\lambda_1\alpha\ \tau\ldots(\tau - n + 1)a^{1-\theta n}x^{1+\theta y-\theta n}| = \gamma \quad .$$

If we let $\Gamma = (1/p)[f^{(n-1)}(b + p) - f^{(n-1)}(b + 1)]$, then we have

$$\Gamma/\gamma \asymp 1 \tag{51}$$

by an elementary calculation. Therefore,

$$|S(\lambda_1\alpha)| << p[(\gamma/\Gamma^2)^{-1/(2^n-2)} + (\gamma p^n)^{-1/2^{n-1}}$$

$$+ (\gamma p/\Gamma)^{-1/2^{n-1}}] \quad ,$$

---

*The notation $f(t) \asymp 1$ means that there exist constants $0 < c' < c''$ such that $c' \leq |f(t)| \leq c''$.

by Lemma 10 and (50) and (51). Consequently,

$$|S(\lambda_1\alpha)| << x^{\theta}[x((1 + \theta y - \theta n)/(2^n - 2))$$

$$+ x(-(1 + \theta y)/2^{n-1})$$

$$+ x(-\theta/2^{n-1})] \quad .$$

We have by (49)

(52) $$1 + \theta y - \theta n = 1 - \theta([\tau + y] + 2 - y)$$

$$< 1 - \theta(\tau + y - 1 + 2 - y) = -\theta \quad ,$$

(53) $$1 + \theta y > \theta - \theta^2 \quad .$$

So by (52) and (53), we have

$$|S(\lambda_1\alpha)| << x^{\theta}x(-(\theta - \theta^2)/(2^n - 2)) \quad .$$

As α varies over J_{22}, $[\tau + y] + 2 = n$ also varies; and in order to obtain a uniform estimate for $S(\lambda_1\alpha)$ for all α in J_{22}, we have to find the largest value of n used to estimate $S(\lambda_1\alpha)$ by Lemma 10. This value is easily seen to be $n = 11$ by the definition of J_{22}. Therefore, for α in J_{22}, we have

(54) $$|S(\lambda_1\alpha)| << x(\theta(1 - (1 - \theta)/(2^{11} - 2))) \quad .$$

Combining (48) and (54), we have Lemma 11.

Lemma 12. $$\int_{\alpha \in J_2} F(\alpha)D(\alpha)d\alpha << x(1 + \theta - (1 - \theta)^r - \theta\Phi) \quad ,$$

where Φ is the value given in the statement of Lemma 11.

Proof. By (16),

$$\int_{\alpha \in J_2} F(\alpha)D(\alpha)d\alpha = \int_{\alpha \in J_2} P(\alpha)Q(\alpha)R(\alpha)D(\alpha)d\alpha$$

$$\leq \max_{\alpha \in J_2} |S(\lambda_1 \alpha)| \int_{\alpha \in J_2} |T(\lambda_3 \alpha)S(\lambda_2 \alpha)Q(\alpha)R(\alpha)| D(\alpha)d\alpha$$

$$\leq x(\theta(1 - \Phi))I_1 I_2 \quad ,$$

where

$$I_1 = \left(\int_{\alpha \in J_2} |T(\lambda_3 \alpha)Q(\alpha)|^2 D(\alpha)d\alpha \right)^{\frac{1}{2}} \quad ,$$

$$I_2 = \left(\int_{\alpha \in J_2} |S(\lambda_2 \alpha)R(\alpha)|^2 D(\alpha)d\alpha \right)^{\frac{1}{2}} \quad ,$$

by Lemma 11 and the Cauchy-Schwarz inequality. But by Lemma 6, we have

$$I_1, I_2 << (x(1 - (1 - \theta)^r))^{\frac{1}{2}} \quad .$$

This proves the lemma.

Proof of Theorem.

By comparing the results of Lemmas 5, 8, 12, we see that the inequality

$$|\lambda_1 k_1^{\tau} + \ldots + \lambda_s k_s^{\tau}| < 1$$

will have infinitely many solutions provided

$$1 + \theta - 2(1 - \theta)^r > \theta - (1 - \theta)^r \quad ,$$

and

$$1 + \theta - 2(1 - \theta)^r > 1 + \theta - (1 - \theta)^r - \theta\Phi \quad ,$$

or, equivalently, provided

(55) $$\theta\Phi > (1 - \theta)^r \quad ,$$

since $1 > (1 - \theta)^r$.

The problem now is to choose r a positive integer so that r is as small as possible, yet (55) holds. It is clear from the definition of Φ that

$$\Phi > 1/3(2\tau + 1)^2 \log(125(2\tau + 1))$$

$$= 1/12\tau^2 \log(250\tau)V \quad ,$$

$$V = (1 + 1/2\tau)^2 \log(125(2\tau + 1))/\log(250\tau)$$

$$> 1/108\,\tau^2 \log(250\tau) \quad ,$$

since $V < 9$ for $\tau \geq 12$. So if we choose r so that

(56) $$\theta\Phi > \theta^3/108 \log(250\tau) > (1 - \theta)^r \quad ,$$

then the theorem will hold for $s = 2r + 1$. Taking the logarithm of both sides of (56), we obtain

$$3 \log \theta - \log(108) - \log \log (250\tau) > r \log (1 - \theta) \quad ,$$

and since $\log(1 - \theta) < 0$, we have

$$r > 3\left\lceil \log \theta / \log(1 - \theta) \right\rceil (1 + o(1)) \quad \text{as} \quad \tau \to \infty,$$

since

$$(\log(108) + \log\log(250\,\tau))/3\log\theta = o(1) \quad \text{as} \quad \tau \to \infty .$$

Now

$$3\log\theta/\log(1-\theta) = 3\,\tau\log\tau(1 + O(1/\tau)) \quad \text{as} \quad \tau \to \infty .$$

So there is an absolute constant $c > 0$ such that for all $\tau > 12$, τ not equal to an integer, and for $s = 2r + 1 > c\,\tau\log\tau$, the inequality

$$|\lambda_1 k_1^{\tau} + \ldots + \lambda_s k_s^{\tau}| < 1$$

has infinitely many solutions in positive integers k_i. This proves the theorem.

PART III

In 1935 Tartakowski [14] proved that, in general, a cubic form in sufficiently many variables with coefficients in an algebraic number field K has a non-trivial zero in that field; and in the case when K is the rational field 57 variables suffices. Here, "in general" means that the coefficients of the form do not lie in a proper subvariety of the coefficient space. Hence, Tartakowski's result holds for almost all cubic forms. Later, Lewis [10] proved that if K is any algebraic number field, $[K : Q] = n$, then there exists a function $\psi(n)$ such that <u>every</u> cubic form over K in $m \geq \psi(n)$ variables has a non-trivial zero in K. His bound, $\psi(n)$, is extremely large; e.g., when K is the rational field, $\psi(1) > 500$.

The above bound was greatly reduced when Davenport [2] proved that a homogeneous, cubic form in m variables with rational coefficients always represents 0 non-trivially if $m \geq 32$. Employing the methods of [2], C. P. Ramanujam [12] showed that any homogeneous, cubic form over any algebraic number field represents 0 non-trivially in that field provided the number of variables is at least 54.

Subsequently, Davenport [3] proved that any homogeneous, cubic form in $m \geq 17$ variables over the rational field represents 0 non-trivially; and this condition was later relaxed [4] to $m \geq 16$. The

object of this section is to show that it is possible to adopt the methods of Davenport [3] and some of those of Ramanujam [12] to prove that the condition $m \geq 54$ for cubic forms over any algebraic number field can also be relaxed to $m \geq 17$.

The distinguishing feature of Davenport's paper [2] is that it marks the first time that the Hardy-Littlewood Circle Method (which was also used in [3] and [4]) was successfully applied to Diophantine equations of non-additive type. Davenport found that with the assumption that the cubic form $C(X_1, \ldots, X_m)$ did not represent 0 non-trivially and $m \geq 32$, then the number of solutions, $N(P)$, of $C(X_1, \ldots, X_m) = 0$ with X_i an integer and $|X_i| < P$ satisfies

$$N(P) = cP^{m-3} + o(P^{m-3}) \quad , \quad \text{as} \quad P \to \infty \quad , \tag{1}$$

where c is a positive constant. From (1) he deduced that $C(X)$ does indeed represent 0 non-trivially; so that the original assumption that $C(X)$ does not represent 0 non-trivially is false. Thus, Davenport showed that $C(X)$ did represent 0 non-trivially if $m \geq 32$, although the asymtotic formula (1) was not valid.

The same logical structure is employed by Davenport in [4] and by Ramanujam in [12] and by myself in this paper. I also use the same general line of proof in this section as that which is used in [3] and [12]. The changes I have made consist of (1) appropriately modifying the arguments of [3] to suit the number field case; (2) expanding some of the lemmas of [12]; and (3) adding some lemmas and remarks of my own to make the proof clear.

The question is still open as to whether or not the methods used by Davenport in [4] to obtain the bound 16 can be modified to prove the same result for the number field case. This would require, among other things, the extension of certain results in the geometry of numbers over the rational integers to similar results over algebraic number fields. Only partial results have been obtained in this direction so far.

Finally, it has been shown that there exist cubic forms in nine variables which do not represent 0 non-trivially (See [3], page 108). On the other hand, Lewis has shown that every cubic form in ten or more variables with coefficients in an algebraic number field K possesses a non-trivial zero in $K_{\mathfrak{p}}$ for every prime $\mathfrak{p}$ of K. It appears likely, then, that any cubic form over any algebraic number field in $m \geq 10$ variables has a non-trivial zero in that field. No counter example to this conjecture has been found as yet, while the results of Davenport [4] and of this section are the best that are known in this direction.

We prove:

Theorem. Let K be an algebraic number field and $\mathcal{O}_K$ its ring of integers. Let $C(X) = \sum_{1 \leq i,j,k \leq m} c_{ijk} X_i X_j X_k$ be a homogeneous, cubic form with coefficients in $\mathcal{O}_K$. Then $C(X)$ represents 0 non-trivially in $\mathcal{O}_K$ provided $m \geq 17$.

If $C(X)$ is degenerate over K, then one can easily prove that $C(X)$ represents 0 non-trivially in $(\mathcal{O}_K)^m$, the m-th Cartesian

product of $\mathcal{O}_K$. So without loss of generality it may be assumed that $C(X)$ is non-degenerate over K.

The proof of the theorem will be accomplished in the next five divisions.

1. Notation

Q, R, C will denote the rational, real, and complex fields, respectively; K will denote an algebraic number field over Q with $[K : Q] = n$; and $\mathcal{Z}$ will denote the rational integers.

Put $\delta^{-1} = \{ \xi \in K \mid S(\lambda \xi) \in \mathcal{Z} \text{ for all } \lambda \in \mathcal{O}_K \}$, so that δ is the different (it is an integral ideal) of K. Let $\{ \omega_1, \ldots, \omega_n \}$ be an integral basis of K, and let $\{ \rho_1, \ldots, \rho_n \}$ denote the dual basis of δ^{-1}, determined uniquely by $S(\omega_i \rho_j) = \delta_{ij}$.

Let K_R denote the n-dimensional commutative algebra $R \otimes_Q K$ over R; i.e., the scalar extension of K to a module over R. If we identify an element $x \in K$ with $1 \otimes X$ of K_R, then $\{ \omega_1, \ldots, \omega_n \}$ is a basis of K_R over R; and for any $y \in K_R$ we can write $y = \sum_{1 \le i \le n} y_i \omega_i$, where $y_i \in R$. For any $y \in K_R$, $S(y)$ and $N(y)$ will denote the trace and norm, respectively, of y over R.

Define a box $B = B(a_1, b_1, \ldots, a_n, b_n)$ in K_R as the set $\{ y \in K_R \mid a_i \le y_i < b_i, \ 1 \le i \le n \}$, where the a_i, b_i are real numbers such that $0 < b_i - a_i \le 1$. B_0 will denote the box $\{ y \in K_R \mid -1 \le y_i < 1 \}$. $(K_R)^m$ will be the m-th Cartesian product

of K_R, considered as an mn-dimensional space over R. $\mathcal{B}$ will denote the Cartesian product of the $B_1, \ldots, B_m$; i.e., $\mathcal{B} = B_1 \times B_2 \times \ldots \times B_m$, a box in $(K_R)^m$. $\mathcal{B}_0$ is the special box $B_0 \times \ldots \times B_0$ in $(K_R)^m$.

For real t, we let $e(t) = e^{2\pi i t}$; and let $\|t\|$ be the distance of t to the nearest integer.

2. General Cubic Exponential Sums

Let $G(X) = \sum_{1 \le i,j,k \le m} g_{ijk} X_i X_j X_k$ be a cubic form with coefficients g_{ijk} in K_R which are symmetric in all three indices. With $G(X)$ we associate the bilinear form $B_j(X,Y) = \sum_{1 \le i,k \le m} g_{ijk} X_i Y_k$, which is defined on $(K_R)^{2m}$ with values in K_R. We also put $B_j(X,Y) = \sum_{p=1}^{n} \lambda_{jp}(X,Y)\rho_p$, where the λ_{jp} are bilinear forms defined on $(K_R)^{2m}$ with values in R. Finally, unless otherwise stated, all sums will be over integral $X = (X_1, \ldots, X_m)$, $X_i = \sum_{1 \le j \le n} X_{ij}\omega_j$, with X_{ij} in $\mathcal{Z}$.

Lemma 2.1. For $P > 1$, let $T = T(P, \mathcal{B}) = \sum_{X \in P\mathcal{B}} e(S(G(X)))$, where $\mathcal{B}$ is a box in $(K_R)^m$ and $P\mathcal{B}$ is the box obtained from it by enlarging each side by the factor P. Then we have the estimate

$$|T|^4 << P^{mn} \sum_{X, Y \in P\mathcal{B}_0} \prod_{1 \le j \le m} \prod_{1 \le p \le n} \min(P, \|6\lambda_{jp}\|^{-1}).$$

Proof. $$|T|^2 = \sum_{Z \in P\mathcal{B}} \sum_{Z' \in P\mathcal{B}} e(S(G(Z) - G(Z')))$$

$$= \sum_{Z' \in P\mathcal{B}} \sum_{Y \in P\mathcal{B} - Z'} e(S(G(Z' + Y) - G(Z')))$$

$$\leq \sum_{Y \in P\mathcal{B}_0} \left| \sum_{Z' \in \mathcal{R}(Y)} e(S(G(Z' + Y) - G(Z'))) \right| ,$$

where $\mathcal{R}(Y)$ is the common part of the boxes $P\mathcal{B}$ and $P\mathcal{B} - Y$, and is itself a box. Similarly, the square of the inner sum does not exceed

$$\sum_{X \in P\mathcal{B}_0} \left| \sum_{Z \in \mathcal{R}(X,Y)} e(S(G(Z+X+Y) - G(Z+X) - G(Z+Y) + G(Z))) \right|$$

where we have denoted the common part of the boxes $\mathcal{R}(Y)$ and $\mathcal{R}(Y) - X$ by $\mathcal{R}(X, Y)$. Now we have

$$G(Z + Y + X) - G(Z + Y) - G(Z + X) + G(X)$$

$$= 6 \sum_{1 \leq i,j,k \leq m} g_{ijk} X_i Y_j Z_k + \Theta$$

$$= 6 \sum_{1 \leq j \leq m} B_j(X, Y) Z_j + \Theta$$

$$= 6 \sum_{1 \leq j \leq m} \sum_{1 \leq p, \ell \leq n} \lambda_{jp}(X, Y) Z_{j\ell} \rho_p \omega_\ell + \Theta ,$$

where Θ is independent of Z and where we have put $Z_j = \sum_{1 \leq \ell \leq n} Z_{j\ell} \omega_\ell$. Since Z is in a box with edges not exceeding P in length, we can apply the inequality

(1) $$\left| \sum_t e(\lambda t) \right| << \min(P, \|\lambda\|^{-1}) ,$$

where the summation is over any set of $<< P$ consecutive integers.

As $S(\rho_p \omega_\ell) = \delta_{p\ell}$, we have

$$\Big| \sum_{Z \in \mathcal{R}(X,Y)} e(S(6 \sum_{1 \le j \le m} B_j(X,Y) Z_j + \Theta)) \Big|$$

$$= \Big| \sum_{Z \in \mathcal{R}(X,Y)} e(6 \sum_{1 \le j \le m} \sum_{1 \le p \le n} \lambda_{jp} Z_{jp}) \Big|$$

$$<< \prod_{1 \le j \le m} \prod_{1 \le p \le n} \min(P, \| 6\lambda_{jp} \|^{-1})$$

by (1). So

$$|T|^4 \le \Big(\sum_{Y \in P\mathcal{B}_0} \Big| \sum_{Z \in \mathcal{R}(Y)} e(S(G(Z+Y) - G(Z))) \Big| \Big)^2$$

$$\le P^{mn} \sum_{Y \in P\mathcal{B}_0} \sum_{Z \in \mathcal{R}(Y)} e(S(G(Z+Y) - G(Z)))\Big|^2$$

by Hölders inequality. Therefore,

$$|T|^4 << P^{mn} \sum_{X,Y \in P\mathcal{B}_0} \prod_{1 \le j \le m} \prod_{1 \le i \le n} \min(P, \| 6\lambda_{jp} \|^{-1})$$

by (2).

Q.E.D.

Lemma 2.2. Assume that $|T| \ge P^{n(m-\kappa)}$ for $0 < \kappa < m$. Let N_1 denote the number of distinct pairs of integral points (X,Y) in $P\mathcal{B}_0$ satisfying $\| 6\lambda_{jp} \| < P^{-1}$ for $1 \le j \le m$, $1 \le p \le n$. Then $N_1 >> (P^{2m-4\kappa} \log^{-m} P)^n$.

Proof. See [13], Lemma 1.2, page 684.

Lemma 2.3. With the assumption of Lemma 2.2, let N_2 denote the number of distinct pairs of integral points $X, Y \in P\mathcal{B}_0$ satisfying $\|6\lambda_{jp}\| < P^{-3+2\theta}$, where $0 < \theta < 1$ is fixed. Then $N_2 >> (P^{2m\theta-4\kappa} \log^{-m} P)^n$.

Proof. See [13], Lemma 1.3, page 685.

Henceforth, $\mathcal{S}(G)$ will denote the set of integral pairs (X, Y) satisfying the conditions of Lemma 2.3 ; and $N_2 = |\mathcal{S}(G)|$.

3. Special Cubic Exponential Sums

We now apply Lemma 2.3 to the particular cubic form

$$G(X) = \sum_{1 \le i,j,k \le m} \alpha c_{ijk} X_i X_j X_k \quad , \tag{3}$$

where $\alpha = \sum_{1 \le i \le n} \alpha_i \rho_i$ and c_{ijk} is in $\mathcal{O}_K$, and α, c_{ijk} are considered in K_R .

Lemma 3.1. Let $0 < \theta < 1$, where θ is independent of P, and let $G(X)$ be the form (3). Then for any fixed $\varepsilon > 0$, there is a $P(\varepsilon)$ such that for all $P > P(\varepsilon)$,

Either (A) There are more than $P^{mn\theta+\varepsilon}$ pairs of integral points X, Y in P_0 satisfying $B_j(X, Y) = 0$, $1 \le j \le m$;

Or (B) The hypothesis $|T| \ge P^{n(m-\frac{m\theta}{4}+\varepsilon)}$ implies there exists a non-zero integer μ in $\mathcal{O}_K$

and a ν in δ^{-1} such that

$$\mu\alpha - \nu = \sum_{1\le i\le n} \beta_i \rho_i \quad , \tag{4}$$

$$\beta_i \in R \quad , \quad |\beta_i| < P^{-3+2\theta} \quad , \tag{5}$$

$$\mu \in P^{2\theta+\varepsilon}\mathcal{B}_0 \quad . \tag{6}$$

Proof. Apply Lemma 2.3 to $G(X)$ with $\kappa = m\theta/4 - \varepsilon$, where ε is chosen very small compared with $m\theta/4$. Then we have

$$6\alpha B_j(X,Y) = 6\sum_{1\le p\le n} \lambda_{jp}\rho_p \quad ,$$

where $\|6\lambda_{jp}\| < P^{-3+2\theta}$. Now if for all integral X, Y in $\mathcal{L}(G)$ and for all j, $1 \le j \le m$, we have $B_j(X,Y) = 0$, then we have Alternative (A). Otherwise, the hypothesis $|T| \ge P^{n(m-m\theta/4+\varepsilon)}$ implies that for some j, $1 \le j \le m$, and for some pair X, Y in $\mathcal{L}(G)$, we have

$$6\alpha B_j(X,Y) = \sum_{1\le p\le n} 6\lambda_{jp}\rho_p$$

$$= \sum_{1\le p\le n} r_p\rho_p + \sum_{1\le p\le n} 6\lambda'_{jp}\rho_p \quad ,$$

where r_j is in $\mathcal{Z}$ and $|6\lambda'_{jp}| < P^{-3+2\theta}$ and $B_j(X,Y) \neq 0$. Therefore, choosing $\mu = 6B_j(X,Y)$ and $\nu = \sum_{1\le p\le n} r_p\rho_p$, and noticing that B_j is in $P^{2\theta+\varepsilon}B_0$, we have (4), (5), (6) satisfied.

It should be noted that Lemma 3.1 holds for any fixed $\varepsilon > 0$ and all $P > P(\varepsilon)$. Henceforth, in any application of Lemma 3.1,

it will be assumed that $P > P(\varepsilon)$, although this will not be explicitly stated.

4. Alternative (A)

In this section it will be shown that Alternative (A) of Lemma 3.1 implies that $C(X)$ represents 0 non-trivially in $(\mathcal{O}_K)^m$.

We prove:

Lemma 4.1. Let ε be any fixed, positive number. Assume that for some arbitrarily large $\Gamma > 0$ there exist more than $\Gamma^{mn+\varepsilon}$ distinct pairs X, Y of integral points in $(\mathcal{O}_K)^m$ such that $0 < |X|, |Y| < \Gamma$, $B_j(X,Y) = 0$ for $1 \leq j \leq m$, where $0 < |X| < \Gamma$ means that $0 < |X_{ij}| < \Gamma$, $X_i = \sum_{1 \leq j \leq n} X_{ij} \omega_j$, $X_{ij} \in \mathcal{J}$, $X = (X_1, \ldots, X_m)$. Then $C(X)$ represents 0 non-trivially in $\mathcal{O}_K$.

Proof. The proof of Lemma 4.1 follows the proof of Alternative (A) in the case of a cubic form over Q very closely. Such a proof is given in [3], Section 14, where the key lemma in that argument is Lemma 35. Certain portions of Lemma 35 in this proof are unclear, however, so the proof of Lemma 35 in the case of a cubic form over K will be proved in detail for these portions.

Lemma 35. Let $f_1(X), \ldots, f_N(X)$ be forms with coefficients in $\mathcal{O}_K$, defined on $(\mathcal{O}_K)^m$. Suppose that N and the

degrees of $f_1, \ldots, f_N$ are bounded in terms of m. Suppose that for some arbitrarily large Γ, there is a set, $\underline{X}$, of integral points X in $(\mathcal{O}_K)^m$ such that $0 < |X| < \Gamma$, and $f_1(X) = 0, \ldots, f_N(X) = 0$. If there are more than $\Gamma^{n(m-r+\varepsilon)}$ points in $\underline{X}$, then for one of them, there exist complex numbers $T_{i\rho}$, $D_{\rho\nu}$ such that

$$\frac{\partial f_i}{\partial X_\nu} = \sum_{1 \le \rho \le r-1} T_{i\rho} D_{\rho\nu}, \quad 1 \le i \le N, \quad 1 \le \nu \le m,$$

at that point.

Proof. The equations $f_1(X) = 0, \ldots, f_N(X) = 0$ define an algebraic set in $(C)^m$. Such an algebraic set is expressible as a union of varieties, the number of which is bounded in terms of m under the present hypotheses. (Proof by elimination theory. See van der Waerden, Algebraische Geometrie, 1939, Section 31.) Hence there is one such variety, V, which contains more than $\Gamma^{n(m-r+\varepsilon/2)}$ points of $\underline{X}$. Let $\alpha = (t_1, \ldots, t_m)$ be a generic point of V and let s be its dimension; i.e., $s = [K(t_1, \ldots, t_m) : K]_{tr}$. By relabeling, if necessary, we can suppose that $t_1, \ldots, t_s$ are independent variables and $t_{s+1}, \ldots, t_m$ are algebraic functions of them. It follows that V contains $\ll \Gamma^{ns}$ integral points X satisfying $|X| < \Gamma$, since there are $\ll \Gamma^n$ possibilities for each of the s coordinates. Comparison with the earlier statement about the number of points of $\underline{X}$ on V shows that $s \ge m - r + 1$.

Since $t_{s+1}, \ldots, t_m$ are algebraically dependent on $t_1, \ldots, t_s$, then for each i, $s+1 \leq i \leq m$, there are non-zero polynomials g for which $g(t_1, \ldots, t_s, t_i) = 0$. Among all such polynomials, for each i, $s+1 \leq i \leq m$, choose $g_i(t_1, \ldots, t_s, t_i)$ so that the degree of g_i in the variable t_i is minimal and non-zero. (Note that there has been an abuse of notation in defining the polynomials g_i. We wish to consider each g_i, $s+1 \leq i \leq m$, as a polynomial in m variables, although the notation $g_i = g_i(t_1, \ldots, t_s, t_i)$ would indicate that each g_i is a polynomial in only $s+1$ variables. So we will consider each g_i, $s+1 \leq i \leq m$, as a polynomial in m variables, where the coefficients of any term involving t_j, j not in $\{1, \ldots, s, i\}$ is zero, and we write as before $g_i = g_i(t_1, \ldots, t_s, t_i)$.)

Let $\mathcal{a} = \{X \in (C)^m \mid g_i(X) = 0, \quad 1 + s \leq i \leq m\}$. Clearly, $\alpha \in V \subseteq \mathcal{a}$. Let W be the variety on $\mathcal{a}$ which contains V and let $u = (u_1, \ldots, u_m)$ be a generic point of W. Now, $\dim W \geq s$, since $[K(u_1, \ldots, u_m) : K]_{tr} \geq [K(t_1, \ldots, t_m) : K]_{tr}$. Furthermore, if $\dim W > s$, say, $\dim W = s+1$, then we can select $u_1, \ldots, u_{s+1}$ as independent variables, relabeling if necessary, and the remaining u_j as algebraic functions of them. Since $u \in W \subseteq \mathcal{a}$, $g_{s+1}(u_1, \ldots, u_{s+1}) = 0$. But this contradicts the assumption that $u_1, \ldots, u_{s+1}$ are algebraically independent, since the degree of g_{s+1} in u_{s+1} is non-zero. Therefore, $\dim W = s$; and $V = W$.

Now put $a_i = \{ X \in (C)^m \mid \frac{\partial g_i(X)}{\partial t_i} = 0 \}$, $s+1 \leq i \leq m$.

Certainly, the generic point of V, α, is not on a_{s+1} by the choice of g_{s+1}. Therefore, $V \cap a_{s+1}$ has dimension $\leq s-1$; and so $V \cap (a_{s+1} \cup \ldots \cup a_m)$ has dimension $\leq s-1$. We conclude that the set of points X on V which satisfy $\prod_{s+1 \leq i \leq m} \frac{\partial g_i(X)}{\partial t_i} = 0$ has dimension $\leq s-1$.

By the Implicit Function Theorem, applied to $g_{s+1}, \ldots, g_m$, the $t_{s+1}, \ldots, t_m$ can be expressed as differentiable functions of $t_1, \ldots, t_s$ in some neighborhood of a point X in $(C)^m$ provided

$$\det \left(\frac{\partial g_i(X)}{\partial t_i}\right) = \prod_{s+1 \leq i \leq m} \frac{\partial g_i(X)}{\partial t_i} \neq 0 \quad .$$

Now if $s = m - r + 1$, then $s - 1 = m - r$. Since the number of points of $\underline{X}$ on V is $\Gamma^{n(m-r+\varepsilon/2}$, there is a point X_0 of $\underline{X}$ on V such that X_0 is not on $\bigcup_{s+1 \leq i \leq m} a_i$; and so X_0 satisfies

$$\prod_{s+1 \leq i \leq m} \frac{\partial g_i(X_0)}{\partial t_i} \neq 0 \quad .$$

Therefore, there is a neighborhood of X_0 in V for which $X_1, \ldots, X_s$ are independent variables and $X_{s+1}, \ldots, X_m$ are single-valued, differentiable functions of them.

The same conclusion holds if $s > m - r + 1$ and if there is an X in $\underline{X}$ which lies on V and not on $\bigcup_{s+1 \leq i \leq m} a_i$.

It may be, however, if $s > m - r + 1$, that all of the points X in $\underline{X}$ which lie on V also lie on $\bigcup_{s+1 \leq i \leq m} a_i$. In this event, the hypothesis of the Implicit Function Theorem would not hold for any X in $\underline{X}$ and X in V.

In order to overcome this difficulty we consider the algebraic set

$$\left\{ X \in (C)^m \mid f_1(X) = 0, \ldots, f_N(X) = 0 ; \frac{\partial g_{s+1}(X)}{\partial t_{s+1}} = 0 \right\} .$$

As before (by van der Waerden), we know that the above set can be decomposed into a union of varieties, the number of which is bounded in terms of m. There is one such variety, V_1, which contains more than $\Gamma^{n(m-r+\varepsilon/2)}$ points of $\underline{X}$; and the dim $V_1 = s_1 \leq s - 1$ by what we have shown before. Let $\alpha = (t_1, \ldots, t_m)$ be a generic point of V_1 (where we use the same notation as before without loss of clarity). By relabeling, if necessary, we can conclude that $t_1, \ldots, t_{s_1}$ are independent variables and $t_{s_1+1}, \ldots, t_m$ are algebraically dependent on them. We obtain $s_1 \geq m - r + 1$ by the same counting argument as before. As before, we can also choose $m - s_1$ non-zero polynomials $h_i(t) = h_i(t_1, \ldots, t_{s_1}, t_i)$, $s_1 + 1 \leq i \leq m$, for which the coefficient of the highest power of t_i is a polynomial in $t_1, \ldots, t_{s_1}$ with coefficients in C such that the degree of g_i in t_i is minimal and non-zero.

If there is a point $X_0 \in \underline{X}$ on V_1 such that

$$\overline{\prod_{s_1+1 \le i \le m}} \frac{\partial h_i(X_0)}{\partial t_i} \neq 0 \quad \text{(which must be so if } s_1 - 1 = m - r + 1\text{)},$$

then there is a neighborhood of X_0 in V such that $X_1, \ldots, X_{s_1+1}$ are independent variables and $X_{s_1+1}, \ldots, X_m$ are single-valued, differentiable functions of them. And if there is no such point, then we must have $s_1 > m - r + 1$. We then repeat the argument, beginning next with the algebraic set

$$\left\{ X \in (C)^m \mid f_1(X) = 0, \ldots, f_N(X) = 0 \; ; \; \frac{\partial g_{s+1}}{\partial X_{s+1}} = 0 \; ; \; \frac{\partial h_{s_1+1}}{\partial t_{s_1+1}}(X) = 0 \right\} .$$

Eventually (and the number of steps is $\le m$), we will obtain a variety U, with generic point $(t_1, \ldots, t_u, \ldots, t_m)$, contained in V which is in

$$\left\{ X \in (C)^m \mid f_1(X) = 0, \ldots, f_N(X) = 0 \right\} ,$$

and a point X_0 in $\underline{X}$ such that X_0 is in U. Furthermore, there will be a neighborhood of X_0 on U such that $X_1, \ldots, X_u$ are independent variables and $X_{u+1}, \ldots, X_m$ are single-valued, differentiable functions of them.

The remainder of the proof follows that of Lemma 35 in the case of forms over Ω practically verbatim.

This proves Lemma 4.1.

5. Alternative (B)

Henceforth, it will be assumed that Alternative (B) holds; i.e., the assumption that $|T(\alpha)| \geq P^{n(m-m\theta/4+\varepsilon)}$ implies that there is an $\mu \neq 0$, $\mu \in \mathcal{O}_K$, and a $\nu \in \delta^{-1}$ satisfying (4), (5), and (6), where

$$T(\alpha) = \sum_{X \in P\mathcal{B}} e(s(\alpha C(X))) \quad , \quad \alpha = \sum_{1 \leq i \leq n} \alpha_i \rho_i, \ \alpha_i \in R \quad .$$

For the remainder of this section, we let

$$\mathcal{R} = \{ \alpha \in K_R \mid 0 < \alpha_i \leq 1 \ ; \quad \alpha = \sum_{1 \leq i \leq n} \alpha_i \rho_i \} \quad . \tag{7}$$

If $N(P)$ denotes the number of solutions of $C(X) = 0$, with $X \in P\mathcal{B}$, we have

$$N(P) = \int T(\alpha) d\alpha \quad , \quad d\alpha = d\alpha_1 \, d\alpha_2 \ldots d\alpha_n \quad . \tag{8}$$

For $\gamma \in K$, let $a(\gamma)$ denote the denominator of the ideal $(\gamma)\delta$; i.e., $a(\gamma)$ is the integral ideal equal to $[(1), (\gamma)\delta)]^{-1}$. For those $\gamma \in K$ which satisfy $\text{Norm}(a(\gamma)) = N(a(\gamma)) \leq P^{2\theta}$, and for any θ such that $0 < \theta < 1$, we let

$$B(\gamma) = B(\gamma, \theta) = \{ \alpha \in K_R \mid \alpha - \gamma = \sum_{1 \leq i \leq n} \beta_i \rho_i \ ; \ |\beta_i| < P^{-3+2\theta} \frac{1}{N(a(\gamma))} \} \tag{9}$$

We define the union of the major arcs to be

$$\mathcal{M} = \bigcup_{\substack{\gamma \,(\text{mod } \delta^{-1}) \\ N(a(\gamma)) \leq P^{2\theta}}} B(\gamma) \tag{10}$$

where θ will be specified later. The totality of minor arcs is denoted by

(11) $$\underline{m} = \mathfrak{R} - \mathfrak{m} \quad ,$$

where $\mathfrak{R}$ is given in (7).

It will now be shown that with a suitable choice of the box $\mathcal{B}$, and under the assumption that $C(X)$ does not represent 0 non-trivially in $(\mathcal{O}_K)^m$, then for $m \geq 17$, we have the asymtotic expression

(12) $$N(P) = J \cdot \mathfrak{S} \cdot P^{n(m-3)} + o(P^{n(m-3)})$$

as $P \to \infty$, where $\mathfrak{S}$ and J are positive constants. But for P sufficiently large we see that (12) implies that $N(P) > 1$, which contradicts the assumption that $C(X)$ represents 0 non-trivially. Thus, the assumption is false, so $C(X)$ does in fact represent 0 non-trivially. Moreover, the expression (12) is not valid as it was derived from a false premise.

Lemma 5.1. Let $L_k(t) = \sum_{1 \leq i \leq n} r_{ik} t_i$ be n linear forms in n variables with r_{ik} in R. To every real $d > 1$, there is an integral $t_0 \neq 0$ such that $\| L_k(t_0) \| < d^{-1}$ and $|t_{i0}| \leq d$ for $1 \leq i,k \leq n$, where $t_0 = t_{10}, t_{20}, \ldots, t_{n0})$.

Proof. See [1], Theorem VI, page 13.

For $0 < \theta < 1$, define

(13) $$(\theta) = \{\alpha \in K_R \mid \mu\alpha - \nu = \sum_{1 \leq i \leq n} \beta_i \rho_i, \ |\beta_i| < P^{-3+2\theta}\} \quad ,$$

where $\nu \in \delta^{-1}$ and μ is any non-zero element of $\mathcal{O}_K$ such that $\mu \in P^{2\theta+\varepsilon}B_0$.

Lemma 5.2. $\mathcal{R} \subseteq \mathcal{R}(3/4 + \varepsilon)$ for any $\varepsilon > 0$.

Proof. Put $\mu = \sum_{1\le i\le n} u_i\omega_i$, $\omega_i\rho_j = \sum_{1\le k\le n} A_{ijk}\rho_k$. Then

$$\mu\alpha = \sum_{1\le i,\, j\le n} u_i\alpha_j\omega_i\rho_j$$

$$= \sum_{1\le k\le n}\Big[\sum_{1\le i,\, j\le n} A_{ijk}u_i\alpha_j\Big]\rho_k$$

$$= \sum_{1\le k\le n}\Big[\sum_{1\le i\le n} r_{ik}u_i\Big]\rho_k ,$$

where we have put $r_{ik} = \sum_{1\le j\le n} A_{ijk}\alpha_j$. Now apply Lemma 5.1 to the forms $L_k(u) = \sum_{1\le i\le n} r_{ik}u_i$ with $d = P^{-3/2}$. We conclude that there is a $(u_{10}, \ldots, u_{n0}) \neq (0, \ldots, 0)$ such that for all k, $1 \le k \le n$, we have $\| \sum_{1\le i\le n} r_{ik}u_{i0}\| < P^{-3/2}$ and $|u_{i0}| < P^{3/2}$. Now choose $\nu = \sum_{1\le k\le n} v_k\rho_k$, where v_k is the nearest integer to $\sum_{1\le i\le n} r_{ik}u_{i0}$. Then, for any α in $\mathcal{R}$, there is a non-zero μ in $\mathcal{O}_K$ (here, $\mu = \sum_{1\le i\le n} u_{i0}\omega_i$) and a ν in δ^{-1} (here, $\nu = \sum_{1\le i\le n} v_k\rho_k$) such that

$$\mu\alpha - \nu = \sum_{1\le i\le n} \beta_i\rho_i ,$$

where $|\beta_i| < P^{-3/2}$. Therefore, α is in $\mathcal{R}(3/4 + \varepsilon)$ for any

$\varepsilon > 0$ by the definition of $\mathcal{R}(\theta)$ given in (13). Since α in $\mathcal{R}$ was arbitrary, this implies that $\mathcal{R} \subseteq \mathcal{R}(3/4 + \varepsilon)$.

Q.E.D.

Lemma 5.3. $\left| \int_{\underline{m}} T(\alpha)d\alpha \right| = o(P^{n(m-3)})$ as $P \to \infty$

provided $m \geq 17$.

Proof. We fix the major arcs from now on by choosing $\theta = 1/2(n+6)$. Also put $\sigma = \theta/3$. For this choice of σ, we will show that $\mathcal{R}(\sigma) \subseteq \mathcal{M}$. To see this, let $\alpha \in \mathcal{R}(\sigma)$. By (13), there is a non-zero μ in $\mathcal{O}_K$ and a ν in δ^{-1} such that $\mu \in P^{2\sigma+\varepsilon}$ and

$$\mu\alpha - \nu = \sum_{1 \leq i \leq n} \beta_i \rho_i \quad ,$$

with $|\beta_i| < P^{-3+2\sigma}$. Dividing by μ and putting $\gamma = \nu/\mu$, the last equation becomes

$$\alpha - \gamma = \sum_{1 \leq i \leq n} (\beta_i/\mu)\rho_i$$

$$= \sum_{1 \leq i \leq n} \beta_i' \rho_i \quad ,$$

where

$$|\beta_i'| < P^{-3+2\sigma}/|\mu|$$

$$<< P^{-3+2\theta/3}$$

$$< P^{-3+2\theta}/N(a(\gamma)) \quad ,$$

since $N(a(\gamma)) = N((\mu)) \leq P^{2\theta/3+\varepsilon}$ for any $\varepsilon > 0$. Hence, α is in $\mathcal{M}$ by definition. Since α in $\mathcal{R}(\sigma)$ was arbitrary, we have $\mathcal{R}(\sigma) \subseteq \mathcal{M}$.

By Lemma 5.2, for any small, but fixed, $\varepsilon > 0$, we have $\mathcal{R} \subseteq \mathcal{R}(\sigma_h)$, where $\sigma_h = 3/4+ \varepsilon$. Therefore, $\mathcal{R}(\sigma_h) - \mathcal{R}(\sigma) \supseteq \mathcal{R} - \mathcal{M} = \underline{m}$. Choose a sequence of positive numbers $\sigma = \sigma_0 < \sigma_1 < \ldots < \sigma_h$ so that $4(\sigma_j - \sigma_{j-1}) - \sigma_{j-1}/4 + \varepsilon < 0$ for $1 \leq j \leq h$. Such a choice of σ_j, $0 \leq j \leq h$ can clearly be made, where the number h is independent of P.

Put

$$\mathcal{R}(\sigma_h) - \mathcal{R}(\sigma_0) = \bigcup_{1 \leq j \leq h} \{\mathcal{R}(\sigma_j) - \mathcal{R}(\sigma_{j-1})\},$$

where the union is meant in the sense of set theory. On the set $\mathcal{R}(\sigma_j) - \mathcal{R}(\sigma_{j-1})$, we have the estimate

$$|T(\alpha)| < P^{n(m-m\sigma_{j-1}/4+\varepsilon)},$$

since we have assumed that Alternative (B) holds. The measure of $\mathcal{R}(\sigma_j) - \mathcal{R}(\sigma_{j-1})$ does not exceed the measure of $\mathcal{R}(\sigma_j)$, which is bounded by a constant factor times $P^{n(-3+4\sigma_j+\varepsilon)}$. Therefore,

$$\left| \int_{\underline{m}} T(\alpha) d\alpha \right| << \sum_{1 \leq j \leq h} P^{n(m-3-m\sigma_{j-1}/4+4\sigma_j+\varepsilon)}$$

$$= o(P^{n(m-3)}).$$

as $P \to \infty$, since $m \geq 17$ and since we have

$$-m\sigma_{j-1}/4 + 4\sigma_j + \varepsilon < 0 \quad .$$

Q.E.D.

We now turn to the integral of $T(\alpha)$ over $\mathfrak{M}$, the major arcs. We will enlarge them from

$$\bigcup_{\substack{\gamma \,(\mathrm{mod}\ \delta^{-1}) \\ N(a(\gamma)) \leq P^{2\theta}}} B(\gamma) \qquad \text{to} \qquad \bigcup_{\substack{\gamma \,(\mathrm{mod}\ \delta^{-1}) \\ N(a(\gamma)) \leq P^{2\theta}}} \underline{B(\gamma)} \quad ,$$

where

$$\underline{B(\gamma)} = \left\{ \alpha \in K_R \;\middle|\; \alpha - \gamma = \sum_{1 \leq i \leq n} \beta_i \rho_i \;,\; |\beta_i| < P^{-3+2\theta} \right\} \quad .$$

This enlargement is justified since the contribution made by the increment to $\int T(\alpha)d\alpha$ is already covered by the estimate in Lemma 5.3.

In order to simplify notation, put

$$\tau = P^{\Delta} \;,\; \Delta = 2\theta \quad . \tag{15}$$

Henceforth, denote the enlarged major arcs by $\underline{\mathfrak{M}}$.

Lemma 5.4. $\int_{\underline{\mathfrak{M}}} T(\alpha)d\alpha = \mathfrak{S}(\tau)J(\tau)P^{n(m-3)} + o(P^{n(m-3)})$ as $P \to \infty$ for $m \geq 17$, where

$$J(\tau) = \int_{|\beta| < \tau} \int_{\mathfrak{B}} e(S(\beta C(\xi)))d\xi \, d\beta \quad ,$$

$$\mathfrak{S}(\tau) = \sum_{Na \leq \tau} \sum_{\substack{\gamma \,(\mathrm{mod}\ \delta^{-1}) \\ a(\gamma) = a}} N^{-mn} S_{\gamma} \;, \text{ and}$$

$$N = N(a(\gamma)), \quad S_\gamma = \sum_{Z (\mathrm{mod}\ N)} e(S(\gamma C(Z))) \quad .$$

Proof. We use $\sum_{Z (\mathrm{mod}\ N)}$ to denote $\sum_{Z_{ij} (\mathrm{mod}\ N)}$ for $1 \le i \le m$, $1 \le j \le n$, where $Z = (Z_1, \ldots, Z_m)$ and $Z_i = \sum_{1 \le j \le m} Z_{ij} \omega_j$. We also put $|\beta| < \tau$ in place of $|\beta_i| < \tau$ for $1 \le i \le n$ and $d\beta = d\beta_1 \ldots d\beta_n$.

The contribution of the enlarged major arcs to $\int_{\mathcal{R}} T(\alpha) d\alpha$ is

$$\sum_{Na \le \tau} \sum_{\substack{\gamma (\mathrm{mod}\ \delta^{-1}) \\ a(\gamma) = a}} \underline{I(\gamma)} \quad ,$$

where

$$\underline{I(\gamma)} = \int_{\underline{B(\gamma)}} T(\alpha) d\alpha \quad .^*$$

For α in $\underline{B(\gamma)}$, put $\alpha = \beta + \gamma$, where $\beta = \sum_{1 \le i \le n} \beta_i \rho_i$, $|\beta_i| < P^{-3+\Delta}$. We have

$$T(\alpha) = \sum_{X \in P\mathcal{B}} e(S(\alpha C(X)))$$

$$= \sum_{Z (\mathrm{mod}\ N)} \sum_{Y} e(S((\beta+\gamma) C(NY + Z))) \quad ,$$

where $N = N(a(\gamma))$. Therefore,

---

*Note that if $\gamma_1 \equiv \gamma_2 \pmod{\delta^{-1}}$, then $\underline{I(\gamma_1)} = \underline{I(\gamma_2)}$.

$$T(\alpha) = \sum_{Z (\mathrm{mod}\, N)} e(S(\gamma C(Z))) \sum_{Y} e(S(\beta C(NY + Z))) \quad ,$$

where the summation in Y is over integral points Y such that $NY + Z$ is in $P\mathcal{B}$. We now estimate the difference between

$$\sum_{Y} e(S(\beta C(NY + Z))) \quad \text{and} \quad \int_{\eta} e(S(\beta C(N\eta + Z)))\, d\eta$$

where the limits of integration on $\eta = (\eta_1, \ldots, \eta_m)$, $\eta_i = \sum_{1 \le j \le n} \eta_{ij} \omega_j$, are such that $N\eta + Z \in P\mathcal{B}$.

Put

$$h(\eta) = e(S(\beta C(N\eta + Z))) \quad ,$$

(where the h here is not to be confused with the h used before). Clearly, $h(\eta)$ is an entire function of the variables η_{ij}, $1 \le i \le m$, $1 \le j \le n$. So if Y is a fixed point in $P\mathcal{B}$ satisfying

$$|Y - \eta| = \max_{\substack{1 \le i \le m \\ 1 \le j \le n}} |Y_{ij} - \eta_{ij}| \le \tfrac{1}{2} \quad ,$$

then we have the estimate

$$|h(Y) - h(\eta)| << \max_{\eta} \max_{\substack{1 \le i \le m \\ 1 \le j \le n}} \left| \frac{\partial h(\eta)}{\partial \eta_{ij}} \right| \quad ,$$

where the maximum over η is taken over all η such that $N\eta + Z \in P\mathcal{B}$. We thus obtain

$$\left| \sum_{Y} h(Y) - \int_{\eta} h(\eta) d\eta \right| << N P^{-3+\Delta} P^{2} (P/N)^{mn} + (P/N)^{mn-1} \quad ,$$

where the second term on the right allows for the difference between the number of integral points in the box $P\mathcal{B}$ and the volume of $P\mathcal{B}$. Summing over the N^{mn} values of Z, we have

$$|T(\alpha) - \sum_{Z(\mathrm{mod}\ N)} e(S(\gamma C(Z))) \int_{\eta} h(\eta)d\eta|$$

$$<< NP^{-3+\Delta+2+mn} + NP^{mn-1}$$

$$<< P^{mn-1+2\Delta} .$$

The right hand side of the above inequality, when integrated over $|\beta| < P^{-3+\Delta}$ and summed over $\gamma(\mathrm{mod}\ \delta^{-1})$, $N(a(\gamma)) \leq P^{\Delta}$, gives a final error

$$<< \sum_{Na \leq \tau} \sum_{\substack{\gamma(\mathrm{mod}\ \delta^{-1}) \\ a(\gamma)=a}} P^{n(-3+\Delta)} P^{mn-1+2\Delta}$$

$$<< P^{n(m-3-1/n+(1+5/n)\Delta)}$$

$$= o(P^{n(m-3)}) ,$$

since $\Delta = 2\theta = 1/(n+6)$ implies

$$-1/n + (1 + 5/n)/(n + 6) < 0 .$$

The left hand side of the same inequality, when summed and integrated over the same region as the right hand side gives $\int_{\mathfrak{M}} T(\alpha)d\alpha - U$, where

$$U = \sum_{Na \leq \tau} \sum_{\substack{\gamma(\mathrm{mod}\ \delta^{-1}) \\ a(\gamma)=a}} \int_{|\beta|<P^{-3+\Delta}} \sum_{Z(\mathrm{mod}\ N)} e(S(\gamma C(Z))) \int h(\eta)d\eta \tag{16}$$

$$(17) \qquad U = \mathfrak{S}(\tau) \int_{|\beta| < P^{-3+\Delta}} \int_{P} e(S(\beta C(\xi'))) d\xi' d\beta \quad ;$$

where we have made the change of variables $\xi' = N\eta + Z$ in the interior integral of (16). Now let $\beta = \beta' P^{-3}$ in (17). We obtain

$$U = \mathfrak{S}(\tau) P^{n(m-3)} \int_{|\beta'| < \tau} \int_{P\mathcal{B}} e(S(\beta' C(\xi'))) d\xi' d\beta'$$

$$= \mathfrak{S}(\tau) J(\tau) P^{n(m-3)} \quad .$$

Therefore,

$$\int_{\mathfrak{M}} T(\alpha) d\alpha = \mathfrak{S}(\tau) J(\tau) P^{n(m-3)} + o(P^{n(m-3)})$$

as $P \to \infty$ for $m \geq 17$.

Q.E.D.

The remainder of the paper is devoted to showing that, for any non-degenerate cubic form in $m \geq 17$ variables over $\mathbf{K}$, we have

$$\lim_{\tau \to \infty} J(\tau) = J > 0$$

$$\lim_{\tau \to \infty} \mathfrak{S}(\tau) = \mathfrak{S} > 0 \quad .$$

Hence, if $m \geq 17$ and $C(X)$ does not represent 0 non-trivially, then

$$\int_{\mathfrak{R}} T(\alpha) d\alpha = \mathfrak{S} J P^{n(m-3)} + o(P^{n(m-3)}) \quad ,$$

as $P \to \infty$.

Lemma 5.5. Put $C(\xi) = \sum_{1 \le r \le n} C_r(\xi_{11}, \ldots, \xi_{mn})\omega_r$,

where each C_r is a cubic form in the variables ξ_{ij} with rational integer coefficients. Then there is a $\xi^* = (\xi_1^*, \ldots, \xi_m^*)$ in $(K_R)^m$ and a set of n distinct couples (p_ℓ, q_ℓ) such that

$$C_r(\xi^*) = 0 \quad , \qquad 1 \le r \le n \quad , \tag{18}$$

$$\det \left| \frac{\partial C_r(\xi^*)}{\partial \xi_{(p_\ell q_\ell)}} \right| \neq 0 \quad , \tag{19}$$

where ℓ runs over the range $1 \le \ell \le n$.

Proof. See [13], Lemma 3.4 (b), page 695, and the bottom of page 699.

Q.E.D.

Without loss of generality it may be assumed that the set of indices $\{(p_\ell, q_\ell) \mid 1 \le \ell \le n\}$ which appear in (19) is just the set $\{(1, \ell) \mid 1 \le \ell \le n\}$, which we designate by D. Also, the set of variables $\{\xi_{(1,1)}, \ldots, \xi_{(1,n)}\}$ will be designated by ξ_D. The complete set of variables $\{\xi_{(i,j)} \mid 1 \le i \le m ; \ 1 \le j \le n\}$ will be designated by ξ_E; and ξ_{E-D} will be the set of variables in ξ_E and not in ξ_D.

Lemma 5.6. $\lim_{\tau \to \infty} J(\tau) = J > 0$ for any cubic form with coefficients in $\mathcal{O}_K$ in more than 16 variables.

Proof.

$$J(\tau) = \int_{|\beta|<\tau} \int_{\mathcal{B}} e(S(\beta C(\xi)))d\xi d\beta$$

(20)

$$= \int_{\mathcal{B}} \prod_{1\le r\le n} \frac{\sin(2\pi\tau C_r(\xi))}{\pi C_r(\xi)} d\xi \quad ,$$

where we have interchanged the order of integration and integrated with respect to β (a multiple integral). We now make our choice of the box $\mathcal{B}$:

$$\mathcal{B} = \{ \xi \in (K_R)^m \mid \xi = \xi^* + t, \ |t| \le a \} \quad , \tag{21}$$

where ξ^* is a point satisfying (18) and (19), and a is a small real number to be specified later. The expression $|t| \le a$ means that $|t_i| \le a$, where $t = (t_1, \ldots, t_m)$. Now make the change of variable $\xi = \xi^* + t$ in (20) to obtain

$$J(\tau) = \pi^{-n} \int_{-a}^{a} \cdots \int_{-a}^{a} \prod_{1\le r\le n} \frac{\sin\phi\, C_r(\xi^*+t)}{C_r(\xi^*+t)}\, dt \quad , \tag{22}$$

where $\phi = 2\pi\tau$.

Finally, since $\frac{\partial C_r}{\partial \xi_{(l,\ell)}}(\alpha\xi) = \alpha^2 \frac{\partial C_r(\xi)}{\partial \xi_{(l,\ell)}}$, we can assume that $\det \left| \frac{\partial C_r}{\partial \xi}_D(\xi^*) \right| = \pm 1$; and since the only property we use of the above determinant is that for t sufficiently small $\frac{\partial C_r}{\partial t}_D(\xi^* + t) \neq 0$,

we can assume without loss of generality that $\det \left| \frac{\partial C_r}{\partial \xi_D} (\xi^*) \right| = 1$.

Then, by the Implicit Function Theorem, for sufficiently small a, we can invert the relations

$$\zeta_r = C_r(\xi^* + t) \quad , \qquad 1 \leq r \leq n \quad ,$$

solving for t_D in terms of $\zeta_1, \ldots, \zeta_n, t_{E-D}$, which we denote by $(\zeta ; t_{E-D})$. For a sufficiently small and for any fixed values of the variables t_{E-D}, with $|t_{E-D}| \leq a$, the mapping: $(t_D ; t_{E-D}) \rightarrow (\zeta ; t_{E-D})$, defined by $\zeta_r = C_r(\xi^* + t)$, is an analytic isomorphism of the domain defined by $|t_D| \leq a$ and $|t_{E-D}| \leq a$ onto a domain $\mathfrak{D}(\zeta ; t_{E-D})$, in the $(\zeta ; t_{E-D})$-space which contains the domain defined by $|t_{E-D}| \leq a$, $|\zeta| \leq b$, where b is some fixed, positive number (See [13], Lemma 3.4 (c), page 695). So for each ℓ, $1 \leq \ell \leq n$, we can express $t_{(1, \ell)}$ as a power series in the variables $(\zeta ; t_{E-D})$. Hence, the determinant $\det \left| \frac{\partial t_{(1, \ell)}}{\partial \zeta_r} \right|$ can also be expressed as a power series, say $\Phi(\zeta; t_{E-D})$, in the same variables.

Now $\Phi(0; 0)$ is 1 by the assumption that

$$\det \left| \frac{\partial C_r(\xi^*)}{\partial \xi_D} \right| = 1 \quad .$$

Moreover, since Φ is a continuous function on $\mathfrak{D}(\zeta ; t_{E-D})$, we can write

$$\Phi = 1 + f(\zeta ; t_{E-D}) \quad ,$$

where f is continuous on the domain $\mathfrak{D}$ and $f(0;0) = 0$. Now split f into the sum of two power series, say $f = f_1 + f_2$, where f_1 consists of the sum of those terms in f which do not involve positive powers of $\zeta_1, \ldots, \zeta_n$, and f_2 is the sum of the remaining terms. Then we can write

$$f_2 = \sum_{1 \le \lambda \le n} \zeta_\lambda \Psi_\lambda (\zeta ; t_{E-D}) \quad ,$$

where Ψ_λ, $1 \le \lambda \le n$, are continuous functions, and so bounded, on the domain $\mathfrak{D}$.

We now choose a so that the box $\mathcal{B}$ defined in (21) does not contain the origin, the sides of the box do not exceed unity in length, and $1 + f_1 \ge \frac{1}{2}$ and $1 + f > 0$ on $\mathfrak{D}$.

In (22) make the change of variables from $(t_D ; t_{E-D})$ to $(\zeta ; t_{E-D})$ given before. The Jacobian of this transformation is $\Phi(\zeta; t_{E-D})$, and we obtain

$$J(\tau) = \pi^{-n} \int \prod_{1 \le r \le n} \frac{\sin \phi \zeta_r}{\zeta_r} \, | \, \Phi(\zeta ; t_{E-D}) \, | \, d\zeta \, dt_{E-D} \quad .$$

Now the domain $\mathfrak{D}$ can be split into 2^n parts in each of which a certain subset of the variables $\zeta_1, \ldots, \zeta_n$ satisfy $|\zeta_i| > b$, while others remain $\le b$; and on any of these subdomains on which at least one ζ_i remains $> b$, the integral over this subdomain of $\prod_{1 \le r \le n} \frac{\sin \phi \zeta_r}{\zeta_r} \, | \, \Phi \, |$ tends to zero uniformly with respect to t_{E-D} as

ϕ tends to infinity. To see this, note that

$\int_{\mathfrak{D}} \prod \frac{\sin \phi \zeta_r}{\zeta_r} |\Phi| \, d\zeta \, dt_{E-D}$ can be expressed as a repeated integral

$$\int_{\mathfrak{D}_1} \prod \frac{\sin \phi \zeta_r}{\zeta_r} \int_{\mathfrak{D}_2} |\Phi| \, dt_{E-D} \, d\zeta$$

$$<< \int_{\mathfrak{D}_1} \prod \frac{\sin \phi \zeta_r}{\zeta_r} \, d\zeta_1 \ldots d\zeta_n \quad ,$$

where $\mathfrak{D}_1$ and $\mathfrak{D}_2$ denote the domains over which ζ and t_{E-D} vary, respectively. If we now assume that on some portion of $\mathfrak{D}_1$, we have $|\zeta_n| > b$, then the last integral is bounded by

$$<< \int \prod_{1 \le r \le n-1} \frac{\sin \phi \zeta_r}{\zeta_r} \, d\zeta_1 \ldots d\zeta_{n-1} \int |\sin \phi \zeta_n| \, d\zeta_n$$

$$<< \left[\int \frac{1}{y} \, dy\right]^{n-1} \frac{1}{\phi} \quad ,$$

where the limits on y are $|y| \le b\phi$, since we have assumed that the variables ζ_r, $1 \le r \le n-1$, satisfy $|\zeta_r| \le b$. The last integral above, then, is $<< \log^{n-1} \phi / \phi$, which tends to zero as ϕ tends to infinity.

Therefore, we can write

$$J(\tau) = \pi^{-n} \int_{|\zeta| \le b} \prod_{1 \le r \le n} \frac{\sin \phi \zeta_r}{\zeta_r} \int_{\mathcal{D}_2} |\Phi| \, dt_{E-D} d\zeta$$

$$+ o(1) \quad \text{as} \quad \phi \to \infty \quad .$$

Since Φ is positive on $\mathcal{D}$, it is positive on the subdomain $(|\zeta| \le b, \mathcal{D}_2)$, so we can remove the absolute value signs from Φ in the last integral. Then write $\Phi = 1 + f_1 + f_2$ and integrate with respect to t_{E-D}. We obtain

$$J(\tau) = \pi^{-n} \int_{|\zeta| \le b} \prod \frac{\sin \phi \zeta_r}{\zeta_r} L \, d\zeta$$

$$+ \pi^{-n} \int_{|\zeta| \le b} \prod \frac{\sin \phi \zeta_r}{\zeta_r} \sum_{1 \le \lambda \le n} \zeta_\lambda F_\lambda(\zeta) d\zeta$$

$$+ o(1) \quad ,$$

where

$$L = \int_{\mathcal{D}_2} (1 + f_1) dt_{E-D} \quad ,$$

$$F_\lambda(\zeta) = \int_2 \Psi_\lambda(\zeta; t_{E-D}) dt_{E-D} \quad .$$

Note that L is an absolute constant independent of ζ, since f_1 was chosen as the sum of those terms in Φ which had no positive power of ζ_i. Moreover, L is positive and bounded away from zero, since $1 + f_1 \ge \frac{1}{2}$ on $\mathcal{D}_2$ and the domain $\mathcal{D}_2$ contains the subdomain

$|t_{E-D}| \leq a$, where a is a constant independent of ϕ.

We have

$$\pi^{-n} \int_{|\zeta| \leq b} L \prod \frac{\sin \phi \zeta_r}{\zeta_r} d\zeta$$

$$= L_1 \int_{|\zeta| \leq b\phi} \prod \frac{\sin \zeta_r}{\zeta_r} d\zeta$$

$$= L_1 \left(\int_{-\infty}^{\infty} \frac{\sin y}{y} dy \right)^n + o(1)$$

as $\phi \to \infty$, where L_1 is a positive constant.

We also have

$$\pi^{-n} \int_{|\zeta| \leq b} \prod \frac{\sin \phi \zeta_r}{\zeta_r} \sum_{1 \leq \lambda \leq n} \zeta_\lambda F_\lambda(\zeta) d\zeta$$

$$= \pi^{-n} \sum_{1 \leq \lambda \leq n} \int_{|\zeta| \leq b} \prod_{\substack{1 \leq r \leq n \\ r \neq \lambda}} \frac{\sin \phi \zeta_r}{\zeta_r} \sin(\phi \zeta_\lambda) F_\lambda$$

$$= \pi^{-n} \sum_{1 \leq \lambda \leq n} o(1), \qquad \text{as } \phi \to \infty$$

$$= o(1), \qquad \text{as } \phi \to \infty,$$

by the same argument which was used to show that the integral of $\prod \frac{\sin \phi \zeta_r}{\zeta_r} |\Phi|$ over any subdomain of D on which some ζ_r

satisfied $|\xi_r| > b$, is $o(1)$ as $\xi \to \infty$. Therefore, we have shown that

$$J(\tau) = J + o(1) \quad ,$$

as $\phi = 2\pi p^{\Delta} \to \infty$, where

$$J = \pi^{-n} L\left(\int_{-\infty}^{\infty} \frac{\sin y}{y}\, dy\right)^n > 0 \ .$$

Q.E.D.

Lemma 5.7. With the assumption that $C(X)$ does not represent 0 non-trivially, we have $|S_\gamma| << N^{mn-m/8+\varepsilon}$ for any $\varepsilon > 0$, where $N = N(a(\gamma))$, $S_\gamma = \sum_{Z (\mathrm{mod}\ N)} e(S(\gamma C(Z)))$.

Proof. We apply Lemma 3.1 with $\alpha = \gamma$ and $\theta = 1/2n - \varepsilon$. Since Alternative (A) has been excluded, the assumption that

$$|S_\gamma| \geq N^{n(m - m\theta/4 + \varepsilon)}$$

$$= N^{mn - m/8 + \varepsilon}$$

implies that there is a non-zero μ in $N^{1/n-\varepsilon} B_0$ and a ν in δ^{-1} such that

$$\mu\gamma - \nu = \sum_{1 \leq i \leq n} \beta_i \rho_i \quad ,$$

and $|\beta_i| < N^{-3+1/n+\varepsilon}$. Since $a(\gamma)(\mu\gamma - \nu)$ is in δ^{-1}, it follows that $\beta_i N(a(\gamma))$ is a rational integer for each i, $1 \leq i \leq n$. But

$$|\beta_i N| < N^{-2+1/n-\varepsilon} < 1 \quad ,$$

which implies that $\beta_i = 0$, $1 \leq i \leq n$. Therefore, μ is in $a(\gamma)$; and so $N(a(\gamma))$ divides $N(\mu)$. But $N(\mu) << N^{1-\varepsilon}$, which implies for N sufficiently large that $N(\mu) = 0$, a contradiction. Therefore, we must have

$$|S_\gamma| << N^{mn-m/8+\varepsilon} \quad \text{for all} \quad \varepsilon > 0.$$

Q.E.D.

Lemma 5.8. Let γ_1, γ_2 be two elements of K which satisfy $(a(\gamma_1), a(\gamma_2)) = (1)$. Then $S_{\gamma_1+\gamma_2} = S_{\gamma_1} S_{\gamma_2}$.

Proof. From the definition of N and S_γ in Lemma 5.7 we have

$$S_\gamma = N^{m(n-1)} G_\gamma \quad ,$$

where

$$G_\gamma = \sum_{X(\text{mod } a(\gamma))} e(S(\gamma C(X))) \quad ,$$

(See [13], Lemma 2.2, page 691). So it suffices to prove that

$$N(a(\gamma_1 + \gamma_2)) = N(a(\gamma_1))N(a(\gamma_2)) \tag{23}$$

$$G(\gamma_1 + \gamma_2) = G(\gamma_1)G(\gamma_2) \quad . \tag{24}$$

To prove (23), we choose integers λ_1 in $a(\gamma_1)$ and λ_2 in $a(\gamma_2)$ such that $((\lambda_i), a(\gamma_1)a(\gamma_2)) = a(\gamma_i)$. Such a choice can be made (See [8], Theorem 2.32). Now put $X_i = \lambda_1 Y_i + \lambda_2 Z_i$. As Y_i, Z_i run over complete residue systems (mod $a(\gamma_2)$) and (mod $a(\gamma_1)$), respectively, X_i runs over a complete residue system

$(\mathrm{mod}\ a(\gamma_1)a(\gamma_2))$, since $(a(\gamma_1),\ a(\gamma_2)) = (1)$. Furthermore, since $a(\gamma_1 + \gamma_2) = a(\gamma_1)a(\gamma_2)$, we have $N(a(\gamma_1 + \gamma_2)) = N(a(\gamma_1))N(a(\gamma_2))$. Therefore,

$$G_{\gamma_1+\gamma_2} = \sum_{X(\mathrm{mod}\ a(\gamma_1+\gamma_2))} e(S((\gamma_1 + \gamma_2)C(X)))$$

$$= \sum_{Y(\mathrm{mod}\ a(\gamma_2))} \sum_{Z(\mathrm{mod}\ a(\gamma_1))} e(S(\gamma_1 + \gamma_2)C(\lambda_1 Y + \lambda_2 Z)))$$

$$= \sum_{Y} e(S(\gamma_1 C(\lambda_1 Y))) \sum_{Z} e(S(\gamma_2 C(\lambda_2 Z)))$$

$$= G_{\gamma_1} G_{\gamma_2} ,$$

since when Y runs over a complete residue system modulo $a(\gamma_2)$, so does $\lambda_1 Y$. The same holds for the sum over Z.

Q. E. D.

Lemma 5.9. $\sum_{\substack{\gamma(\mathrm{mod}\ \delta^{-1}) \\ a(\gamma)=a}} 1 \ll Na = N$.

Proof. $(\gamma)\delta = b(\gamma)/a(\gamma)$, where $(b(\gamma),\ a(\gamma)) = (1)$. So $(\gamma) = b(\gamma)\delta^{-1}/a(\gamma)$, and γ is in $(a\delta)^{-1}$. Therefore, the sum in the statement of the lemma does not exceed the number of γ in a complete residue system of $(a\delta)^{-1}$ modulo δ^{-1}, which is Na.

Q.E.D.

We now will show that the limit $\lim_{\tau\to\infty} \mathfrak{S}(\tau)$ exists and is positive. By definition, we have

$$\mathfrak{S}(\tau) = \sum_{Na=1}^{\infty} \sum_{\substack{\gamma \pmod{\delta^{-1}} \\ a(\gamma)=a}} N^{-mn}(a(\gamma))S_{\gamma} .$$

Therefore,

$$\lim_{\tau \to \infty} \mathfrak{S}(\tau) = \sum_{Na=1}^{\infty} \sum_{\substack{\gamma \pmod{\delta^{-1}} \\ a(\gamma)=a}} N^{-mn} S_{\gamma} ,$$

which we designate by .

By Lemma 5.8, we can also write

$$\mathfrak{S} = \prod_{\mathfrak{p}} \mathfrak{X}(\mathfrak{p}) , \tag{25}$$

where

$$\mathfrak{X}(\mathfrak{p}) = 1 + \sum_{\ell=1}^{\infty} (N\mathfrak{p})^{-m\ell} \sum_{\substack{\gamma \pmod{\delta^{-1}} \\ a(\gamma)=\mathfrak{p}^{\ell}}} G_{\gamma} ,$$

and where the product in (25) is over all prime ideals $\mathfrak{p}$ of K.

If it can be shown that the infinite sum defining $\mathfrak{S}$ is absolutely convergent, then the product (25) is absolutely convergent. In that case, $\mathfrak{S}$ will be positive if we can show that $\mathfrak{X}(\mathfrak{p}) > 0$ for all primes $\mathfrak{p}$.

Lemma 5.10. $\mathfrak{S} = \sum_{Na=1}^{\infty} \sum_{\substack{\gamma \pmod{\delta^{-1}} \\ a(\gamma)=a}} N^{-mn}(a(\gamma))S_{\gamma}$ is absolutely convergent when $m \geq 17$.

Proof. By Lemma 5.7,

$$\left| \sum_{\substack{\gamma \pmod{\delta^{-1}} \\ a(\gamma)=a}} N^{-mn}(a(\gamma))S_{\gamma} \right| << N^{-mn} N^{mn-m/8+\varepsilon} \sum_{\substack{\gamma \pmod{\delta^{-1}} \\ a(\gamma)=a}} 1 ,$$

where $N = Na$. By Lemma 5.9, $\sum_{\substack{\gamma \pmod{\delta^{-1}} \\ a(\gamma)=a}} << N$; and since the number of integral ideals in K which have a given norm N is $<< N^{\varepsilon}$ for all $\varepsilon > 0$, the inner sum defining $\mathfrak{G}$ is bounded by

$$<< N^{-mn} N^{mn-m/8+\varepsilon} N^{\varepsilon}$$

$$= N^{1+\varepsilon-m/8} \leq N^{-1-u} \qquad u > 0 \quad ,$$

since $m \geq 17$. Therefore, the sum defining $\mathfrak{G}$ is absolutely convergent.

Q.E.D.

Lemma 5.11. Let $M(\mathfrak{p}^H)$ denote the number of incongruent solutions modulo $\mathfrak{p}^H$ of the congruence $C(X) \equiv 0 \pmod{\mathfrak{p}^H}$, where H is a non-negative integer and $X = (X_1, \ldots, X_m)$, $X_i \in \mathcal{O}_K$. Then

$$M(\mathfrak{p}^H) = (N\mathfrak{p})^{H(m-1)} \sum_{h=0}^{H} (N\mathfrak{p})^{-mh} \sum_{\substack{\gamma \pmod{\delta^{-1}} \\ a(\gamma)=\mathfrak{p}^H}} G_{\gamma} \quad .$$

Proof.

$$\sum_{\gamma} e(S(\gamma C(X))) = \begin{cases} 0 & \text{if } C(X) \not\equiv 0 \pmod{\mathfrak{p}^H} \\ N(\mathfrak{p}^H) & \text{if } C(X) \equiv 0 \pmod{\mathfrak{p}^H} \end{cases} ,$$

where the sum is over a complete residue system of $(\mathfrak{p}^H\delta)^{-1}$ modulo δ^{-1}. Therefore,

$$M(\mathfrak{p}^H) = (N\mathfrak{p})^{-H} \sum_{X(\mathrm{mod}\,\mathfrak{p}^H)} \sum_{\gamma} e(S(\gamma C(X)))$$

$$= (N\mathfrak{p})^{-H} \sum_{X(\mathrm{mod}\,\mathfrak{p}^H)} \sum_{h=0}^{H} \sum_{\substack{\gamma\,(\mathrm{mod}\,\delta_h^{-1}) \\ a(\gamma)=\mathfrak{p}^h}} e(S(\gamma C(X)))$$

$$= (N\mathfrak{p})^{-H} \sum_{h=0}^{H} (N\mathfrak{p})^{m(H-h)} \sum_{\substack{\gamma\,(\mathrm{mod}\,\delta_H^{-1}) \\ a(\gamma)=\mathfrak{p}^H}} \sum_{X(\mathrm{mod}\,\mathfrak{p}^H)} e(S(\gamma C(X$$

$$= (N\mathfrak{p})^{H(m-1)} \sum_{h=0}^{H} (N\mathfrak{p})^{-mh} \sum_{\substack{\gamma(\mathrm{mod}\,\delta_H^{-1}) \\ a(\gamma)=\mathfrak{p}^H}} G_\gamma \quad .$$

Q.E.D.

Therefore, $\lim_{H\to\infty} (N\mathfrak{p})^{-H(m-1)} M(\mathfrak{p}^H) = \mathfrak{X}(\mathfrak{p})$. Since $C(X)$ is non-degenerate over K, it is non degenerate over $K_{\mathfrak{p}}$, the completion of K at the prime $\mathfrak{p}$. Also, since $C(X)$ has more than nine variables, $C(X)$ has a non-singular zero in $K_{\mathfrak{p}}$; i.e., there exists $\underline{X}$ in $(K_{\mathfrak{p}})^m$ such that

(26) $$C(\underline{X}) = 0$$

(27) $$\frac{\partial C}{\partial X_i}(\underline{X}) \neq 0 \quad \text{for some } i, \quad 1 \leq i \leq m \quad .$$

The proof of this follows from the main theorem of [9], and with the existence of a zero, we can obtain a non-singular zero.

With this fact, we will now be able to show that $M(\mathfrak{p}^{2\ell+1+\nu}) \geq (N\mathfrak{p})^{(m-1)\nu}$ for all $\nu \geq 0$ and for some positive integer ℓ. We then can immediately conclude that $\mathfrak{X}(\mathfrak{p}) > 0$.

Lemma 5.12. For some positive integer ℓ and all $\nu \geq 0$,

$$M(\mathfrak{p}^{2\ell-1+\nu}) \geq (N\mathfrak{p})^{(m-1)\nu} .$$

Proof. As an immediate consequence of (26), (27), there is a positive integer ℓ and an $\underline{X} \in (\mathcal{O}_K)^m$ such that

$$\frac{\partial}{\partial X_i} C(\underline{X}) \equiv 0 \pmod{\mathfrak{p}^{\ell-1}} \quad \text{all } i, \ 1 \leq i \leq m \tag{28}$$

$$\frac{\partial}{\partial X_i} C(\underline{X}) \not\equiv 0 \pmod{\mathfrak{p}^{\ell}} \quad \text{for some } i \tag{29}$$

$$C(\underline{X}) \equiv 0 \pmod{\mathfrak{p}^{2\ell-1}} . \tag{30}$$

We shall prove by induction on ν that the congruence $C(X) \equiv 0 \pmod{\mathfrak{p}^{2\ell-1+\nu}}$ has at least $(N\mathfrak{p})^{(m-1)\nu}$ solutions satisfying (28) and (29), these solutions being mutually incongruent to the modulus $\mathfrak{p}^{\ell+\nu}$; and, therefore, incongruent to the modulus $2\ell-1+\nu$.

When $\nu = 0$, the above assertion is just (28), (29), (30). Assume that the result holds for a particular integer $\nu \geq 1$; and let $X_1, \ldots, X_m$ be any one of the $(N\mathfrak{p})^{(m-1)\nu}$ solutions of $C(X) \equiv 0 \pmod{\mathfrak{p}^{2\ell-1+\nu}}$, all of which satisfy (28) and (29). Therefore, for some $\lambda \in \mathcal{O}_K$ and $\pi \in \mathfrak{p} - \mathfrak{p}^2$, we have $C(X) = \lambda \pi^{2\ell-1+\nu}$; and by (28) and (29), there exist $d_i \in \mathcal{O}_K$, $\pi_i \in \mathfrak{p} - \mathfrak{p}^2$ such that $\frac{\partial C}{\partial X_i} = d_i \pi_i^{\ell-1}$, $1 \leq i \leq m$, where $d_i \not\equiv 0 \pmod{\mathfrak{p}}$ for some i, say $i = 1$. Now for $u = (u_1, \ldots, u_m) \in (\mathcal{O}_K)^m$, we have

$$C(X + \pi^{\ell+\nu} u) \equiv C(X) + \pi^{\ell+\nu} \left(u_1 \frac{\partial C}{\partial X_1} + \ldots + u_m \frac{\partial C}{\partial X_m}\right) \pmod{\mathfrak{p}^{2\ell+2\nu}}.$$

Hence, $C(X + \pi^{\ell+\nu}u) \equiv 0 \pmod{\mathfrak{p}^{2\ell+\nu}}$ holds if $\lambda\pi^{\ell-1} + u_1 d_1 \pi_1^{\ell-1} + \ldots + u_m d_m \pi_m^{\ell-1} \equiv 0 \pmod{\mathfrak{p}^{\ell}}$. But this last congruence has $(N\mathfrak{p})^{m-1}$ distinct solutions u, where u_i, $2 \leq i \leq m$ runs over a complete residue system modulo $\mathfrak{p}$. Hence, corresponding to each X we obtain $(N\mathfrak{p})^{m-1}$ values of $y = X + \pi^{\ell+\nu}u$, which satisfy $C(y) \equiv 0 \pmod{\mathfrak{p}^{2\ell+\nu}}$ and $y \equiv X \pmod{\mathfrak{p}^{\ell+\nu}}$. It follows that each y satisfies (28) and (29); and we obtain altogether $(N\mathfrak{p})^{(m-1)(\nu+1)}$ values for y that are mutually incongruent modulo $\mathfrak{p}^{\ell+\nu+1}$. Hence, the result holds for $\nu + 1$ in place of ν. This proves the lemma.

Q.E.D.

Therefore,

$$\begin{aligned} \mathfrak{X}(\mathfrak{p}) &= \lim_{H\to\infty} (N\mathfrak{p})^{-H(m-1)} M(\mathfrak{p}^H) \\ &\geq \lim_{H\to\infty} (N\mathfrak{p})^{-H(m-1)} (N\mathfrak{p})^{(m-1)(H-L)} \\ &\geq (N\mathfrak{p})^{-L(m-1)} , \end{aligned}$$

where L is a positive integer independent of H. Therefore, $\mathfrak{X}(\mathfrak{p}) > 0$ for all $\mathfrak{p}$. As we have already stated on page 78, this suffices to prove the theorem.

BIBLIOGRAPHY

1. Cassells, J. W. S. An Introduction to Diophantine Approximation, (1957), Cambridge University Press.

2. Davenport, H. Cubic Forms in 32 Variables. Philosophical Transactions of the Royal Society of London, Ser. A, (251), (1958), 193-232.

3. _____. Analytic Methods for Diophantine Equations and Inequalities, (1962), Ann Arbor, Ann Arbor Publishers.

4. _____. Cubic Forms in 16 Variables. Proceedings of the Royal Society, Ser. A, (272), (1963), 285-303.

5. Davenport, H., and Roth, K. F. The Solubility of Certain Diophantine Inequalities. Mathematika, (4), 81-96.

6. Erdős, P., and Heilbronn, H. On the addition of Residue Classes mod p. Acta Arithmetika, (IX), (1964), 149-159.

7. Hua, L. K. Enzyklopädie der Mathematischen Wissenschaften, Band I, Teil 2, (1958), Leipzig, Teubner.

8. LeVeque, W. J. Topics in Number Theory. Vol. 2, (1956), Reading, Addison-Wesley.

9. Lewis, D. J. Cubic Homogeneous Polynomials over $\mathfrak{p}$ -adic Number Fields. Annals of Mathematics, (56), No. 3, (1952), 473-478.

10. _____. Cubic Forms over Algebraic Number Fields. Mathematika, (4), (1957), 97-101.

11. Mann, H. B. The Addition Theorems of Number Theory and Group Theory. (1965), New York, Interscience Publishers.

12. Mann, H. B., and Olson, J. E. Sums of Sets in the Elementary Abelian Group of type (p,p). Math Research Center, United States Army, Madison, Wisconsin.

13. Ramanujam, C. P. Cubic Forms over Algebraic Number Fields. Proceedings of the Cambridge Philosophical Society, (59), (1963), 683-705.

14. Tartakowskĭ, W. Über Asymtotische Gesetze der "Allgemeinen" Diophantischen Analyse mit vielen Unbekannten. Bulletin of the Academy of Sciences, U. S. S. R., (1935), 483-524.

15. Vinogradov, I. M. The Method of Trigonometrical Sums in the Theory of Numbers, (1947), London, Interscience Publishers.