DIOPHANTINE APPROXIMATION IN FIELDS OF CHARACTERISTIC p

BY

L. CARLITZ

1. **Introduction.** Let $\Phi = GF\{p^n, x\}$ denote the field consisting of the quantities

$$(1.1) \qquad \alpha = \sum_{-\infty}^{m} c_i x^i \qquad (c_i \in GF(p^n)),$$

where x is an indeterminate and the coefficients c_i all belong to a fixed finite field $GF(p^n)$. We shall discuss a number of problems of "diophantine approximation" related to the numbers of Φ.

We first (§3) prove an analogue of Kronecker's theorem; the theorem has been proved previously by Mahler [8, p. 514]. We next define uniform distribution of sequences of numbers in Φ (see [9], also [7, chap. 8]) and prove a number of theorems similar to the theorems of Weyl's well known paper. The sum $S = \sum e(\phi(A))$, extended over polynomials $A \in GF[p^n, x]$ of degree less than m, where $\phi(u)$ is a polynomial of degree k and $e(\alpha)$ is defined in (2.3) below, is studied by Weyl's method of approximation. It is found that if at least one coefficient of $\phi(u) - \phi(0)$ is irrational and $1 \leqq k < p$, then $S = o(p^{nm})$ as $m \rightarrow \infty$. The case $k \geqq p$ is left open; there are polynomials of degree p for which $S = p^{nm}$ (see (6.8) and (6.9)).

For $k = 2$, $p > 2$, we make a more detailed study of the sum

$$S_m(\alpha, \beta) = \sum_{\deg m < A} e(\alpha A^2 + 2\beta A) \qquad (\alpha, \beta \in \Phi);$$

here we follow [6, II]. The main tool is the following analogue of the Hardy-Littlewood "approximate functional equation":

$$(1.2) \qquad S_m(\alpha, \beta) = \eta p^{na/2} S_{m-a}(1/\alpha, \alpha/\beta) \qquad (|\eta| = 1),$$

where $\deg \alpha = -a < 0$, $\deg \beta < 0$. From (1.2) it follows easily that

$$(1.3) \qquad S_m(\alpha, \beta) = o(p^{nm}) \qquad (m \rightarrow \infty)$$

for all irrational α; moreover, if the continued fraction for α has partial quotients of bounded degree, then $S_m(\alpha, \beta) = O(p^{nm/2})$. It also follows from (1.2) that (at least for $\beta = 0$) (1.3) cannot in general be improved.

We show also that for all α

$$(1.4) \qquad |S_m(\alpha, 0)| \geqq p^{nm/2}.$$

Presented to the Society, September 6, 1951; received by the editors July 2, 1951.

For arbitrary β we can assert that either $S_m(\alpha, \beta)=0$ or $|S_m(\alpha, \beta)| \geqq p^{nm/2}$.

2. **Notation and preliminaries.** Polynomials in $GF[p^n, x]$ will be denoted by italic capitals $A, B, \cdots, U, V$; however, the letters K, N, R, S will stand for certain functions to be defined presently. The numbers of $\Phi = GF\{p^n, x\}$ will usually be denoted by lower case Greek letters unless some other meaning is indicated. If

$$\alpha = \sum_{-\infty}^{m} c_i x^i \qquad (c_m \neq 0) \tag{2.1}$$

is a typical number of Φ, we define $\deg \alpha = m$, where m may be positive, zero, or negative. The sum $\sum_0^m c_i x^i$ is called the integral part of α; for the fractional part we shall use the symbol

$$((\alpha)) = \sum_{-\infty}^{-1} c_i x^i. \tag{2.2}$$

By the statement $\alpha \equiv \beta \pmod 1$ is meant $\alpha = \beta + A$, where A is a polynomial $\in GF[p^n, x]$; when there is no danger of confusion, we shall usually omit the phrase "mod 1." Thus, every α is congruent (mod 1) to a unique β such that $\deg \beta < 0$.

Let θ define the $GF(p^n)$. Then for c_{-1} in (2.1) we put

$$c_{-1} = a_1\theta^{n-1} + \cdots + a_n \qquad (a_i \in GF(p))$$

and define the function

$$e(\alpha) = e^{2\pi i a_1/p}. \tag{2.3}$$

It follows at once from (2.3) that

$$e(\alpha+\beta) = e(\alpha)e(\beta), \qquad e(\alpha) = e(\beta) \qquad \text{for } \alpha \equiv \beta \pmod 1. \tag{2.4}$$

(It is easy to identify the function $e(A/H)$ with the function $\epsilon(A, H)$ previously defined [4, §2]. We remark also that in (2.3) we could replace $e^{2\pi i/p}$ by any primitive pth root of unity, and a_1 by the trace of c_{-1}.) The following result will be used frequently.

THEOREM 1. *The sum*

$$\sum_{\deg A<m} e(A\alpha) = \begin{cases} p^{mn} & (\deg((\alpha)) < -m), \\ 0 & (\deg((\alpha)) \geqq -m). \end{cases} \tag{2.5}$$

The proof is similar to that of [3, Lemma 1] and will be omitted.

An immediate consequence of Theorem 1 is contained in

$$\lim_{r=\infty} p^{-rn} \sum_{\deg A<r} e(A\alpha) = \begin{cases} 1 & (\alpha \equiv 0), \\ 0 & (\alpha \not\equiv 0); \end{cases} \tag{2.6}$$

in other words, the limit $=1$ if and only if α is *integral.*

A number of Φ is *irrational* if it is not contained in $GF(p^n, x)$, that is, not a quotient of polynomials A/B. Thus (2.6) implies that for α irrational and B an arbitrary polynomial $\in GF[p^n, x]$, we have

$$\lim_{r=\infty} p^{-rn} \sum_{\deg A<r} e(AB\alpha) = 0. \tag{2.7}$$

3. **Kronecker's theorem for Φ.** The numbers $\alpha_1, \cdots, \alpha_k$ of Φ are *linearly independent* if $\sum_{i=1}^{k} A_i\alpha_i=0$ $(A_i\in GF[p^n, x])$ implies all $A_i=0$.

We shall now prove the following theorem.

THEOREM 2. *Let $k\geqq 1$; $\alpha_1, \cdots, \alpha_k, \lambda_1, \cdots, \lambda_k\in\Phi$; $1, \lambda_1, \cdots, \lambda_k$ linearly independent. Also let m, $m_0\geqq 1$. Then there exists a polynomial $A\in GF[p^n, x]$, $\deg A\geqq m_0$, such that*

$$\deg ((A\lambda_i - \alpha_i)) < -m \qquad (i = 1, \cdots, k). \tag{3.1}$$

Proof. (Compare [2].) We construct the function

$$\phi(t) = p^{-nm} \sum_{\deg B<m} \sum_{i=1}^{k} e(B(\lambda_i t - \alpha_i)),$$

where $t\in\Phi$. In view of Theorem 1, it will suffice to show the existence of a polynomial A, $\deg A\geqq m_0$, such that $\phi(A)=k$.

We put

$$K(t) = K_m(t) = \sum_{\deg B<m} e(Bt) \geqq 0,$$

$$\Lambda(t) = \Lambda_m(t) = K(\lambda_1 t - \alpha_1) \cdots K(\lambda_k t - \alpha_k).$$

Then, evidently

$$\phi(t)\Lambda(t) = k + R(t), \tag{3.2}$$

where $R(t)$ is a sum of terms $e(\mu_i t-\beta_i)$, and, by the linear independence of $1, \lambda_1, \cdots, \lambda_k$, none of the $\mu_i=0$. If now we notice that Theorem 1 implies, for r sufficiently large,

$$p^{-nr} \sum_{\deg A=r}' e(A\alpha) = \begin{cases} 1 & (\alpha \equiv 0), \\ 0 & (\alpha \not\equiv 0), \end{cases} \tag{3.3}$$

the sum now being restricted to *primary* A of degree r (that is, polynomials with highest coefficient $=1$), it follows that

$$p^{-nr} \sum_{\deg A=r}' R(A) = 0 \qquad (r \geqq r_0). \tag{3.4}$$

But by (3.2) and (3.4), for $r\geqq r_0$,

$$k = p^{-nr} \sum_{\deg A=r}' \phi(A)\Lambda(A) \leqq \max_{\deg A=r} \phi(A)\cdot p^{-nr} \sum_{\deg A=r}' \Lambda(A).$$

However, by (3.3) and the definition of $\Lambda(t)$, we have

$$p^{-nr} \sum_{\deg A=r}' \Lambda(A) = 1 \qquad (r \geqq r_0)$$

and therefore

$$k \leqq \max_{\deg A=r} \phi(A).$$

Since max $\phi(A)$ cannot exceed k, it follows that $k = \max \phi(A)$, which completes the proof of the theorem. Actually, since A is primary we have proved a little more; indeed the proof shows that the highest coefficient of A may be any preassigned nonzero number of $GF(p^n)$.

For a proof of the one-dimensional case of Theorem 2 see [5, §5].

4. **Uniform distribution.** Given a sequence of numbers $\alpha_1, \alpha_2, \alpha_3, \cdots \in \Phi$, and an arbitrary number $\beta \in \Phi$. Let $N_k = N_k(m) = N_k(m, \beta)$ be the number of α_i, $1 \leqq i \leqq m$, such that

$$\deg((\alpha_i - \beta)) < -k, \tag{4.1}$$

where m and k are preassigned positive integers. We shall say that the sequence $\{\alpha_i\}$ is *uniformly distributed* (mod 1) provided

$$\lim_{m=\infty} \frac{1}{m} N_k(m) = p^{-nk} \tag{4.2}$$

for any $k \geqq 1$ and for all $\beta \in \Phi$.

We now prove the following criterion.

THEOREM 3. *For any sequence* $\alpha_1, \alpha_2, \alpha_3, \cdots$, (4.2) *holds if and only if*

$$\sum_{i=1}^{m} e(A\alpha_i) = o(m) \qquad \textit{for all } A \neq 0. \tag{4.3}$$

Proof. (i) We first show that (4.3) implies (4.2). By Theorem 1,

$$\sum_{\deg A<k} e(A(\alpha_i - \beta)) = \begin{cases} p^{nk} & (\deg((\alpha_i - \beta)) < -k), \\ 0 & (\deg((\alpha_i - \beta)) \geqq -k). \end{cases}$$

If we sum over $i = 1, \cdots, m$ and separate the terms in which $A = 0$, this becomes

$$m + \sum_{\deg A<k, A\neq 0} e(-A\beta) \sum_{i=1}^{m} e(A\alpha_i) = p^{nk} N_k. \tag{4.4}$$

Now assume (4.3); then (4.4) implies

$$m + o(m) = p^{nk} N_k, \tag{4.5}$$

which is equivalent to (4.2).

(ii) We now show that (4.2) implies (4.3), or what is the same thing, that (4.5) implies (4.3).

By Theorem 1 the sum

$$\sum_{\deg A<k}\sum_{i=1}^{m} e(A(\alpha_i-\beta)) = p^{nk}N_k. \tag{4.6}$$

Clearly for $A=0$, the left member of (4.6) $=m$; hence, using (4.5) we get

$$\sum_{\deg A<k,\, A\neq 0} e(-A\beta)\sum_{i=1}^{m} e(A\alpha_i) = o(m), \tag{4.7}$$

which is valid for all $\beta\in\Phi$. Now in (4.7) take $\beta=U/x^k$, where U is a polynomial, multiply both sides by $e(x^{-k}UB)$, where B is another polynomial, and sum over deg $U<k$. We get

$$\sum_{\deg U<k}\ \sum_{\deg A<k,\, A\neq 0} e(x^{-k}U(B-A))\sum_{i=1}^{m} e(A\alpha_i) = o(m). \tag{4.8}$$

Let deg $B<k$, $B\neq 0$, then by (2.5) the sum $\sum_U e(x^{-k}U(B-A))$ vanishes unless $A=B$. Thus (4.8) becomes $\sum_{i=1}^{m} e(B\alpha_i)=o(m)$ $(B\neq 0)$. Since deg $B<k$ and k is arbitrary this evidently proves (4.3).

For most applications a weaker condition than (4.2) seems to suffice; namely, we restrict the variable m to a subsequence of the integers. We remark that the proof of Theorem 3 shows that if (4.2) holds when m is restricted to a subsequence, then (4.3) also holds for the same subsequence and conversely. In particular, we shall be interested in the case when m is of the form p^{nr}. Accordingly, we state the following theorem.

THEOREM 4. *For any sequence $\alpha_1, \alpha_2, \alpha_3, \cdots$ the condition*

$$\lim_{m=\infty} p^{-nm}N_k(p^{nm}) = p^{-nk} \tag{4.9}$$

for all β is equivalent to

$$\sum_{i=1}^{p^{nm}} e(A\alpha_i) = o(p^{nm}) \qquad \text{for all } A\neq 0. \tag{4.10}$$

A sequence satisfying (4.9) may be called weakly uniformly distributed, but if there is no danger of confusion we shall simply call it uniformly distributed in this case also.

As an immediate consequence of Theorem 4 and (2.7) we have the following theorem.

THEOREM 5. *If $\xi\in\Phi$, $\xi\notin GF(p^n, x)$, then the sequence $\{A\xi\}$, where A runs through the polynomials of $GF[p^n, x]$, deg $A<m$, is (weakly) uniformly distributed.*

Here and elsewhere, in speaking of the sequence $\{A\xi\}$, it is to be understood that the A's are arranged in a sequence according to degree and otherwise arbitrary.

5. **Uniform distribution (general case).** Let $s \geqq 1$ and fixed. A set of s ordered numbers $(\alpha_1, \cdots, \alpha_s)$, $\alpha_i \in \Phi$, will be called a point. Two points $(\alpha_1, \cdots, \alpha_s)$, $(\beta_1, \cdots, \beta_s)$ are congruent (mod 1) provided $\alpha_i \equiv \beta_i$ (mod 1), $i=1, \cdots, s$. Thus, any point is congruent to a unique point $(\beta_1, \cdots, \beta_s)$ such that $\deg \beta_i < 0$ for $i=1, \cdots, s$.

Consider the sequence of points

$$(5.1) \qquad \{\alpha(i)\} = (\alpha_1(i), \cdots, \alpha_s(i)) \qquad (i = 1, 2, \cdots).$$

Let $k_1, \cdots, k_s \geqq 1$ and let $N_k = N_{k_1, \cdots, k_s}(m)$ be the number of points in the sequence (5.1) such that $1 \leqq i \leqq m$ and

$$(5.2) \qquad \deg\,((\alpha_j(i) - \beta_j)) < - k_j \qquad (j = 1, \cdots, s),$$

where $(\beta_1, \cdots, \beta_s)$ is an arbitrary point. We shall say that the sequence (5.1) is uniformly distributed (mod 1) provided

$$(5.3) \qquad \lim_{m=\infty} \frac{1}{m} N_k(m) = p^{-n(k_1+\cdots+k_s)}$$

for arbitrary $k_1, \cdots, k_s \geqq 1$ and all $(\beta_1, \cdots, \beta_s)$. We now prove the following criterion which includes Theorem 3 as a special case.

THEOREM 6. *For any sequence* (5.1) *and arbitrary* $k_1, \cdots, k_s \geqq 1$, *the condition* (5.3) *is equivalent to*

$$(5.4) \qquad \sum_{i=1}^{m} e(A_1\alpha_1(i) + \cdots + A_s\alpha_s(i)) = o(m)$$

for all $(A_1, \cdots, A_s) \neq (0, \cdots, 0)$.

Proof. (i) We first show that (5.4) implies (5.3). By Theorem 1,

$$\sum_{\deg A_1 < k_1} \cdots \sum_{\deg A_s < k_s} e(A_1(\alpha_1(i) - \beta_1) + \cdots + A_s(\alpha_s(i) - \beta_s)) = \begin{cases} p^{n(k_1+\cdots+k_s)} \\ 0 \end{cases}$$

according as (5.2) is or is not satisfied. Summing over $i=1, \cdots, m$ and separating the terms in which $A_1, \cdots, A_s = (0, \cdots, 0)$, this becomes

$$(5.5) \qquad m + \sum_{\deg A_j < k_j}{}' e(-A_1\beta_1 - \cdots - A_s\beta_s) \cdot \sum_{i=1}^{m} e(A_1\alpha_1(i) + \cdots + A_s\alpha_s(i)) = p^{n(k_1+\cdots+k_s)} N_k(m),$$

where the accent indicates that the combination $(0, \cdots, 0)$ is omitted.

Now assume (5.4); then (5.5) implies

$$m + o(m) = p^{n(k_1+\cdots+k_s)}N_k(m), \tag{5.6}$$

which is equivalent to (5.3).

(ii) We now show that (5.6) implies (5.4). As in the proof of Theorem 3, we have, using (5.6),

$$\sum_{\deg A_j<k_j}{}' e(-A_1\beta_1 - \cdots - A_s\beta_s)\sum_{i=1}^{m} e(A_1\alpha_1(i) + \cdots + A_s\alpha_s(i)) = o(m)$$

for all $(\beta_1, \cdots, \beta_s)$, where the $\sum'$ has the same meaning as above. Now put $\beta_j = x^{-k_j}U_j$, multiply both sides by $e(x^{-k_1}U_1B_1 + \cdots + x^{-k_s}U_sB_s)$, and sum over $\deg U_j < k_j$. We get

$$\sum_{\deg U_j<k_j}\sum_{A_j}{}' e(x^{-k_1}U_1(B_1 - A_1) + \cdots + x^{-k_s}U_s(B_s - A_s))$$
$$\cdot \sum_{i=1}^{m} e(A_1\alpha_1(i) + \cdots + A_s\alpha_s(i)) = o(m).$$

Now take $\deg B_j < k_j$, $(B_1, \cdots, B_s) \neq (0, \cdots, 0)$, then by (2.5) the sum $\sum_{U_j} = 0$ unless $(A_1, \cdots, A_s) = (B_1, \cdots, B_s)$. Hence,

$$\sum_{i=1}^{m} e(B_1\alpha_1(i) + \cdots + B_s\alpha_s(i)) = o(m)$$

for all $(B_1, \cdots, B_s) \neq (0, \cdots, 0)$, $\deg B_j < k_j$. This completes the proof of (5.4).

As in §4 we find it desirable to define weak uniform distribution. The sequence (5.1) is weakly uniformly distributed provided

$$\lim_{m=\infty} p^{-nm}N_k(p^{nm}) = p^{-n(k_1+\cdots+k_s)} \tag{5.7}$$

for arbitrary $k_1, \cdots, k_s \geqq 1$. We have the following theorem.

THEOREM 7. *For any sequence* (5.1) *the condition* (5.7) *is equivalent to*

$$\sum_{i=1}^{p^{nm}} e(A_1\alpha_1(i) + \cdots + A_s\alpha_s(i)) = o(p^{nm}) \tag{5.8}$$

for all $(A_1, \cdots, A_s) \neq (0, \cdots, 0)$.

As an immediate corollary we have:

THEOREM 8. *If* $\xi_1, \cdots, \xi_s \in \Phi$ *and* $1, \xi_1, \cdots, \xi_s$ *are linearly independent, then the sequence* $(A\xi_1, \cdots, A\xi_s)$, *where* A *runs through the polynomials in* $GF[p^n, x]$, *is* (*weakly*) *uniformly distributed.*

Theorem 2 is evidently contained in Theorem 8.

6. **The sum** $\sum e(\phi(A))$. In this section we shall prove the following theorem.

THEOREM 9. *Let $\phi(u)=\alpha_1 u+\cdots+\alpha_k u^k$, $\alpha_i\in\Phi$, be a polynomial of degree k with at least one irrational coefficient. Assume $1\leqq k<p$. Then*

$$S=\sum_{\deg A<m} e(\phi(A)) = o(p^{nm}) \qquad (m\rightarrow\infty). \tag{6.1}$$

The proof of this theorem depends upon the following theorem.

THEOREM 10. *Let ξ be an irrational number of Φ, $s\geqq 1$. Let N denote the number of sets of polynomials $A_1,\cdots,A_k$, $\deg A_i<m$, such that*

$$\deg((A_1\cdots A_k\xi-\beta)) < -s, \tag{6.2}$$

where β is an arbitrary number of Φ. Then

$$\lim_{m=\infty} p^{-nmk}N = p^{-ns}. \tag{6.3}$$

Proof. In view of Theorem 4 it suffices to show that

$$\sum_{A_1,\cdots,A_k,\deg A_j<m} e(A_1\cdots A_k\xi) = o(p^{nmk}) \tag{6.4}$$

for arbitrary irrationals ξ. We shall prove (6.4) by induction on k. For $k=1$ the result has already been proved. Now the left member of (6.4) may be written as

$$\sum_{A_1,\cdots,A_{k-1}}\sum_{A_k} e(BA_k\xi) \qquad (B=A_1\cdots A_{k-1}), \tag{6.5}$$

and by Theorem 1 the inner sum in (6.5) is 0 unless $\deg((B\xi))<-m$. Now for $r\geqq 1$, the number of sets of polynomials $A_1,\cdots,A_{k-1}$, $\deg A_j<m$, such that $\deg((A_1\cdots A_{k-1}\xi))<-r$, is asymptotic to $p^{nm(k-1)-nr}$ by the inductive hypothesis and therefore less than $2p^{nm(k-1)-nr}$ for sufficiently large m. Now if $\deg((A_1\cdots A_{k-1}\xi))\geqq -r$, the inner sum in (6.5) vanishes for $m\geqq r$. Hence, the sum (6.5) is less than

$$2p^{nm(k-1)-nr}p^{nm}=2p^{nmk-nr}.$$

Since r is arbitrary this proves (6.4).

We now prove Theorem 9 by Weyl's method. To begin with we assume α_k irrational. Then by (6.1)

$$|S|^2=\sum_{\deg A<m,\ \deg B<m} e(\phi(A+B)-\phi(B)) = \sum_{A,B} e(A\phi(A,B)),$$

where $\phi(u+v)-\phi(v)=u\phi(u,v)$, and $\deg \phi(u,v)=k-1$. Hence,

$$|S|^4\leqq p^{nm}\sum_A\left|\sum_B e(A\phi(A,B))\right|^2.$$

But

$$\left|\sum_{B} e(A\phi(A, B))\right|^{2} = \sum_{B, C} e(A\phi(A, B + C) - A\phi(A, C))$$

$$= \sum_{B, C} e(AB\phi(A, B, C)),$$

where $\phi(u, v+w)-\phi(u, w)=v\phi(u, v, w)$, so that

$$|S|^{4} \leqq p^{nm}\sum_{A, B}\sum_{C} e(AB\phi(A, B, C)).$$

Proceeding in this way we get after $k-1$ steps

$$|S|^{K} \leqq p^{nm(K-k)} \sum_{A_1, \cdots, A_k} e(A_1 \cdots A_k\xi) \qquad (K = 2^{k-1}), \tag{6.6}$$

where $\xi=k!\alpha_k$. Let $s\geqq 1$; then by Theorem 10 the number of sets $A_1, \cdots, A_{k-1}$, $\deg A_j<m$, $\deg ((A_1 \cdots A_{k-1}\xi))<-s$, is at most $2p^{nm(k-1)-ns}$ for sufficiently large m. Since the inner sum in (6.6) vanishes for $\deg ((A_1 \cdots A_{k-1}\xi)) \geqq -s$, $m\geqq s$, it follows that

$$|S|^{K} \leqq p^{nm(K-k)}\cdot 2p^{nm(k-1)-ns}\cdot p^{nm} = p^{nmK-ns}.$$

Since s is arbitrary this evidently implies the truth of (6.1) in the case α_k irrational.

Finally let $\alpha_k, \cdots, \alpha_{l+1}$ be rational, while α_l is irrational, and let G denote the least common denominator of $\alpha_k, \cdots, \alpha_{l+1}$, $\deg G=g$. Then replacing A by $GA+B$, we have

$$\sum_{\deg A<m+g} e(\phi(A)) = \sum_{\deg B<g} \sum_{\deg A<m} e(\phi(GA + B)). \tag{6.7}$$

But for fixed B, $\phi(Gu+B)$ is congruent (mod 1) to a polynomial of degree l with highest coefficient $\alpha_l G^l$ which is irrational. Hence, the previous case of the theorem applies to the inner sum in the right member of (6.7) and (6.1) holds in this case also. This completes the proof of Theorem 9.

The condition $k<p$ in Theorem 9 can apparently not be dropped. For example, the sum

$$\sum_{\deg A<m} e(A^{p}\alpha) = p^{nm} \tag{6.8}$$

for $\alpha=\sum_1^\infty c_i x^{-i}$, $i\not\equiv 1 \pmod p$. Again (for $n=1$) it is easily verified that

$$\sum_{\deg A<m} e((A^{p} - A)\alpha) = p^{nm} \tag{6.9}$$

for $\alpha=x^{-1}(c_0+\sum_1^\infty c_i\beta_i)$, $\beta_i=\sum_{j=0}^\infty x^{-ip^j}$. Each β_i is irrational (indeed algebraic). Thus, it is not evident for which polynomials $\phi(u)$, of degree not less than p, (6.1) holds.

7. **The sum** $\sum'\phi(A)$. We now consider the sum

$$S' = \sum_{\deg A=m}' e(\phi(u)), \tag{7.1}$$

where $\phi(u)$ has the same meaning as in Theorem 9, and $\sum'$ denotes that the sum is over primary polynomials of degree m only (that is, polynomials with highest coefficient $=1$). The method of proof used in Theorem 9 may be applied to S'. At the first step we get

$$\begin{aligned} |S'|^2 &= \sum_{A,B}' e(\phi(A) - \phi(B)) = \sum_{\deg A<m} \sum_{\deg B=m}' e(\phi(A + B) - \phi(B)) \\ &= \sum_{A} \sum_{B}' e(A\phi(A, B)), \end{aligned}$$

$$|S'|^4 \leqq p^{nm} \sum_{\deg A<m} \left| \sum_{B}' e(A\phi(A, B)) \right|^2.$$

Thus, the next step becomes

$$\left| \sum_{\deg B=m}' e(A\phi(A, B)) \right|^2 = \sum_{\deg B<m} \sum_{\deg C=m}' e(A\phi(A, B + C) - A\phi(A, C)),$$

and so on. Proceeding in this way we get

$$|S'|^K \leqq p^{nm(K-k)} \sum_{A_1,\cdots,A_{k-1}} \sum_{A_k}' e(A_1 \cdots A_k\xi), \tag{7.2}$$

the notation being the same as in (6.6); note that the inner sum is over primary A_k of degree m, while the outer sum is over all A_j of degree $<m$. Now apply Theorem 10, and we have proved the following theorem.

THEOREM 11. *For $\phi(u)$ as in Theorem 9, $1 \leqq k < p$,*

$$\sum_{\deg A=m}' e(\phi(A)) = o(p^{nm}) \qquad (m \to \infty). \tag{7.3}$$

We note that Theorem 11 can be deduced from Theorem 9 by placing $\phi(A) = \phi(x^m + B) = \phi_1(B)$, where $\deg B < m$; similarly, Theorem 9 is a corollary of Theorem 11. The direct proof is perhaps of interest. We also remark that there are cases for which $S' = 0$ while $S \neq 0$ and *vice versa.*

As an immediate corollary of Theorem 11 we mention

$$\sum_{\deg A\leqq m}' \frac{e(\phi(A))}{|A|} = o(m), \tag{7.4}$$

where $|A| = p^{n \deg A}$. We have also

$$\sum_{\deg A\leqq m}' \frac{e(\phi(A))}{|A|^r} = o(p^{nm(1-r)}) \qquad (r < 1). \tag{7.5}$$

The convergence of $\sum' e(\phi(A))|A|^{-r}$ for $r>1$ is trivial. The formulas (7.4), (7.5) are easily generalized.

That (7.4) and (7.5) cannot in general be improved (at least for $k=2$) will be clear from Theorem 23 below.

8. **Some applications.** We begin with the following theorem.

THEOREM 12. *Let*

$$\phi(u) = \alpha_0 + \alpha_1 u + \cdots + \alpha_k u^k \qquad (1 \leqq k < p), \tag{8.1}$$

and assume that at least one of the coefficients $\alpha_1, \cdots, \alpha_k$ *is irrational. Then the sequence* $\{e(\phi(A))\}$, *where* A *runs through* $GF[p^n, x]$, *is uniformly distributed* (mod 1).

This result is an immediate consequence of Theorems 4 and 9. As a particular case of Theorem 12 we see that the sequence $\{A^k\xi\}$ is uniformly distributed, provided $1 \leqq k < p$, ξ irrational.

THEOREM 13. *Let* $\phi_1(u), \cdots, \phi_s(u)$ *be* s *polynomials with coefficients in* Φ *such that any relation*

$$B_1\phi_1(u) + \cdots + B_s\phi_s(u) \equiv \alpha \pmod 1 \tag{8.2}$$

with $B_i \in GF[p^n, x]$ *implies* $B_i = 0$. *Then the sequence of points* $(\phi_1(A), \cdots, \phi_s(A))$ $(A \in GF[p^n, x])$ *is uniformly distributed* (mod 1).

Proof. The left member of (8.2) defines a polynomial $\phi(u)$ to which Theorem 9 may be applied.

THEOREM 14. *Let* ξ *be irrational*; $s_1, \cdots, s_k \geqq 1$; $\beta_1, \cdots, \beta_k$ *arbitrary numbers of* Φ. *Then the number of polynomials* A, deg $A < m$, *such that*

$$\deg((A^i\xi - \beta_i)) < -s_i \qquad (i = 1, \cdots, k)$$

is asymptotically

$$p^{nm-n(s_1+\cdots+s_k)} \qquad (m \to \infty).$$

Proof. In view of (5.3) this theorem is a special case of Theorem 13.

Another special case of interest is the following:

THEOREM 15. *Let* $\xi_1, \cdots, \xi_s \in \Phi$; $1, \xi_1, \cdots, \xi_s$ *linearly independent. Let* $\beta_{ij} \in \Phi$, $r_{ij} \geqq 1$; $i=1, \cdots, k$; $j=1, \cdots, s$. *Then the number of polynomials* A, deg $A < m$, *such that*

$$\deg((A^i\xi_j - \beta_{ij})) < -r_{ij} \qquad (i = 1, \cdots, k; j = 1, \cdots, s)$$

is asymptotically

$$p^{n(m-r)} \qquad \left(r = \sum_{i=1}^{k}\sum_{j=1}^{s} r_{ij}, m \to \infty\right).$$

9. **More general sequences.** Let α be a number of Φ and $A_1, A_2, A_3, \cdots$ a sequence of polynomials. Put

$$S(\alpha) = \sum_{i=1}^{m} e(A_i\alpha). \tag{9.1}$$

We shall show that

$$S(\alpha) = O(m^{1/2+\epsilon}) \tag{9.2}$$

for "almost all" α. First, we must explain what will be meant by "almost all."

Let $r \geqq 1$ be fixed. Two fractions G/H, G'/H' are *equivalent* provided [3, §3]

$$\deg ((G'H - GH')) < h + h' - r, \tag{9.3}$$

where $h = \deg H$, $h' = \deg H'$; we write $G/H \sim G'/H'$. It will be convenient to replace (9.3) by the equivalent condition

$$\deg ((G/H - G'/H')) < - r. \tag{9.4}$$

The fraction G/H is *primitive* (for r) provided $G/H \sim G'/H'$ implies $\deg H' \geqq \deg H$; in particular, all G/H are primitive for $\deg H \leqq r/2$. A *fundamental set* is a set of rationals $\alpha_1, \cdots, \alpha_s$ such that (i) no two are equivalent, and (ii) any given rational is equivalent to some α_i of the set. It follows that $s = p^{nr}$.

Let α be an arbitrary number of Φ. Then in the first place relatively prime polynomials G', H' can be found such that

$$\deg (H'\alpha - G') < - r \qquad (\deg H \leqq r). \tag{9.5}$$

If, in (9.5), G'/H' is not primitive, we replace it by an equivalent primitive fraction G/H. Then (9.5) and (9.4) imply

$$\deg (\alpha - G/H) < - r \qquad (\deg H \leqq r). \tag{9.6}$$

It is natural to extend the definition of equivalence to arbitrary numbers of Φ. If $\alpha, \beta \in \Phi$, we define $\alpha \sim \beta$ provided

$$\deg ((\alpha - \beta)) < - r. \tag{9.7}$$

Clearly $\sim$ is an equivalence relation. Thus, in view of (9.6) every α is equivlent to a primitive G/H.

We shall now say that almost all α have a certain property provided that the number N of nonequivalent α not having the property is such that N/p^{nr} is arbitrarily small (as $r \to \infty$).

Returning to (9.1) consider the sum

$$\sum_{\alpha}{}^{*} | S(\alpha) |^2 = \sum_{i,j=1}^{m} \sum_{\alpha}{}^{*} e((A_i - A_j)\alpha), \tag{9.8}$$

where $\sum^*$ denotes summation over a fundamental set of α's and $r>\deg A_i$, $i=1, \cdots, m$. Now, for $\deg A<r$ we have $\sum^* e(A\alpha)=0$ unless $A=0$ (for proof see [3, (3.13)]). Hence, (9.8) implies

$$(9.9) \qquad \sum_\alpha{}^* \left| S(\alpha) \right|^2 = mp^{nr}.$$

Now let N be the number of nonequivalent α such that

$$(9.10) \qquad \left| S(\alpha) \right| \geqq \eta m^{1/2+\epsilon},$$

where $\eta>0$, $\epsilon>0$. Then by (9.9)

$$mp^{nr} \geqq N\eta^2 m^{1+2\epsilon},$$

so that

$$(9.11) \qquad N \leqq \frac{p^{nr}}{\eta^2 m^{2\epsilon}} \cdot$$

This proves the following theorem.

THEOREM 16. *Let $A_1, \cdots, A_m$ be distinct polynomials, $r>A_i$, $\epsilon>0$, $\eta>0$. If N is the number of nonequivalent α for which* (9.10) *is satisfied, then* (9.11) *holds.*

In other words this shows that for almost all α, (9.2) holds.

In (9.1) it clearly makes no difference if we require $\deg \alpha<0$. This is no longer true for the more general sum

$$(9.12) \qquad S(\alpha) = S_\lambda(\alpha) = \sum_{i=1}^m e(\lambda_i\alpha),$$

where the λ_i are arbitrary numbers of Φ. In the sum (9.12) we therefore restrict ourselves to $\deg \alpha<0$. Now for $\deg \beta<0$ it follows that $\deg(\alpha\beta)<-1$ so that $e(\alpha\beta)=1$. Thus, if we put $\lambda_i=A_i+\beta_i$, $\beta_i=((\lambda_i))$, $\deg \beta_i<0$, we have $e(\lambda_i\alpha)=e(A_i\alpha)$. We therefore have the following extension of Theorem 16:

THEOREM 16′. *Let $\lambda_1, \cdots, \lambda_m$ be a set of distinct numbers of Φ, $r>\deg \lambda_i$, $\epsilon>0$, $\eta>0$. If N is the number of nonequivalent α, $\deg \alpha<0$, for which*

$$\left| \sum_{i=1}^m e(\lambda_i\alpha) \right| \geqq \eta m^{1/2+\epsilon},$$

then (9.11) *holds. In other words,*

$$\left| S_\lambda(\alpha) \right| < \eta m^{1/2+\epsilon}$$

for almost all α, $\deg \alpha<0$.

For $\alpha=\sum_0^\infty c_i x^{-p^i}$ and any sequence $\{A_i\}=\{x^{e_i}\}$, $e_i<e_{i+1}$, we have

$S(\alpha)=\Omega(m)$, except possibly when infinitely many e_i are of the form p^j-1; all α defined by the above series are irrational. Other examples of this kind are easily constructed.

Another conclusion can be drawn from (9.9); namely, the assertion $S(\alpha)=o(m^{1/2})$ for all α is false. We have therefore the following theorem.

THEOREM 17. *For any sequence* $\{\lambda_j\}$ *there exist irrationals* α *such that*

$$S_\lambda(\alpha) = \Omega(m^{1/2}) \qquad (m\rightarrow\infty).$$

10. **The sum** $S_m(\alpha, \beta)$. In the remainder of the paper we assume p odd. Let $\alpha, \beta\in\Phi$ and define

$$S_m(\alpha, \beta) = \sum_{\deg A<m} e(\alpha A^2 + 2\beta A). \tag{10.1}$$

To begin with let $\beta\equiv 0 \pmod 1$ and put

$$S_m(\alpha) = S_m(\alpha, 0) = \sum_{\deg A<m} e(\alpha A^2). \tag{10.2}$$

We shall again make use of the properties of equivalence in Φ as defined in §9; we take $r=2m$. Let $\alpha\sim G/H$, where G/H is primitive; then clearly

$$S_m(\alpha) = \sum_{\deg A<m} e(GA^2/H) = S_m(G/H). \tag{10.3}$$

The sum (10.3) has been discussed previously [3, p. 1134] and we have

$$S_m(G/H) = \begin{cases} S(G/H) & (h > m), \\ p^{n(m-h)}S(G/H) & (h \leqq m), \end{cases} \tag{10.4}$$

where $h=\deg H$ and

$$S(G, H) = \sum_{A \pmod H} e(GA^2/H) \tag{10.5}$$

is a Gauss sum. Thus, in particular,

$$| S_m(\alpha) |^2 = \begin{cases} p^{nh} & (h > m), \\ p^{n(2m-h)} & (h \leqq m). \end{cases} \tag{10.6}$$

But this does not indicate explicitly that $S_m(\alpha)=o(p^{nm})$; in Theorem 19 below we show that this is indeed true for all irrational α.

There is no loss in generality in assuming $\deg \alpha=-a<0$. Now consider the sum $S_{m-a}(1/\alpha)$. In the first place $\deg (\alpha-G/H)<-r$, where G/H is primitive, implies

$$\deg\left(\frac{1}{\alpha}-\frac{H}{G}\right) < -(r-2a); \tag{10.7}$$

also H/G is primitive for $r-2a$ for otherwise G/H is not primitive for r, as is easily verified. Then as in (10.3) and (10.4) we have, for $m \geqq a$,

$$(10.8) \qquad S_{m-a}\left(\frac{1}{\alpha}\right) = S_{m-a}(H/G) = \begin{cases} S(H/G) & (g > m - a), \\ p^{n(m-a-g)}S(H/G) & (g \leqq m - a), \end{cases}$$

where $g = \deg G$. (Note that in the proof of (10.4), H is assumed primary; since G need not be primary, a little care is needed in using (10.8).)

Since $h - g = a$ it is clear that $h > m$ if and only if $g > m - a$ so that the side conditions in (10.4) and (10.8) correspond. Comparison of these two formulas now leads at once to

$$(10.9) \qquad S_m(\alpha) = \eta p^{na/2} S_{m-a}\left(\frac{1}{\alpha}\right) \qquad (m \geqq a),$$

where η is a complex number of absolute value 1; indeed $\eta = \pm 1, \pm i$. It is easy to give an explicit formula for η but this will not be required in the applications.

Returning to the general sum (10.1) we first note several easily proved formulas

$$(10.10) \qquad \begin{aligned} S_m(\alpha, \beta) &= S_m(\alpha_1, \beta_1) && (\alpha \equiv \alpha_1, \beta \equiv \beta_1 \pmod 1), \\ S_m(\alpha, \beta + B\alpha) &= e(-\alpha B^2 - 2\beta B) S_m(\alpha, \beta) && (\deg B < m). \end{aligned}$$

$$(10.11) \qquad S_m(\alpha, \beta + \beta_1) S_m(\alpha, \beta - \beta_1) = S_m(2\alpha, 2\alpha) S_m(2\alpha, 2\beta_1).$$

To prove (10.11) we substitute from (10.1) in the left member. This gives

$$\sum_{A,B} e(\alpha(A^2 + B^2) + 2(\beta + \beta_1)A + 2(\beta - \beta_1)B);$$

now put $A = A' + B'$, $B = A' - B'$, and (10.11) follows immediately.

As in the proof of (10.9), let $\deg \alpha = -a < 0$, $\deg (\alpha - G/H) < -r$, where G/H is primitive. Then in the first place

$$(10.12) \qquad S_m(\alpha, \beta) = S_m(G/H, \beta).$$

Next we have

$$(10.13) \qquad \begin{aligned} |S_m(G/H, \beta)|^2 &= \sum_{A,B} e\left(\frac{G(A+B)^2}{H} + 2\beta(A+B) - \frac{GB^2}{H} - 2\beta B\right) \\ &= \sum_{\deg A < m} e\left(\frac{GA^2}{H} + 2\beta A\right) \sum_{\deg B < m} e\left(2\frac{GAB}{H}\right). \end{aligned}$$

Now by Theorem 1 the inner sum in (10.13) vanishes unless

$$(10.14) \qquad \deg ((AG/H)) < -m.$$

Assume first that $h = \deg H \leqq m$. Then (10.14) implies $AG \equiv 0 \pmod H$, and therefore $H|A$. Thus, (10.13) becomes

$$|S_m(G/H,\beta)|^2 = p^{nm} \sum_{\deg C<m-h} e(2\beta HC) \qquad (h \leqq m). \tag{10.15}$$

In the next place let $h>m$. We put (10.14) in the form

$$AG = HU + V \qquad (\deg V < h - m). \tag{10.16}$$

Since $(G, H)=1$ we can find polynomials G_1, H_1 such that

$$GH_1 - G_1H = 1 \qquad (h_1 < h,\ h + h_1 \leqq r), \tag{10.17}$$

where $h_1=\deg H_1$. (The inequality $h+h_1>r$ contradicts G/H primitive.) Now by (10.16) and (10.17) we have

$$\frac{G}{H} - \frac{U}{A} = \frac{V}{HA}, \qquad \frac{G}{H} - \frac{G_1}{H_1} = \frac{1}{HH_1},$$

so that

$$\frac{G_1}{H_1} = \frac{U}{A} = \frac{1}{H}\left(\frac{V}{A} - \frac{1}{H_1}\right)$$

and therefore

$$G_1A - H_1U = \frac{1}{H}(VH_1 - A). \tag{10.18}$$

Now, by (10.16), $\deg (VH_1) < h+h_1-m \leqq m < h$ and $\deg A < m < h$; therefore, (10.18) implies $A = VH_1$. Note also that (10.14) implies $\deg ((GA^2/H)) < -1$ so that $e(GA^2/H)=1$. Thus, (10.13) leads to

$$|S_m(G/H,\beta)|^2 = p^{nm} \sum_{\deg V<h-m} e(2\beta H_1V) \qquad (h > m), \tag{10.19}$$

which may be compared with (10.15). We now apply Theorem 1 to (10.15) and (10.19) and get

$$|S_m(G/H,\beta)|^2 = \begin{cases} p^{n(2m-h)} & (\deg ((\beta H)) < h - m), \\ 0 & (\deg ((\beta H)) \geqq h - m) \end{cases} \tag{10.20}$$

for $h \leqq m$,

$$|S_m(G/H,\beta)|^2 = \begin{cases} p^{nh} & (\deg ((\beta H_1)) < m - h), \\ 0 & (\deg ((\beta H_1)) \geqq m - h) \end{cases} \tag{10.21}$$

for $h>m$.

We can now complete the proof of the following theorem of which (10.9) is a special case.

THEOREM 18. *If* $\deg \alpha = -a < 0$, $\deg \beta < 0$, $m \geqq a$, *then*

$$S_m(\alpha, \beta) = \eta p^{na/2} S_{m-a}\left(\frac{1}{\alpha}, \frac{\beta}{\alpha}\right), \tag{10.22}$$

where η is a complex number of absolute value 1.

Proof. It will be convenient to write down the formulas corresponding to (10.20) and (10.21) for the sum $S_{m-a}(1/\alpha, \beta/\alpha)$. As in the proof (10.9) we have first

$$S_{m-a}(1/\alpha, \beta/\alpha) = S_{m-a}(H/G, H\beta/G), \tag{10.12'}$$

while (10.20) and (10.21) become

$$|S_{m-a}(H/G, H\beta/G)|^2 = \begin{cases} p^{n(2m-2a-g)} & (\deg ((\beta H)) < g - m + a), \\ 0 & (\deg ((\beta H)) \geqq g - m + a) \end{cases} \tag{10.20'}$$

for $g \leqq m - a$,

$$|S_{m-a}(H/G, H\beta/G)|^2 = \begin{cases} p^{ng} & (\deg ((G_1 H\beta/G)) < m - a - g), \\ 0 & (\deg ((G_1 H\beta/G)) \geqq m - a - g) \end{cases} \tag{10.21'}$$

for $g > m - a$.

Now we recall that the condition $h \leqq m$ is equivalent to $g \leqq m - a$. Thus, comparison of (10.20′) with (10.20) shows that the theorem is correct in the case $h \leqq m$. For $h > m$ we must examine the side condition $\deg ((G_1 H\beta/G)) < m - a - g = m - h$. It follows from (10.17) that

$$\deg ((H_1\beta)) - \deg ((G_1 H\beta/G)) = \deg (\beta/G) < -g < m - h,$$

so that the side conditions in (10.21) and (10.21′) are indeed equivalent. This evidently completes the proof of the theorem.

Theorem 18 may be compared with Theorem 2.128 of [6].

11. **Bounds for $S_m(\alpha, \beta)$.** As in [6, p. 211] let the irrational α be exhibited as a simple continued fraction [1, p. 190]

$$\alpha = \frac{1}{A_1 +} \frac{1}{A_2 +} \cdots; \tag{11.1}$$

also put

$$\alpha = \frac{1}{A_1 + \alpha_1}, \quad \alpha_1 = \frac{1}{A_2 + \alpha_2}, \cdots \qquad (\deg A_i \geqq 1), \tag{11.2}$$
$$\beta_1 = ((\beta/\alpha)), \quad \beta_2 = ((\beta_1/\alpha_1)), \cdots,$$

so that $\deg \alpha_i = -a_i < 0$, $\deg \beta_i < 0$.

Then by (10.20)

$$S_m(\alpha, \beta) = np^{na/2}S_{m-a}\left(\frac{1}{\alpha}, \frac{\beta}{\alpha}\right) = \eta p^{na/2}S_{m-a}(\alpha_1, \beta_1),$$

where η denotes a complex number of absolute value 1, which may change from equation to equation. Transforming $S_{m-a}(\alpha_1, \beta_1)$ in the same way, we get

$$S_{m-a}(\alpha_1, \beta_1) = \eta p^{na_1/2}S_{m-a-a_1}(\alpha_2, \beta_2),$$

so that

$$S_m(\alpha, \beta) = \eta p^{n(a+a_1)/2}S_{m-a-a_1}(\alpha_2, \beta_2).$$

Continuing in this way we have

$$S_m(\alpha, \beta) = \eta p^{nt/2}S_{m-t}(\alpha_s, \beta_s), \tag{11.3}$$

provided $m-t\geqq 0$, where $t=a+a_1+\cdots+a_{s-1}$.

We now fix s by means of the inequalities

$$a + a_1 + \cdots + a_{s-1} \leqq m < a + a_1 + \cdots + a_s. \tag{11.4}$$

Clearly $t\rightarrow\infty$ as $s\rightarrow\infty$; hence, it follows from (11.3) that

$$S_m(\alpha, \beta) = O(p^{nt/2}p^{n(m-t)}) = o(p^{nm})$$

uniformly in β.

We have therefore the following theorem.

THEOREM 19. *If α is irrational, then*

$$S_m(\alpha, \beta) = o(p^{nm}) \qquad (m\rightarrow\infty)$$

uniformly for all β. In particular, $S_m(\alpha)=o(p^{nm})$.

THEOREM 20. *If the partial quotients A_i in the infinite continued fraction* (11.1) *are of bounded degree, then*

$$S_m(\alpha, \beta) = O(p^{nm/2}) \qquad (m\rightarrow\infty) \tag{11.5}$$

uniformly for all β.

This is an immediate consequence of (11.3) for

$$S_{m-t}(\alpha_s, \beta_s) = O(p^{n(m-t)}) = O(p^{na_s}) = O(1).$$

THEOREM 21. *If α is irrational and $a_m=o(m)$, then*

$$S_m(\alpha, \beta) = O(p^{nm(1/2+\epsilon)}) \tag{11.6}$$

for all $\epsilon>0$.

Indeed, we have

$$t/2 + (m - t) < t/2 + a_s \leqq m/2 + a_m \leqq m(1 + \epsilon)/2,$$

which proves the theorem.

THEOREM 22. *If α is irrational and $a_m < \delta m$ for m sufficiently large, $\delta > 0$, then*

$$S_m(\alpha, \beta) = O(p^{nm(1+\delta'+\epsilon)/2}) \qquad \left(\delta' = \frac{\delta}{1+\delta}\right) \tag{11.7}$$

for all $\epsilon > 0$.

Proof. We shall require the following formula:

$$| S_m(\alpha, \beta) | \leqq \begin{cases} p^{na/2} & (m < a < 2m), \\ p^{nm} & (2m < a) \end{cases} \tag{11.8}$$

for deg $\alpha = -a$, $a > m$.

The second half of (11.8) is obvious from the definition of $S_m(\alpha, \beta)$. To prove the first half of the formula we start with

$$| S_m(\alpha, \beta) |^2 = \sum_{\deg A < m} e(\alpha A^2 + 2\beta A) \sum_{\deg B < m} e(2AB).$$

The inner sum vanishes unless deg $((\alpha A)) < -m$. Since deg $\alpha < -m$, this implies deg $A < a - m$ and the formula follows.

In the next place we remark that δ may be considered the minimal δ for which the hypothesis of the theorem holds; otherwise, Theorem 21 applies. Hence, there is an infinite sequence of integers $s_1, s_2, s_3, \cdots$, such that

$$m_i \geqq a + a_1 + \cdots + a_{s_i} \geqq s_i + a_{s_i} > s_i(1 + \delta_1)$$

for all positive $\delta_1 < \delta$. Then by (11.3), (11.4), and (11.8), we have for $m - t < a_s < 2(m-t)$

$$\frac{t}{2} + \frac{a_s}{2} \leqq \frac{m}{2} + \frac{\delta s}{2} < \frac{m}{2}\left(1 + \frac{\delta}{\delta_1}\right);$$

while for $a_s > 2(m-t)$, we have

$$\frac{t}{2} + (m - t) < \frac{t}{2} + \frac{a_s}{2} < \frac{m}{2}\left(1 + \frac{\delta}{\delta_1}\right).$$

Thus (11.7) certainly holds for the sequence $\{m_i\}$; but for other values of m the proof indicates that the formula will hold with a smaller value for δ'. Thus, the theorem is true in general.

12. **Ω-theorems.** For $\beta = 0$, (11.3) becomes

$$S_m(\alpha) = \eta p^{nt/2} S_{m-t}(\alpha_s). \tag{12.1}$$

We shall now prove the following theorem.

THEOREM 23. *If $\phi(m)>0$, $\phi(m)\rightarrow\infty$ as $m\rightarrow\infty$, then there exist irrationals α such that*

$$S_m(\alpha) = \Omega(p^{nm}/\phi(m)) \qquad (m \rightarrow \infty). \tag{12.2}$$

This result shows that the equation $S_m(\alpha)=o(p^{nm})$ is the best result that can be stated for *all* irrationals.

To prove Theorem 23 we first remark that

$$S_m(\alpha) = p^{nm} \qquad (\deg \alpha \leqq -2m), \tag{12.3}$$

which is evident from (10.2). Thus,

$$S_{m-t}(\alpha_s) = p^{n(m-t)} \qquad (a_s \geqq 2(m-t)). \tag{12.4}$$

Substituting from (12.4) in (12.2) we get

$$S_m(\alpha) = p^{n(m-t/2)}. \tag{12.5}$$

Hence, to prove (12.2) it will suffice to exhibit an irrational α and a sequence $m_1, m_2, m_3, \cdots \rightarrow \infty$ such that

$$p^{n(m-t/2)} \geqq p^{nm}/\phi(m),$$

or what is the same thing, $p^{nt/2} \leqq \phi(m)$, and also $a_s \geqq 2(m-t)$. We take

$$m_s = a + a_1 + \cdots + a_{s-1} + a_s/2;$$

then the corresponding value of t is

$$t_s = a + a_1 + \cdots + a_{s-1}$$

(so that $a_s = 2(m-t)$). Thus, the only condition remaining to be satisfied is

$$p^{n(a+a_1+\cdots+a_{s-1})/2} \leqq \phi(a + a_1 + \cdots + a_{s-1} + a_s/2). \tag{12.6}$$

Take $a=1$; if $a_1, \cdots, a_{s-1}$ have already been found, then clearly a_s can be determined so that (12.6) holds. Thus, a sequence a_s can be found which satisfies the several requirements. Finally, given the $\{a_s\}$ we can find polynomials A_s and therefore α by means of (11.1); in particular, we may take $A_s = x^{a_s-1}$. That all such α's are irrational is clear from the fact that the continued fraction (11.1) is not terminating.

To extend (12.2) to general $S_m(\alpha, \beta)$ we note first that in place of (12.3) we have $S_m(\alpha,\beta)=0$ or p^{nm} for $\deg \alpha \leqq -2m$. The remainder of the proof goes through so that we may state the following theorem.

THEOREM 23′. *There exist irrationals α such that either $S_m(\alpha, \beta)=0$ or*

$$S_m(\alpha, \beta) = \Omega(p^{nm}/\phi(m)) \qquad (m \rightarrow \infty).$$

A condition for the vanishing of $S_m(\alpha, \beta)$ is contained in (10.20) and (10.21), but it is not very simple.

In the next place it is easy to get a lower bound for $S_m(\alpha)$ which is valid for all α, rational as well as irrational. Indeed, by (10.6) we have $|S_m(\alpha)|^2 \geqq p^{nm}$. As for $S_m(\alpha, \beta)$, we again use (10.20) and (10.21). We may state the following:

THEOREM 24. *For all α we have*

$$S_m(\alpha) \geqq p^{nm/2}.$$

For all α, β, either $S_m(\alpha, \beta) = 0$ or

$$|S_m(\alpha, \beta)| \geqq p^{nm/2}.$$

This result shows that (11.5) cannot be improved.

Finally, we prove:

THEOREM 25. *There exist irrationals α such that $a_m < \delta m$ for m sufficiently large, $\delta > 0$, and*

$$|S_m(\alpha)| \geqq p^{nm(1+\delta')/2} \qquad \left(\delta' = \frac{\delta}{1+\delta}\right).$$

Comparing with the proof of Theorem 22, we select a sequence of integers $s_1, s_2, s_3, \cdots$ and take $a=1$, $a_s = 1$ for $s \neq s_i$, a_{s_i} = smallest integer not less than δs_i. We also require the inequality

$$(12.7) \qquad |S_m(\alpha)| \geqq p^{na/2} \qquad (a = \deg \alpha > m),$$

which follows from (10.6). Then, by (12.1) and (12.7),

$$|S_m(\alpha)| \geqq p^{nt/2} p^{na_s/2}.$$

It will therefore suffice to show that

$$t_s + a_s \geqq m_s(1 + \delta'),$$

which surely holds provided

$$(12.8) \qquad \delta s_i \geqq (1 + \delta')(m_s - t_s) + \delta' t_s.$$

Since the sequence $\{s_i\}$ is at our disposal, it is clear that we can select it in such a way that (12.8) is satisfied. This completes the proof of the theorem.

REFERENCES

1. E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*, Math. Zeit. vol. 19 (1924) pp. 153–206.

2. H. Bohr and B. Jessen, *One more proof of Kronecker's theorem*, J. London Math. Soc. vol. 7 (1932) pp. 274–275.

3. L. Carlitz, *Representation of arithmetic functions in $GF[p^n, x]$*, Duke Math. J. vol. 14 (1947) pp. 1121–1137.

4. ———, *The singular series for sums of squares of polynomials*, Duke Math. J. vol. 14 (1947) pp. 1105–1120.

5. ——, *Some applications of a theorem of Chevalley*, Duke Math. J. vol. 18 (1951) pp. 811–820.

6. G. H. Hardy and J. E. Littlewood, *Some problems of Diophantine approximation*, Acta Math. vol. 37 (1914) pp. 155–239.

7. J. F. Koksma, *Diophantische Approximationen*, Berlin, 1936.

8. K. Mahler, *An analogue to Minkowski's geometry of numbers in a field of series*, Ann. of Math. vol. 42 (1941) pp. 488–522.

9. Hermann Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. vol. 77 (1916) pp. 313–352.

Duke University,
Durham, N. C.