Hence (A) holds with $M = 1$ if m is odd. But if m is even, (A) holds for $m/2$ with $M = 1$. Since (A) represents 2, (A) also represents m. If $m \equiv 0 \pmod 3$, $x = 3X$, $z = 3Z$ and we have again (A).

Take finally (C) and multiply by $1^2 - 3 \cdot 1^2 = -2$. Then

$$(x-3y)^2 - 3(x-y)^2 - 4z^2 + 12w^2 = -2m.$$

Write this as

$$AB - 3CD = -2m, \tag{11}$$

where

$$A = x-3y+2z, \quad B = x-3y-2z, \quad C = x-y+2w, \quad D = x-y-2w.$$

We require the condition that x, y, z, w be integers for given integers A, B, C, D. These are obviously,

$$A \equiv B \pmod 4, \quad C \equiv D \pmod 4;$$

and

$$A+B-C-D \equiv 0 \pmod 4, \quad \text{i.e.,} \quad A \equiv C \pmod 2,$$

since

$$x-3y = \frac{A+B}{2}, \quad x-y = \frac{C+D}{2}.$$

Hence

$$A^2 - 3C^2 \equiv -2m \pmod 4.$$

If $m \equiv 1 \pmod 2$, we take $A \equiv C \equiv 1 \pmod 2$. Then we can satisfy formula (11) by taking $A \equiv B \equiv C \equiv D \equiv 1 \pmod 4$.

If $m \equiv 0 \pmod 2$, (C) holds for $m/2$ and also for 2 with $M = 1$, and so also for m.

A similar argument holds when $m \equiv 0 \pmod 3$.

There is no need to give further instances of the method.

ST. JOHNS COLLEGE,
CAMBRIDGE, ENGLAND

Reçu par la Rédaction le 17. 1. 1966

ACTA ARITHMETICA
XII (1966)

Uniform distribution of sequences in GF[q, x]*

by

JOHN H. HODGES (Boulder, Colorado)

1. Introduction and preliminaries. Let $\Phi = \mathrm{GF}[q, x]$, denote the ring of polynomials in an indeterminate x over an arbitrary finite field $\mathrm{GF}(q)$ of q elements. Throughout this paper italic capitals $A, B, M, H, \ldots$ will denote elements of Φ, except as indicated.

Let M be any element of Φ of degree $m > 0$. Then a complete residue system modulo M (in Φ) contains q^m elements. One such complete residue system consists of all elements of Φ of degree $< m$. (For this purpose, the zero polynomial may be regarded as having degree $< m$ for all $m > 0$.) Let $\theta = \{A_i\}$ be an infinite sequence of elements of Φ. For any $B \in \Phi$ and any integer $n \geqslant 1$, define $\theta(n, B, M)$ as the number of terms among $A_1, \ldots, A_n$ such that $A_i \equiv B \pmod M$. Then following Niven ([5], § 1) we say that the sequence θ is *uniformly distributed modulo* M, abbreviated as u.d. (mod M), if and only if

$$\lim_{n\to\infty} \theta(n, B, M)/n = q^{-m} \quad (\text{all } B \in \Phi). \tag{1.1}$$

Furthermore, we say that the sequence θ is *uniformly distributed*, abbreviated as u.d., if and only if it is u.d. (mod M) for every M of degree > 0 in Φ.

For certain questions of interest concerning sequences in Φ, a somewhat weaker condition than (1.1) must be used. Let $\theta = \{A_i\}$ be any infinite sequence of elements of Φ in which no element of Φ appears infinitely many times. For any $B \in \Phi$, any integer $n \geqslant 1$ and any $M \in \Phi$ of degree $m > 0$, let

$$\begin{cases} \theta(n) = \text{number of terms of } \theta \text{ such that } \deg A_i < n, \\ N(\theta, n, B, M) = \text{number of terms of } \theta \text{ such that } \deg A_i < n \\ \qquad\qquad \text{and } A_i \equiv B \pmod M. \end{cases} \tag{1.2}$$

* Supported by NSF Research Grant GP 2542 and NSF Science Faculty Fellowship 64203.

Then θ is called *weakly uniformly distributed modulo* M, abbreviated as w.u.d. (mod M), if and only if

$$\lim_{n\to\infty} N(\theta, n, B, M)/\theta(n) = q^{-m} \quad \text{(all } B \in \Phi\text{)}, \tag{1.3}$$

and is called *weakly uniformly distributed*, abbreviated as w.u.d., if and only if it is w.u.d. (mod M) for every M of degree > 0 in Φ.

Note that in (1.1) and (1.3) we need only let B run through the q^m elements of any complete residue system modulo M, and that without any loss of generality we can restrict our study to the case where M is *monic* (or *primary*), that is, has coefficient of x^m equal to 1. The case $M = 1$ is omitted because it is trivial here and also because the phrases "uniformly distributed (mod 1)" and "weakly uniformly distributed (mod 1)" have been given a different meaning, as indicated in § 4 of the present paper, by Carlitz ([2], § 4). Throughout this paper, therefore, the term monic will mean *monic of positive degree.*

In this paper we investigate some properties of uniform distribution and weak uniform distribution of sequences of elements of Φ. Unless otherwise noted, the word sequence whenever used here will mean *infinite* sequence of elements of Φ. All of the results obtained in the paper, as well as most of the proofs given, are the analogs for sequences in Φ of results given by Ivan Niven ([5]) for sequences of rational integers. In § 2 we consider the relationship between w.u.d. (mod M) for a *rising* sequence θ (an analog for Φ of a strictly increasing sequence of positive integers) and various *density* properties possessed by θ and its *complementary* sequence θ^*. In § 3 we prove a number of elementary theorems concerning the relationships that exist among uniform distribution (and weak uniform distribution) of a sequence with respect to different moduli M and F and to their product MF. In § 4 several theorems are proved concerning weak uniform distribution of sequences of polynomials generated by certain *irrationals* in a field Φ' which contains the quotient field of Φ. Finally, in § 5, an exponential property of sequences and its relation to uniform distribution (weak uniform distribution) is discussed.

In a subsequent paper the author will consider the analogs for Φ of results proved by Niven ([5], § 4), Burke Zane ([7]) and Stephan R. Cavior ([3], [4]) for sequences of integers generated by polynomials with integral coefficients.

It is an immediate consequence of the definitions given above that a sequence $\theta = \{A_i \mid i \geqslant 1\}$ is u.d. (mod M) [w.u.d. (mod M)] if and only if the truncated sequence $\theta_r = \{A_i \mid i \geqslant r\}$ is u.d. (mod M) [w.u.d. (mod M)] for any fixed positive integer r. Similarly, θ is u.d. (mod M) [w.u.d. (mod M)] if and only if $\theta + C = \{A_i + C \mid i \geqslant 1\}$ is u.d. (mod M) [w.u.d. (mod M)] where C is any element of Φ.

If M is monic, it is easily shown that for any integer $t \geqslant m$, each residue class modulo M in Φ contains the same number, namely $(q-1)q^{t-m}$, of different polynomials of degree t.

2. Weak uniform distributivity and complementary sequences. A sequence $\theta = \{A_i\}$ will be called a *rising* sequence if and only if degree $A_i \leqslant$ degree A_{i+1} for all integers $i \geqslant 1$ and $A_i \neq A_j$ for $i < j$. (This is an analog for Φ of a strictly increasing sequence of positive integers.) In particular, any sequence Γ containing all of the elements of Φ, each occurring once, arranged according to monotonically increasing degree is a rising sequence. In view of the remark at the end of § 1, it is clear that every such Γ is w.u.d. However, a given such Γ need not be u.d. since there may exist a monic M for which Γ is not u.d. (mod M). For example, let M be an arbitrary monic polynomial of degree m. Let Γ be any rising sequence containing all elements of Φ and such that for every integer $t \geqslant m$, the $(q-1)q^{t-m}$ elements of Φ of degree t which are congruent to 0 modulo M are preceded by all the other $(q-1)(q^m-1)q^{t-m}$ elements of Φ of degree t. Then for any such t, with $n_t = q^t + (q-1)(q^m-1)q^{t-m}$ we have $\Gamma(n_t, 0, M) = q^{t-m}$ so that

$$\Gamma(n_t, 0, M)/n_t = [q(q^m-1)+1]^{-1} < q^{-m}.$$

Therefore,

$$\lim_{t\to\infty} \Gamma(n_t, 0, M)/n_t = [q(q^m-1)+1]^{-1} < q^{-m},$$

so that in view of (1.1), Γ is not u.d. (mod M).

For sequences of integers the problem illustrated above does not arise. That is, for a strictly increasing sequence of positive integers, the analogs of the concepts of uniform distributivity (mod M) and weak uniform distributivity (mod M) are equivalent. (See [5], § 1.) For a rising sequence θ in Φ, of course, if θ is u.d. (mod M) then θ is w.u.d. (mod M).

If θ is a rising sequence in Φ and for all integers $n \geqslant 1$, $\theta(n)$ is defined by (1.2), we define

$$\begin{cases} \textit{asympotic density of } \theta = \liminf\limits_{n\geqslant 1} q^{-n}\theta(n), \\ \textit{natural density of } \theta = \lim\limits_{n\to\infty} q^{-n}\theta(n) \text{ (if limit exists)}. \end{cases} \tag{2.1}$$

Let θ be any rising sequence. If the set complement of θ in Φ is finite, then we define the *complementary sequence* of θ to be any finite sequence formed by use of all the elements of this set complement. If the set complement of θ in Φ is infinite, then we define the *complementary sequence* of θ to be *any rising* sequence formed by use of all the elements of this

set complement. The complementary sequence of θ will be simply called the *complement* of θ and will be denoted by θ^*. We note that definitions (1.2) and (2.1) can be extended without change to any finite complement θ^* with the result that θ^* has natural (and so also asymptotic) density equal to 0. It is also clear that for an infinite complement θ^*, both the asympototic density and the natural density (when it exists) of θ^* are uniquely defined as functions of θ, that is, are independent of the particular choice of order of occurrence in θ^* of elements of the same degree. Thus, with respect to the properties that we will be concerned with here, there is no ambiguity involved in speaking of the complement θ^* of θ.

We now prove two theorems concerning the relationship between weak uniform distributivity (mod M) of a rising sequence θ and density properties possessed by θ or θ^*. First we have (compare with [5], § 2)

THEOREM 2.1. *If θ is a rising sequence whose complement θ^* has natural density equal to* 0, *then θ is* w.u.d., *that is, θ is* w.u.d. (mod M) *for every monic M in Φ.*

Proof. If θ^* is finite so that θ contains all except a finite number of elements of Φ, in view of the remarks at the end of § 1, it is clear that since θ is a rising sequence it is w.u.d. (mod M) for all monic M in Φ.

Therefore, suppose that θ^* is infinite. If Γ denotes any rising sequence formed by using all the elements of Φ, then for all integers $n \geqslant 1$

$$\Gamma(n) = \theta(n) + \theta^*(n) = q^n.$$

Also for any $B \in \Phi$, any monic M of degree m and all $n \geqslant 1$,

$$N(\Gamma, n, B, M) = N(\theta, n, B, M) + N(\theta^*, n, B, M). \tag{2.2}$$

Since by hypothesis θ^* has natural density 0 and by definition (1.2) $0 \leqslant N(\theta^*, n, B, M) \leqslant \theta^*(n)$ for all $n \geqslant 1$, then

$$1 = \lim_{n\to\infty} q^{-n}\Gamma(n) = \lim_{n\to\infty} q^{-n}[\theta(n) + \theta^*(n)] = \lim_{n\to\infty} q^{-n}\theta(n) \tag{2.3}$$

and

$$\lim_{n\to\infty} q^{-n} N(\theta^*, n, B, M) = 0. \tag{2.4}$$

Consequently, since Γ is clearly w.u.d. (mod M) in view of the remark at the end of § 1, using (2.2), (2.3) and (2.4) we get

$$q^{-m} = \lim_{n\to\infty} N(\Gamma, n, B, M)/\Gamma(n) = \lim_{n\to\infty} q^{-n}[N(\theta, n, B, M) + N(\theta^*, n, B, M)]$$

$$= \lim_{n\to\infty} [q^{-n}\theta(n)][N(\theta, n, B, M)/\theta(n)] = \lim_{n\to\infty} N(\theta, n, B, M)/\theta(n).$$

Thus, in view of the definition, θ is w.u.d. (mod M). Since this is true for all monic M it follows that θ is w.u.d.

Using Theorem 2.1 we can show that the answer to both of the following questions is no. Let θ be a rising sequence whose complement θ^* is infinite. If θ is w.u.d. (mod M) [or w.u.d.] must θ^* also be? For let θ be any rising sequence containing all the elements of Φ except for a a sequence $\theta^* = \{A_i^*\}$ whose ith element A_i^* is a prime polynomial of degree i for all $i \geqslant 1$. (Compare with the example given by Niven [5], § 2, to answer the analogous questions for strictly increasing sequences of positive integers.) Then θ^* is the complement of θ and clearly has natural density equal to 0. Therefore by Theorem 2.1, θ is w.u.d. (mod M) for every monic M. But for every such M, there exists at most one value of i such that $A_i^* \equiv 0 \pmod M$ so that θ^* is not w.u.d. (mod M). However, it is easy to give an example to show that for a rising sequence θ and a monic polynomial M, the fact that θ has natural density equal to 0 does not imply that θ is not w.u.d. (mod M). For instance, if $q = 2$, taking $M = x$ and $\theta = \{A_i\}$ with $A_i = x^i$ for i odd and $A_i = 1 + x^i$ for i even, then θ is in fact u.d. (mod x).

On the other hand, the complement θ^* of a rising sequence θ, just as in the corresponding situation for strictly increasing sequences of positive integers ([5], Theorem 2.1), does inherit weak uniform distributivity from θ in case θ^* has positive asymptotic density. This is the content of

THEOREM 2.2. *Let θ be a rising sequence whose complement θ^* has positive asymptotic density. Then if θ is* w.u.d. (mod M) *for a given monic M in Φ, so is θ^*. Thus if θ is* w.u.d., *then so is θ^*.*

Proof. In view of the definition of w.u.d. we need only prove the first of the two assertions. Let $B \in \Phi$ be arbitrary and M be monic of degree m such that θ is w.u.d. (mod M). Recalling the definition (1.2) of $N(\theta, n, B, M)$ for any integer $n \geqslant 1$ as the number of terms of the rising sequence $\theta = \{A_i\}$ such that degree $A_i < n$ and $A_i \equiv B \pmod M$, we can show that

$$N(\theta, n, B, M) + N(\theta^*, n, B, M) = q^{n-m} + \alpha_n \quad (\alpha_n \text{ rational}, \ |\alpha_n| < 1). \tag{2.5}$$

To prove (2.5) we need to show that the number of $C \in \Phi$ such that degree $C < n$ and $C \equiv B \pmod M$ is given by the right side of the equation. Clearly there exists a unique $R \in \Phi$ of degree $< m$ such that $R \equiv B \pmod M$. First suppose that $1 \leqslant n < m$. Then if degree $R < n$, there is one such C namely $C = R$, and this situation is described by (2.5) with $\alpha_n = 1 - q^{n-m}$. On the other hand, if $n \leqslant$ degree R, then there are no such elements $C \in \Phi$ and this is described by (2.5) with $\alpha_n = -q^{n-m}$. Now consider the case $n \geqslant m$. In view of the remark at the end of § 1 concerning the distribution of polynomials of degree $\geqslant m$ in the various residue classes

modulo M, it follows that for each $m \leqslant i \leqslant n$, the number of different C of degree i in Φ such that $C \equiv B \pmod M$ is $(q-1)q^{i-m}$. Summing this value for i from m to n and adding 1 to count R gives the right side of (2.5) with $a_n = 0$.

Now (2.5) leads directly to

$$[N(\theta, n, B, M)/\theta(n)][q^{-n}\theta(n)]+[N(\theta^*, n, B, M)/\theta^*(n)][q^{-n}\theta^*(n)] = q^{-m}+a_n q^{-n}.$$

Since $\theta(n)+\theta^*(n) = q^n$, replacing $q^{-n}\theta(n)$ by $1-q^{-n}\theta^*(n)$ in this last equation, we get

$$(2.6)\qquad [q^{-n}\theta^*(n)][N(\theta^*, n, B, M)/\theta^*(n)-N(\theta, n, B, M)/\theta(n)] = q^{-m}-N(\theta, n, B, M)/\theta(n)+a_n q^{-n}.$$

Since we are assuming that θ is w.u.d. (mod M), the right side of (2.6) tends to zero as $n \to \infty$. Furthermore, since the asymptotic density of θ^* is assumed to be positive, the quotient $q^{-n}\theta^*(n)$ is bounded away from zero for n sufficiently large, so that for every $B \in \Phi$ and monic M of degree m, (2.6) implies

$$\lim_{n\to\infty} N(\theta^*, n, B, M)/\theta^*(n) = \lim_{n\to\infty} N(\theta, n, B, M)/\theta(n) = q^{-m}.$$

Thus, θ^* is w.u.d. (mod M).

A final theorem relating weak uniform distributivity of a rising sequence and the density of the sequence is (compare with [5], Theorem 2.2)

THEOREM 2.3. *If a rising sequence θ is* w.u.d. *and contains an infinite set of the form $\{KB+C\}$ for all K of sufficiently large degree, where C is any fixed element of Φ and B is monic of degree b, then θ has natural density equal to* 1.

Proof. Since θ contains all polynomials of the form $KB+C$ for K of sufficiently large degree and the number of K of degree $< n-b$ is q^{n-b}, it follows that

$$N(\theta, n, C, B) = q^{n-b}+o(q^n).$$

Therefore, since θ is w.u.d. (mod B),

$$\lim_{n\to\infty} N(\theta, n, C, B)/\theta(n) = q^{-b} = \lim_{n\to\infty} [q^{n-b}+o(q^n)]/\theta(n) = q^{-b}\lim_{n\to\infty} q^n/\theta(n),$$

which implies that $\lim \theta(n)/q^n = 1$.

3. Uniform distribution with respect to different moduli. In this section we prove a number of elementary theorems concerning the relationships which exist among uniform distributivity of a sequence θ with respect to monic moduli M and F and to their product MF. Throughout this section we will assume that M and F are monic of degrees m and f, respectively. First we have

THEOREM 3.1. (a) *If a sequence θ is* u.d. (mod M) *and F divides M, then θ is* u.d. (mod F). (b) *If a sequence θ is not* u.d., *then there exist infinitely many moduli M for which θ is not* u.d. (mod M).

Proof. Part (b) is an easy consequence of part (a). For if sequence θ is not u.d. then there exists an F for which θ is not u.d. (mod F) and, assuming (a), this property is shared by all of the infinitely many different monic multiples M of F.

To prove (a) suppose that F divides M and that sequence θ is u.d. (mod M). Let B be any element of a complete residue system modulo F. Without loss of generality we may assume degree $B < f$. If A is any element of degree $< m$ in a complete residue system modulo M and $A \equiv B \pmod F$, then $A = KF+B$, where degree $K < m-f$. (K is the *zero polynomial* if $f = m$.) Since θ is u.d. (mod M), for any such B and K,

$$(3.1)\qquad \lim_{n\to\infty} \theta(n, KF+B, M)/n = q^{-m}.$$

Furthermore, for any fixed B of degree $< f$, since F divides M we have

$$(3.2)\qquad \theta(n, B, F) = \sum \theta(n, KF+B, M),$$

where the summation is over all K of degree $< m-f$. Since the number of such K is q^{m-f}, we see from (3.1) and (3.2) that for any such B,

$$\lim_{n\to\infty} \theta(n, B, F)/n = \sum_{\deg K<m-f} \lim_{n\to\infty} \theta(n, KF+B, M)/n = q^{m-f}q^{-m} = q^{-f}.$$

Thus, θ is u.d. (mod F).

Next, to supplement part (a) of Theorem 3.1 we prove

THEOREM 3.2. *If F does not divide M, then there exists a sequence θ that is* u.d. (mod M) *but is not* u.d. (mod F).

Proof. Suppose that F does not divide M and let $\{K_i\}$ be any fixed sequence with degree $K_j = j$ for all integers $j \geqslant 1$. Let $\{R_i \mid 1 \leqslant i \leqslant q^m\}$ be a complete residue system modulo M with $R_1 = M$ and $0 \leqslant$ degree $R_i < m$ for all $2 \leqslant i \leqslant q^m$. For every integer $j \geqslant 1$, define $\theta_j = \{FK_j+R_i \mid 1 \leqslant i \leqslant q^m\}$ and let $\theta = \{A_s\}$ be any sequence such that for all integers $j \geqslant 1$, $\{A_s \mid (j-1)q^m < s \leqslant jq^m\} = \theta_j$. Since for each value of j, the set θ_j is a complete residue system modulo M, θ is u.d. (mod M).

But θ is not u.d. (mod F). For if $m < f$, then for all $1 \leqslant i \leqslant q^m$ and all integers $j \geqslant 1$,

$$FK_j+R_i \equiv R_i \not\equiv 0 \pmod F,$$

so that the assertion is true for this case. On the other hand, suppose that $f \leqslant m$. Then all of the q^f-1 R_i of degree $< f$ are incongruent modulo F. For each z, $f \leqslant z \leqslant m$, the $(q-1)q^z$ R_i of degree z are divided evenly among the q^f residue classes modulo F, each residue class containing $(q-1)q^{z-f}$ such R_i. Thus for each $B \not\equiv 0$ of degree $< f$, the number of R_i of degree $< m$ such that $R_i \equiv B \pmod F$ is

$$c = 1 + \sum_{z=f}^{m-1} (q-1)q^{z-f} = q^{m-f}.$$

However, since $R_1 = M \not\equiv 0 \pmod F$, the *total* number of R_i such that $R_i \equiv 0 \pmod F$ is equal to the number of such R_i of degree $< m$ which is equal to $c-1$. Also for some $B_1 \not\equiv 0$ of degree $< f$, $R_1 = M \equiv B_1 \pmod F$ so that the total number of R_i such that $R_i \equiv B_1 \pmod F$ is $c+1$. Since, for every $j \geqslant 1$, the elements of θ_j are congruent modulo F to the elements of the set $\{R_i \mid 1 \leqslant i \leqslant q^m\}$ it follows that θ is not u.d. (mod F).

By analogy with the construction given by Niven ([5], § 5) to prove the analog of Theorem 3.2 for sequences of integers, in the preceding proof for the polynomial case F can be replaced by any of its nonzero multiples, in particular, by the least common multiple of F and M.

Another important and easily proved property is given by

THEOREM 3.3. *If a sequence θ is both* u.d. (mod M) *and* u.d. (mod F) *where M and F are relatively prime, then θ need not be* u.d. (mod MF).

Proof. The following is an analog of the example given by Niven ([5], § 5) to prove the corresponding property for sequences of integers. Let $a_1, \ldots, a_q$ be the elements of GF(q) listed in any fixed order. Let $H = x^2(x+1)$ and $\theta = \{A_i\}$ be any rising sequence such that for all integers $i \geqslant 1$, if $i = aq+b$ with a, b integers such that $1 \leqslant b \leqslant q$, then $A_i \equiv x^2+x+a_b \pmod H$. Then with $M = x$ and $F = x+1$, θ is u.d. (mod M) and u.d. (mod F), but θ is not u.d. (mod MF), even though M and F are relatively prime, since no element of θ is congruent modulo $MF = x^2+x$ to the linear polynomial x. Note that θ is not even w.u.d. (mod MF).

By use of a polynomial analog of a construction given by Niven ([5], § 5) we can prove a theorem of a slightly different sort, namely

THEOREM 3.4. *There exists a sequence θ which is not* u.d. *but which is* u.d. (mod P^e) *for every monic irreducible P and every integer $e \geqslant 1$.*

Proof. Let $a_1, \ldots, a_q$ be the elements of GF(q) listed in any fixed order with $a_1 = 0$. Let $\Gamma = \{B_k\}$ be the rising sequence formed by using all the elements of Φ as follows. For every integer $j \geqslant 1$, let

$$\Gamma_j = \{B_k \mid (j-1)q < k \leqslant jq\},$$

where in particular, $B_k = a_k$ if $B_k \in \Gamma_1$, that is, if $0 < k \leqslant q$. For $2 \leqslant j \leqslant q$ define

$$\Gamma_j = a_j x + \Gamma_1 = \{a_j x + a_k \mid 0 < k \leqslant q\},$$

where for fixed j the elements of Γ_j are arranged according to increasing subscript on a_k. Then by induction on $j > q$, if j satisfies

$$1 < q^t < j = aq^t + b \leqslant q^{t+1} \quad (1 \leqslant b \leqslant q^t,\ 1 \leqslant a \leqslant (q-1)),$$

define

$$\Gamma_j = a_{a+1}x^{t+1} + \Gamma_b,$$

where for fixed j the elements of Γ_j are arranged according to the order of elements in Γ_b.

In the proof of Theorem 5.3 of this paper, it is essentially shown that if M is any monic polynomial of degree m, then each successive set of q^m elements of Γ as defined comprises a complete residue system modulo M. This clearly implies that Γ is u.d. (mod M) (and so is u.d.). In particular, Γ is u.d. (mod P^e) for every monic irreducible P and every integer $e \geqslant 1$.

Given any positive integer k, for each (nonconstant) monic irreducible P define $j = j(P, k)$ by means of the inequalities $dj \leqslant k < d(j+1)$, where $d =$ degree P. Then let $\theta = \{A_k\}$ be any sequence satisfying all of the following conditions:

(i) degree $A_{k+1} >$ degree A_k all $k \geqslant 1$,

(ii) $A_k \equiv B_k \pmod{P^j}$, for every monic irreducible $P \neq x$ of degree $\leqslant k$.

(iii) for $P = x$, if R_k is the remainder in the division of B_k by x^2+x, then modulo x^j

$$A_k \equiv \begin{cases} B_k + a & (\text{if } R_k = ax \text{ for } a \neq 0 \text{ in GF}(q)), \\ B_k - a & (\text{if } R_k = a(x+1) \text{ for } a \neq 0 \text{ in GF}(q)), \\ B_k & (\text{otherwise}). \end{cases}$$

For each integer $k \geqslant 1$, since there are only a finite number of congruences to be satisfied in conditions (ii) and (iii) and the various moduli involved are relatively prime in pairs, by the Chinese Remainder Theorem for Φ, polynomials A_k exist which satisfy all of the conditions in (i), (ii) and (iii). Thus, such a sequence $\theta = \{A_k\}$ exists.

Then θ is u.d. (mod P^e) for every monic irreducible P and every integer $e \geqslant 1$. For given P of degree d, we can ignore the finite number of terms A_k at the beginning of θ for which $k < de$, considering only those terms for which $de \leqslant k$ so that $e \leqslant j$, where $j = j(P, k)$ is defined above. If $P \neq x$, by condition (ii) it follows for every $k \geqslant de$ that A_k

$\equiv B_k \pmod{P^e}$ and since Γ is u.d. $\pmod{P^e}$ so is θ. If $P = x$, since $e \leqslant j$, the conditions (iii) hold modulo x^e. Since as noted before, the numbers of elements B_k in Γ of any given degree $\geqslant 2$ which are congruent modulo x^2+x to any linear polynomial are the same, it follows that since Γ is u.d. $\pmod{x^e}$ so is θ.

However, θ is not u.d. since it is not u.d. $\pmod{x^2+x}$. This is true since for all integers $k \geqslant 1$, $A_k \not\equiv x+1 \pmod{x^2+x}$. For if $A_k \equiv x+1 \pmod{x^2+x}$ for some k, then $A_k \equiv x+1 \equiv 1 \pmod{x}$ and in view of condition (ii) above, $B_k \equiv A_k \equiv x+1 \equiv 0 \pmod{x+1}$. This last congruence implies that the remainder R_k in the division of B_k by x^2+x is $a(x+1)$ for some $a \in \mathrm{GF}(q)$. If $a \neq 0$ then, by condition (iii) above, $A_k \equiv B_k - a \equiv 0 \pmod{x}$ and if $a = 0$ then, again by condition (iii), $A_k \equiv B_k \equiv 0 \pmod{x}$, in either case contradicting $A_k \equiv 1 \pmod{x}$. Thus, θ is not u.d. $\pmod{x^2+x}$.

We remark that all of the results (and proofs with obvious changes) of this section hold if u.d. and u.d. $\pmod{M}$ are replaced by w.u.d. and w.u.d. $\pmod{M}$, respectively.

4. Sequences of polynomials generated by irrationals. Let $\Phi' = \mathrm{GF}\{q, x\}$ denote the extension field of $\Phi = \mathrm{GF}[q, x]$ consisting of all the expressions

$$\alpha = \sum_{i=-\infty}^{m} c_i x^i \qquad (c_i \in \mathrm{GF}(q)), \tag{4.1}$$

where x is an indeterminate and the coefficients c_i all belong to a fixed arbitrary $\mathrm{GF}(q)$. In this section, lower case Greek letters will denote elements of Φ'. If α has the representation (4.1) with $c_m \neq 0$, following Carlitz ([2], § 2) we define the *degree* of α by $\deg \alpha = m$, where m is a rational integer which may be positive, negative or zero. We extend this definition by writing $\deg 0 = -\infty$, where $-\infty < k$ for all integers k. The *integral part* and *fractional part* of α, denoted by $[\alpha]$ and $((\alpha))$ respectively, are defined by

$$[\alpha] = \sum_{i=0}^{m} c_i x^i, \qquad ((\alpha)) = \alpha - [\alpha] = \sum_{i=-\infty}^{-1} c_i x^i, \tag{4.2}$$

so that $[\alpha]$ is a polynomial. An important property of this concept of integral parts (obviously *not* shared by its real analog) which follows immediately from the definition, is that for $\alpha, \beta \in \Phi'$, $[\alpha+\beta] = [\alpha]+[\beta]$. The statement $\alpha \equiv \beta \pmod 1$ is defined to mean that $\alpha = \beta + A$ where $A \in \Phi$, that is, A is a polynomial. Thus, every α is congruent (mod 1) to a unique β, namely $\beta = ((\alpha))$, such that $\deg \beta < 0$.

The following definitions are also due to Carlitz ([2], § 4). Given an infinite sequence of elements $\alpha_1, \alpha_2, \ldots$ in Φ', an arbitrary element β of Φ' and any positive integers n and k, let $N_k(n, \beta)$ be the number of α_i with $1 \leqslant i \leqslant n$ such that

$$\deg((\alpha_i - \beta)) < -k. \tag{4.3}$$

Then the sequence $\{\alpha_i\}$ is said to be *uniformly distributed* (mod 1) in Φ' if and only if for all $k \geqslant 1$ and all $\beta \in \Phi'$

$$\lim_{n\to\infty} N_k(n, \beta)/n = q^{-k}, \tag{4.4}$$

and is said to be *weakly uniformly distributed* (mod 1) in Φ' if and only if for all $k \geqslant 1$ and all $\beta \in \Phi'$

$$\lim_{t\to\infty} N_k(q^t, \beta)/q^t = q^{-k}. \tag{4.5}$$

An element $\xi \in \Phi'$ is called *irrational* if it is not contained in $\mathrm{GF}(q, x)$, that is, it is not a quotient A/B of elements $A, B \in \Phi$. The following theorem proved by Carlitz ([2], Theorem 5) is an analog for Φ' of the well-known theorem of Weyl ([6]) concerning uniform distribution (mod 1) of certain sequences of real numbers generated by real irrationals.

THEOREM 4.1. *If $\xi \in \Phi' = \mathrm{GF}\{q, x\}$, ξ is irrational and $\{A_i\}$ is any rising sequence formed by using all the elements of $\Phi = \mathrm{GF}[q, x]$, then the sequence $\{A_i\xi\}$ is weakly uniformly distributed* (mod 1) *in Φ'.*

We remark that this theorem (see [2], Theorem 8) and in fact all of the results of the present paper, can easily be extended to sequences of *n-tuples* of elements of Φ or Φ' as the case may be.

By use of this theorem of Carlitz we can prove an analog for Φ of a theorem of Niven ([5], Theorem 3.1) concerning sequences of integers generated by real irrational numbers. Recalling the definition of w.u.d. for sequences in Φ as given in § 1, we prove

THEOREM 4.2. *Let $\xi \in \Phi'$ and $\{A_i\}$ be any rising sequence formed by using all the elements of Φ. Then the sequence $\theta = \theta(\xi) = \{[A_i\xi]\}$ of integral parts of the sequence $\{A_i\xi\}$ of elements of Φ' is* w.u.d. *(in Φ) if and only if ξ is irrational or $\xi = A/B$ for $A, B \in \Phi$ with degree $A \leqslant$ degree B.*

Proof. First suppose that ξ is irrational and let M be any monic polynomial. Then ξ/M is irrational in Φ' so that by Theorem 4.1, the sequence $\{\alpha_i\}$ with $\alpha_i = A_i\xi/M$ all $i \geqslant 1$ is weakly uniformly distributed (mod 1) in Φ'. Let $B \in \Phi$ be arbitrary of degree $< m$ so that for any integer $k \geqslant 1$, by (4.5) we have

$$\lim_{t\to\infty} q^{-t} N_k(q^t, B/M) = q^{-k}, \tag{4.6}$$

where $N_k(q^t, B/M)$ is the number of α_i with $1 \leqslant i \leqslant q^t$ such that $\deg((\alpha_i - B/M)) < -k$. If α_i satisfies this condition then we can write

$$\alpha_i - B/M = F_i + ((\alpha_i - B/M)) \qquad (F_i \in \Phi). \tag{4.7}$$

If we multiply this equation by M and consider the special case $k = m$ we see that

$$A_i\xi = B + MF_i + M((a_i - B/M)),$$

where $\deg M((a_i - B/M)) < 0$ so that

$$[A_i\xi] = B + MF_i \equiv B \pmod{M}. \tag{4.8}$$

Conversely, (4.8) implies (4.7) with $\deg((a_i - B/M)) < -m$. Suppose that $\deg \xi = d$. Let t be an arbitrary integer such that $t + d \geqslant 1$. As i runs through the integers $1 \leqslant i \leqslant q^t$, A_i runs through all q^t elements of Φ of degree $< t$ and, if $[A_i\xi] \neq 0$, $\deg [A_i\xi] = \deg A_i\xi < t + d$. Therefore, $\theta(t+d) = q^t$ and by the equivalence of (4.8) and (4.7), $N(\theta, t+d, B, M) = N_m(q^t, B/M)$. Therefore by (4.6) with $k = m$, for all such $B \in \Phi$

$$\lim_{t\to\infty} N(\theta, t+d, B, M)/\theta(t+d) = \lim_{t\to\infty} q^{-t} N_m(q^t, B/M) = q^{-m}.$$

Thus, θ is w.u.d. (mod M) and since M was arbitrary, $\theta = \theta(\xi)$ is w.u.d.

Next suppose that $\theta(\xi)$ is w.u.d., where ξ is rational, that is, $\xi = A/B$ with $A, B \in \Phi$ and $B \neq 0$. If $\xi = 0$, it is trivial that $\theta(\xi)$ is not w.u.d. so that we may assume $\xi \neq 0$. Let $a = \deg A$, $b = \deg B$ and suppose $a > b$. Then for every integer $t \geqslant 1$, of the first q^{tb} elements of $\theta(\xi)$ (corresponding to the set of all A_i of degree $< tb$) at least q^{tb-b} are congruent to 0 modulo A, namely those elements corresponding to all $A_i = BF$, where F has degree $< tb - b$. Since $\deg \xi = a - b$, for all q^{tb} A_i of degree $< tb$, it follows that

$$\deg [A_i\xi] = \deg A_i\xi = \deg A_i + \deg \xi < tb + (a - b).$$

Therefore, recalling the definitions (1.2) we have for every integer $t \geqslant 1$

$$\theta(tb + a - b) = q^{tb},$$
$$N(\theta, tb + a - b, 0, A) \geqslant q^{tb-b}.$$

This implies that (if the limit exists)

$$\lim_{n\to\infty} N(\theta, n, 0, A)/\theta(n) \geqslant q^{-b} > q^{-a},$$

which implies that θ is not w.u.d. (mod A) so is not w.u.d. Thus, we conclude that if $\theta(\xi)$ is w.u.d. for rational $\xi = A/B \neq 0$, then $a \leqslant b$.

Finally, we prove that if $\xi = A/B \neq 0$ with degree $A = a \leqslant b$ = degree B, then $\theta(\xi)$ is w.u.d. Now the first q^{b-a} terms of $\theta(\xi)$ correspond to the terms of the rising sequence $\{A_i\}$ which are of degree $< b - a$. For all such A_i, degree $A_iA < b$ so that $[A_iA/B] = 0$. The next $(q-1)q^{b-a}$ terms of $\theta(\xi)$ correspond to all the terms of $\{A_i\}$ which are of degree $b - a$.

As A_i runs through all polynomials of degree $b - a$, A_iA runs through all polynomials of degree b, with each of the $(q-1)$ possible leading coefficients occurring exactly q^{b-a} times. Thus $[A_iA/B]$ runs through all of the nonzero constant polynomials, each occurring q^{b-a} times. Therefore, the first q^{b-a+1} terms of $\theta(\xi)$ consist of the q constant polynomials in Φ, each occurring q^{b-a} times. By induction, it follows that for all integers $t \geqslant 1$, the first q^{b-a+t} terms of $\theta(\xi)$ consist of all the q^t elements of Φ of degree $< t$, each occurring q^{b-a} times, and we have $\theta(t) = q^{b-a+t}$.

Let M be any monic polynomial, $m =$ degree M and let C be any element of Φ of degree $< m$. By the argument above, for all integers $r \geqslant 1$, the first $q^{b-a+m+r}$ terms of $\theta(\xi)$ consist of the q^{m+r} elements of Φ of degree $< m + r$, each occurring q^{b-a} times. C itself occurs q^{b-a} times among these terms. In addition, for each $0 \leqslant j < r$, each of the $(q-1)q^j$ polynomials of degree $m + j$ which is congruent to C modulo M occurs q^{b-a} times among these terms. Thus, of the first $q^{b-a+m+r}$ terms of $\theta = \theta(\xi)$, the number which are congruent to C modulo M is

$$N(\theta, m+r, C, M) = q^{b-a}\Big[1 + \sum_{j=0}^{r-1} (q-1)q^j\Big] = q^{b-a+r}. \tag{4.9}$$

Therefore, it follows that for all such C, since $\theta(m+r) = q^{b-a+m+r}$,

$$\lim_{n\to\infty} N(\theta, n, C, M)/\theta(n) = \lim_{r\to\infty} N(\theta, m+r, C, M)/\theta(m+r) = q^{-m},$$

which implies that $\theta(\xi)$ is w.u.d. (mod M). Since M was arbitrary, $\theta(\xi)$ is w.u.d.

Since uniform distributivity of a sequence in Φ is invariant under addition of any fixed polynomial and as noted earlier, $[\alpha+\beta] = [\alpha]+[\beta]$ for all $\alpha, \beta \in \Phi'$, a trivial consequence of the preceding theorem is (see [5], Theorem 3.2, for the somewhat less trivial analog for sequences of integers).

COROLLARY 4.3. *If $\xi \in \Phi'$ is irrational or $\xi = A/B \neq 0$ for $A, B \in \Phi$ with degree $A \leqslant$ degree B, $\beta \in \Phi'$ is arbitrary, and $\{A_i\}$ is any rising sequence formed by using all the elements of Φ, then the sequence $\theta(\xi, \beta) = \{[A_i\xi + \beta]\}$ is* w.u.d. *in Φ.*

It is interesting to see that, as in the analogous situation ([5], p. 56) for sequences of integers, the conclusion of Carlitz's Theorem 4.1 follows as a consequence of assuming for all irrationals in Φ' the conclusion of Theorem 4.2. That is,

THEOREM 4.4. *If $\{A_i\}$ is any fixed rising sequence formed by using all the elements of Φ and for every irrational $\xi \in \Phi'$, the sequence $\theta(\xi) = \{[A_i\xi]\}$ is* w.u.d. *in Φ, then for every irrational $\xi \in \Phi'$ the sequence $\{A_i\xi\}$ is weakly uniformly distributed* (mod 1) *in Φ'.*

Proof. Suppose that the hypothesis holds and that $\xi \in \Phi'$ is any irrational. For any integer $m \geqslant 1$, let M be any fixed monic polynomial of degree m. Then $M\xi$ is also irrational so that $\theta_m = \theta(M\xi) = \{[A_i M\xi]\}$ is w.u.d. in Φ and so is w.u.d. (mod M).

Now let B be any polynomial of degree $< m$ and suppose that $[A_i M\xi] \equiv B \pmod M$. Then $A_i\xi = [A_i\xi] + ((A_i\xi))$ so that $A_i M\xi = M[A_i\xi] + M((A_i\xi))$ and so

$$[A_i M\xi] = M[A_i\xi] + [M((A_i\xi))] \equiv [M((A_i\xi))] \equiv B \pmod M. \tag{4.10}$$

Since $\deg M((A_i\xi)) < m$, $[M((A_i\xi))]$ is a polynomial of degree $< m$ so that (4.10) implies $[M((A_i\xi))] = B$. Thus (4.10) leads to

$$\left[A_i M\xi - M[A_i\xi]\right] = [A_i M\xi] - M[A_i\xi] = B. \tag{4.11}$$

Therefore $A_i M\xi - M[A_i\xi] = B + \beta$ with $\deg \beta < 0$ so that

$$((A_i\xi)) = A_i\xi - [A_i\xi] = B/M + \beta/M, \tag{4.12}$$

where $-m \leqslant \deg(B/M) < 0$ if $B \neq 0$ and $\deg(\beta/M) < -m$.

Now as B runs through a complete residue system modulo M in Φ, with degree $B < m$, the quotient

$$B/M = \sum_{j=-\infty}^{-1} b_j x^j$$

runs through a set of q^m different elements in Φ' in which each of the q^m different choices of all of the coefficients b_j, for $-m \leqslant j \leqslant -1$, appears exactly once. For suppose that B_1 and B_2 are both of degree $< m$ and that $B_1/M = \beta_1 + \beta$, $B_2/M = \beta_2 + \beta$ with β_1, β_2 both of deg $< -m$. Then $B_1 - B_2 = M(\beta_1 - \beta_2)$ so that $\deg(B_1 - B_2) < 0$. Since B_1 and B_2 are polynomials, this implies that $B_1 = B_2$.

Therefore for any $\alpha \in \Phi'$, in view of (4.12) and the comments above concerning the distribution of B/M in Φ', there is a unique polynomial B of degree $< m$ such that for all integers $i \geqslant 1$, $[A_i M\xi] \equiv B \pmod M$ if and only if

$$((A_i\xi - \alpha)) = ((B/M - \alpha)) < -m. \tag{4.13}$$

Since for any integer $t \geqslant 1$, $\deg A_i < t$ for all $1 \leqslant i \leqslant q^t$, if $\deg \xi = d$ then $[A_i M\xi] = 0$ or

$$\deg [A_i M\xi] = \deg A_i M\xi < t + m + d.$$

Thus for any $\alpha \in \Phi'$ and the corresponding $B \in \Phi$ of degree $< m$ as above, in view of (4.13) we have (with N_m referring to $\{A_i\xi\}$)

$$\theta_m(t+m+d) = q^t,$$
$$N(\theta_m, t+m+d, B, M) = N_m(q^t, \alpha).$$

Since $\theta_m = \theta(M\xi)$ is w.u.d. (mod M),

$$\lim_{t\to\infty} q^{-t} N_m(q^t, \alpha) = \lim_{t\to\infty} N(\theta_m, t+m+d, B, M)/\theta(t+m+d) = q^{-m}. \tag{4.14}$$

Since (4.14) holds for every $\alpha \in \Phi'$ and every integer $m \geqslant 1$, by definition the sequence $\{A_i\xi\}$ is weakly uniformly distributed (mod 1) in Φ'.

It is easy to show that all of Niven's comments ([5], § 3) concerning the cardinality and other properties of the sets of uniformly distributed and non-uniformly distributed sequences of positive integers, hold as well for the sets of *weakly* uniformly distributed and *weakly* non-uniformly distributed sequences in Φ. These comments will not be repeated here. (It may be noted, however, that in order to define the analogous correspondence between sequences and the real numbers in the interval $0 < x \leqslant 1$ expressed in the binary system, it is necessary to first choose any fixed well-ordering of Φ.)

5. An exponential property related to uniform distribution. In this section assume that $q = p^r$, that GF(q) is defined by a zero β of an irreducible polynomial of degree r in GF[p, x], and that small Greek letters always denote elements of GF(q). For $\alpha \in$ GF(q) so that $\alpha = a_1\beta^{r-1} + \ldots + a_r$ with $a_i \in$ GF(p) all $1 \leqslant i \leqslant r$, define $t(\alpha) = a_1$. Then for $A, M \in \Phi$ with M monic of degree m, if

$$A \equiv a_1 x^{m-1} + \ldots + a_m \pmod M, \tag{5.1}$$

we define ([1], § 2)

$$e(A, M) = \exp[2\pi i t(a_1)/p]. \tag{5.2}$$

From these definitions it follows immediately that $e(A, M) = 1$ if $M|A$ and that $e(A, M) = e(A', M)$ if $A \equiv A' \pmod M$. Furthermore, Carlitz ([1], Theorem 1) has proved that

$$\sum_{C \pmod M} e(AC, M) = \begin{cases} q^m & (\text{if } M|A), \\ 0 & (\text{if } M \nmid A), \end{cases} \tag{5.3}$$

where the summation is over a complete residue system modulo M in Φ. If $m = 1$, a complete residue system modulo M is isomorphic to GF(q) itself and (5.3) reduces for $A = \alpha \in$ GF(q) to

$$\sum_{\gamma} \exp[2\pi i t(\alpha\gamma)/p] = \begin{cases} q & (\alpha = 0), \\ 0 & (\alpha \neq 0), \end{cases} \tag{5.4}$$

where the summation is over all $\gamma \in$ GF(q).

Making use of (5.2) we will say that a sequence $\theta = \{A_k\}$ of elements of Φ has *zero exponential density* (mod M) if and only if

$$\lim_{n\to\infty}\Big[\sum_{k=1}^{n} e(A_k, M)\Big]/n = 0. \tag{5.5}$$

By analogy with Niven's proof ([5], § 6) of the corresponding property of sequences of integers we can prove

THEOREM 5.1. *If a sequence $\theta = \{A_k\}$ of elements of Φ is* u.d. (mod M) *for any monic M, then θ has zero exponential density* (mod M).

Proof. Since θ is u.d. (mod M), for any integer $n \geqslant 1$

$$\begin{aligned}\sum_{k=1}^{n} e(A_k, M) &= \sum_{B(\mathrm{mod}\, M)} \theta(n, B, M)\, e(B, M) \\ &= \sum_{B(\mathrm{mod}\, M)} \{nq^{-m} + o(B, n)\}\, e(B, M),\end{aligned} \tag{5.6}$$

where $o(B, n)$ denotes a function of B and n of order $o(n)$ in n. Since $M \nmid 1$, in view of (5.3), (5.6) simplifies to

$$\sum_{k=1}^{n} e(A_k, M) = \sum_{B(\mathrm{mod}\, M)} \{o(B, n)\}\, e(B, M) = o(n),$$

which implies the desired conclusion.

Concerning the converse of the preceding theorem we can easily prove (compare with the result in [5], § 6)

THEOREM 5.2. *The fact that a sequence $\theta = \{A_k\}$ of elements of $\Phi = \mathrm{GF}[q, x]$ for $q = p^r$, p a prime, has zero exponential density* (mod M), *where M is monic of degree m, does not in general imply that θ is* u.d. (mod M) [*nor even* w.u.d. (mod M)], *except in the two special cases where $r = 1$, $m = 1$ and $p = 2$ or 3.*

Proof. Let M be any monic polynomial of degree m. First, for any prime p consider the case $r \geqslant 1$ and $m > 1$ and let β generate $\mathrm{GF}(q)$ over $\mathrm{GF}(p)$ as indicated at the beginning of this section. Also let $\theta = \{A_k\}$ where for all $k \geqslant 1$, if $k = sp + j$ with j, s integers such that $0 \leqslant j < p$, then $A_k = (j\beta^{r-1})x^{m-1} + M^k$ (with j here regarded as an element of $\mathrm{GF}(p)$) so that $e(A_k, M) = \exp[2\pi ij/p]$. It is clear that θ as defined has zero exponential density (mod M). However, θ is not u.d. (mod M) [nor even w.u.d. (mod M)] since it contains no elements congruent modulo M to the nonzero constant polynomials.

Next, for any prime p, consider the case $r > 1$ and $m = 1$. If $\theta = \{A_k\}$ is defined as in the preceding case (with $x^0 = 1$) so that all the A_k are constant polynomials, then again θ has zero exponential density (mod M). But again θ is not u.d. (mod M) [nor even w.u.d. (mod M)] since all

of its elements lie in only p of the $q = p^r > p$ different residue classes modulo M in Φ (those p classes represented by $j\beta^{r-1}$ for $0 \leqslant j < p$).

Finally, suppose that $r = 1$, $m = 1$ and that $\theta = \{A_k\}$ is any sequence which has zero exponential density (mod M). Then for every integer $k \geqslant 1$, $A_k \equiv a_k \pmod M$, where $a_k \in \mathrm{GF}(p)$, so that a_k may be regarded as in integer (mod p). Since $r = 1$, $t(a_k) = a_k$ so that $e(A_k, M) = \exp[2\pi i a_k/p]$ and so in this case the question of uniform distributivity reduces to the analogous question for uniform distribution (mod p) of sequences of integers as considered by Niven. From Niven's results ([5], § 6) we infer that in the polynomial case with $m = 1$, $r = 1$, the fact that θ has zero exponential density (mod M) implies that θ is u.d. (mod M) if and only if $p = 2$ or 3.

Another result of the same sort as that given by Theorem 5.2 is contained in (see the analogous result in [5], § 6)

THEOREM 5.3. *The fact that a sequence $\theta = \{A_k\}$ of elements of Φ has zero exponential density* (mod M) *for all monic M in Φ does not imply that θ is* u.d.

Proof. Let $a_1, a_2, \ldots, a_q$ denote the elements of $\mathrm{GF}(q)$ arranged in any fixed order with $a_1 = 0$ and $a_q = -1$. Let $\Gamma = \{B_k\}$ be the unique rising sequence, with first term equal go $a_1 = 0$, formed by using all the elements of Φ, where the elements of each degree are arranged according to the ordering of the subscripts on their coefficients from left to right, with all elements written in descending form. (For example, if $B = a_i x^m + a_a x^{m-1} + \ldots$ and $C = a_i x^m + a_b x^{m-1} + \ldots$ with $a < b$, then B precedes C in the sequence Γ.) Now define $\theta = \{A_k\}$, where for each integer $k \geqslant 1$, if $k = tq + s$ with t, s integers such that $1 \leqslant s \leqslant q$, then $A_k = xB_k + a_s$. We will prove that θ has zero exponential density (mod M) for all monic M, but that θ is not u.d. since it is not u.d. (mod x^2).

Let M be an arbitrary monic polynomial of degree $\geqslant 1$. Since the sequence $\Gamma = \{B_k\}$ is clearly u.d. (mod M), by Theorem 5.1 it follows that Γ has zero exponential density (mod M). In view of the definition of $e(A, M)$ given by (5.1) and (5.2), we see for all integers $k \geqslant 1$, since xM has degree $\geqslant 2$, that

$$e(A_k, xM) = e(B_k, M).$$

Therefore

$$\lim_{n\to\infty}\Big[\sum_{k=1}^{n} e(A_k, xM)\Big]/n = \lim_{n\to\infty}\Big[\sum_{k=1}^{n} e(B_k, M)\Big]/n = 0.$$

Thus we see that $\theta = \{A_k\}$ has zero exponential density (mod xM) for all monic M of degree $\geqslant 1$, that is for all monic $M_1 = xM$ of degree $\geqslant 2$.

Furthermore, since $A_k \equiv a_s \pmod{x}$ with s defined above for all integers $k \geqslant 1$, for any integer $n = tq+j \geqslant 1$ with $0 \leqslant j < q$, in view of (5.4) we have

$$\begin{aligned}\Big|\sum_{k=1}^{n} e(A_k, x)\Big| &= \Big|\sum_{k=1}^{tq} e(A_k, x) + \sum_{k=tq+1}^{n} e(A_k, x)\Big| \\ &= \Big|t\sum_{s=1}^{q} \exp[2\pi i t(a_s)/p] + \sum_{s=1}^{j} \exp[2\pi i t(a_s)/p]\Big| \\ &= \Big|\sum_{s=1}^{j} \exp[2\pi i t(a_s)/p]\Big| \leqslant j < q.\end{aligned}$$

Therefore it follows from the definition (5.5) that θ also has zero exponential density (mod x).

Next, let M be any fixed monic polynomial of degree $m \geqslant 2$ such that $(M, x) = 1$. (This latter condition is not really necessary, but the case where $x|M$ has already been taken care of.) Trivially, $M \nmid x$. It follows directly from (5.1) and (5.2) that for all integers $k \geqslant 1$

$$e(A_k, M) = e(xB_k + a_s, M) = e(xB_k, M), \tag{5.7}$$

since $m \geqslant 2$. Now the terms of the sequence $\Gamma = \{B_k\}$ occur in certain finite sets $\Gamma_j = \Gamma_j(m)$ of q^m elements each, defined for all integers $j \geqslant 1$ by

$$\Gamma_j = \{B_k \mid (j-1)q^m < k \leqslant jq^m\}. \tag{5.8}$$

In particular, Γ_1 consists of all the q^m terms of Γ of degree $< m$ and so comprises a complete residue system modulo M in Φ. In fact, for all $j \geqslant 1$, Γ_j comprises a complete residue system modulo M. To see this, first consider the case $1 < j \leqslant q$. It follows from the definition of Γ in terms of the fixed ordering of GF(q) that for any such j

$$\Gamma_j = a_j x^m + \Gamma_1 = \{a_j x^m + B_k \mid B_k \in \Gamma_1\}.$$

Since Γ_1 comprises a complete residue system (mod M), so does Γ_j. Secondly, we can prove by induction on $j > q$ that if j satisfies

$$1 < q^t < j = aq^t + b \leqslant q^{t+1} \quad (1 \leqslant b \leqslant q^t,\ 1 \leqslant a \leqslant (q-1)), \tag{5.9}$$

then

$$\Gamma_j = a_{a+1} x^{m+t} + \Gamma_b. \tag{5.10}$$

Thus, again by use of induction, it follows that for all $j > q$, Γ_j comprises a complete residue system modulo M.

Now for any integer $n \geqslant 1$, if $n = fq^m + v$ with $0 \leqslant v < q^m$, in view of (5.3) and the property of the sets Γ_j proved above, since $M \nmid x$ we have

$$\begin{aligned}\Big|\sum_{k=1}^{n} e(xB_k, M)\Big| &= \Big|\sum_{u=1}^{f}\sum_{B_k \in \Gamma_u} e(xB_k, M) + \Big|\sum_{k=n-v+1}^{n} e(xB_k, M)\Big| \\ &= \Big|\sum_{k=n-v+1}^{n} e(xB_k, M)\Big| < q^m.\end{aligned} \tag{5.11}$$

Together (5.7) and (5.11) imply that θ has zero exponential density (mod M).

We must now prove that θ has zero exponential density (mod M), where M is any monic polynomial of degree 1 different from x. By analogy with the sets Γ_j above corresponding to the sequence $\Gamma = \{B_k\}$ (but here using $m = 1$), define sets θ_j for all integers $j \geqslant 1$, each containing q elements of $\theta = \{A_k\}$. In particular, recalling the definition of Γ and θ we see that

$$\theta_1 = \{a_u(x+1) \mid 1 \leqslant u < q\}.$$

Let $M = x - a_s$ be arbitrary but fixed with $1 < s < q$, if any such s exist. (When $s = 1$, $M = x$ which has already been considered and when $s = q$, $M = x+1$ which requires special consideration.) Then the elements of θ_1 satisfy

$$a_u(x+1) \equiv a_u(a_s+1) \pmod{M} \quad (1 \leqslant u \leqslant q),$$

so that since $(a_s+1) \neq 0$, θ_1 comprises a complete residue system modulo $M = x - a_s$. (That is, θ_1 modulo $x - a_s$ is just GF(q).) Then by analogy with the proof outlined above for the Γ_j, modulo monic polynomials of degree $\geqslant 2$, it follows that for all integers $j \geqslant 1$, θ_j comprises a complete residue system modulo $M = x - a_s$ in Φ. Thus for any integer $n \geqslant 1$, by using (5.4) we obtain as the analog of (5.11), the inequality

$$\Big|\sum_{k=1}^{n} e(A_k, x - a_s)\Big| < q,$$

which implies that θ has zero exponential density (mod $x - a_s$). Finally, consider the special monic linear polynomial $M = x - a_s = x+1$. We see that in this case the elements of θ_1 satisfy

$$a_u(x+1) \equiv 0 \pmod{x+1} \quad (1 \leqslant u \leqslant q).$$

Furthermore, for any $1 < s \leqslant q$, $\theta_s = a_s x^2 + \theta_1$ so that the elements of θ_s satisfy

$$a_s x^2 + a_u(x+1) \equiv a_s \pmod{x+1} \quad (1 \leqslant u \leqslant q).$$

Therefore, taken together the elements of $\theta_1, \ldots, \theta_q$, which contain the first q^2 elements of θ, comprise q different complete residue systems modulo $M = x+1$, that is these first q^2 elements comprise the elements of GF(q), each element occurring q times. By analogy with the results above for monic M of degree $\geqslant 2$ and for all $M = x-a_s \neq x+1$, we find that each successive set of q^2 elements of θ has the same property modulo $x+1$ as the first set of q^2 elements. Therefore, for any integer $n \geqslant 1$,

$$\left|\sum_{k=1}^{n} e(A_k, x+1)\right| < q^2,$$

which implies that θ has zero exponential density (mod $x+1$).

We have now proved that the sequence $\theta = \{A_k\}$ as defined has zero exponential density (mod M) for *all* monic M. However, θ is not u.d. (mod x^2) and so not u.d. since for all integers $k \geqslant 1$, if $k = tq+s$ with t, s integers such that $1 \leqslant s \leqslant q$, then from the definition of $\Gamma = \{B_k\}$ it follows that $B_k \equiv a_s \pmod{x}$. Therefore, for all integers $k \geqslant 1$

$$A_k = xB_k + a_s \equiv a_s x + a_s \not\equiv x \pmod{x^2}.$$

We remark that this proof of Theorem 5.3 is quite different from Niven's proof of the analogous theorem for sequences of integers, which makes use of the analog of Theorem 4.2 applied to sequences of integers generated by certain related irrationals. The proof of Theorem 5.3 given here for polynomials is not adaptable to the analogous theorem for integers.

By analogy with the way the definition of uniform distributivity (mod M) was modified in § 1 to define for certain sequences the concept of weak uniform distributivity (mod M), we can modify the definition of zero exponential density (mod M) to define for these same sequences the concept of *zero weak exponential density* (mod M). Then the analogs of all the theorems (and the proofs with only minor modifications) of this section hold for weak uniform distributivity and weak exponential density.

References

[1] L. Carlitz, *The singular series for sums of squares of polynomials*, Duke Math. J. 14 (1947), pp. 1105-1120.

[2] — *Diophantine approximation in fields of characteristic p*, Trans. Amer. Math. Soc. 72 (1952), pp. 187-208.

[3] Stephan R. Cavior, *Uniform distribution of polynomials modulo m*, Amer. Math. Monthly 73 (1966), pp. 171-172.

[4] Stephan R. Cavior, *Constructing polynomials which are uniformly distributed* (mod m), to appear.

[5] Ivan Niven, *Uniform distribution of sequences of integers*, Trans. Amer. Math. Soc. 98 (1961), pp. 52-61.

[6] H. Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. 77 (1916), pp. 313-352.

[7] Burke Zane, *Uniform distribution modulo m of monomials*, Am. Math. Monthly 71 (1964), pp. 162-164.

UNIVERSITY OF COLORADO

Reçu par la Rédaction le 19. 1. 1966