MATH. SCAND. 38 (1976), 53–77

ON THE CYCLE STRUCTURE OF LINEAR RECURRING SEQUENCES

H. NIEDERREITER*)

1. Introduction and summary.

We shall discuss two aspects of the theory of linear recurring sequences, both of them concerning the structure of the period (or cycle) of such sequences. On the one hand, we establish results on the length of the period in a general setting, and secondly, we study the distribution of elements occurring in the period.

Questions about the length of the period of a linear recurring sequence are usually dealt with in the framework of the residue class rings $\mathbf{Z}/m\mathbf{Z}$, $m \geqq 2$, or of finite fields. Especially in the latter case, a number of powerful methods have been developed. See Selmer [9] for an excellent survey. Unfortunately, most of these methods break down in a more general setting. In Section 2, we outline an approach that can be carried out for linear recurring sequences in modules over finite rings. The results are not only of interest in themselves, but will also serve to throw more light on the meaning of the estimates occurring in the subsequent sections, simply because these estimates depend on certain parameters that are tied together by the theorems of Section 2.

The results in Section 3 are of an auxiliary nature. We discuss an estimate for character sums over the full period of linear recurring sequences that was established by the author [7], and we improve upon the author's previous estimate for the corresponding sums over parts of the period. It should be mentioned that estimates of this type also play a fundamental role in the recent work of the author [6], [8] on pseudo-random numbers generated by the linear congruential method.

Hall [4] showed an estimate concerning the number of occurrences of elements in the period of a linear recurring sequence in a finite field, under the assumption that the characteristic polynomial of the recurrence be irreducible over the finite field. In Section 4, we prove an estimate analogous to Hall's for any linear recurring sequence in a finite field. In

*This research was supported by NSF grant MPS 72–05055 A02.
Received December 16, 1974.

order to achieve this, we employ an analytic method based on the estimates for character sums in Section 3. The same method yields results about the number of occurrences of elements in segments of the period. Roughly, these results may be summarized as follows: for a linear recurring sequence with a sufficiently long period, the elements in the full period (or in a sufficiently long segment of the period) are nearly equidistributed over the finite field. We also discuss the extent to which these estimates are best possible.

In Section 5, we study distribution properties of linear recurring sequences in $\mathbf{Z}/m\mathbf{Z}$, $m \geqq 2$. In principle, the results are quite analogous to those for finite fields, the proofs, however, are technically more involved.

Expositions of the theory of linear recurring sequences in finite fields are to be found in Birkhoff and Bartee [1, Chapter 13], Selmer [9], and Zierler [12]. For important facts on linear recurring sequences in $\mathbf{Z}/m\mathbf{Z}$, see Ward [10] and Hall [3].

2. Linear recurrences in modules over finite rings.

Let R be a finite ring (not necessarily commutative) with identity, and let M be a unitary left R-module. All the subsequent results have obvious analogues for unitary right R-modules. We consider a sequence (y_n), $n = 0, 1, \ldots$, of elements of M satisfying the recurrence relation

$$(1) \qquad y_{n+k} = a_{k-1}y_{n+k-1} + a_{k-2}y_{n+k-2} + \ldots + a_0 y_n + a \quad \text{for } n = 0, 1, \ldots,$$

where k is a positive integer, $a \in M$, $a_i \in R$ for $i = 0, 1, \ldots, k-1$, and $y_0, \ldots, y_{k-1} \in M$ are given initial values. If $a = 0$, then (1) is called a (kth order) homogeneous linear recurrence relation, otherwise it is a (kth order) inhomogeneous linear recurrence relation. The sequence (y_n) itself is called a (kth order) homogeneous, or inhomogeneous. linear recurring sequence in M, respectively. If no distinction has to be made between these two cases, we simply speak of a linear recurring sequence in M.

We shall call a k-tuple $\boldsymbol{x} = (x_0, \ldots, x_{k-1})$ of elements of M a row vector (over M) and its transpose $\boldsymbol{x}^{\mathrm{T}}$ a column vector (over M), although, strictly speaking, these are in general not elements of a vector space. A similar convention will apply to k-tuples of elements of R.

Let (y_n), $n = 0, 1, \ldots$, be a linear recurring sequence in M satisfying the recurrence relation (1). For each $n \geqq 0$, we define a row vector $\boldsymbol{y}_n$ over M by $\boldsymbol{y}_n = (y_n, y_{n+1}, \ldots, y_{n+k-1})$, called the nth state vector. We note that one sees immediately by induction that each y_n lies in the submodule L of M generated by $y_0, \ldots, y_{k-1}$, and a. But L is finite as a finitely generated

module over a finite ring, and so there are only finitely many possibilities for state vectors over L. Therefore, the sequence (y_n) must ultimately be periodic. Let n_0 be the length of the preperiod and τ the length of the period of the sequence (y_n), so that $y_{n+\tau}=y_n$ for all $n \geqq n_0$. The following is an important sufficient condition for (y_n) to be purely periodic, i.e., for n_0 to be zero.

THEOREM 2.1. *If* (y_n), $n=0, 1, \ldots$, *is a linear recurring sequence in* M *and if the coefficient* a_0 *in* (1) *is a unit in* R, *then the sequence* (y_n) *is purely periodic.*

PROOF. Since (y_n) is ultimately periodic, there exist integers i and j with $i>j>0$ such that $\boldsymbol{y}_i=\boldsymbol{y}_j$. From (1) with $n=i-1$ and the fact that a_0 is a unit in R, one sees that y_{i-1} is uniquely determined by $y_i, \ldots, y_{i+k-1}$. Using (1) with $n=j-1$, one finds for y_{j-1} the same expression as for y_{i-1}, hence $\boldsymbol{y}_{i-1}=\boldsymbol{y}_{j-1}$. Continuing in this manner, one arrives at $\boldsymbol{y}_{i-j}=\boldsymbol{y}_0$. Thus, the sequence (y_n) is purely periodic.

REMARK 2.2. For homogeneous linear recurring sequences in finite commutative rings, the above result was already shown by Ward [11].

With a linear recurring sequence (y_n) in M, we associate a matrix A as follows. Suppose (y_n) satisfies the linear recurrence relation (1); then the $k \times k$-matrix A over R is defined by

$$A = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ a_0 & a_1 & a_2 & \ldots & a_{k-1} \end{pmatrix}. \tag{2}$$

If $k=1$, then A is understood to be (a_0). The matrix A depends, of course, only on the linear recurrence relation.

THEOREM 2.3. *Let* (y_n), $n=0, 1, \ldots$, *be a* k*th order homogeneous linear recurring sequence in* M *with the coefficient* a_0 *in* (1) *being a unit in* R. *Then the period* τ *of* (y_n) *divides the order of the matrix* A *from* (2) *in the general linear group* $\mathrm{GL}(k, R)$.

PROOF. We note first that $\det A=(-1)^{k-1}a_0$ is a unit in R, so that A is indeed an element of $\mathrm{GL}(k,R)$. The matrix A operates from the left in an obvious way on column vectors over M. Let $\boldsymbol{y}_0=(y_0, \ldots, y_{k-1})$ be the

initial state vector. Then one checks easily that $\boldsymbol{y}_1^{\mathrm{T}} = A\boldsymbol{y}_0^{\mathrm{T}}$, and so it follows by induction that

$$\boldsymbol{y}_n^{\mathrm{T}} = A^n \boldsymbol{y}_0^{\mathrm{T}} \quad \text{for } n = 0, 1, \ldots . \tag{3}$$

Let σ be the order of A in $\mathrm{GL}(k, R)$. Then $\boldsymbol{y}_\sigma^{\mathrm{T}} = A^\sigma \boldsymbol{y}_0^{\mathrm{T}} = \boldsymbol{y}_0^{\mathrm{T}}$, hence $\boldsymbol{y}_\sigma = \boldsymbol{y}_0$. Consequently, σ is a (not necessarily the least) period of $(\boldsymbol{y}_n)$. It follows that τ, the least period, divides σ.

REMARK 2.4. From the above theorem, it follows in particular that τ divides the order of $\mathrm{GL}(k, R)$. This order is known for the most interesting classes of finite rings R. For instance, if $R = \mathsf{F}_q$, a finite field with q elements, then the order of $\mathrm{GL}(k, \mathsf{F}_q)$ is given by

$$q^{(k^2-k)/2}(q-1)(q^2-1)\ldots(q^k-1)$$

(cf. [5, Theorem VII. 12]), and if $R = \mathbf{Z}/m\mathbf{Z}$ with a positive integer m, then the order of $\mathrm{GL}(k, \mathbf{Z}/m\mathbf{Z})$ is equal to

$$m^{k^2} \prod_{p \mid m} \prod_{j=1}^{k} (1 - p^{-j}) ,$$

as can be seen by combining the results in Theorem VII. 6, Theorem VII. 16, and Chapter VII, Section 2, of [5]. Here, p runs through the distinct prime divisors of m.

Let $(\boldsymbol{y}_n)$ be an inhomogeneous linear recurring sequence in M satisfying (1). By using (1) with n replaced by $n+1$ and subtracting from it the original form of (1), we obtain

$$\boldsymbol{y}_{n+k+1} = b_k \boldsymbol{y}_{n+k} + b_{k-1} \boldsymbol{y}_{n+k-1} + \ldots + b_0 \boldsymbol{y}_n \quad \text{for } n = 0, 1, \ldots , \tag{4}$$

where $b_0 = -a_0$, $b_j = a_{j-1} - a_j$ for $j = 1, 2, \ldots, k-1$, and $b_k = a_{k-1} + 1$. Thus, the sequence $(\boldsymbol{y}_n)$ can be interpreted as a $(k+1)$st order homogeneous linear recurring sequence in M. It is then natural to associate with $(\boldsymbol{y}_n)$ the $(k+1) \times (k+1)$-matrix B over R defined by

$$B = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ b_0 & b_1 & b_2 & \ldots & b_k \end{pmatrix}. \tag{5}$$

THEOREM 2.5. *Let $(\boldsymbol{y}_n)$, $n = 0, 1, \ldots$, be a kth order inhomogeneous linear recurring sequence in M with the coefficient a_0 in (1) being a unit in R. Then the period τ of $(\boldsymbol{y}_n)$ divides the order of the matrix B from (5) in the general linear group $\mathrm{GL}(k+1, R)$.*

PROOF. As we have observed above, (y_n) may be viewed as a $(k+1)$st order homogeneous linear recurring sequence in M satisfying (4). Since $b_0 = -a_0$ is a unit in R, the result follows from Theorem 2.3.

REMARK 2.6. If $M = R$, considered as a module over itself, one may proceed in the following alternative way. Let (y_n) be as in Theorem 2.5 and consider the $(k+1) \times (k+1)$-matrix C over R defined by

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ a & a_0 & a_1 & a_2 & \dots & a_{k-1} \end{pmatrix}.$$

If $k = 1$, take

$$C = \begin{pmatrix} 1 & 0 \\ a & a_0 \end{pmatrix}.$$

Introduce modified state vectors $\boldsymbol{y}_n' = (1, y_n, y_{n+1}, \dots, y_{n+k-1})$, $n = 0, 1, \dots$. Then it is easily seen that $(\boldsymbol{y}_1')^{\mathrm{T}} = C(\boldsymbol{y}_0')^{\mathrm{T}}$, and so $(\boldsymbol{y}_n')^{\mathrm{T}} = C^n(\boldsymbol{y}_0')^{\mathrm{T}}$ for $n = 0, 1, \dots$ by induction. Since $\det C = (-1)^{k-1}a_0$ is a unit in R, the matrix C is an element of $\mathrm{GL}(k+1, R)$. One shows then as in the proof of Theorem 2.3 that the period τ of (y_n) divides the order of C in $\mathrm{GL}(k+1, R)$. This result was proved by Brenner [2] in a very special case.

To a linear recurring sequence (y_n) in M satisfying (1), we associate now two positive integers μ and ν in the following way. Let (d_n), $n = 0, 1, \dots$, be the homogeneous linear recurring sequence in R satisfying the recurrence relation

$$d_{n+k} = a_{k-1}d_{n+k-1} + a_{k-2}d_{n+k-2} + \dots + a_0 d_n \quad \text{for } n = 0, 1, \dots,$$

with the initial values $d_0 = d_1 = \dots = d_{k-2} = 0, d_{k-1} = 1$ ($d_0 = 1$ if $k = 1$). Thus, (d_n) is an "impulse response sequence" (cf. [9, p. 31]). The number ν associated with (y_n) is defined to be the length of the period of (d_n), and μ is defined to be the sum of the length of the period and the length of the preperiod of (d_n). The numbers μ and ν depend, of course, only on the linear recurrence relation. If a_0 is a unit in R, then $\mu = \nu$ according to Theorem 2.1.

THEOREM 2.7. *Let (y_n), $n = 0, 1, \dots$, be a homogeneous linear recurring sequence in M, and let τ be the length of its period. Then τ divides ν and, consequently, $\tau \leqq \mu$.*

PROOF. Let $\boldsymbol{d}_n$ be the nth state vector of the sequence (d_n). Suppose i and j are nonnegative integers such that $\boldsymbol{d}_i = \boldsymbol{d}_j$. Then $\boldsymbol{d}_{i+r} = \boldsymbol{d}_{j+r}$ for every $r \geqq 0$. If (y_n) satisfies (1) (with $a = 0$, of course), let A be the matrix from (2). According to (3), we have

$$\boldsymbol{d}_{i+r}^{\mathrm{T}} = A^{i+r}\boldsymbol{d}_0^{\mathrm{T}} \quad \text{and} \quad \boldsymbol{d}_{j+r} = A^{j+r}\boldsymbol{d}_0^{\mathrm{T}}$$

for every $r \geqq 0$, so that

$$(A^{i+r} - A^{j+r})\boldsymbol{d}_0^{\mathrm{T}} = \boldsymbol{0} \quad \text{for every } r \geqq 0 .$$

This implies $(A^i - A^j)A^r\boldsymbol{d}_0^{\mathrm{T}} = \boldsymbol{0}$, or, using (3) again,

$$(A^i - A^j)\boldsymbol{d}_r^{\mathrm{T}} = \boldsymbol{0} \quad \text{for every } r \geqq 0 . \tag{6}$$

Taking $r = 0$ in (6), we see that the last column vector of $A^i - A^j$ is zero. Using this information and (6) with $r = 1$, we find that the next to last column vector of $A^i - A^j$ is zero. By continuing in this manner until we arrive at $r = k-1$, always taking into account the special form of $\boldsymbol{d}_r$ for $0 \leqq r \leqq k-1$, we can show that all the column vectors of $A^i - A^j$ are zero. Hence, we have proved that $\boldsymbol{d}_i = \boldsymbol{d}_j$ implies $A^i = A^j$.

By definition, ν is the length of the period of (d_n), so that $\boldsymbol{d}_{j+\nu} = \boldsymbol{d}_j$ for some $j \geqq 0$. From this we infer $A^{j+\nu} = A^j$, and then (3) yields $\boldsymbol{y}_{j+\nu} = \boldsymbol{y}_j$. This shows that ν is a (not necessarily the least) period for (y_n), so that τ, the least period, divides ν. The inequality $\tau \leqq \mu$ is now trivial since $\nu \leqq \mu$.

THEOREM 2.8. *Let (y_n), $n = 0, 1, \ldots$, be an inhomogeneous linear recurring sequence in M satisfying* (1), *and let τ be the length of its period. Then τ divides ν' and $\tau \leqq \mu'$, where μ' and ν' are the numbers associated with the linear recurrence relation* (4).

PROOF. This follows from Theorem 2.7 and the fact that (y_n) can be viewed as a homogeneous linear recurring sequence in M satisfying (4).

THEOREM 2.9 *If (y_n), $n = 0, 1, \ldots$, is a linear recurring sequence in M satisfying* (1) *with a unit a_0 in R, then both μ and ν are equal to the order of the matrix A from* (2) *in the general linear group* $\mathrm{GL}(k, R)$.

PROOF. We have already observed that $\mu = \nu$ in the case under consideration. Furthermore, it follows from Theorem 2.3, applied to the sequence (d_n) in R, that ν divides the order σ of A in $\mathrm{GL}(k, R)$. Since (d_n) is purely periodic, we have $\boldsymbol{d}_\nu = \boldsymbol{d}_0$. We have seen in the first part of the proof of Theorem 2.7 that this implies $A^\nu = A^0$. Thus σ divides ν, and we are done.

3. Character sums.

Let R be again a finite ring with identity, and let M be a unitary left R-module. By a character of M, we shall mean a character of the additive group of M. Given a linear recurring sequence (y_n), $n=0,1,\ldots$, in M, we will estimate character sums over a full period of (y_n) and also over segments of the full period, with the character being nontrivial in a certain sense. Let n_0 be the length of the preperiod and τ the length of the period of (y_n), and let μ be the positive integer associated with (y_n) as described in Section 2. We shall write $e(t)=e^{2\pi it}$ for real t. From [7, Lemma 3 and Theorem 1] we obtain the following fundamental result.

THEOREM 3.1. *Let (y_n), $n=0,1,\ldots$, be a kth order linear recurring sequence in M, and let χ be a character of M that is nontrivial on each cyclic submodule Rb of M with $b\in M$, $b\neq 0$. Then, for every integer h we have*

$$|\textstyle\sum_{n=u}^{u+\tau-1}\chi(y_n)e(hn/\tau)| \leqq (\operatorname{card} R)^{k/2}(\tau/\mu)^{\frac{1}{2}} \quad \text{for all } u \geqq n_0 . \tag{7}$$

In particular, we have

$$|\textstyle\sum_{n=u}^{u+\tau-1}\chi(y_n)| \leqq (\operatorname{card} R)^{k/2}(\tau/\mu)^{\frac{1}{2}} \quad \text{for all } u \geqq n_0 . \tag{8}$$

COROLLARY 3.2. *Let F_q be a finite field with q elements, let (y_n), $n=0,1,\ldots$, be a kth order linear recurring sequence in F_q, and let χ be a nontrivial additive character of F_q. Then, for every integer h we have*

$$|\textstyle\sum_{n=u}^{u+\tau-1}\chi(y_n)e(hn/\tau)| \leqq q^{k/2}(\tau/\mu)^{\frac{1}{2}} \quad \text{for all } u \geqq n_0 . \tag{9}$$

In particular,

$$|\textstyle\sum_{n=u}^{u+\tau-1}\chi(y_n)| \leqq q^{k/2}(\tau/\mu)^{\frac{1}{2}} \quad \text{for all } u \geqq n_0 . \tag{10}$$

PROOF. Take $M=\mathsf{F}_q$, considered as a module over itself. Since the only nonzero ideal in F_q is F_q itself, the given character χ will satisfy the condition in Theorem 3.1. The inequalities (9) and (10) are thus special cases of (7) and (8), respectively.

COROLLARY 3.3. *Let $m\geqq 2$ and s be relatively prime integers, let (y_n), $n=0,1,\ldots$, be a kth order linear recurring sequence of integers, and let τ, μ, and n_0 be the numbers associated with the sequence $(y_n+m\mathbf{Z})$, $n=0,1,\ldots$, in $\mathbf{Z}/m\mathbf{Z}$. Then, for every integer h we have*

$$|\textstyle\sum_{n=u}^{u+\tau-1}e(sy_n/m)e(hn/\tau)| \leqq m^{k/2}(\tau/\mu)^{\frac{1}{2}} \quad \text{for all } u \geqq n_0 . \tag{11}$$

In particular,

$$|\textstyle\sum_{n=u}^{u+\tau-1}e(sy_n/m)| \leqq m^{k/2}(\tau/\mu)^{\frac{1}{2}} \quad \text{for all } u \geqq n_0 . \tag{12}$$

PROOF. Take $M = \mathbf{Z}/m\mathbf{Z}$, considered as a module over itself. Then $\chi(t+m\mathbf{Z}) = e(st/m)$ for $t \in \mathbf{Z}$ defines a character of M for which $\chi(t+m\mathbf{Z}) \neq 1$ as soon as $t \not\equiv 0 \pmod{m}$, so that the condition in Theorem 3.1 is satisfied. The inequalities (11) and (12) are thus special cases of (7) and (8), respectively.

REMARK 3.4. It is interesting to note that the sums in (9) and (11) contain certain Gaussian sums as special cases. Consider first a finite field $\mathbf{F}_q$ with q elements. Let g be a primitive element of $\mathbf{F}_q$, i.e., a generator of the multiplicative group $\mathbf{F}_q^*$ of $\mathbf{F}_q$. Let (y_n), $n = 0, 1, \ldots$, be a linear recurring sequence in $\mathbf{F}_q$ with $y_{n+1} = gy_n$ for $n = 0, 1, \ldots$ and $y_0 \neq 0$. Then $\tau = \mu = q-1$ and $n_0 = 0$. Define a multiplicative character ψ of $\mathbf{F}_q$ as follows: for $x \in \mathbf{F}_q^*$, we have $x = g^n$ for some n that is uniquely determined modulo τ; set $\psi(x) = e(hn/\tau)$. Then we can write

$$\sum_{n=0}^{\tau-1} \chi(y_n) e(hn/\tau) = \sum_{n=0}^{\tau-1} \chi(g^n y_0) e(hn/\tau) = \sum_{x \in \mathbf{F}_q^*} \chi(xy_0)\psi(x) ,$$

with the last sum being a Gaussian sum in $\mathbf{F}_q$. The inequality (9) reduces now to a well-known inequality for Gaussian sums. In fact, if h is not divisible by τ, then we even have equality in (9), which shows that the inequalities (7) and (9) cannot be improved for $k = 1$.

Now let $m = p^\alpha$ with an odd prime p and $\alpha \geqq 2$, and let λ be a primitive root modulo m. Let (y_n), $n = 0, 1, \ldots$, be a linear recurring sequence of integers with $y_{n+1} = \lambda y_n$ for $n = 0, 1, \ldots$ and $(y_0, m) = 1$. Then $n_0 = 0$ and $\tau = \mu = \varphi(m)$, where φ is Euler's totient function. Define a Dirichlet character ψ modulo m as follows: for $(t, m) = 1$, we have $\lambda^n \equiv t \pmod{m}$ for some n that is uniquely determined modulo τ; set $\psi(t) = e(hn/\tau)$. Then we can write

$$\sum_{n=0}^{\tau-1} e(sy_n/m) e(hn/\tau) = \sum_{n=0}^{\tau-1} e(sy_0\lambda^n/m) e(hn/\tau) = \sum_{\substack{j=0 \\ (j,m)=1}}^{m-1} e(sy_0 j/m)\psi(j) ,$$

where the last sum is a Gaussian sum modulo m. The inequality (11) reduces now to a well-known inequality for Gaussian sums. If h is not divisible by p, then ψ is a primitive character modulo m, and in this case we even have equality in (11). This shows that the inequalities (7) and (11) cannot be improved for $k = 1$.

We consider now the problem of estimating character sums over segments of the period of a linear recurring sequence. This will lead to an improvement of [7, Theorem 2]. To this end, the following auxiliary result is needed.

LEMMA 3.5. *For any positive integers r and s, we have*

$$\sum_{h=0}^{r-1}\left|\sum_{j=0}^{s-1}e(hj/r)\right| < (2/\pi)r\log r + \tfrac{2}{5}r + s\,. \tag{13}$$

PROOF. The lemma is trivial for $r=1$. For $r\geqq 2$, we have

$$\left|\sum_{j=0}^{s-1}e(hj/r)\right| = \frac{|e(hs/r)-1|}{|e(h/r)-1|} \leqq \frac{1}{\sin\pi\|h/r\|} \quad \text{for } 1\leqq h\leqq r-1\,,$$

where $\|t\|$ denotes the absolute distance from the real number t to the nearest integer. It follows that

$$\sum_{h=0}^{r-1}\left|\sum_{j=0}^{s-1}e(hj/r)\right| \leqq \sum_{h=1}^{r-1}(\sin\pi\|h/r\|)^{-1}+s \leqq 2\sum_{h=1}^{[r/2]}(\sin(\pi h/r))^{-1}+s\,. \tag{14}$$

By the usual method of comparing sums with integrals, we obtain

$$\begin{aligned}\sum_{h=1}^{[r/2]}(\sin(\pi h/r))^{-1} &= (\sin(\pi/r))^{-1} + \sum_{h=2}^{[r/2]}(\sin(\pi h/r))^{-1}\\ &\leqq (\sin(\pi/r))^{-1} + \int_1^{[r/2]}\frac{dx}{\sin(\pi x/r)} \leqq (\sin(\pi/r))^{-1} + (r/\pi)\int_{\pi/r}^{\pi/2}\frac{dt}{\sin t}\\ &= (\sin(\pi/r))^{-1} + (r/\pi)\log\cot(\pi/2r) \leqq (\sin(\pi/r))^{-1} + (r/\pi)\log(2r/\pi)\,.\end{aligned}$$

For $r\geqq 6$ we have $(\pi/r)^{-1}\sin(\pi/r)\geqq(\pi/6)^{-1}\sin(\pi/6)$, hence $\sin(\pi/r)\geqq 3/r$. This implies

$$\sum_{h=1}^{[r/2]}(\sin(\pi h/r))^{-1} \leqq (r/\pi)\log r + (\tfrac{1}{3}-\pi^{-1}\log\tfrac{1}{2}\pi)r \quad \text{for } r\geqq 6\,,$$

and so

$$\sum_{h=1}^{[r/2]}(\sin(\pi h/r))^{-1} < (r/\pi)\log r + \tfrac{1}{5}r \quad \text{for } r\geqq 6\,. \tag{15}$$

The inequality (15) is easily checked for $r=3$, 4, and 5, so that (13) holds for $r\geqq 3$ in view of (14). For $r=2$, the inequality (13) is shown by inspection.

THEOREM 3.6. *Let (y_n) and χ be as in Theorem* 3.1. *Then,*

$$\left|\sum_{n=u}^{u+N-1}\chi(y_n)\right| < (\operatorname{card}R)^{k/2}(\tau/\mu)^{\frac{1}{2}}((2/\pi)\log\tau + \tfrac{2}{5} + N/\tau) \quad \textit{for } u\geqq n_0 \tag{16}$$

and $1\leqq N\leqq\tau$.

PROOF. We start from the identity

$$\sum_{n=u}^{u+N-1}\chi(y_n) = \sum_{n=u}^{u+\tau-1}\chi(y_n)\sum_{j=0}^{N-1}\tau^{-1}\sum_{h=0}^{\tau-1}e(h(n-u-j)/\tau) \quad \text{for } 1\leqq N\leqq\tau\,,$$

which holds since the sum over j is 1 for $u\leqq n\leqq u+N-1$ and 0 for $u+N\leqq n\leqq u+\tau-1$. Rearranging terms, we get

$$\sum_{n=u}^{u+N-1}\chi(y_n) = \tau^{-1}\sum_{h=0}^{\tau-1}\Big(\sum_{j=0}^{N-1}e(-h(u+j)/\tau)\Big)\Big(\sum_{n=u}^{u+\tau-1}\chi(y_n)e(hn/\tau)\Big)\,,$$

and so, by Theorem 3.1,

$$|\sum_{n=u}^{u+N-1}\chi(y_n)| \leqq \tau^{-1}\sum_{h=0}^{\tau-1}|\sum_{j=0}^{N-1} e(-h(u+j)/\tau)|\,|\sum_{n=u}^{u+\tau-1}\chi(y_n)e(hn/\tau)|$$
$$\leqq \tau^{-1}(\operatorname{card} R)^{k/2}(\tau/\mu)^{\frac{1}{2}}\sum_{h=0}^{\tau-1}|\sum_{j=0}^{N-1}e(hj/\tau)| .$$

An application of Lemma 3.5 yields the inequality (16).

COROLLARY 3.7. *Let F_q be a finite field with q elements, let (y_n), $n=0,1,\ldots$, be a kth order linear recurring sequence in F_q, and let χ be a nontrivial additive character of F_q. Then,*

$$|\sum_{n=u}^{u+N-1}\chi(y_n)| < q^{k/2}(\tau/\mu)^{\frac{1}{2}}((2/\pi)\log\tau+\tfrac{2}{5}+N/\tau) \quad \text{for } u\geqq n_0 \text{ and } 1\leqq N\leqq\tau .$$

COROLLARY 3.8. *Let $m\geqq 2$ and s be relatively prime integers, let (y_n), $n=0,1,\ldots$, be a kth order linear recurring sequence of integers, and let τ, μ, and n_0 be the numbers associated with the sequence $(y_n+m\mathbf{Z})$, $n=0,1,\ldots$, in $\mathbf{Z}/m\mathbf{Z}$. Then,*

$$|\sum_{n=u}^{u+N-1}e(sy_n/m)| < m^{k/2}(\tau/\mu)^{\frac{1}{2}}((2/\pi)\log\tau+\tfrac{2}{5}+N/\tau) \text{ for } u\geqq n_0$$
$$\text{and } 1\leqq N\leqq\tau .$$

4. Distribution properties of linear recurring sequences in finite fields.

The estimates in Section 3 are now applied to the problem of the distribution of elements in the period (or in segments of the period) of a linear recurring sequence in a finite field.

Let F_q be a finite field with q elements, let (y_n), $n=0,1,\ldots$, be a kth order linear recurring sequence in F_q satisfying (1) with $a,a_0,\ldots,a_{k-1}\in\mathsf{F}_q$, and let the associated numbers τ, μ, and n_0 be defined as in Section 2. For a subset W of F_q, let $A(W)$ be the number of elements in a full period of (y_n) that belong to W. If W is a singleton $\{w\}$, we write $A(w)$ instead of $A(\{w\})$.

THEOREM 4.1. *For any kth order linear recurring sequence (y_n), $n=0,1,\ldots$, in a finite field F_q with q elements and for any subset W of F_q, we have*

$$|A(W)-(\tau/q)\operatorname{card} W| \leqq q^{k/2-1}(\tau/\mu)^{\frac{1}{2}}\sum_{\chi\neq\chi_0}|\sum_{w\in W}\chi(w)| ,$$

where the sum is extended over all nontrivial additive characters χ of F_q.

PROOF. For $w\in\mathsf{F}_q$, let c_w be the characteristic function of the singleton $\{w\}$. We have

$$c_w(x) = q^{-1}\sum_{\chi}\chi(x-w) \quad \text{for all } x\in\mathsf{F}_q ,$$

where the sum is extended over all additive characters χ of F_q. It follows that

$$A(w) = \sum_{n=n_0}^{n_0+\tau-1} c_w(y_n) = \sum_{n=n_0}^{n_0+\tau-1} q^{-1} \sum_{\chi} \chi(y_n - w) = q^{-1} \sum_{\chi} \overline{\chi(w)} \sum_{n=n_0}^{n_0+\tau-1} \chi(y_n),$$

and so

$$A(W) = q^{-1} \sum_{\chi} \sum_{w \in W} \overline{\chi(w)} \sum_{n=n_0}^{n_0+\tau-1} \chi(y_n) .$$

If χ_0 denotes the trivial character of F_q, then

$$A(W) - (\tau/q) \operatorname{card} W = q^{-1} \sum_{\chi \neq \chi_0} \sum_{w \in W} \overline{\chi(w)} \sum_{n=n_0}^{n_0+\tau-1} \chi(y_n) . \tag{17}$$

Thus, by using (10), we obtain

$$\begin{aligned} |A(W) - (\tau/q) \operatorname{card} W| &\leqq q^{-1} \sum_{\chi \neq \chi_0} \Big| \sum_{w \in W} \overline{\chi(w)} \Big| \Big| \sum_{n=n_0}^{n_0+\tau-1} \chi(y_n) \Big| \\ &\leqq q^{k/2-1} (\tau/\mu)^{\frac{1}{2}} \sum_{\chi \neq \chi_0} \Big| \sum_{w \in W} \chi(w) \Big| . \end{aligned}$$

COROLLARY 4.2. *For any kth order linear recurring sequence* (y_n), $n = 0, 1, \ldots$, *in a finite field* F_q *with* q *elements and for any* $w \in \mathsf{F}_q$, *we have*

$$|A(w) - \tau/q| \leqq (1 - 1/q) q^{k/2} (\tau/\mu)^{\frac{1}{2}} .$$

REMARK 4.3. A result of the type of Corollary 4.2 was shown by a completely different method by Hall [4], but only for the case where (y_n) is a homogeneous linear recurring sequence in F_q with the characteristic polynomial $f(x) = x^k - a_{k-1}x^{k-1} - \ldots - a_0$ of the recurrence being irreducible over F_q. For $q = 2$, Selmer [9, p. 125] extended Hall's result to the case where f is the product of two distinct irreducible polynomials over F_q, with (y_n) still assumed to be homogeneous. It should be noted that, according to Theorem 2.7, we have $\tau \leqq \mu$ for homogeneous (y_n). In the case considered by Hall, it is well known that we have in fact $\tau = \mu$ as soon as the initial state vector $(y_0, \ldots, y_{k-1})$ is not the zero vector (cf. [9, p. 46]).

REMARK 4.4. The sum $\sum_{\chi \neq \chi_0} |\sum_{w \in W} \chi(w)|$ occurring in Theorem 4.1 may be estimated as follows. By the Cauchy-Schwarz inequality, we have

$$\begin{aligned} \Big(\sum_{\chi \neq \chi_0} \Big| \sum_{w \in W} \chi(w) \Big| \Big)^2 &\leqq (q-1) \sum_{\chi \neq \chi_0} \Big| \sum_{w \in W} \chi(w) \Big|^2 \\ &= (q-1) \Big(\sum_{\chi} \Big| \sum_{w \in W} \chi(w) \Big|^2 - (\operatorname{card} W)^2 \Big) \\ &= (q-1) \Big(\sum_{\chi} \sum_{w_1, w_2 \in W} \chi(w_1 - w_2) - (\operatorname{card} W)^2 \Big) \\ &= (q-1) \Big(\sum_{w_1, w_2 \in W} \sum_{\chi} \chi(w_1 - w_2) - (\operatorname{card} W)^2 \Big) \\ &= (q-1)(q \operatorname{card} W - (\operatorname{card} W)^2) . \end{aligned}$$

Therefore,

$$\sum_{\chi \neq \chi_0} |\sum_{w \in W} \chi(w)| \leq (q-1)^{\frac{1}{2}} (\operatorname{card} W)^{\frac{1}{2}} (q - \operatorname{card} W)^{\frac{1}{2}} .$$

We consider now the distribution of elements in segments of the period of a linear recurring sequence (y_n) in $\mathbf{F}_q$. This problem cannot be treated at all by Hall's method. For a subset W of $\mathbf{F}_q$, for $N_0 \geq n_0$ and $1 \leq N \leq \tau$, let $A(W; N_0, N)$ be the number of n, $N_0 \leq n \leq N_0 + N - 1$, such that $y_n \in W$. If W is a singleton $\{w\}$, we write $A(w; N_0, N)$ instead of $A(\{w\}; N_0, N)$.

THEOREM 4.5. *For any kth order linear recurring sequence (y_n), $n = 0, 1, \ldots$, in a finite field $\mathbf{F}_q$ with q elements and for any subset W of $\mathbf{F}_q$, we have*

$$|A(W; N_0, N) - (N/q) \operatorname{card} W| \leq q^{k/2-1} (\tau/\mu)^{\frac{1}{2}} ((2/\pi) \log \tau + \tfrac{2}{5} + N/\tau) \cdot \cdot \sum_{\chi \neq \chi_0} |\sum_{w \in W} \chi(w)|$$

for $N_0 \geq n_0$ and $1 \leq N \leq \tau$.

PROOF. By the same arguments that led to (17), one shows

$$A(W; N_0, N) - (N/q) \operatorname{card} W = q^{-1} \sum_{\chi \neq \chi_0} \sum_{w \in W} \overline{\chi(w)} \sum_{n=N_0}^{N_0+N-1} \chi(y_n) .$$

Thus, by using Corollary 3.7, one obtains

$$\begin{aligned} |A(W; N_0, N) - (N/q) \operatorname{card} W| &\leq q^{-1} \sum_{\chi \neq \chi_0} |\sum_{w \in W} \overline{\chi(w)}| \, |\sum_{n=N_0}^{N_0+N-1} \chi(y_n)| \\ &\leq q^{k/2-1} (\tau/\mu)^{\frac{1}{2}} ((2/\pi) \log \tau + \tfrac{2}{5} + N/\tau) \sum_{\chi \neq \chi_0} |\sum_{w \in W} \chi(w)| . \end{aligned}$$

COROLLARY 4.6. *For any kth order linear recurring sequence (y_n), $n = 0, 1, \ldots$, in a finite field $\mathbf{F}_q$ with q elements and for any $w \in \mathbf{F}_q$, we have*

$$|A(w; N_0, N) - N/q| \leq (1 - q^{-1}) q^{k/2} (\tau/\mu)^{\frac{1}{2}} ((2/\pi) \log \tau + \tfrac{2}{5} + N/\tau)$$

for $N_0 \geq n_0$ and $1 \leq N \leq \tau$.

REMARK 4.7. A negative result can be shown in connection with Corollary 4.6. We first recall that a polynomial $f(x) = x^k - a_{k-1} x^{k-1} - \ldots - a_0 \in \mathbf{F}_q[x]$ is called primitive if it is the minimal polynomial over $\mathbf{F}_q$ of a generator of the multiplicative group $\mathbf{F}_{q^k}^*$. Any kth order homogeneous linear recurring sequence (y_n), $n = 0, 1, \ldots$, in $\mathbf{F}_q$ having a nonzero initial state vector and satisfying the linear recurrence relation $y_{n+k} = a_{k-1} y_{n+k-1} + \ldots + a_0 y_n$ for $n = 0, 1, \ldots$ is called a maximal period sequence (associated with the primitive polynomial f). Any such maximal period sequence is purely periodic with $\tau = \mu = q^k - 1$. Now let χ be a nontrivial additive character of $\mathbf{F}_q$. Then it was shown in [7, Theorem 5] that there

exist a maximal period sequence (y_n), $n=0,1,\ldots$, in F_q (associated with the given primitive polynomial f) and an $N, 1 \leqq N \leqq \tau$, such that

$$|\textstyle\sum_{n=0}^{N-1}\chi(y_n)| > \frac{1}{2}q^{k/2}\,. \tag{18}$$

On the other hand, we can write

$$\textstyle\sum_{n=0}^{N-1}\chi(y_n) = \sum_{w\in\mathsf{F}_q}A(w;\,0,N)\chi(w) = \sum_{w\in\mathsf{F}_q}(A(w;\,0,N)-N/q)\chi(w)\,,$$

so that

$$|\textstyle\sum_{n=0}^{N-1}\chi(y_n)| \leqq \sum_{w\in\mathsf{F}_q}|A(w;\,0,N)-N/q|\,.$$

It follows then from (18) that there exists a $w\in\mathsf{F}_q$ such that

$$|A(w;\,0,N)-N/q| > \tfrac{1}{2}q^{k/2-1}\,. \tag{19}$$

REMARK 4.8. If arbitrary subsets W of F_q are considered such as in Theorem 4.5, then (19) can be improved, thereby yielding a result that complements Theorem 4.5. Choose a nontrivial additive character χ of F_q, and consider again a maximal period sequence (y_n) and an integer $N, 1 \leqq N \leqq \tau$, such that (18) holds. If p is the characteristic of F_q, then $(\chi(w))^p = \chi(pw) = 1$ for every $w\in\mathsf{F}_q$, and so the values of χ are pth roots of unity. For $j=1,2,\ldots,p$, let

$$W_j = \{w\in\mathsf{F}_q:\ \chi(w) = e(j/p)\}\,.$$

Then we can write

$$\begin{aligned}\textstyle\sum_{n=0}^{N-1}\chi(y_n) &= \textstyle\sum_{j=1}^{p}\sum_{w\in W_j}(A(w;\,0,N)-N/q)\chi(w)\\ &= \textstyle\sum_{j=1}^{p}(A(W_j;\,0,N)-(N/q)\operatorname{card}W_j)e(j/p)\,.\end{aligned}$$

Using summation by parts, we obtain

$$\textstyle\sum_{n=0}^{N-1}\chi(y_n) = \sum_{j=1}^{p-1}(A(X_j;\,0,N)-(N/q)\operatorname{card}X_j)(e(j/p)-e((j+1)/p))\,,$$

where $X_j = W_1\cup\ldots\cup W_j$ for $j=1,2,\ldots,p-1$. It follows that for some $\theta, 0\leqq\theta<1$, we have

$$\begin{aligned}|\textstyle\sum_{n=0}^{N-1}\chi(y_n)| &= |\textstyle\sum_{j=1}^{p-1}(A(X_j;\,0,N)-(N/q)\operatorname{card}X_j)(e(j/p)-e((j+1)/p))|\\ &= e(\theta)\textstyle\sum_{j=1}^{p-1}(A(X_j;\,0,N)-(N/q)\operatorname{card}X_j)\big(e(j/p)-e\big((j+1)/p\big)\big)\\ &= \textstyle\sum_{j=1}^{p-1}(A(X_j;\,0,N)-(N/q)\operatorname{card}X_j)\big(e(j/p+\theta)-e\big((j+1)/p+\theta\big)\big)\,.\end{aligned}$$

Since the last expression represents a real number, we get

$$\begin{aligned}|\textstyle\sum_{n=0}^{N-1}\chi(y_n)| &= \textstyle\sum_{j=1}^{p-1}(A(X_j;\,0,N)-(N/q)\operatorname{card}X_j)\big(\cos 2\pi(j/p+\theta)-\\ &\qquad -\cos 2\pi\big((j+1)/p+\theta\big)\big)\\ &\leqq \textstyle\sum_{j=1}^{p-1}|A(X_j;\,0,N)-(N/q)\operatorname{card}X_j|\,|\cos 2\pi(j/p+\theta)-\\ &\qquad -\cos 2\pi\big((j+1)/p+\theta\big)|\,.\end{aligned}$$

Suppose $|A(X_j; 0, N) - (N/q) \operatorname{card} X_j|$ attains its maximum for $j = h$. Then

$$|\textstyle\sum_{n=0}^{N-1} \chi(y_n)| \leqq |A(X_h; 0, N) - (N/q) \operatorname{card} X_h| \sum_{j=1}^{p-1} |\cos 2\pi(j/p + \theta) - \cos 2\pi((j+1)/p + \theta)| .$$

If we set

$$C_p(\theta) = \textstyle\sum_{j=1}^{p-1} |\cos 2\pi(j/p + \theta) - \cos 2\pi((j+1)/p + \theta)| \quad \text{for } 0 \leqq \theta < 1$$

and $C_p = \sup_\theta C_p(\theta)$, then we have

$$|\textstyle\sum_{n=0}^{N-1} \chi(y_n)| \leqq |A(X_h; 0, N) - (N/q) \operatorname{card} X_h| C_p .$$

By combining this with (18), we obtain

$$|A(X_h; 0, N) - (N/q) \operatorname{card} X_h| > (2C_p)^{-1} q^{k/2} ,$$

which is the desired improvement of (19). We note that $C_p(\theta)$ is bounded from above by the variation of the function $g(x) = \cos 2\pi(x + \theta)$ on the interval $[0, 1]$, so that $C_p \leqq 4$ for all p. This can be ameliorated easily for small values of p. For instance, it is trivial that $C_2 = 2$, and it is not hard to show that $C_3 = 3$. On the other hand, it is clear that $C_p \to 4$ as p tends to infinity through the prime numbers.

5. Distribution properties of linear recurring sequences modulo m.

Let (y_n), $n = 0, 1, \ldots$, be a kth order linear recurring sequence of integers and let $m \geqq 2$ be a fixed modulus. We shall be interested in distribution properties of the sequence (y_n) considered modulo m.

Let τ, μ, and n_0 be the numbers associated with the sequence $(y_n + m\mathbf{Z})$, $n = 0, 1, \ldots$, in $\mathbf{Z}/m\mathbf{Z}$, as described in Section 2. For a positive integer d, let $\tau(d)$ and $\mu(d)$ be the numbers associated with the sequence $(y_n + d\mathbf{Z})$, $n = 0, 1, \ldots$, in $\mathbf{Z}/d\mathbf{Z}$. Thus $\tau = \tau(m)$ and $\mu = \mu(m)$. For a subset V of $\{0, 1, \ldots, m-1\}$, let $A_m(V)$ be the number of n, $n_0 \leqq n \leqq n_0 + \tau - 1$, such that $y_n \equiv v \pmod m$ for some $v \in V$. Thus $A_m(V)$ is the number of elements in a full period of (y_n) modulo m that fall into the residue classes modulo m determined by the elements of V. If V is a singleton $\{v\}$, we write $A_m(v)$ instead of $A_m(\{v\})$.

THEOREM 5.1. *Let $m \geqq 2$ be an integer, and let (y_n), $n = 0, 1, \ldots$, be a kth order linear recurring sequence of integers. Then, for any subset V of $\{0, 1, \ldots, m-1\}$ we have*

$$|A_m(V) - (\tau/m) \operatorname{card} V| \leqq b(V)(\tau/m) \textstyle\sum_{\substack{d \mid m \\ d > 1}} \varphi(d) d^{k/2} (\tau(d)\mu(d))^{-\frac{1}{2}} , \tag{20}$$

where φ is Euler's totient function and where

$$b(V) = \max_{r=1,\dots,m-1} \left|\sum_{v\in V} e(rv/m)\right| . \tag{21}$$

PROOF. For an integer v, $0 \leqq v \leqq m-1$, the characteristic function c_v of the residue class $v+m\mathbf{Z}$ is given by

$$c_v(x) = m^{-1}\sum_{r=0}^{m-1} e(r(x-v)/m) \quad \text{for } x \in \mathbf{Z} .$$

Therefore,

$$A_m(v) = \sum_{n=n_0}^{n_0+\tau-1} c_v(y_n) = m^{-1}\sum_{r=0}^{m-1} e(-rv/m)\sum_{n=n_0}^{n_0+\tau-1} e(ry_n/m) ,$$

and so

$$A_m(V) = m^{-1}\sum_{r=0}^{m-1}\sum_{v\in V} e(-rv/m)\sum_{n=n_0}^{n_0+\tau-1} e(ry_n/m) .$$

It follows that

$$A_m(V) - (\tau/m)\operatorname{card} V = m^{-1}\sum_{r=1}^{m-1}\sum_{v\in V} e(-rv/m)\sum_{n=n_0}^{n_0+\tau-1} e(ry_n/m) ,$$

hence

$$\begin{aligned} |A_m(V) - (\tau/m)\operatorname{card} V| &\leqq m^{-1}\sum_{r=1}^{m-1} \left|\sum_{v\in V} e(rv/m)\right| \left|\sum_{n=n_0}^{n_0+\tau-1} e(ry_n/m)\right| \\ &\leqq (b(V)/m)\sum_{r=1}^{m-1} \left|\sum_{n=n_0}^{n_0+\tau-1} e(ry_n/m)\right| . \end{aligned} \tag{22}$$

For fixed r with $1 \leqq r \leqq m-1$, set $d=(r,m)$. Then we can write

$$\sum_{n=n_0}^{n_0+\tau-1} e(ry_n/m) = \sum_{n=n_0}^{n_0+\tau-1} e\left(\frac{(r/d)y_n}{m/d}\right).$$

It is clear that the length of the preperiod of (y_n) modulo m/d is at most n_0 and that τ is a period of (y_n) modulo m/d, which implies that $\tau(m/d)$ divides τ. Therefore,

$$\begin{aligned} \left|\sum_{n=n_0}^{n_0+\tau-1} e\left(\frac{(r/d)y_n}{m/d}\right)\right| &= \frac{\tau}{\tau(m/d)} \left|\sum_{n=n_0}^{n_0+\tau(m/d)-1} e\left(\frac{(r/d)y_n}{m/d}\right)\right| \\ &\leqq \frac{\tau}{\tau(m/d)}\left(\frac{m}{d}\right)^{k/2}\left(\frac{\tau(m/d)}{\mu(m/d)}\right)^{\frac{1}{2}} \end{aligned}$$

by (12). If we note that for each positive proper divisor d of m the number of r, $1 \leqq r \leqq m-1$, with $(r,m)=d$ is given by $\varphi(m/d)$, then we obtain from (22) that

$$\begin{aligned} |A_m(V) - (\tau/m)\operatorname{card} V| &\leqq b(V)(\tau/m)\sum_{\substack{d\mid m \\ 1\leq d<m}} \varphi(m/d)(m/d)^{k/2}(\tau(m/d)\mu(m/d))^{-\frac{1}{2}} \\ &= b(V)(\tau/m)\sum_{\substack{d\mid m \\ d>1}} \varphi(d)d^{k/2}(\tau(d)\mu(d))^{-\frac{1}{2}} , \end{aligned}$$

which completes the proof of the theorem.

COROLLARY 5.2. *Let $m \geqq 2$ be an integer, and let (y_n), $n = 0, 1, \ldots$, be a kth order linear recurring sequence of integers. Then, for any $v, 0 \leqq v \leqq m-1$, we have*

$$|A_m(v) - (\tau/m)| \leqq (\tau/m) \sum_{\substack{d \mid m \\ d>1}} \varphi(d) d^{k/2} (\tau(d)\mu(d))^{-\frac{1}{2}}.$$

The sum on the right-hand side of (20) can be estimated further, with the upper bound depending on the prime factorization of m. The case where m is a prime need not be considered here, since this has already been dealt with in Section 4. Next, let m be a prime power. Then we obtain the following result.

THEOREM 5.3. *Let $m = p^\alpha$ with a prime p and $\alpha \geqq 2$, and let (y_n), $n = 0, 1, \ldots$, be a kth order linear recurring sequence of integers. Then, for any subset V of $\{0, 1, \ldots, m-1\}$ we have*

$$\left| A_m(V) - \frac{\tau}{m} \operatorname{card} V \right| \leqq b(V) \left(1 - \frac{1}{p}\right) p^{k/2} \frac{m^{k/2} - \omega^{\alpha/2}}{p^{k/2} - \omega^{\frac{1}{2}}} \left(\frac{\tau}{\mu}\right)^{\frac{1}{2}}, \tag{23}$$

where $b(V)$ is given by (21) and where $\omega = \max_{s=1,\ldots,\alpha-1} \tau(p^{s+1})/p\tau(p^s)$. In particular, for any $v, 0 \leqq v \leqq m-1$, we have

$$\left| A_m(v) - \frac{\tau}{m} \right| \leqq \left(1 - \frac{1}{p}\right) p^{k/2} \frac{m^{k/2} - \omega^{\alpha/2}}{p^{k/2} - \omega^{\frac{1}{2}}} \left(\frac{\tau}{\mu}\right)^{\frac{1}{2}}. \tag{24}$$

PROOF. Suppose (y_n) satisfies the linear recurrence relation

$$y_{n+k} = a_{k-1} y_{n+k-1} + a_{k-2} y_{n+k-2} + \ldots + a_0 y_n + a \quad \text{for } n = 0, 1, \ldots,$$

with integers $a, a_0, \ldots, a_{k-1}$. Let (d_n), $n = 0, 1, \ldots$, be the associated impulse response sequence, i.e., the sequence of integers satisfying the recurrence relation

$$d_{n+k} = a_{k-1} d_{n+k-1} + a_{k-2} d_{n+k-2} + \ldots + a_0 d_n \quad \text{for } n = 0, 1, \ldots,$$

with initial values $d_0 = d_1 = \ldots = d_{k-2} = 0$, $d_{k-1} = 1$ ($d_0 = 1$ if $k = 1$). For a positive integer d, let $n_1(d)$ and $\nu(d)$ be the length of the preperiod and the length of the period of (d_n) modulo d, respectively. Thus, $\mu(d) = n_1(d) + \nu(d)$. Let A be the $k \times k$-matrix over $\mathbf{Z}$ defined by (2). In the same way as (3), one shows that

$$\boldsymbol{d}_n^{\mathrm{T}} = A^n \boldsymbol{d}_0^{\mathrm{T}} \quad \text{for } n = 0, 1, \ldots. \tag{25}$$

For given $s \geqq 1$, we have

$$\boldsymbol{d}_{n_1(p^s)+\nu(p^s)} \equiv \boldsymbol{d}_{n_1(p^s)} (\mathrm{mod}\, p^s),$$

hence, by using (25) and proceeding in the same way as in the first part of the proof of Theorem 2.7, we arrive at

$$A^{n_1(p^s)+\nu(p^s)} \equiv A^{n_1(p^s)} \pmod{p^s}.$$

Setting $D = A^{\nu(p^s)} - E$, with E being the $k \times k$ identity matrix over $\mathbf{Z}$, we may also write this in the form

$$A^{n_1(p^s)} D \equiv 0 \pmod{p^s}. \tag{26}$$

We note that all the matrices employed in this discussion will commute since they are polynomials in A. By raising the identity $A^{\nu(p^s)} = E + D$ to the pth power, we obtain

$$A^{p\nu(p^s)} - E = \binom{p}{1} D + \binom{p}{2} D^2 + \ldots + \binom{p}{p-1} D^{p-1} + D^p,$$

and so

$$A^{n_1(p^s)}(A^{p\nu(p^s)} - E) \equiv A^{n_1(p^s)} D^p \pmod{p^{s+1}} \tag{27}$$

by (26). Now we note that $\nu(p^s)$ is a period of (d_n) modulo p. Therefore,

$$\boldsymbol{d}_{n_1(p)+\nu(p^s)} \equiv \boldsymbol{d}_{n_1(p)} \pmod{p},$$

and by using (25) and the argument in the first part of the proof of Theorem 2.7, this implies

$$A^{n_1(p)+\nu(p^s)} \equiv A^{n_1(p)} \pmod{p},$$

which we may write in the form

$$A^{n_1(p)} D \equiv 0 \pmod{p}. \tag{28}$$

Multiplying (27) by $A^{n_1(p)}$, we obtain

$$A^{n_1(p^s)+n_1(p)}(A^{p\nu(p^s)} - E) \equiv (A^{n_1(p^s)} D)(A^{n_1(p)} D) D^{p-2} \equiv 0 \pmod{p^{s+1}}$$

according to (26) and (28). By going back to (25), this shows that

$$\boldsymbol{d}_{n_1(p^s)+n_1(p)+p\nu(p^s)} \equiv \boldsymbol{d}_{n_1(p^s)+n_1(p)} \pmod{p^{s+1}}. \tag{29}$$

We infer from (29) that $n_1(p^{s+1}) \leqq n_1(p^s) + n_1(p)$ and $\nu(p^{s+1}) \leqq p\nu(p^s)$. It follows that

$$\mu(p^{s+1}) = n_1(p^{s+1}) + \nu(p^{s+1}) \leqq n_1(p^s) + n_1(p) + p\nu(p^s) \leqq 2n_1(p^s) + p\nu(p^s),$$

since $\boldsymbol{d}_{n_1(p^s)+\nu(p^s)} \equiv \boldsymbol{d}_{n_1(p^s)} \pmod{p}$ implies $n_1(p) \leqq n_1(p^s)$. Therefore,

$$\mu(p^{s+1}) \leqq p\mu(p^s) \quad \text{for } s \geqq 1. \tag{30}$$

We are now ready to estimate the sum in (20). We have

$$\sum_{\substack{d \mid m \\ d>1}} \varphi(d) d^{k/2} (\tau(d)\mu(d))^{-\frac{1}{2}} = \sum_{j=1}^{\alpha} \varphi(p^j) p^{jk/2} (\tau(p^j)\mu(p^j))^{-\frac{1}{2}}.$$

Moreover, repeated application of (30) yields $\mu \leqq p^{\alpha-j}\mu(p^j)$ for $1 \leqq j \leqq \alpha$. Similarly, the inequality $\tau(p^{s+1}) \leqq \omega p \tau(p^s)$ for $1 \leqq s \leqq \alpha-1$ yields $\tau \leqq \omega^{\alpha-j}p^{\alpha-j}\tau(p^j)$ for $1 \leqq j \leqq \alpha$. Therefore,

$$\tau(p^j)\mu(p^j) \geqq \omega^{j-\alpha}p^{2j-2\alpha}\tau\mu \quad \text{for } 1 \leqq j \leqq \alpha,$$

and so, by (20),

$$(31) \quad |A_m(V) - \frac{\tau}{m}\operatorname{card} V| \leqq b(V)\frac{\tau}{m(\tau\mu)^{\frac{1}{2}}}\sum_{j=1}^{\alpha}\varphi(p^j)p^{jk/2}\omega^{(\alpha-j)/2}p^{\alpha-j}$$

$$= b(V)\left(\frac{\tau}{\mu}\right)^{\frac{1}{2}}\left(1-\frac{1}{p}\right)\omega^{\alpha/2}\sum_{j=1}^{\alpha}\left(\frac{p^{k/2}}{\omega^{\frac{1}{2}}}\right)^j.$$

The following argument shows that $\omega < p^k$. For $s \geqq 1$, let $n_0(p^s)$ be the length of the preperiod of (y_n) modulo p^s, and consider the state vectors

$$\mathbf{y}_{n_0(p^s)+g\tau(p^s)}, \quad g = 0, 1, \ldots .$$

They are all congruent to each other modulo p^s. There are p^k possibilities for pairwise incongruent k-tuples of integers modulo p^{s+1} to which these state vectors may be congruent modulo p^{s+1}. Thus, by the pigeon-hole principle, we have

$$\mathbf{y}_{n_0(p^s)+g\tau(p^s)} \equiv \mathbf{y}_{n_0(p^s)+h\tau(p^s)} (\mathrm{mod}\, p^{s+1})$$

for some g and h with $0 \leqq g < h \leqq p^k$. It follows that $\tau(p^{s+1}) \leqq (h-g)\tau(p^s) \leqq p^k\tau(p^s)$, and so $\omega \leqq p^{k-1} < p^k$. By summing the finite geometric series in (31), we readily obtain (23). The inequality (24) is an immediate consequence thereof.

REMARK 5.4. There are various interesting cases in which the number ω defined in the statement of Theorem 5.3 satisfies $\omega \leqq 1$. For instance, if (y_n) is a homogeneous linear recurring sequence with

$$y_{n+k} = a_{k-1}y_{n+k-1} + a_{k-2}y_{n+k-2} + \ldots + a_0 y_n \quad \text{for } n = 0, 1, \ldots ,$$

if (y_n) is purely periodic modulo $m = p^\alpha$, and if, in the double modulus notation of Ward [10], the polynomial

$$U(x) = y_0 x^{k-1} + (y_1 - a_{k-1}y_0)x^{k-2} + \ldots + (y_{k-1} - a_{k-1}y_{k-2} - \ldots - a_1)$$

is a unit modd$(p, x^k - a_{k-1}x^{k-1} - \ldots - a_0)$, then it follows easily from [10, p. 606] that $\omega \leqq 1$. Furthermore, if the conditions of [10, Theorem 13.1] are satisfied, we have again $\omega \leqq 1$ (note that the term "characteristic number" is used in that paper to denote the length of the period).

Using the information obtained in the proof of Theorem 5.3, the case of a general modulus m can also be treated.

THEOREM 5.5. *Let $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ be the canonical factorization of the integer $m \geqq 2$, and let (y_n), $n = 0, 1, \dots$, be a kth order linear recurring sequence of integers. Then, for any subset V of $\{0, 1, \dots, m-1\}$ we have*

$$|A_m(V) - (\tau/m) \operatorname{card} V| \leqq b(V)(\tau/\mu)^{\frac{1}{2}} P_m , \tag{32}$$

where

$$P_m = \prod_{j=1}^{r} \left(\frac{(p_j^{\alpha_j k/2} - \omega_j^{\alpha_j/2})(p_j - 1) p_j^{k/2-1}}{p_j^{k/2} - \omega_j^{\frac{1}{2}}} + \frac{(\tau(p_j^{\alpha_j})\mu(p_j^{\alpha_j}))^{\frac{1}{2}}}{p_j^{\alpha_j}} \right) - \prod_{j=1}^{r} \frac{(\tau(p_j^{\alpha_j})\mu(p_j^{\alpha_j}))^{\frac{1}{2}}}{p_j^{\alpha_j}} ,$$

where $b(V)$ is given by (21) *and where $\omega_j = \max_{s=1,\dots,\alpha_j-1} \tau(p_j^{s+1})/p_j \tau(p_j^s)$ if $\alpha_j > 1$ and $\omega_j = 1$ if $\alpha_j = 1$. In particular, for any v, $0 \leqq v \leqq m-1$, we have*

$$|A_m(v) - (\tau/m)| \leqq (\tau/\mu)^{\frac{1}{2}} P_m . \tag{33}$$

PROOF. Let $d > 1$ be a fixed divisor of m. If necessary, we change the enumeration of the prime divisors of m in such a way that we can write $d = p_1^{\beta_1} \dots p_t^{\beta_t}$ for some t, $1 \leqq t \leqq r$, and with $1 \leqq \beta_i \leqq \alpha_i$ for $1 \leqq i \leqq t$. By a result of Ward [10, Theorem 7.1], we have

$$\tau = [\tau(p_1^{\alpha_1}), \dots, \tau(p_r^{\alpha_r})] \quad \text{and} \quad \tau(d) = [\tau(p_1^{\beta_1}), \dots, \tau(p_t^{\beta_t})] ,$$

where, as usual, the square brackets denote the least common multiple of the integers enclosed. For $1 \leqq i \leqq t$, $\tau(p_i^{\beta_i})$ divides $\tau(p_i^{\alpha_i})$, so that $\tau(p_i^{\alpha_i}) = c_i \tau(p_i^{\beta_i})$ with an integer c_i satisfying $c_i \leqq (\omega_i p_i)^{\alpha_i - \beta_i}$ by the definition of ω_i. Now

$$\tau = [[\tau(p_1^{\alpha_1}), \dots, \tau(p_t^{\alpha_t})], \tau((p_{t+1})^{\alpha_{t+1}} \dots p_r^{\alpha_r})] ,$$

where

$$[\tau(p_1^{\alpha_1}), \dots, \tau(p_t^{\alpha_t})] = [c_1 \tau(p_1^{\beta_1}), \dots, c_t \tau(p_t^{\beta_t})]$$

divides $c_1 \dots c_t \tau(d)$. It follows that τ divides $[c_1 \dots c_t \tau(d), \tau((p_{t+1})^{\alpha_{t+1}} \dots p_r^{\alpha_r})]$, and so

$$\tau \leqq c_1 \dots c_t \tau(d) \tau((p_{t+1})^{\alpha_{t+1}} \dots p_r^{\alpha_r}) \leqq \omega_1^{\alpha_1 - \beta_1} \dots \omega_t^{\alpha_t - \beta_t} p_1^{\alpha_1 - \beta_1} \dots p_t^{\alpha_t - \beta_t} \tau(d) \tau((p_{t+1})^{\alpha_{t+1}} \dots p_r^{\alpha_r}) . \tag{34}$$

A similar inequality relating μ and $\mu(d)$ will now be established. In the proof of Theorem 5.3 we have shown, using the notation introduced there, that $\nu(p^{s+1}) \leqq p\nu(p^s)$ for any prime p and any $s \geqq 1$. By the same argument that led to (34), we obtain then

$$\nu \leqq p_1^{\alpha_1 - \beta_1} \dots p_t^{\alpha_t - \beta_t} \nu(d) \nu((p_{t+1})^{\alpha_{t+1}} \dots p_r^{\alpha_r}) . \tag{35}$$

If (d_n) is the impulse response sequence associated with (y_n), let n_1 be the length of the preperiod of (d_n) modulo m and $n_1(d)$ the length of the preperiod of (d_n) modulo d. By a result of Ward [10, Theorem 7.1] (note that the term "numeric" is used in that paper to denote the length of the preperiod), we have

$$n_1 = \max(n_1(p_1^{\alpha_1}), \ldots, n_1(p_r^{\alpha_r})),$$

and a similar formula for $n_1(d)$. In the proof of Theorem 5.3, we have shown that $n_1(p^{s+1}) \leqq n_1(p^s) + n_1(p)$ for any prime p and any $s \geqq 1$. Therefore,

$$n_1(p_i^{\alpha_i}) \leqq n_1(p_i^{\beta_i}) + (\alpha_i - \beta_i)n_1(p_i) \leqq n_1(d)(1 + \max_{1 \leqq i \leqq t}(\alpha_i - \beta_i))$$
$$\text{for} \quad 1 \leqq i \leqq t,$$

and so

$$n_1 \leqq \max\big(n_1(d)(1 + \max_{1 \leqq i \leqq t}(\alpha_i - \beta_i)), n_1((p_{t+1})^{\alpha_{t+1}} \ldots p_r^{\alpha_r})\big). \tag{36}$$

Since $1 + \max_{1 \leqq i \leqq t}(\alpha_i - \beta_i) \leqq \max_{1 \leqq i \leqq t} p_i^{\alpha_i - \beta_i}$, we clearly have

$$n_1(d)(1 + \max_{1 \leqq i \leqq t}(\alpha_i - \beta_i)) \leqq p_1^{\alpha_1 - \beta_1} \ldots p_t^{\alpha_t - \beta_t} n_1(d) \nu((p_{t+1})^{\alpha_{t+1}} \ldots p_r^{\alpha_r}),$$

and so, by (36),

$$n_1 \leqq p_1^{\alpha_1 - \beta_1} \ldots p_t^{\alpha_t - \beta_t} n_1(d) \nu((p_{t+1})^{\alpha_{t+1}} \ldots p_r^{\alpha_r}) + p_1^{\alpha_1 - \beta_1} \ldots p_t^{\alpha_t - \beta_t} \cdot \nu(d) n_1((p_{t+1})^{\alpha_{t+1}} \ldots p_r^{\alpha_r}).$$

Combining this with (35), we obtain

$$\mu = \nu + n_1 \leqq p_1^{\alpha_1 - \beta_1} \ldots p_t^{\alpha_t - \beta_t}\big(\nu(d)\nu((p_{t+1})^{\alpha_{t+1}} \ldots p_r^{\alpha_r}) + n_1(d)\nu((p_{t+1})^{\alpha_{t+1}} \ldots p_r^{\alpha_r}) + \nu(d) n_1((p_{t+1})^{\alpha_{t+1}} \ldots p_r^{\alpha_r})\big)$$
$$\leqq p_1^{\alpha_1 - \beta_1} \ldots p_t^{\alpha_t - \beta_t}(\nu(d) + n_1(d))\big(\nu((p_{t+1})^{\alpha_{t+1}} \ldots p_r^{\alpha_r}) + n_1((p_{t+1})^{\alpha_{t+1}} \ldots p_r^{\alpha_r})\big).$$

Hence,

$$\mu \leqq p_1^{\alpha_1 - \beta_1} \ldots p_t^{\alpha_t - \beta_t} \mu(d) \mu((p_{t+1})^{\alpha_{t+1}} \ldots p_r^{\alpha_r}). \tag{37}$$

From (20), we have

$$|A_m(V) - (\tau/m) \operatorname{card} V| \leqq b(V)(\tau/m) \sum_{\substack{d \mid m \\ d > 1}} \varphi(d) d^{k/2} (\tau(d)\mu(d))^{-\frac{1}{2}} \tag{38}$$
$$= b(V) \sum_{t=1}^{r} \sum_{1 \leqq j_1 < j_2 < \ldots < j_t \leqq r} S_{j_1, \ldots, j_t},$$

where

$$S_{j_1, \ldots, j_t} = (\tau/m) \sum_{d} \varphi(d) d^{k/2} (\tau(d)\mu(d))^{-\frac{1}{2}},$$

with the sum being extended over all positive divisors d of m that are divisible exactly by the primes $p_{j_1}, \ldots, p_{j_t}$. For simplicity of notation, we

will just estimate $S_{1,\dots,t}$, the argument for the others being completely analogous. We have

$$S_{1,\dots,t} = (\tau/m)\textstyle\sum_{\beta_1=1}^{\alpha_1}\cdots\sum_{\beta_t=1}^{\alpha_t}\varphi(p_1^{\beta_1}\dots p_t^{\beta_t})(p_1^{\beta_1}\dots p_t^{\beta_t})^{k/2}\cdot$$
$$\cdot\big(\tau(p_1^{\beta_1}\dots p_t^{\beta_t})\mu(p_1^{\beta_1}\dots p_t^{\beta_t})\big)^{-\frac{1}{2}}.$$

From (34) and (37), we get

$$\big(\tau(p_1^{\beta_1}\dots p_t^{\beta_t})\mu(p_1^{\beta_1}\dots p_t^{\beta_t})\big)^{-\frac{1}{2}}$$
$$\leqq \frac{p_1^{\alpha_1}\dots p_t^{\alpha_t}\omega_1^{(\alpha_1-\beta_1)/2}\dots\omega_t^{(\alpha_t-\beta_t)/2}\big(\tau((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r})\mu((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r})\big)^{\frac{1}{2}}}{p_1^{\beta_1}\dots p_t^{\beta_t}(\tau\mu)^{\frac{1}{2}}},$$

and so

$$S_{1,\dots,t} \leqq \left(\frac{\tau}{\mu}\right)^{\frac{1}{2}}\frac{\omega_1^{\alpha_1/2}\dots\omega_t^{\alpha_t/2}\big(\tau((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r})\mu((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r})\big)^{\frac{1}{2}}}{(p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r}}\cdot$$
$$\cdot\textstyle\sum_{\beta_1=1}^{\alpha_1}\cdots\sum_{\beta_t=1}^{\alpha_t}\dfrac{\varphi(p_1^{\beta_1}\dots p_t^{\beta_t})}{p_1^{\beta_1}\dots p_t^{\beta_t}}(p_1^{\beta_1}\dots p_t^{\beta_t})^{k/2}\omega_1^{-\beta_1/2}\dots\omega_t^{-\beta_t/2}$$
$$= \left(\frac{\tau}{\mu}\right)^{\frac{1}{2}}\frac{\omega_1^{\alpha_1/2}\dots\omega_t^{\alpha_t/2}\big(\tau((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r})\mu((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r})\big)^{\frac{1}{2}}}{(p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r}}\cdot$$
$$\cdot\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_t}\right)\textstyle\sum_{\beta_1=1}^{\alpha_1}\cdots\sum_{\beta_t=1}^{\alpha_t}\left(\dfrac{p_1^{k/2}}{\omega_1^{\frac{1}{2}}}\right)^{\beta_1}\cdots\left(\dfrac{p_t^{k/2}}{\omega_t^{\frac{1}{2}}}\right)^{\beta_t}$$
$$= \left(\frac{\tau}{\mu}\right)^{\frac{1}{2}}\frac{\big(\tau((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r})\mu((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r})\big)^{\frac{1}{2}}}{(p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r}}\prod_{i=1}^{t}\left(1-\frac{1}{p_i}\right)\omega_i^{\alpha_i/2}\cdot$$
$$\cdot\left(\textstyle\sum_{\beta_i=1}^{\alpha_i}\left(\dfrac{p_i^{k/2}}{\omega_i^{\frac{1}{2}}}\right)^{\beta_i}\right).$$

By an argument in the proof of Theorem 5.3, we have $\omega_j < p_j^k$ for $1 \leqq j \leqq r$. Therefore,

$$S_{1,\dots,t} \leqq \left(\frac{\tau}{\mu}\right)^{\frac{1}{2}}\frac{\big(\tau((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r})\mu((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r})\big)^{\frac{1}{2}}}{(p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r}}f_1\dots f_t,$$

where

$$f_j = \frac{(p_j^{\alpha_j k/2}-\omega_j^{\alpha_j/2})(p_j-1)p_j^{k/2-1}}{p_j^{k/2}-\omega_j^{\frac{1}{2}}} \quad \text{for } 1 \leqq j \leqq r.$$

Since $\tau((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r}) = [\tau((p_{t+1})^{\alpha_{t+1}}),\dots,\tau(p_r^{\alpha_r})]$, we have $\tau((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r}) \leqq \tau((p_{t+1})^{\alpha_{t+1}})\dots\tau(p_r^{\alpha_r})$. The inequality (37) shows that $\mu(dd') \leqq \mu(d)\mu(d')$ for d and d' relatively prime, and so $\mu((p_{t+1})^{\alpha_{t+1}}\dots p_r^{\alpha_r}) \leqq \mu((p_{t+1})^{\alpha_{t+1}})\dots\mu(p_r^{\alpha_r})$. Thus,

$$S_{1,\ldots,t} \leqq \left(\frac{\tau}{\mu}\right)^{\frac{1}{2}} \frac{\left(\tau((p_{t+1})^{\alpha_{t+1}})\mu((p_{t+1})^{\alpha_{t+1}})\right)^{\frac{1}{2}}}{(p_{t+1})^{\alpha_{t+1}}} \cdot \ldots \cdot \frac{(\tau(p_r{}^{\alpha_r})\mu(p_r{}^{\alpha_r}))^{\frac{1}{2}}}{p_r{}^{\alpha_r}} f_1 \ldots f_t$$

(39)

$$= \left(\frac{\tau}{\mu}\right)^{\frac{1}{2}} g_1 \ldots g_r \frac{f_1 \ldots f_t}{g_1 \ldots g_t},$$

where

$$g_j = \frac{(\tau(p_j{}^{\alpha_j})\mu(p_j{}^{\alpha_j}))^{\frac{1}{2}}}{p_j{}^{\alpha_j}} \quad \text{for } 1 \leqq j \leqq r.$$

It follows from (38) and (39) that

$$\begin{aligned} |A_m(V) - (\tau/m) \operatorname{card} V| &\leqq b(V)(\tau/\mu)^{\frac{1}{2}} g_1 \ldots g_r \textstyle\sum_{t=1}^{r} \sum_{1 \leqq j_1 < j_2 < \ldots < j_t \leqq r} \dfrac{f_{j_1} \ldots f_{j_t}}{g_{j_1} \ldots g_{j_t}} \\ &= b(V)(\tau/\mu)^{\frac{1}{2}} g_1 \ldots g_r (\textstyle\prod_{j=1}^{r}(1 + f_j/g_j) - 1) \\ &= b(V)(\tau/\mu)^{\frac{1}{2}} (\textstyle\prod_{j=1}^{r}(f_j + g_j) - \prod_{j=1}^{r} g_j), \end{aligned}$$

which is just (32). The inequality (33) is an immediate consequence.

The results obtained so far in this section deal with the distribution of elements in a full period of (y_n) modulo m. Our method can also be applied to yield information about the distribution of elements in segments of the period of (y_n) modulo m. We shall use the notation introduced in the beginning of this section. Furthermore, for a subset V of $\{0,1,\ldots, m-1\}$, for $N_0 \geqq n_0$ and $1 \leqq N \leqq \tau$, let $A_m(V; N_0, N)$ be the number of n, $N_0 \leqq n \leqq N_0 + N - 1$, such that $y_n \equiv v \pmod m$ for some $v \in V$. If V is a singleton $\{v\}$, we write $A_m(v; N_0, N)$ instead of $A_m(\{v\}; N_0, N)$.

THEOREM 5.6. *Let $m \geqq 2$ be an integer, and let (y_n), $n = 0,1,\ldots$, be a kth order linear recurring sequence of integers. Then, for any subset V of $\{0,1,\ldots,m-1\}$, for any $N_0 \geqq n_0$ and for any N with $1 \leqq N \leqq \tau$ we have*

$$|A_m(V; N_0, N) - (N/m) \operatorname{card} V| \leqq b(V)(N/m) \textstyle\sum_{\substack{d \mid m \\ d > 1}} \varphi(d) d^{k/2} (\tau(d)\mu(d))^{-\frac{1}{2}} +$$

(40)

$$+ (b(V)/m) \textstyle\sum_{\substack{d \mid m \\ d > 1}} \varphi(d) d^{k/2} (\tau(d)/\mu(d))^{\frac{1}{2}} ((2/\pi) \log \tau(d) + \tfrac{2}{5}),$$

where $b(V)$ is given by (21). *In particular, for every integer v, $0 \leqq v \leqq m-1$, for any $N_0 \geqq n_0$ and for any N with $1 \leqq N \leqq \tau$ we have*

$$|A_m(v; N_0, N) - (N/m)| \leqq (N/m) \textstyle\sum_{\substack{d \mid m \\ d > 1}} \varphi(d) d^{k/2} (\tau(d)\mu(d))^{-\frac{1}{2}} +$$

(41)

$$+ m^{-1} \textstyle\sum_{\substack{d \mid m \\ d > 1}} \varphi(d) d^{k/2} (\tau(d)/\mu(d))^{\frac{1}{2}} ((2/\pi) \log \tau(d) + \tfrac{2}{5}).$$

PROOF. By the same arguments that led to (22), we obtain

$$(42)\quad |A_m(V; N_0, N) - (N/m)\operatorname{card} V| \leqq (b(V)/m)\sum_{r=1}^{m-1}\left|\sum_{n=N_0}^{N_0+N-1} e(ry_n/m)\right|.$$

For fixed r with $1 \leqq r \leqq m-1$, set $d=(r,m)$. Then we can write

$$\sum_{n=N_0}^{N_0+N-1} e(ry_n/m) = \sum_{n=N_0}^{N_0+N-1} e\left(\frac{(r/d)y_n}{m/d}\right).$$

By the division algorithm, we have $N = q\tau(m/d)+h$ with an integer $q \geqq 0$ and $0 \leqq h < \tau(m/d)$. Then,

$$\begin{aligned}\sum_{n=N_0}^{N_0+N-1} e\left(\frac{(r/d)y_n}{m/d}\right) &= \sum_{n=N_0}^{N_0+q\tau(m/d)-1} e\left(\frac{(r/d)y_n}{m/d}\right) + \sum_{n=N_0+q\tau(m/d)}^{N_0+q\tau(m/d)+h-1} e\left(\frac{(r/d)y_n}{m/d}\right)\\ &= q\sum_{n=N_0}^{N_0+\tau(m/d)-1} e\left(\frac{(r/d)y_n}{m/d}\right) + \sum_{n=N_0+q\tau(m/d)}^{N_0+q\tau(m/d)+h-1} e\left(\frac{(r/d)y_n}{m/d}\right).\end{aligned}$$

We note that the length of the preperiod of (y_n) modulo m/d is at most n_0. Therefore, by (12) and Corollary 3.8,

$$\begin{aligned}\left|\sum_{n=N_0}^{N_0+N-1} e\left(\frac{(r/d)y_n}{m/d}\right)\right| &\leqq q\left(\frac{m}{d}\right)^{k/2}\left(\frac{\tau(m/d)}{\mu(m/d)}\right)^{\frac{1}{2}} + \left(\frac{m}{d}\right)^{k/2}\left(\frac{\tau(m/d)}{\mu(m/d)}\right)^{\frac{1}{2}}\cdot\\ &\quad\cdot\left(\frac{2}{\pi}\log\tau\left(\frac{m}{d}\right)+\frac{2}{5}+\frac{h}{\tau(m/d)}\right)\\ &= \left(\frac{m}{d}\right)^{k/2}\left(\frac{\tau(m/d)}{\mu(m/d)}\right)^{\frac{1}{2}}\left(\frac{2}{\pi}\log\tau\left(\frac{m}{d}\right)+\frac{2}{5}+\frac{N}{\tau(m/d)}\right)\\ &= N\left(\frac{m}{d}\right)^{k/2}\left(\tau\left(\frac{m}{d}\right)\mu\left(\frac{m}{d}\right)\right)^{-\frac{1}{2}} + \left(\frac{m}{d}\right)^{k/2}\left(\frac{\tau(m/d)}{\mu(m/d)}\right)^{\frac{1}{2}}\left(\frac{2}{\pi}\log\tau\left(\frac{m}{d}\right)+\frac{2}{5}\right).\end{aligned}$$

Since for each positive proper divisor d of m the number of r, $1 \leqq r \leqq m-1$, with $(r,m)=d$ is given by $\varphi(m/d)$, we obtain from (42) that

$$\begin{aligned}|A_m(V; N_0, N) - (N/m)\operatorname{card} V| &\leqq b(V)(N/m)\sum_{\substack{d\mid m\\ 1\leqq d<m}} \varphi(m/d)(m/d)^{k/2}\cdot\\ &\cdot(\tau(m/d)\mu(m/d))^{-\frac{1}{2}} + (b(V)/m)\sum_{\substack{d\mid m\\ 1\leqq d<m}} \varphi(m/d)(m/d)^{k/2}(\tau(m/d)/\mu(m/d))^{\frac{1}{2}}\cdot\\ &\cdot((2/\pi)\log\tau(m/d)+\tfrac{2}{5}),\end{aligned}$$

which yields (40). The inequality (41) is a special case thereof.

THEOREM 5.7. *Let $m = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ be the canonical factorization of the integer $m \geqq 2$, and let (y_n), $n=0,1,\ldots$, be a kth order linear recurring sequence of integers. Let $\omega_1,\ldots,\omega_r$ be defined as in Theorem 5.5, and set $\varrho =$*

$\max \tau(d)/\mu(d)$, *where the maximum is extended over all divisors* $d > 1$ *of* m. *Then, for any subset* V *of* $\{0, 1, \ldots, m-1\}$, *for any* $N_0 \geqq n_0$ *and for any* N *with* $1 \leqq N \leqq \tau$ *we have*

$$|A_m(V; N_0, N) - (N/m) \operatorname{card} V| \leqq b(V) N (\tau\mu)^{-\frac{1}{2}} P_m + b(V) m^{k/2} \varrho^{\frac{1}{2}} ((2/\pi) \log \tau + \tfrac{2}{5}), \tag{43}$$

where $b(V)$ *is given by* (21), *and* P_m *is defined in Theorem* 5.5. *In particular, for every integer* $v, 0 \leqq v \leqq m-1$, *we have*

$$|A_m(v; N_0, N) - (N/m)| \leqq N (\tau\mu)^{-\frac{1}{2}} P_m + m^{k/2} \varrho^{\frac{1}{2}} ((2/\pi) \log \tau + \tfrac{2}{5}) \tag{44}$$

for $N_0 \geqq n_0$ *and* $1 \leqq N \leqq \tau$.

Proof. We start from (40). Since the bound in (32) was obtained as an upper bound of the right-hand side of (20), it is clear that an upper bound for the first term on the right-hand side of (40) is given by N/τ times the bound in (32). This accounts for the first term on the right-hand side of (43). For the second term on the right-hand side of (40), we have

$$(b(V)/m) \sum_{\substack{d \mid m \\ d>1}} \varphi(d) d^{k/2} (\tau(d)/\mu(d))^{\frac{1}{2}} ((2/\pi) \log \tau(d) + \tfrac{2}{5}) \leqq (b(V)/m) \varrho^{\frac{1}{2}} \cdot \cdot ((2/\pi) \log \tau + \tfrac{2}{5}) \sum_{d \mid m} \varphi(d) d^{k/2},$$

where the last sum is extended over all positive divisors d of m. Denoting this sum by $G(m)$, we observe that G is a multiplicative arithmetic function. For a prime p and $\alpha \geqq 1$, one obtains by a straightforward calculation,

$$G(p^\alpha) = 1 + \frac{p^{k/2+1} - p^{k/2}}{p^{k/2+1} - 1} (p^{\alpha(k/2+1)} - 1) \leqq p^{\alpha(k/2+1)}. \tag{45}$$

This implies $G(m) \leqq m^{k/2+1}$, and so

$$(b(V)/m) \sum_{\substack{d \mid m \\ d>1}} \varphi(d) d^{k/2} (\tau(d)/\mu(d))^{\frac{1}{2}} ((2/\pi) \log \tau(d) + \tfrac{2}{5}) \leqq b(V) m^{k/2} \varrho^{\frac{1}{2}} ((2/\pi) \log \tau + \tfrac{2}{5}).$$

Thus, (43) is established. The inequality (44) is an immediate consequence.

Remark 5.8. If (y_n) is a homogeneous linear recurring sequence of integers or if (y_n) is at least homogeneous modulo m, then the number ϱ defined in Theorem 5.7 satisfies $\varrho \leqq 1$ in view of Theorem 2.7.

REMARK 5.9. Bounds that are slightly better, but even more complicated than those in (43) and (44) can be given by using the exact formula for $G(p^\alpha)$ in (45) instead of the upper bound established there.

REFERENCES

1. G. Birkhoff and T. C. Bartee, *Modern Applied Algebra*, McGraw-Hill, New York, 1970.
2. J. L. Brenner, *Linear recurrence relations*, Amer. Math. Monthly 61 (1954), 171–173.
3. M. Hall, *An isomorphism between linear recurring sequences and algebraic rings*, Trans. Amer. Math. Soc. 44 (1938), 196–218.
4. M. Hall, *Equidistribution of residues in sequences*, Duke Math. J. 4 (1938), 691–695.
5. M. Newman, *Integral Matrices*, Academic Press, New York – London, 1972.
6. H. Niederreiter, *On the distribution of pseudo-random numbers generated by the linear congruential method.* II, Math. Comp. 28 (1974), 1117–1132.
7. H. Niederreiter, *Some new exponential sums with applications to pseudo-random numbers*, Colloquium on Number Theory (Debrecen, 1974), North-Holland Publ. Co., Amsterdam, to appear.
8. H. Niederreiter, *On the distribution of pseudo-random numbers generated by the linear congruential method.* III, Math. Comp., to appear.
9. E. S. Selmer, *Linear Recurrence Relations over Finite Fields*, mimeographed notes, Univ. of Bergen, 1966.
10. M. Ward, *The arithmetical theory of linear recurring series*, Trans. Amer. Math. Soc. 35 (1933), 600–628.
11. M. Ward, *Arithmetical properties of sequences in rings*, Ann. of Math. (2) 39 (1938), 210–219.
12. N. Zierler, *Linear recurring sequences*, J. Soc. Industr. Appl. Math. 7 (1959), 31–48.

SCHOOL OF MATHEMATICS
THE INSTITUTE FOR ADVANCED STUDY
PRINCETON, NEW JERSEY 08540
U.S.A.