PERIODICITY OVER THE RING OF MATRICES

R. J. DECARLI
Rosary Hill College, Buffalo, New York

Let \( R \) be the ring of \( t \times t \) matrices with integral entries and identity \( I \). Consider the sequence \( \{M_m\} \) of elements of \( R \), recursively defined by

\[
M_{m+2} = A_1 M_{m+1} + A_0 M_m \quad \text{for} \quad m \geq 0,
\]

where \( M_0, M_1, A_0, \) and \( A_1 \) are arbitrary elements of \( R \). In [1] we established identities for such a sequence over an arbitrary ring with unity. In this paper we establish an analogue of Robinson's [3] result concerning periodicity modulo \( k \) where \( k \) is an integer greater than 1. We need the following definitions.

**Definition 1.** Let \( A = [a_{ij}] \) be an element of \( R \). We reduce \( A \) modulo \( k \) by reducing each entry modulo \( k \). If \( B = [b_{ij}] \in R \), then \( A \equiv B \pmod{k} \) if and only if \( a_{ij} \equiv b_{ij} \pmod{k} \) for all \( i, j \).

**Definition 2.** We say that the sequence defined by (1) is periodic modulo \( k \) if there exists an integer \( L \geq 2 \) such that \( M_i \equiv M_{i+L} \pmod{k} \) for \( i = 0, 1, 2, \ldots \). By the nature of the sequence we see that this is equivalent to the existence of an \( L \geq 2 \) such that \( M_0 \equiv M_L \pmod{k} \) and \( M_i \equiv M_{i+L} \pmod{k} \).

We assume for all matrices in the following Theorem that reduction modulo \( k \) has already taken place and we employ the usual notation for relative primeness. For \( A \in R \) we let \( \det A \) stand for the determinant of \( A \).

**Theorem 1.** If \( (\det A, k) = 1 \), then the \( \{M_m\} \) sequence defined by (1) is periodic modulo \( k \).

**Proof.** Let

\[
W_1 = \begin{bmatrix} 0 & 1 \\ A_0 & A_1 \end{bmatrix},
\]

where the entries are matrices from \( R \). If we set

\[
S_m = \begin{bmatrix} M_m \\ M_{m+1} \end{bmatrix}
\]

for \( n \geq 0 \), then a simple induction argument yields

\[
S_m = W_1^m S_0.
\]

If we can find a \( L \) such that \( W_1^L \equiv I \pmod{k} \), then \( S_L = W_1^L S_0 \equiv I S_0 \equiv S_0 \pmod{k} \) and we will have

\[
466
\]
which gives us periodicity. To show that such an \( L \) exists consider the sequence of matrices

\[
I, \quad W_1, \quad W_1^2, \quad \ldots.
\]

We first show that each matrix in (4) has an inverse modulo \( k \). Laplace's method for evaluating determinants immediately gives

\[
\det W_1^r = (\det W_1)^r = ((-1)^t \det A_0)^r \neq 0 \pmod{k},
\]

since \( \det A_0, k = 1 \). Also, \( \det A_0, k = 1 \) implies \( ((-1)^t \det A_0)^r, k = 1 \) and thus

\[
\det W_1^r, k = 1.
\]

For \( r = 0 \), \( W_1^0 = I \) which is its own inverse. For \( r > 0 \) we let \( w_{ij} \) denote the entries of \( W_1^r \) and \( A_{ij} \) the cofactor of \( w_{ij} \) in \( \det W_1^r \). We observe that \( A_{ij} \) is always integral. Using matrix methods we have

\[
(W_1^r)^{-1} = \begin{bmatrix}
\frac{A_{ij}}{\det W_1^r}
\end{bmatrix}^T,
\]

where \( T \) stands for the transpose. An entry in the right-hand side of (6) is of the form

\[
\frac{c}{\det W_1^r},
\]

where \( c \) is an integer. The equation \( (\det W_1^r)x \equiv c \pmod{k} \) has a unique solution since from (5) we have \( (\det W_1^r, k) = 1 \). Thus each entry in the right side of (6) is an integer and \( W_1^r \) has an inverse mod \( k \) for all \( r \geq 0 \). Because we only have \( k \) distinct integers mod \( k \) and \((2t)^2\) places to put them, we have at most \( k(2t)^2 \) different matrices in (4). Since the sequence is infinite we must have

\[
W_1^{L+r} \equiv W_1^r \pmod{k} \quad \text{for some} \quad L.
\]

Multiplying both sides of (7) by \( (W_1^r)^{-1} \) yields

\[
W_1^L \equiv I \pmod{k}.
\]

Since \( W_1 \neq I \) we see that \( L \geq 2 \). Thus we have

\[
S_L = W_1^L S_0 \equiv IS_0 = S_0 \pmod{k}
\]

which implies \( M_L \equiv M_0 \) and \( M_{L+1} \equiv M_1 \) and establishes periodicity.
The central role played by $A_0$ is more clearly illustrated if we consider a higher order recurrence defined for a fixed $d \geq 2$ by:

$$M_{m+d} = A_{d-1} M_{m+d-1} + A_{d-2} M_{m+d-2} + \cdots + A_0 M_m, \quad m \geq 0,$$

where the $A_i$ and the $M_i$, $0 \leq i \leq d - 1$, are arbitrary elements from $R$. Even though there are $2d$ arbitrary elements that determine this sequence, the question of periodicity still depends on the nature of $A_0$. If $\det (A_0, k) = 1$, then we again have periodicity. This is proved using

$$V = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots \\ \vdots \\ A_0 & A_1 & A_2 & \cdots & A_{d-1} \end{bmatrix}$$

in place of $W_1$ and

$$S_m = \begin{bmatrix} M_m \\ M_{m+1} \\ \vdots \\ \vdots \\ M_{m+d-1} \end{bmatrix}$$

It is easy to show that $S_m = V^m S_0$ and that $\det V$ depends on $\det A_0$. The rest of the proof follows as in the proof of Theorem 1. A close look at the position of $A_0$ in $V$ clearly indicates why it is so important in determining periodicity.

REFERENCES