A MATRIX REPRESENTATION OF THE PRIMITIVE RESIDUE CLASSES (mod 2n)

K. MAHLER

A problem in the geometry of numbers recently lead me to consider some simple matrices with elements 0, 1, and −1. I found to my surprise that these matrices had inverses of the same kind, that they were commutative, and that they in fact formed an Abelian group. These matrices are discussed in the present note.

1. Let m and n be two positive integers such that

\[ 1 \leq m < n, \quad (m, n) = 1. \]

Let further \( s \neq 0 \) be a parameter and \( t \) one of its \( n \)th roots,

\[ t^n = s. \]

There are thus \( n \) distinct possible values for \( t \), the values \( t_1, t_2, \ldots, t_n \) say.

Now denote by

\[ A(m, n) = (a_{hk}) \quad \text{and} \quad B(m, n) = (b_{hk}) \]

the two \( n \times n \) matrices with the following elements. For each pair of suffixes \( h, k = 1, 2, \ldots, n \) determine integers \( i, j, q, \) and \( r \) such that

\[ km - h \equiv i \pmod{n}, \quad 0 \leq i \leq n - 1, \quad q = \frac{km - h - i}{n}, \]

and

\[ km + h \equiv j \pmod{n}, \quad 1 \leq j \leq n, \quad r = \frac{km + h - j}{n}. \]

Then put

\[ a_{hk} = s^q \text{ if } 0 \leq i \leq m - 1, \quad a_{hk} = 0 \text{ if } m \leq i \leq n - 1; \]

\[ b_{hk} = s^{r-1} \text{ if } 1 \leq j \leq m, \quad b_{hk} = 0 \text{ if } m + 1 \leq j \leq n. \]

Thus, by way of example,
We shall study these matrices mainly in the case when $m$ is odd and $s$ has the value $-1$, but, for the present, do not yet impose these restrictions.

2. Denote by 

$$x = (x_h), \quad y = (y_h), \quad z = (z_h)$$

three variable $n \times 1$ matrices (column vectors) such that 

$$y = A(m, n)x \quad \text{and} \quad z = B(m, n)x,$$

or in explicit form,

$$y_n = \sum_{k=1}^{n} a_{hk} x_k, \quad z_n = \sum_{k=1}^{n} b_{hk} x_k.$$ 

Further put, for shortness,

$$Y = y_1 + t y_2 + t^2 y_3 + \cdots + t^{n-1} y_n,$$

$$Z = t^{n-1} z_1 + t^{n-2} z_2 + \cdots + t z_{n-1} + z_n.$$ 

Then

$$Y = \sum_{h=1}^{n} \sum_{k=1}^{n} t^{h-1} a_{hk} x_k = \sum_{k=1}^{n} \mathcal{U}_k x_k,$$

where

$$\mathcal{U}_k = \sum_{h=1}^{n} t^{h-1} a_{hk},$$

and similarly

$$Z = \sum_{h=1}^{n} \sum_{k=1}^{n} t^{n-h} b_{hk} x_k = \sum_{k=1}^{n} \mathcal{V}_k x_k,$$

where

$$\mathcal{V}_k = \sum_{h=1}^{n} t^{n-h} b_{hk}.$$
3. These expressions can be replaced by simpler ones. From the definition of $a_{hk}$ it is evident that

$$t^{h-1}a_{hk} = \begin{cases} 
\sum_{i=0}^{m-1} t^{km-i-1} & \text{if } km - h = nq + i, \ 0 \leq i \leq m - 1, \\
0 & \text{if } km - h = nq + i, \ m \leq i \leq n - 1.
\end{cases}$$

Therefore

$$u_h = \sum_{h=1}^{n} t^{h-1}a_{hk} = \sum_{i=0}^{m-1} t^{km-i-1} = t^{(k-1)m} \frac{1 - t^m}{1 - t},$$

whence

$$Y = \sum_{k=1}^{n} t^{(k-1)m} \frac{1 - t^m}{1 - t} x_k = \frac{1 - t^m}{1 - t} (x_1 + t^m x_2 + t^{2m} x_3 + \cdots + t^{(n-1)m} x_n).$$

On combining this formula with the definition of $Y$, we obtain the First Identity,

$$(1 - t)(y_1 + ty_2 + t^2y_3 + \cdots + t^{n-1}y_n) = (1 - t^m)(x_1 + t^m x_2 + t^{2m} x_3 + \cdots + t^{(n-1)m} x_n).$$

Similarly, by the definition of $b_{hk}$,

$$t^{n-h}b_{hk} = \begin{cases} 
\sum_{i=1}^{j} t^{km-i} & \text{if } km + h = nr + j, \ 1 \leq j \leq m, \\
0 & \text{if } km + h = nr + j, \ m + 1 \leq j \leq n.
\end{cases}$$

Thus now

$$v_k = \sum_{h=1}^{n} t^{n-h}b_{hk} = \sum_{j=1}^{m} t^{km-i} = t^{(k-1)m} \frac{1 - t^m}{1 - t},$$

hence

$$Z = \sum_{k=1}^{n} t^{(k-1)m} \frac{1 - t^m}{1 - t} x_k = \frac{1 - t^m}{1 - t} (x_1 + t^m x_2 + t^{2m} x_3 + \cdots + t^{(n-1)m} x_n),$$

and therefore, from the definition of $Z$,

$$(1 - t)(t^{n-1}z_1 + t^{n-2}z_2 + \cdots + tz_{n-1} + z_n) = (1 - t^m)(x_1 + t^m x_2 + t^{2m} x_3 + \cdots + t^{(n-1)m} x_n).$$

Here the left-hand side may also be written as
\[-t^n(1-t^{-1})(z_1 + t^{-1}z_2 + t^{-2}z_3 + \cdots + t^{-(n-1)}z_n)\].

Since \(t^n = s\), we obtain then the Second Identity,

\[-s(1-t^{-1})(z_1 + t^{-1}z_2 + t^{-2}z_3 + \cdots + t^{-(n-1)}z_n) = (1-t^m)(x_1 + t^m x_2 + t^{2m} x_3 + \cdots + t^{(n-1)m} x_n)\].

4. Denote by \(\tau\) an arbitrary parameter, by

\[\xi = (\xi_h)\]

an arbitrary \(n \times 1\) matrix (column vector), and put

\[\Phi(\xi | \tau) = (1 - \tau)(\xi_1 + \tau \xi_2 + \tau^2 \xi_3 + \cdots + \tau^{n-1} \xi_n)\].

In this notation, the two identities (1) and (2) take the simple form

\[\Phi(y | t) = \Phi(x | t^m)\]

and \(-s\Phi(z | t^{-1}) = \Phi(x | t^m)\), respectively. Here, for \(s \neq 0\), \(t\) may be any one of \(t_1, t_2, \ldots, t_n\).

**Lemma 1.** Let \(\sigma\) be distinct from 0 and 1, and let \(\tau_1, \tau_2, \ldots, \tau_n\) denote the \(n\) roots of the equation \(\tau^n = \sigma\). For any \(n\) given numbers \(\phi_1, \phi_2, \ldots, \phi_n\) there exists one and only one vector \(\xi\) such that

\[\Phi(\xi | \tau_h) = \phi_h \quad (h = 1, 2, \ldots, n)\].

**Proof.** The expression \(\Phi\) may also be written as

\[\Phi(\xi | \tau_h) = (\xi_1 - \sigma \xi_n) + \tau_h(\xi_2 - \xi_1) + \tau_h^2(\xi_3 - \xi_2) + \cdots + \tau_h^{n-1}(\xi_n - \xi_{n-1})\].

The hypothesis \(\sigma \neq 0\) implies that the \(n\) roots \(\tau_1, \tau_2, \ldots, \tau_n\) are all distinct, hence that the Vandermonde determinant

\[|\tau_h^{k-1}|_{h,k=1,2,\ldots,n}\]

does not vanish. The assertion is therefore proved if it can be shown that the \(n\) linear forms

\[\xi_1 - \sigma \xi_n, \quad \xi_2 - \xi_1, \quad \xi_3 - \xi_2, \ldots, \xi_n - \xi_{n-1}\]

in \(\xi_1, \xi_2, \ldots, \xi_n\) are linearly independent. However, the determinant of these forms evidently equals \(1 - \sigma\) and so, by \(\sigma \neq 1\), does not vanish, whence the assertion.

**Lemma 2.** Let \(s^m\), hence also \(s\) and \(s^{-1}\), be distinct from 0 and 1, and let \(t_1, t_2, \ldots, t_n\) be the roots of \(t^n = s\). The \(n\) equations

\[\Phi(y | t_h) = \Phi(x | t_h^m) \quad (h = 1, 2, \ldots, n)\]
define a nonsingular linear mapping of \( x \) on \( y \) and vice versa; and the \( n \) equations

\[
-s\Phi(z \mid l_h^{-1}) = \Phi(x \mid l_h^m) \quad (h = 1, 2, \ldots, n)
\]

similarly define a nonsingular linear mapping of \( x \) on \( z \) and vice versa.

**Proof.** The assertion is contained in Lemma 1 applied with \( \sigma = s \), \( \sigma = s^{-1} \), and \( \sigma = s^m \), respectively.

**Corollary.** If \( s^m \) is distinct from 0 and 1, then the two matrices \( A(m, n) \) and \( B(m, n) \) are both nonsingular.

5. From now on we impose the additional conditions that

\[
m \text{ is odd, and } s = -1.
\]

Hence \( t_1, t_2, \ldots, t_n \) now satisfy the equation

\[
t^n = -1.
\]

Thus, for odd \( n \), \( -t_1, -t_2, \ldots, -t_n \) are all the \( n \)th roots of unity, while, for even \( n \), \( t_1, t_2, \ldots, t_n \) are all those \( (2n) \)th roots of unity which are not also \( n \)th roots of unity. The equations (3) connecting \( x \) and \( y \) remain unchanged, but the equations (4) between \( x \) and \( z \) now become

\[
\Phi(z \mid l_h^{-1}) = \Phi(x \mid l_h^m) \quad (h = 1, 2, \ldots, n),
\]
or equivalent to this,

\[
\Phi(z \mid l_h) = \Phi(x \mid l_h^{-m}) \quad (h = 1, 2, \ldots, n).
\]

Since, by hypothesis, \( m \) is prime to \( n \), and further \( m \) is odd, it is obvious that both the \( m \)th powers

\[
l_1^m, l_2^m, \ldots, l_n^m,
\]

and the \((-m)\)th powers

\[
l_1^{-m}, l_2^{-m}, \ldots, l_n^{-m}
\]
of \( t_1, t_2, \ldots, t_n \) are again these same roots, only possibly arranged in a different order.

For, first, \( t^n = -1 \) implies that also \((t^m)^n = (t^{-m})^n = -1 \) because \( m \) is odd. Secondly, by \((m, n) = 1\), there exist integers \( M \) and \( N \) such that \( mM + nN = 1 \). Hence, if \( t^n = t'^n = -1 \) and \( t \neq t' \), then

\[
\left( \frac{t^m}{t'^m} \right)^M \left( \frac{t^n}{t'^n} \right)^N = \frac{t}{t'} \neq 1 \quad \text{and therefore } t^m \neq t'^m, t^{-m} \neq t'^{-m}.
\]
6. From now on we change the notation slightly and allow $m$ to be a positive or negative integer such that

$$(m, n) = 1, \quad 1 \leq |m| \leq n - 1, \quad m \text{ is odd.}$$

In extension of the previous notation we then put

$$A(m, n) = \begin{cases} A(m, n) & \text{if } m > 0, \\ B(-m, n) & \text{if } m < 0. \end{cases}$$

Therefore, in either case, the mapping

$$y = A(m, n)x$$

is equivalent to the system of $n$ formulae,

$$\Phi(y | t_h) = \Phi(x | t_h^m) \quad (h = 1, 2, \ldots, n).$$

Next, let $m'$ be a second integer satisfying the conditions (6); the case when $m' = m$ is not excluded. Further let

$$z = A(m', n)y$$

so that also

$$z = A(m', n)A(m, n)x.$$ 

The definition of $z$ implies that

$$\Phi(z | t_h) = \Phi(y | t_h^{m'}) \quad (h = 1, 2, \ldots, n).$$

Now, as we saw above, we can write

$$t_h^{m'} = t_{k(h)}$$

where

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ k(1) & k(2) & \cdots & k(n) \end{pmatrix}$$

is a certain permutation. Therefore

$$\Phi(z | t_h) = \Phi(y | t_h^{m'}) = \Phi(y | t_{k(h)}) = \Phi(x | t_{k(h)}^{m'})$$

and finally

$$\Phi(z | t_h) = \Phi(x | t_h^{m'm}) \quad (h = 1, 2, \ldots, n).$$

By the hypothesis, $mm'$ is odd and prime to $n$, hence also prime to $2n$. Hence there exists a unique integer $\mu$ such that
\[ \mu \equiv m'm \pmod{2n}, \quad 1 \leq |\mu| \leq n - 1 \]

and therefore also

\[ (\mu, n) = 1, \quad \mu \text{ is odd.} \]

The congruence for \( \mu \) implies in particular that

\[ t_h^m \equiv t_h^\mu \pmod{n} \quad (h = 1, 2, \ldots, n). \]

It follows then that

\[ \Phi(x \mid t_h) = \Phi(x \mid t_h^\mu) \quad (h = 1, 2, \ldots, n). \]

These equations show, however, that necessarily

\[ z = A(\mu, n)x \]

and we obtain the final result that

\[ A(m', n)A(m, n) = A(\mu, n). \]

The following theorem has thus been proved.

**Theorem.** The \( \phi(2n) \) matrices \( A(m, n) \), where

\[ (m, 2n) = 1, \quad 1 \leq |m| \leq n - 1, \]

form under multiplication an Abelian group which is isomorphic to the group of primitive residue classes \((\text{mod } 2n)\). The isomorphism is defined by

\[ A(m, n) \leftrightarrow \{m \pmod{2n}\}. \]

Manchester University, Manchester, England