# INVERSION OF TWO CYCLOTOMIC MATRICES 

Kurt Girstmair<br>Institut für Mathematik, Universität Innsbruck, Innsbruck, Austria<br>Kurt. Girstmair@uibk.ac.at

Received: 9/5/18, Accepted: 6/19/19, Published: 7/31/19


#### Abstract

Let $n \geq 3$ be a square-free natural number. We explicitly describe the inverses of the matrices $$
\left(2 \sin \left(2 \pi j k^{*} / n\right)\right)_{j, k} \quad \text { and } \quad\left(2 \cos \left(2 \pi j k^{*} / n\right)\right)_{j, k}
$$ where $k^{*}$ denotes a multiplicative inverse of $k \bmod n$ and $j, k$ run through the set $\{l ; 1 \leq l \leq n / 2,(l, n)=1\}$. These results are based on cyclotomy, in particular, on the theory of Gauss sums.


## 1. Introduction and Results

In the paper [3] Lehmer states that there are only few classes of matrices for which explicit formulas for the determinants, the eigenvalues and the inverses are known. He gives a number of examples of this kind. Further examples can be found in the papers [1], [4], [6] and [5]. All of these examples are based on number theory. The closest analogue of the matrices considered here is contained in the article [5], namely, the matrix

$$
(\sin (\pi j k / n))_{j, k}
$$

where $1 \leq j, k \leq n,(j k, n)=1$. The author of [5] determines the characteristic polynomial of this matrix, the respective eigenvalues being divisors of $n$ or equal to 0 . But the multiplicities of these eigenvalues are quite involved. In the present paper the eigenvalues of similar matrices $S$ and $C$ turn out to be Gauss sums belonging to Dirichlet characters mod $n$. The main results, however, are explicit formulas for the inverses $S^{-1}$ and $C^{-1}$ in the cases when these matrices are invertible. This is in contrast to the papers we have quoted, since explicit formulas for inverses are scarcely given there.

Let $n \geq 3$ be a natural number. Let $\mathcal{R}$ denote a system of representatives of the $\operatorname{group}(\mathbb{Z} / \mathbb{Z} n)^{\times} /\{ \pm 1\}$. Suppose that $\mathcal{R}$ is ordered in some way. Typically, $\mathcal{R}$ is the set $\{k ; 1 \leq k \leq n / 2,(k, n)=1\}$ with its natural order. For $k \in \mathbb{Z},(k, n)=1$, let $k^{*}$
denote a multiplicative inverse of $k \bmod \mathrm{n}\left(\operatorname{so} k k^{*} \equiv 1 \bmod n\right)$. We define

$$
s_{k}=2 \sin (2 \pi k / n) \quad \text { and } \quad c_{k}=2 \cos (2 \pi k / n)
$$

where $k \in \mathbb{Z},(k, n)=1$. We consider the matrices

$$
S=\left(s_{j k^{*}}\right)_{j, k \in \mathcal{R}} \quad \text { and } \quad C=\left(c_{j k^{*}}\right)_{j, k \in \mathcal{R}}
$$

which we call the sine matrix and the cosine matrix, respectively.
We think that the matrices $S$ and $C$ deserve some interest not only because of their simple structure but also by reason of their connection with cyclotomy, in particular, with Gauss sums (see [7] for the history of this topic).

In order to be able to enunciate our main results, we define

$$
\begin{equation*}
\lambda(k)=|\{q ; q \geq 3, q \mid n, k \equiv 1 \bmod q\}| \tag{1}
\end{equation*}
$$

for $k \in \mathbb{Z},(k, n)=1$. Furthermore, put

$$
\begin{equation*}
\widehat{s}_{k}=\frac{1}{n} \sum_{l \in \mathcal{R}}(\lambda(l k)-\lambda(-l k)) s_{l}, \tag{2}
\end{equation*}
$$

for $k \in \mathbb{Z},(k, n)=1$. For the same numbers $k$ put

$$
\begin{equation*}
\widehat{c}_{k}=\frac{1}{n} \sum_{l \in \mathcal{R}}\left(\lambda(l k)+\lambda(-l k)+\rho_{n}\right) c_{l} \tag{3}
\end{equation*}
$$

with

$$
\rho_{n}= \begin{cases}2, & \text { if } n \text { is odd }  \tag{4}\\ 4, & \text { if } n \text { is even }\end{cases}
$$

Our main results are as follows.
Theorem 1. The sine matrix $S$ is invertible if, and only if, $n$ is square-free or $n=4$. In this case

$$
S^{-1}=\left(\widehat{s}_{j k^{*}}\right)_{j, k \in \mathcal{R}}
$$

with $\widehat{s}_{j k^{*}}$ defined by (2).
Theorem 2. The cosine matrix $C$ is invertible if, and only if, $n$ is square-free. In this case

$$
C^{-1}=\left(\widehat{c}_{j k^{*}}\right)_{j, k \in \mathcal{R}}
$$

with $\widehat{c}_{j k^{*}}$ defined by (3).

Remark. If the sine matrix $S$ is invertible, then the numbers $s_{l}, l \in \mathcal{R}$, are $\mathbb{Q}$-linearly independent. This can be seen by application of Galois automorphisms of the $n$th cyclotomic field $\mathbb{Q}\left(\zeta_{n}\right)$ to a relation $\sum_{l \in \mathcal{R}} \lambda_{l} i s_{l}=0$ with $\lambda_{l} \in \mathbb{Q}$ and $i s_{l}=\zeta_{n}^{l}-\zeta_{n}^{-l}$.

Accordingly, the representation (2) of $\widehat{s}_{k}$ as a rational linear combination of the numbers $s_{l}, l \in \mathcal{R}$, is unique in this case. The same holds in the case of the cosine matrix and (3).

The entries of $S$ have the form $\pm s_{l}, l \in \mathcal{R}$. This is due to the fact that

$$
s_{j k^{*}}=\varepsilon s_{l}
$$

with $\varepsilon \in\{ \pm 1\}, l \in \mathcal{R}$, if $j k^{*} \equiv \varepsilon l \bmod n$. In the same way we have

$$
\widehat{s}_{j k^{*}}=\varepsilon \widehat{s}_{l}
$$

if $j k^{*} \equiv \varepsilon l \bmod n$. This means that it suffices to compute the numbers $\widehat{s}_{l}$ only for $l \in \mathcal{R}$ in order to write down the matrix $S^{-1}$. Indeed, this matrix arises from $S$ if we replace each entry $\varepsilon s_{l}$ of $S$ by the respective entry $\varepsilon \widehat{s}_{l}$.

The same procedure works in the case of the cosine matrix, whose entries have the form $c_{l}, l \in \mathcal{R}$.

Examples. 1. Let $n=15$ and $\mathcal{R}=\{1,2,4,7\}$. Then $S$ can be written

$$
S=\left(\begin{array}{rrrr}
s_{1} & -s_{7} & s_{4} & -s_{2}  \tag{5}\\
s_{2} & s_{1} & -s_{7} & -s_{4} \\
s_{4} & s_{2} & s_{1} & s_{7} \\
s_{7} & -s_{4} & -s_{2} & s_{1}
\end{array}\right)
$$

Theorem 1 yields $\widehat{s}_{1}=\left(3 s_{1}-s_{2}+s_{7}\right) / 15, \widehat{s}_{2}=\left(-s_{1}-s_{4}-3 s_{7}\right) / 15, \widehat{s}_{4}=\left(-s_{2}+\right.$ $\left.3 s_{4}+s_{7}\right) / 15$, and $\widehat{s}_{7}=\left(s_{1}-3 s_{2}+s_{4}\right) / 15$. We obtain $S^{-1}$ if we put a circumflex on each $s$ occurring in (5).
2. Let $n=35$ and $\mathcal{R}=\{1,2,3,4,6,8,9,11,12,13,16,17\}$. In the case of the cosine matrix we have
$\widehat{c}_{1}=\frac{1}{35}\left(5 c_{1}+2 c_{2}+2 c_{3}+3 c_{4}+4 c_{6}+3 c_{8}+3 c_{9}+3 c_{11}+2 c_{12}+3 c_{13}+3 c_{16}+2 c_{17}\right)$.
The remaining elements $\widehat{c}_{l}$ have the same coefficients in a permuted order.
Remark. If $n=p$ is a prime, Theorem 1 shows that $S^{-1}$ is particularly simple, namely, $S^{-1}=\frac{1}{p} S^{t}\left(S^{t}\right.$ is the transpose of $\left.S\right)$. There is no analogue for the cosine matrix. For instance, if $p=7$ and $\mathcal{R}=\{1,2,3\}$, we have $\widehat{c}_{1}=\left(3 c_{1}+2 c_{2}+2 c_{3}\right) / 7$. The prime number case of the sine matrix can also be settled by means of a simple trigonometric argument. This, however, seems to be hardly possible if $n$ consists of at least two prime factors $p>q \geq 3$.

## 2. Proofs

First we prove Theorem 1, then we indicate the changes required by the proof of Theorem 2. Let $\mathcal{X}$ denote the set of Dirichlet characters $\bmod n$, and $\mathcal{X}^{-}$and $\mathcal{X}^{+}$
the subsets of odd and even characters, respectively. The matrix $S$ is connected with $\mathcal{X}^{-}$, whereas $C$ is connected with $\mathcal{X}^{+}$. We note the orthogonality relation

$$
\sum_{\chi \in \mathcal{X}^{-}} \chi(k)= \begin{cases}0, & \text { if } k \not \equiv \pm 1 \bmod n  \tag{6}\\ \varphi(n) / 2, & \text { if } k \equiv 1 \bmod n \\ -\varphi(n) / 2, & \text { if } k \equiv-1 \bmod n\end{cases}
$$

see [2, p. 210]. Here $(k, n)=1$ and $\varphi$ denotes Euler's function.
Suppose that the set $\mathcal{X}^{-}$is ordered in some way. Then we can define the matrix

$$
X=\sqrt{n / \varphi(n)}(\chi(k))_{k \in \mathcal{R}, \chi \in \mathcal{X}^{-}}
$$

Since $|\mathcal{R}|=\left|\mathcal{X}^{-}\right|=\varphi(n) / 2, X$ is a square matrix. We note the following lemma.
Lemma 1. The matrix $X$ is unitary, i.e., $X^{-1}=\bar{X}^{t}$ (the transpose of the complexconjugate matrix).

Proof. This is an immediate consequence of the orthogonality relation (6) (observe that $\left.\bar{\chi}(k)=\chi\left(k^{*}\right)\right)$.

Let $\zeta_{n}=e^{2 \pi i / n}$ be the standard primitive $n$th root of unity. For $\chi \in \mathcal{X}^{-}$let

$$
\begin{equation*}
\tau(\chi)=\sum_{k=1}^{n} \chi(k) \zeta_{n}^{k} \tag{7}
\end{equation*}
$$

be the corresponding Gauss sum, see [2, p. 445]. We consider the diagonal matrix

$$
T=\operatorname{diag}(\tau(\bar{\chi}))_{\chi \in \mathcal{X}^{-}}
$$

Proposition 1. The sine matrix $S$ is normal. Indeed,

$$
\bar{X}^{t} S X=-i T
$$

Proof. We show $X T \bar{X}^{t}=i S$. Obviously, the entry $\left(X T \bar{X}^{t}\right)_{j, k}$ equals

$$
\frac{2}{\varphi(n)} \sum_{\chi \in \mathcal{X}^{-}} \chi(j) \tau(\bar{\chi}) \bar{\chi}(k)=\frac{2}{\varphi(n)} \sum_{\chi \in \mathcal{X}^{-}} \chi\left(j k^{*}\right) \sum_{(l, n)=1} \chi\left(l^{*}\right) \zeta_{n}^{l}
$$

where the index $l$ satisfies $1 \leq l \leq n,(l, n)=1$. This can be written

$$
\frac{2}{\varphi(n)} \sum_{(l, n)=1} \zeta_{n}^{l} \sum_{\chi \in \mathcal{X}^{-}} \chi\left(j k^{*} l^{*}\right)
$$

Now the orthogonality relation (6), together with $\zeta_{n}^{l}-\zeta_{n}^{-l}=i s_{l}$, shows that this is just $i s_{j k^{*}}$.

In order to study the vanishing of the eigenvalues of $S$, we use the reduction formula

$$
\begin{equation*}
\tau(\bar{\chi})=\mu\left(\frac{n}{f_{\chi}}\right) \bar{\chi}_{f}\left(\frac{n}{f_{\chi}}\right) \tau\left(\bar{\chi}_{f}\right) \tag{8}
\end{equation*}
$$

see [2, p. 448]. Here $\mu$ means the Möbius function, $f_{\chi}$ the conductor of the character $\chi, \chi_{f}$ the primitive character belonging to $\chi$ (which is a Dirichlet character mod $\left.f_{\chi}\right)$ and $\tau\left(\bar{\chi}_{f}\right)$ the Gauss sum

$$
\sum_{k=1}^{f_{\chi}} \bar{\chi}_{f}(k) \zeta_{f_{\chi}}^{k}
$$

Since

$$
\begin{equation*}
\tau\left(\chi_{f}\right) \tau\left(\bar{\chi}_{f}\right)=-f_{\chi} \tag{9}
\end{equation*}
$$

(see [2, p. 269]), formula (8) shows when the eigenvalue $-i \tau(\bar{\chi})$ vanishes. We obtain the following result.

Proposition 2. The matrix $S$ is invertible if, and only if, $n$ is square-free or $n=4$.
Proof. If $n$ is square-free, then $n / f_{\chi}$ is square-free and $\left(f_{\chi}, n / f_{\chi}\right)=1$. By (8) and (9), all Gauss sums $\tau(\chi)$ are different from 0 . If $n=4$ and $\chi \in \mathcal{X}^{-}$, then $f_{\chi}=4$ and $n / f_{\chi}=1$.

Conversely, suppose that $n$ is not square-free and different from 4. Then one of the following three cases occurs. There is a prime $p \geq 3$ such that $p^{2} \mid n$, or $4 p \mid n$, or $8 \mid n$. In the first and the second case there is a character $\chi \in \mathcal{X}^{-}$with $f_{\chi}=p$. Accordingly, $\chi_{f}\left(n / f_{\chi}\right)=0$ or $\mu\left(n / f_{\chi}\right)=0$. In the third case there is a character $\chi \in \mathcal{X}^{-}$with $f_{\chi}=4$. Therefore, $\chi_{f}\left(n / f_{\chi}\right)=0$.

Lemma 2. Let $n$ be square-free or equal to 4 . For $k \in \mathbb{Z},(k, n)=1$, we have

$$
\sum_{\chi \in \mathcal{X}^{-}} \frac{\chi(k)}{f_{\chi}}=\frac{\varphi(n)}{2 n}(\lambda(k)-\lambda(-k))
$$

the $\lambda$ 's being defined by (1).
Proof. Obviously,

$$
\sum_{\chi \in \mathcal{X}^{-}} \frac{\chi(k)}{f_{\chi}}=\sum_{d \mid n} \frac{1}{d} \sum_{\substack{\chi \in \mathcal{X}^{-} \\ f_{\chi}=d}} \chi(k)
$$

Möbius inversion gives

$$
\sum_{\substack{\chi \in \mathcal{X}^{-} \\ f_{\chi}=d}} \chi(k)=\sum_{q \mid d} \mu\left(\frac{d}{q}\right) \sum_{f_{\chi} \mid q} \chi(k) .
$$

Here we note that the characters $\chi \in \mathcal{X}^{-}$with $f_{\chi} \mid q$ are in one-to-one correspondence with the odd Dirichlet characters $\bmod q$. Indeed, if $\chi \in \mathcal{X}^{-}$, one defines the Dirichlet character $\chi_{q} \bmod q$ in the following way. If $(j, q)=1$, there is an integer $l$ with $(l, n)=1$ such that $l \equiv j \bmod q$. Then $\chi_{q}(j)=\chi(l)$; see $[2$, p. 217]. Accordingly,

$$
\sum_{f_{\chi} \mid q} \chi(k)=\sum_{\chi_{q}} \chi_{q}(k) .
$$

From (6) we obtain

$$
\sum_{\chi_{q}} \chi_{q}(k)= \begin{cases}0, & \text { if } q \leq 2 \text { or } q \geq 3 \text { and } k \not \equiv \pm 1 \bmod q  \tag{10}\\ \varphi(q) / 2, & \text { if } q \geq 3 \text { and } k \equiv 1 \bmod q \\ -\varphi(q) / 2, & \text { if } q \geq 3 \text { and } k \equiv-1 \bmod q\end{cases}
$$

(observe that there are no odd characters $\chi_{q}$ if $q \leq 2$ ). Therefore, we have

$$
\sum_{\substack{\chi \in \mathcal{X}^{-} \\ f_{\chi}=d}} \chi(k)=\sum_{\substack{q \mid d, q \geq 3 \\ k \equiv \pm 1 \\ \bmod q}} \pm \mu\left(\frac{d}{q}\right) \frac{\varphi(q)}{2}
$$

where the $\pm$ sign in the summand corresponds to the respective sign in the summation index. If we write $d=q \cdot r$, we have

$$
\sum_{\chi \in \mathcal{X}^{-}-} \frac{\chi(k)}{f_{\chi}}=\sum_{\substack{q \mid n, q \geq 3 \\ k \equiv \pm 1 \bmod q}} \pm \frac{\varphi(q)}{2} \sum_{r \left\lvert\, \frac{n}{q}\right.} \frac{\mu(r)}{q r}
$$

Since

$$
\sum_{r \left\lvert\, \frac{n}{q}\right.} \frac{\mu(r)}{r}=\prod_{p \left\lvert\, \frac{n}{q}\right.}\left(1-\frac{1}{p}\right)=\frac{\varphi(n / q)}{n / q}
$$

we obtain

$$
\begin{equation*}
\sum_{\chi \in \mathcal{X}^{-}} \frac{\chi(k)}{f_{\chi}}=\sum_{\substack{q \mid n, q \geq 3 \\ k \equiv \pm 1 \bmod q}} \pm \frac{\varphi(q)}{2 q} \cdot \frac{\varphi(n / q)}{n / q} \tag{11}
\end{equation*}
$$

However, $n$ is square-free or equal to 4 , and so $\varphi(q) \varphi(n / q)=\varphi(n)$. This implies

$$
\sum_{\chi \in \mathcal{X}_{-}} \frac{\chi(k)}{f_{\chi}}=\frac{\varphi(n)}{2 n}(\lambda(k)-\lambda(-k))
$$

Proof of Theorem 1. By Proposition 1, $S^{-1}=i X T^{-1} \bar{X}^{t}$, which means that the entry $\left(S^{-1}\right)_{j, k}, j, k \in \mathcal{R}$, of $S^{-1}$ is given by

$$
\left(S^{-1}\right)_{j, k}=\frac{2 i}{\varphi(n)} \sum_{\chi \in \mathcal{X}^{-}} \chi(j) \tau(\bar{\chi})^{-1} \bar{\chi}(k)
$$

From (8) and (9) we obtain

$$
\tau(\bar{\chi})^{-1}=\frac{\mu\left(n / f_{\chi}\right) \chi_{f}\left(n / f_{\chi}\right) \tau\left(\chi_{f}\right)}{-f_{\chi}}=-\frac{\tau(\chi)}{f_{\chi}}
$$

Therefore,

$$
\left(S^{-1}\right)_{j, k}=\frac{-2 i}{\varphi(n)} \sum_{\chi \in \mathcal{X}^{-}} \frac{\chi\left(j k^{*}\right)}{f_{\chi}} \tau(\chi)
$$

Now (7) yields

$$
\left(S^{-1}\right)_{j, k}=\frac{-2 i}{\varphi(n)} \sum_{(l, n)=1} \zeta_{n}^{l} \sum_{\chi \in \mathcal{X}^{-}} \frac{\chi\left(l j k^{*}\right)}{f_{\chi}}
$$

By Lemma 2,

$$
\left(S^{-1}\right)_{j, k}=\frac{-2 i}{\varphi(n)} \sum_{(l, n)=1} \zeta_{n}^{l} \frac{\varphi(n)}{2 n}\left(\lambda\left(l j k^{*}\right)-\lambda\left(-l j k^{*}\right)\right)
$$

Altogether, we have

$$
\left(S^{-1}\right)_{j, k}=\frac{-i}{n} \sum_{(l, n)=1} \zeta_{n}^{l}\left(\lambda\left(l j k^{*}\right)-\lambda\left(-l j k^{*}\right)\right)
$$

On observing that $s_{l}=-i\left(\zeta_{n}^{l}-\zeta_{n}^{-l}\right)$, we obtain Theorem 1 .

The setting of the proof of Theorem 2 is slightly different. Indeed, the unitary matrix $X$ is defined by

$$
X=\sqrt{n / \varphi(n)}(\chi(k))_{k \in \mathcal{R}, \chi \in \mathcal{X}^{+}} .
$$

The cosine matrix $C$ is normal, and $\bar{X}^{t} C X=T$, with $T=\operatorname{diag}(\tau(\bar{\chi}))_{\chi \in \mathcal{X}+}$. In this case it is easy to see that $T$ (and, hence, $C$ ) is invertible if, and only if, $n$ is square-free. Instead of (9) we have

$$
\tau\left(\chi_{f}\right) \tau\left(\bar{\chi}_{f}\right)=f_{\chi}
$$

The analogue of Lemma 2 reads

$$
\begin{equation*}
\sum_{\chi \in \mathcal{X}^{+}} \frac{\chi(k)}{f_{\chi}}=\frac{\varphi(n)}{2 n}\left(\lambda(k)+\lambda(-k)+\rho_{n}\right) \tag{12}
\end{equation*}
$$

with $\rho_{n}$ as in (4). This is due to the fact that the counterpart of formula (10) takes the form

$$
\sum_{\chi_{q}} \chi_{q}(k)= \begin{cases}1, & \text { if } q \leq 2 \\ 0, & \text { if } q \geq 3 \text { and } k \not \equiv \pm 1 \bmod q \\ \varphi(q) / 2, & \text { if } q \geq 3 \text { and } k \equiv \pm 1 \bmod q\end{cases}
$$

Accordingly, formula (11) has the equivalent

$$
\sum_{\chi \in \mathcal{X}+} \frac{\chi(k)}{f_{\chi}}=\sum_{\substack{q \mid n, q \geq 3 \\ k \equiv \pm 1}} \frac{\varphi(q)}{2 q} \cdot \frac{\varphi(n / q)}{n / q}+\sum_{\substack{d \mid n \\ 2 \nmid d}} \frac{\mu(d)}{d}
$$

which gives (12). Up to these differences, the proof follows the pattern of the proof of Theorem 1.

## References

[1] L. Carlitz, Some cyclotomic matrices, Acta Arith. 5 (1959), 293-308.
[2] H. Hasse, Vorlesungen über Zahlentheorie (2nd ed.), Springer, Berlin 1964.
[3] D. H. Lehmer, On certain character matrices, Pacific J. Math. 6 (1956), 491-499.
[4] D. H. Lehmer, Power character matrices, Pacific J. Math. 10 (1960), 895-907.
[5] G. Molteni, About two trigonometric matrices, Linear Algebra Appl. 382 (2004), 39-59.
[6] P. Morton, On the eigenvectors of Schur's matrix, J. Number Theory 12 (1980), 122-127.
[7] A. Weil, La cyclotomie jadis et naguère, Séminaire Bourbaki 1973-74, exp. nr. 452, 318-338.

