Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Linear Algebra and its Applications 382 (2004) 39–59
LINEAR ALGEBRA AND ITS APPLICATIONS
www.elsevier.com/locate/laa

About two trigonometric matrices

G. Molteni

Dipartimento di Matematica, Università di Milano, Via Saldini 50, I-20133 Milano, Italy

Received 17 March 2003; accepted in revised form 2 December 2003

Submitted by V. Mehrmann

Abstract

Let r, s be coprime integers, $s > 1$ and odd. The characteristic polynomials of the matrices

$$\left[\sin\left(\frac{rmn\pi}{s}\right)\right]_{0<m,n<s} \quad \text{and} \quad \left[\sin\left(\frac{rmn\pi}{s}\right)\right]_{\substack{0<m,n<s\\(mn,s)=1}}$$

are determined.

AMS classification: 15A18; 11A99

Keywords: Trigonometric matrices; Dirichlet characters

1. Notations

The symbol $\delta_{\text{something}}$ assumes the value 1 when *something* holds, 0 otherwise. For $m, n, s \in \mathbb{N}$, (m, n) is the greatest common divisor of m, n; $m|n$ means that m divides n; $m \equiv n(s)$ and $m = n \bmod (s)$ mean that $s|(m-n)$; n is said *squarefree* when $p^2 \nmid n$ for every prime p; $\binom{m}{n}$ is the Jacobi symbol, i.e., the completely multiplicative extension of the quadratic character for odd m, n; μ is the Möbius function, i.e., the multiplicative function such that $\mu(p) = -1$ and $\mu(p^h) = 0$ when $h > 1$, for every prime p; ϕ is the Euler function, i.e., the multiplicative function such that $\phi(p^h) = p^{h-1}(p-1)$ for every power of prime p^h; $\psi := \mu * \phi$ is the Dirichlet convolution of μ and ϕ, i.e., $\psi(n) = \sum_{d|n} \mu(n/d)\phi(d)$. By the definition of μ, $\mu(s) \neq 0$, $|\mu(s)| = 1$ and s squarefree are three equivalent events. Moreover, $\sum_{d|s} \mu(d) = \delta_{s=1}$ and $\sum_{d|s} \psi(d) = \phi(s)$ for every s. At last, we denote by $\lfloor x \rfloor$, $\operatorname{Re} x$ and $\operatorname{Im} x$ the integer, the real and the imaginary part of x, respectively.

E-mail address: giuseppe.molteni@mat.unimi.it (G. Molteni).

0024-3795/$ - see front matter © 2004 Published by Elsevier Inc.
doi:10.1016/j.laa.2003.12.016

2. Introduction and motivations

Schur introduced the matrix

$$\Phi := \left[\exp\left(\frac{2\pi \mathrm{i} mn}{s}\right)\right]_{0\leqslant m,n<s},$$

where s is a positive integer. Since $\Phi^4 = s^2\mathbb{I}$, the eigenvalues are the numbers $\mathrm{i}^\nu\sqrt{s}$ for $0 \leqslant \nu \leqslant 3$. Schur has determined the multiplicity of every eigenvalue and used such result to evaluate the Gaussian sum $\sum_{n=1}^{s} \mathrm{e}^{2\pi \mathrm{i} n^2/s}$ which is the trace of Φ (see [12]). Moreover, such matrix represents the discrete Fourier transform on s points, therefore it is extensively studied in Approximation Theory and Numerical Analysis. In particular, there exists a broad literature about its eigenvalues and eigenvectors (see [2,4,7,9,10]).

In this paper we study the four matrices

$$M_{r,s} := \sqrt{2}\left[\sin\left(\frac{rmn\pi}{s}\right)\right]_{0<m,n<s}, \quad M_{2r,s} := \left[\sin\left(\frac{2rmn\pi}{s}\right)\right]_{0<m,n<s},$$

$$M'_{r,s} := \sqrt{2}\left[\sin\left(\frac{rmn\pi}{s}\right)\right]_{\substack{0<m,n<s\\(mn,s)=1}}, \quad M'_{2r,s} := \left[\sin\left(\frac{2rmn\pi}{s}\right)\right]_{\substack{0<m,n<s\\(mn,s)=1}},$$

where r, s are odd integers with $(r, s) = 1$ and $s > 1$. In particular we found their eigenvalues, multiplicity included. Since these matrices are symmetric, also their characteristic polynomials are determined. The normalizating factor $\sqrt{2}$ in the definition of $M_{r,s}$ and $M'_{r,s}$ is introduced by convenience. Moreover, note that $M_{2(r+s),s} = M_{2r,s}$ and $M'_{2(r+s),s} = M'_{2r,s}$, hence the fact that r is odd is not a true restriction but only a convenient assumption simplifying the proof of the results.

Matrices $M_{\cdot,s}$ and $M'_{\cdot,s}$ are evidently related to Φ, but only $M_{r,s}$, satisfying the identity $M_{r,s}^2 = s\mathbb{I}$, has a behavior like that one of Φ. The following examples show that the structure of the characteristic polynomial of the other matrices is strongly influenced by the arithmetical properties of the parameters r and s: in all cases the eigenvalues are 0 and $\pm\sqrt{d}$ where d is a divisor of s but for non-squarefree s not every divisor appears and the rule selecting the eigenvalues and their multiplicity is not evident.

$$\begin{aligned}
&\det(x\mathbb{I} - M_{2,7}) = x^3(x^2 - 7)(x - \sqrt{7})\\
&\det(x\mathbb{I} - M_{6,7}) = x^3(x^2 - 7)(x + \sqrt{7})\\
&\det(x\mathbb{I} - M_{2,15}) = x^7(x^2 - 15)^3(x - \sqrt{15})\\
&\det(x\mathbb{I} - M_{14,15}) = x^7(x^2 - 15)^3(x + \sqrt{15}),
\end{aligned}$$

$$\begin{aligned}
&\det(x\mathbb{I} - M'_{2,7}) = x^3(x^2 - 7)(x - \sqrt{7})\\
&\det(x\mathbb{I} - M'_{6,7}) = x^3(x^2 - 7)(x + \sqrt{7})\\
&\det(x\mathbb{I} - M'_{2,15}) = x^4(x - \sqrt{3})(x^2 - 5)(x - \sqrt{15})\\
&\det(x\mathbb{I} - M'_{14,15}) = x^4(x - \sqrt{3})(x^2 - 5)(x + \sqrt{15}),
\end{aligned}$$

s	$\det(x\mathbb{I} - M'_{1,s})$
$3\cdot 5$	$(x^2-3)(x^2-5)^2(x^2-3\cdot 5)$
$5\cdot 11$	$(x^2-5)^2(x^2-11)^5(x^2-5\cdot 11)^{13}$
5^2	$x^4(x^2-5^2)^8$
5^3	$x^{20}(x^2-5^3)^{40}$
7^2	$x^6(x^2-7^2)^{18}$
7^3	$x^{42}(x^2-7^3)^{126}$
11^2	$x^{20}(x^2-11^2)^{50}$
11^3	$x^{110}(x^2-11^3)^{550}$
$3^2\cdot 5$	$x^8(x^2-3^2)^2(x^2-3^2\cdot 5)^6$
$3^3\cdot 5$	$x^{24}(x^2-3^3)^6(x^2-3^3\cdot 5)^{18}$
$3\cdot 5^2$	$x^8(x^2-5^2)^8(x^2-3\cdot 5^2)^8$
$3^2\cdot 5^2$	$x^{56}(x^2-3^2\cdot 5^2)^{32}$
$3^3\cdot 5^2$	$x^{168}(x^2-3^3\cdot 5^2)^{96}$
$3^2\cdot 7$	$x^{12}(x^2-3^2)^2(x^2-3^2\cdot 7)^{10}$
$3^3\cdot 7$	$x^{36}(x^2-3^3)^6(x^2-3^3\cdot 7)^{30}$
$3\cdot 7^2$	$x^{12}(x^2-7^2)^{18}(x^2-3\cdot 7^2)^{18}$
$3^2\cdot 7^2$	$x^{108}(x^2-3^2\cdot 7^2)^{72}$
$3^2\cdot 5\cdot 7$	$x^{48}(x^2-3^2)^2(x^2-3^2\cdot 5)^6(x^2-3^2\cdot 7)^{10}(x^2-3^2\cdot 5\cdot 7)^{30}$

In Section 3 we will provide some non-trivial preparatory results belonging to the Number Theory, in Section 4 we will prove Theorem 7 giving the characteristic polynomials of the matrices $M_{\cdot,s}$, in Section 5 we will prove Theorems 8 and 9 giving the characteristic polynomials of the matrices $M'_{\cdot,s}$. Some interesting corollaries are there proved, too.

Our approach to this problem is the following. A direct search of the eigenvectors of $M_{\cdot,s}$ ($M'_{\cdot,s}$) appears difficult, but the matrix $M^2_{\cdot,s}$ ($M'^2_{\cdot,s}$) have integer entries and the search of its eigenvalues seems to be an easier problem. Actually, we find a base of eigenvectors of $M^2_{\cdot,s}$ ($M'^2_{\cdot,s}$). It is interesting to remark here that such eigenvectors are given in terms of the values of suitable characters modulo s, in a similar (but much more involuted) way to that one employed by Morton [10] to describe a base of eigenvectors of Φ. Every eigenvalue d of $M^2_{\cdot,s}$ ($M'^2_{\cdot,s}$) produces a pair of eigenvalues $\pm\sqrt{d}$ for $M_{\cdot,s}$ ($M'_{\cdot,s}$) whose multiplicities $m_{d,\pm}$ can be determined by the fact that $\sum_{d \text{ eigenvalue}}(m_{d,+} - m_{d,-})\sqrt{d} = \operatorname{Tr} M_{\cdot,s}$ ($\operatorname{Tr} M'_{\cdot,s}$). In fact, the trace of $M_{\cdot,s}$ ($M'_{\cdot,s}$) can be directly calculated and the numbers $\sqrt{d}$ appearing in this formula are $\mathbb{Q}$-linear independent so that we can find $m_{d,+} - m_{d,-}$ for every d. Then, since $m_{d,+} + m_{d,-}$ is the known multiplicity of d as eigenvalue of $M^2_{\cdot,s}$ ($M'^2_{\cdot,s}$), the values of each $m_{d,\pm}$ is found.

At last, a word about the origin of our interest for these matrices. Let m, s be integers, $s > 1$, s odd and $0 < m < s$. For every $a \in \mathbb{N}$, let

$$H^a_{m,s} := \sum_{n=1}^{\infty} \frac{r_{m,s}(n)}{n^{2a+1}}, \quad \text{where } r_{m,s}(n) := \begin{cases} 1 & \text{if } n = m \bmod (2s), \\ -1 & \text{if } n = -m \bmod (2s), \\ 0 & \text{otherwise.} \end{cases}$$

(The series converges conditionally also when $a = 0$.) We are looking for a formula giving the value of $H^a_{m,s}$.

The referee pointed to our attention the fact that $m^{2a+1} H^a_{m,s} = \sigma_{2a}(m/2s)$ where

$$\sigma_k(z) := \sum_{\nu=-\infty}^{\infty} \left(\frac{z}{\nu + z} \right)^{k+1}$$

has been defined and extensively studied by Ehlich [5] (see also [6]). In particular, the connection of $\sigma_k(z)$ with the Bernoulli polynomials is known. Our approach is different. Let

$$F_a(x) := \sum_{n=1}^{\infty} \frac{(-1)^n}{(n\pi)^{2a+1}} \sin(n\pi x),$$

uniformly convergent on every compact subset of $(-1, 1)$, for every $a \in \mathbb{N}$. A comparison with the known Fourier expansion of the Bernoulli polynomials $B_k(x)$ (see [13, Chapter 1.0]) shows that for $x \in (-1, 1)$

$$F_a(x) = \frac{(-4)^a}{(2a+1)!} B_{2a+1}\left(\frac{1-x}{2} \right). \tag{1}$$

Since the Bernoulli polynomials can be easily recovered by the identity

$$\sum_{k=0}^{\infty} \frac{B_k(x)}{k!} y^k = \frac{y e^{xy}}{e^y - 1},$$

the values of F_a can be easily calculated. The relevance of F_a in this context comes from the fact that from the definition of $H^a_{m,s}$ we have

$$\sum_{m=1}^{s-1} (-1)^m H^a_{m,s} \sin\left(\frac{mn\pi}{s} \right) = \pi^{2a+1} F_a\left(\frac{n}{s} \right) \quad \text{for every } n \in \mathbb{Z}, \tag{2}$$

so that by taking $0 < n < s$, we recover a set of $s-1$ linear equations for the $s-1$ numbers $H^a_{m,s}$, with $0 < m < s$.

A second identity can be deduced noting that $H^a_{dm,ds} = d^{-2a-1} H^a_{m,s}$ for every integer d, so that from (2) we have

$$\sum_{d|s} \sum_{\substack{m=1 \\ \left(m, \frac{s}{d}\right)=1}}^{s/d} \frac{(-1)^m}{d^{2a+1}} H^a_{m,\frac{s}{d}} \sin\left(\frac{mn\pi}{s/d} \right) = \pi^{2a+1} F_a\left(\frac{n}{s} \right) \quad \forall n \in \mathbb{Z},$$

that by the Möbius inversion formula (see [13, Chapter I.2, Theorem 8]) gives

$$\sum_{\substack{m=1\\(m,s)=1}}^{s} (-1)^m H^a_{m,s} \sin\left(\frac{mn\pi}{s}\right)$$
$$= \pi^{2a+1} \sum_{d|s} \mu\left(\frac{s}{d}\right)\left(\frac{d}{s}\right)^{2a+1} F_a\left(\frac{n}{d}\right) \quad \forall n \in \mathbb{Z}. \tag{3}$$

Considering this identity for $0 < n < s$, n coprime with s, we get a set of $\phi(s)$ linear equations where only the $\phi(s)$ numbers $H^a_{m,s}$ with $(m, s) = 1$ appear.

At last, we can generalize the previous equations by substituting n by rn in (2) and (3), where r is a fixed integer coprime with s and n runs in $0 < n < s$ (n coprime with s for (3).)

Identities (2) or (3) allow us to recover $H^a_{m,s}$ as linear combination of values of F_a but only if the matrices $M_{r,s}$ and $M'_{r,s}$, respectively, are invertible. For computational purposes we are also interested to find an efficient algorithm for the inverse matrix so that not only the invertibility of those matrices but also the structure of their characteristic polynomials has to be studied.

Actually, using the identity $M^2_{1,s} = s\mathbb{I}$, from (2) we get the formula we are looking for

$$H^a_{m,s} = (-1)^m \frac{2\pi^{2a+1}}{s} \sum_{n=1}^{s-1} F_a\left(\frac{n}{s}\right) \sin\left(\frac{mn\pi}{s}\right) \quad \text{for } 0 < m < s. \tag{4}$$

Now that the constants $H^a_{m,s}$ have been calculated, we can use them to provide a new proof of the known formula for the values of the Dirichlet L-functions (for the definition see [3]). In fact, let χ be a Dirichlet *odd* character modulo $2s$ and let $L(\cdot, \chi)$ be the corresponding Dirichlet L-function, then

$$L(2a+1, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^{2a+1}} = \sum_{m=1}^{s} \chi(m) H^a_{m,s} \tag{5}$$

so that substituting (4) in (5) we get (note that $\chi(m) = 0$ if m is even)

$$L(2a+1, \chi) = -\frac{2\pi^{2a+1}}{s} \sum_{n=1}^{s-1} F_a\left(\frac{n}{s}\right) \sum_{m=1}^{s} \chi(m) \sin\left(\frac{mn\pi}{s}\right).$$

Let χ^* be the character mod s inducing χ and suppose χ^* to be primitive, then a long and a slightly tricky computation proves the identity

$$2\mathrm{i}\bar{\chi}^*(2) \sum_{m=1}^{s} \chi(m) \sin\left(\frac{mn\pi}{s}\right) = (-1)^n \bar{\chi}^*(n)\tau(\chi^*),$$

where $\tau(\chi^*)$ is the Gaussian sum, so that from the previous formula we deduce

$$L(2a+1, \chi) = \chi^*(2) \frac{\pi^{2a+1}\mathrm{i}\tau(\chi^*)}{s} \sum_{n=1}^{s-1} (-1)^n \bar{\chi}^*(n) F_a\left(\frac{n}{s}\right).$$

Substituting (1) in this equation we obtain a formula giving $L(2a+1,\chi)$ in terms of the generalized Bernoulli numbers. Such formula is not new (see for example Theorem 4.2 of [14]), but we think that our non-standard deduction is of some interest.

We conclude this section noting that by the orthogonality of the Dirichlet characters modulo $2s$ we can represent $H^a_{m,s}$ as a finite sum of the values of Dirichlet L-functions, i.e.,

$$H^a_{m,s} = \frac{2}{\phi(s)} \sum_{\substack{\chi \bmod 2s \\ \chi \text{ odd}}} \bar{\chi}(m) L(2a+1,\chi),$$

therefore to determinate $H^a_{m,s}$ and to determinate the values of $L(\cdot,\chi)$ at odd integers are equivalent problems.

3. Tools from Number Theory

Proposition 1. *Let $s>1$ be odd and $D|s$. Let*

$$\kappa(D,s) := \sum_{d:\, \substack{d|s \\ D|d}} \mu\left(\frac{s}{d}\right) \frac{\phi(s)}{\phi(d)}\, d.$$

Then

$$\kappa(D,s) = D \left|\mu\left(\frac{s}{D}\right)\right| \delta_{(D,s/D)=1}.$$

Proof. We remark that $\kappa(1,s)$ is the Dirichlet convolution of multiplicative functions of s, therefore it is multiplicative, too. As a consequence, in order to get the claim when $D=1$ it is sufficient to verify that $\kappa(1,p^h) = |\mu(p^h)|$ for every power of prime p^h. In fact,

$$\begin{aligned}\kappa(1,p^h) &= \sum_{d|p^h} \mu\left(\frac{p^h}{d}\right) \frac{\phi(p^h)}{\phi(d)}\, d \\ &= \frac{\phi(p^h)}{\phi(p^h)}\, p^h - \frac{\phi(p^h)}{\phi(p^{h-1})}\, p^{h-1} = \begin{cases} 1 & \text{if } h=1 \\ 0 & \text{if } h>1 \end{cases}\end{aligned}$$

which is the claim.

For $D \neq 1$, $\kappa(D,s)$ is not multiplicative and a different approach is necessary. We note that $D|s$ so that it is possible to find α, α', β and γ such that

$$D = \alpha\beta, \quad s = \alpha'\beta\gamma,$$

with

$$(\alpha,\beta) = (\alpha,\gamma) = (\beta,\gamma) = 1, \quad \alpha|\alpha' \quad \text{and} \quad p|\alpha \Longleftrightarrow p|\alpha'.$$

As a consequence, every d dividing s and divided by D can be written as

$$d = A\beta S, \quad \text{where } \alpha|A,\ A|\alpha' \text{ and } S|\gamma.$$

By this decomposition we have

$$\begin{aligned}\kappa(D,s) &= \sum_{A:\,\substack{A|\alpha'\\ \alpha|A}} \sum_{S|\gamma} \mu\left(\frac{\alpha'\beta\gamma}{A\beta S}\right) \frac{\phi(\alpha'\beta\gamma)}{\phi(A\beta S)} A\beta S \\ &= \sum_{A:\,\substack{A|\alpha'\\ \alpha|A}} \sum_{S|\gamma} \mu\left(\frac{\alpha'}{A}\right) \mu\left(\frac{\gamma}{S}\right) \frac{\phi(\alpha')}{\phi(A)} \frac{\phi(\gamma)}{\phi(S)} A\beta S \\ &= \beta \sum_{A:\,\substack{A|\alpha'\\ \alpha|A}} \mu\left(\frac{\alpha'}{A}\right) \frac{\phi(\alpha')}{\phi(A)} A \sum_{S|\gamma} \mu\left(\frac{\gamma}{S}\right) \frac{\phi(\gamma)}{\phi(S)} S \\ &= \beta\kappa(1,\gamma) \sum_{A:\,\substack{A|\alpha'\\ \alpha|A}} \mu\left(\frac{\alpha'}{A}\right) \frac{\phi(\alpha')}{\phi(A)} A \\ &= \beta|\mu(\gamma)| \sum_{A:\,\substack{A|\alpha'\\ \alpha|A}} \mu\left(\frac{\alpha'}{A}\right) \frac{\phi(\alpha')}{\phi(A)} A.\end{aligned}$$

We note that $\frac{\phi(\alpha')}{\phi(A)} A = \alpha'$, since the hypotheses imply that $p|A \iff p|\alpha \iff p|\alpha'$, hence we get

$$\begin{aligned}\kappa(D,s) &= \alpha'\beta|\mu(\gamma)| \sum_{A:\,\substack{A|\alpha'\\ \alpha|A}} \mu\left(\frac{\alpha'}{A}\right) \\ &= \alpha'\beta|\mu(\gamma)| \sum_{A|\alpha'/\alpha} \mu(A) = \alpha'\beta|\mu(\gamma)|\delta_{\alpha'=\alpha}.\end{aligned}$$

The proof concludes noting that $\alpha = \alpha'$ if and only if $(D, s/D) = 1$. $\square$

Proposition 2. *Let k, n be coprime odd integers. Then*

$$G(k,n) := \sum_{l=1}^{n} \mathrm{e}^{2\pi \mathrm{i} \frac{kl^2}{n}} = \binom{k}{n}\sqrt{n^*}. \tag{6}$$

In this formula $\binom{k}{n}$ is the Jacobi symbol, $n^* = n$ if $n = 1 \bmod (4)$ and $n^* = -n$ if $n = -1 \bmod (4)$ and $\sqrt{-n} = \mathrm{i}\sqrt{n}$ where i is the same square root of -1 occurring in the definition of $G(k, n)$.

This important result is due to Gauss and its original proof is reproduced in Rademacher [11]. A different proof due to Dirichlet is reproduced in Davenport [3], other proofs can be found in [1]. Actually, the papers we consulted show in a detailed way the proof of (6) only in the case of $G(1, n)$, the validity of the general case $G(k, n)$ being claimed without any particular comment. We think that this passage deserves more attention, therefore we show here how (6) follows from the particular cases which are well documented in literature, i.e., those ones of $G(1,n)$ and $G(k,p)$, where n is an odd integer, p is an odd prime and k is an odd integer coprime with p.

Proof. The proof is by induction on the number of different primes dividing n. Suppose $n=p^u$. When $u=1$, $G(k,p)$ is the simplest Gaussian sum and the claim is well known (see [8, Proposition 8.2.1]). Suppose $u>1$. It is evident that $G(kr^2,p^u)=G(k,p^u)$ for every r which is coprime with p, therefore there exists S, *independent of* k, such that

$$G(k,p^u)=\begin{cases} G(1,p^u) & \text{if } k \text{ is a square mod } (p^u),\\ S & \text{if } k \text{ is not a square mod } (p^u).\end{cases}$$

The value of S can be determined by summing $G(k,p^u)$ over k: we have

$$\frac{\phi(p^u)}{2}(G(1,p^u)+S)=\sum_{\substack{k=1\\ p\nmid k}}^{p^u} G(k,p^u)=\sum_{k=1}^{p^u}\sum_{l=1}^{p^u} \mathrm{e}^{2\pi \mathrm{i}\frac{kl^2}{p^u}}-\sum_{k=1}^{p^{u-1}}\sum_{l=1}^{p^u} \mathrm{e}^{2\pi \mathrm{i}\frac{kl^2}{p^{u-1}}},$$

changing the order of summation we get

$$\begin{aligned}\frac{\phi(p^u)}{2}(G(1,p^u)+S)&=p^u\sum_{l=1}^{p^u}\delta_{p^u|l^2}-p^{u-1}\sum_{l=1}^{p^u}\delta_{p^{u-1}|l^2}\\ &=p^u p^{u-\left\lfloor\frac{u+1}{2}\right\rfloor}-p^{u-1}p^{u-\left\lfloor\frac{u}{2}\right\rfloor}=p^{u-1}p^{\frac{u}{2}}(p-1)\delta_{2|u}.\end{aligned}$$

Since $G(1,p^u)=\sqrt{(p^u)^*}$ (see [3]), we get

$$S=2p^{\frac{u}{2}}\delta_{2|u}-\sqrt{(p^u)^*}. \tag{7}$$

Let k be a non-square residue mod (p^u). If u is even then $(p^u)^*=p^u$ and $\left(\frac{k}{p^u}\right)=1$ so that by (7) $S=p^{\frac{u}{2}}=\left(\frac{k}{p^u}\right)\sqrt{(p^u)^*}$. If u is odd we have $\left(\frac{k}{p^u}\right)=\left(\frac{k}{p}\right)=-1$, so that by (7) again $S=-\sqrt{(p^u)^*}=\left(\frac{k}{p^u}\right)\sqrt{(p^u)^*}$, completing the proof of (6) when n is a power of a prime.

To complete the induction it is sufficient to remark that for every coprime m,n the isomorphism $\mathbb{Z}/mn\mathbb{Z}\approx\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ gives

$$\begin{aligned}G(k,mn)&=\sum_{l=1}^{mn}\mathrm{e}^{2\pi\mathrm{i}\frac{kl^2}{mn}}=\sum_{u=1}^{m}\sum_{v=1}^{n}\mathrm{e}^{2\pi\mathrm{i}\frac{k(un+vm)^2}{mn}}\\ &=\sum_{u=1}^{m}\sum_{v=1}^{n}\mathrm{e}^{2\pi\mathrm{i}\left(\frac{knu^2}{m}+\frac{kmv^2}{n}\right)}=G(km,n)G(kn,m),\end{aligned} \tag{8}$$

and that

$$\frac{\sqrt{m^*}\sqrt{n^*}}{\sqrt{(mn)^*}} = (-1)^{\frac{(m-1)(n-1)}{4}} = \binom{m}{n}\binom{n}{m} \tag{9}$$

by the quadratic reciprocity law (see [8, Chapter 5]). Using (8), (9) and the inductive hypothesis, in fact, we conclude that for $(k, np^u) = (n, p^u) = 1$,

$$\begin{aligned} G(k, np^u) &= G(kp^u, n)G(kn, p^u) = \binom{kp^u}{n}\binom{kn}{p^u}\sqrt{n^*}\sqrt{(p^u)^*} \\ &= \binom{k}{np^u}\binom{p^u}{n}\binom{n}{p^u}\sqrt{n^*}\sqrt{(p^u)^*} = \binom{k}{np^u}\sqrt{(np^u)^*}. \qquad \square \end{aligned}$$

Proposition 3. *Let k, n be coprime odd integers. Let*

$$R(k, n) := \sum_{\substack{l=1 \\ (l,n)=1}}^{n} \mathrm{e}^{2\pi\mathrm{i}\frac{kl^2}{n}}.$$

Then

$$R(k, n) = \begin{cases} \prod_{p|n} \left(\binom{kn/p}{p}\sqrt{p^*} - 1\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right)\binom{kn/d}{d}\sqrt{d^*} & \text{if } n \text{ is squarefree}, \\ 0 & \text{otherwise}, \end{cases}$$

where p runs on primes dividing n.

Proof. Firstly, let p be and odd prime, then by Proposition 2 we get

$$R(k, p^u) = \begin{cases} \binom{k}{p}\sqrt{p^*} - 1 & \text{if } u = 1, \\ 0 & \text{otherwise.} \end{cases}$$

In fact this is immediate for $u = 1$ and for $u \geqslant 2$ we have

$$\begin{aligned} R(k, p^u) &= \sum_{l=1}^{p^u} \mathrm{e}^{2\pi\mathrm{i}\frac{kl^2}{p^u}} - \sum_{l=1}^{p^{u-1}} \mathrm{e}^{2\pi\mathrm{i}\frac{kp^2l^2}{p^u}} = \sum_{l=1}^{p^u} \mathrm{e}^{2\pi\mathrm{i}\frac{kl^2}{p^u}} - p\sum_{l=1}^{p^{u-2}} \mathrm{e}^{2\pi\mathrm{i}\frac{kl^2}{p^{u-2}}} \\ &= G(k, p^u) - pG(k, p^{u-2}) = \binom{k}{p^u}\sqrt{(p^u)^*} - p\binom{k}{p^{u-2}}\sqrt{(p^{u-2})^*} \\ &= 0. \end{aligned}$$

To complete the proof it is sufficient to remark that for every coprime m, n the isomorphism $(\mathbb{Z}/mn\mathbb{Z})^* \approx (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ gives

$$\begin{aligned} R(k, mn) &= \sum_{\substack{l=1 \\ (l,mn)=1}}^{mn} \mathrm{e}^{2\pi\mathrm{i}\frac{kl^2}{mn}} = \sum_{\substack{u=1 \\ (u,m)=1}}^{m} \sum_{\substack{v=1 \\ (v,n)=1}}^{n} \mathrm{e}^{2\pi\mathrm{i}\frac{k(un+vm)^2}{mn}} \\ &= \sum_{\substack{u=1 \\ (u,m)=1}}^{m} \sum_{\substack{v=1 \\ (v,n)=1}}^{n} \mathrm{e}^{2\pi\mathrm{i}\left(\frac{knu^2}{m} + \frac{kmv^2}{n}\right)} = R(km, n)R(kn, m), \end{aligned}$$

so that the claim follows by induction over the number of different primes dividing n as for Proposition 2. □

The following proposition gives the value of the trace of $M'_{\cdot,s}$.

Proposition 4. *Let* r, s *be coprime odd integers*, $s > 1$. *Then* $\operatorname{Tr} M'_{r,s} = 0$ *and*

$$\operatorname{Tr} M'_{2r,s} = |\mu(s)| \sum_{\substack{d|s \\ d\equiv 3\ (4)}} \mu\left(\frac{s}{d}\right)\binom{ls/d}{d}\sqrt{d}.$$

Proof. The claim about $\operatorname{Tr} M'_{r,s}$ is quite immediate. In fact,

$$\operatorname{Tr} M'_{r,s} = \sqrt{2}\sum_{\substack{l=1 \\ (l,s)=1}}^{s} \sin\left(\frac{rl^2\pi}{s}\right),$$

but

$$\sin\left(\frac{r(s-l)^2\pi}{s}\right) = \sin\left(rs\pi - 2rl\pi + \frac{rl^2\pi}{s}\right) = -\sin\left(\frac{rl^2\pi}{s}\right),$$

so that adding this identity for $l = 1, \ldots, s$, with $(l, s) = 1$ we get $\operatorname{Tr} M'_{r,s} = -\operatorname{Tr} M'_{r,s}$. The claim about $\operatorname{Tr} M'_{2r,s}$ follows by Proposition 3, since $\operatorname{Tr} M'_{2r,s} = \operatorname{Im} R(r, s)$. □

For every integer D let V_D be the $\mathbb{C}$-vector space which is generated by the *primitive* characters modulo D. Moreover, let $E_D \subseteq V_D$ and $O_D \subseteq V_D$ be the subspaces which are generated by even and odd characters, respectively. The following proposition gives the dimensions of O_D and E_D.

Proposition 5. *Let* $D > 1$ *be odd. Then*

$$\dim O_D = \tfrac{1}{2}(\psi(D) - \mu(D)), \quad \dim E_D = \tfrac{1}{2}(\psi(D) + \mu(D)).$$

Proof. For every $d|D$ there are $\phi(d)$ characters modulo D which are induced by some character modulo d, therefore by the inclusion-exclusion principle the number of primitive characters modulo D is $\sum_{d|D}\mu(d)\phi(\frac{D}{d}) = \psi(D)$. We prove the claim by induction over the number of different primes dividing D. Suppose $D = p^h$ for some odd prime p. Let g be a generator of the cyclic group $(\mathbb{Z}/D\mathbb{Z})^*$. Every character modulo D is known when its value at g is known, therefore $\{\chi_l\}_{l=0}^{\phi(D)-1}$ where $\chi_l(g) = \mathrm{e}^{2\pi i l/\phi(D)}$ is a complete set of the characters. Moreover, χ_l is primitive if and only if $p\nmid l$ and it is an even character if and only if l is even, so that there are $(\psi(D) - \mu(D))/2$ characters in O_D. The $\mathbb{C}$-linear independence of distinct characters is known, hence the proof of the claim when $D = p^h$ is complete. Suppose now $D = mn$ for some odd and coprime integers m, n. Let χ and η be characters of V_m

and V_n, respectively. Then $\chi\eta$ is a primitive character modulo mn, i.e., an element of V_D. It is easy to verify the linear independence of the characters which are generated in this way. In fact, suppose $\sum_{\chi,\eta} a_{\chi,\eta}(\chi\eta)(r) = 0$ for every r, where χ runs on V_m and η on V_n. Take a generic $r = um + vn$ so that

$$\sum_{\eta}\left(\sum_{\chi} a_{\chi,\eta}\chi(vn)\right)\eta(um) = 0 \quad \forall u, v.$$

By hypothesis $(m, n) = 1$ and the characters modulo n are $\mathbb{C}$-linear independent, therefore the previous identity implies

$$\sum_{\chi} a_{\chi,\eta}\chi(vn) = 0 \quad \forall v, \eta.$$

Using again the $\mathbb{C}$-linear independence of the characters modulo m we get

$$a_{\chi,\eta} = 0 \quad \forall\chi, \eta.$$

Evidently $\chi \in O_m, \eta \in O_n$ or $\chi \in E_m, \eta \in E_n$ imply $\chi\eta \in E_D$ while $\chi \in E_m, \eta \in O_n$ or $\chi \in O_m, \eta \in E_n$ imply $\chi\eta \in O_D$, therefore, from the previous argument and the inductive hypothesis we have

$$\begin{aligned}\dim O_D &\geqslant \dim E_m \dim O_n + \dim E_n \dim O_m \\ &= \tfrac{1}{4}\big((\psi(m) + \mu(m))(\psi(n) - \mu(n)) \\ &\quad + (\psi(n) + \mu(n))(\psi(m) - \mu(m))\big) \\ &= \tfrac{1}{2}(\psi(D) - \mu(D)).\end{aligned}$$

Similarly

$$\begin{aligned}\dim E_D &\geqslant \dim E_m \dim E_n + \dim O_m \dim O_n \\ &= \tfrac{1}{4}\big((\psi(m) + \mu(m))(\psi(n) + \mu(n)) \\ &\quad + (\psi(m) - \mu(m))(\psi(n) - \mu(n))\big) \\ &= \tfrac{1}{2}(\psi(D) + \mu(D)).\end{aligned}$$

Therefore

$$\begin{aligned}\psi(D) &= \dim V_D = \dim O_D + \dim E_D \\ &\geqslant \tfrac{1}{2}(\psi(D) - \mu(D)) + \tfrac{1}{2}(\psi(D) + \mu(D)) = \psi(D),\end{aligned}$$

so that the equalities $\dim O_D = \frac{1}{2}(\psi(D) - \mu(D))$, $\dim E_D = \frac{1}{2}(\psi(D) + \mu(D))$ follow. $\square$

Remark 6. The previous proposition proves that for every pair of coprime odd integers m, n we have the isomorphisms

$$O_{mn} \simeq (E_m \otimes O_n) \oplus (O_m \otimes E_n), \quad E_{mn} \simeq (E_m \otimes E_n) \oplus (O_m \otimes O_n).$$

4. Eigenvalues of $M_{\cdot,s}$

Theorem 7. *The characteristic polynomials of the matrices* $M_{\cdot,s}$ *are*

$$\det(x\mathbb{I} - M_{r,s}) = \left(x^2 - s\right)^{\frac{s-1}{2}},$$

and

$$\det(x\mathbb{I} - M_{2r,s}) = x^{\frac{s-1}{2}}(x - \sqrt{s})^{m_+}(x + \sqrt{s})^{m_-},$$

where

$$\begin{cases} m_+ + m_- = \frac{s-1}{2}, \\ m_+ - m_- = \binom{r}{s}\delta_{s\equiv 3\ (4)}. \end{cases}$$

Proof. *The first claim.* We already remarked that $M_{r,s}^2 = s\mathbb{I}$, therefore $x^2 - s$ is the minimal polynomial of $M_{r,s}$ and its characteristic polynomial must be

$$\det(x\mathbb{I} - M_{r,s}) = (x - \sqrt{s})^{m_+}(x + \sqrt{s})^{m_-} \tag{10}$$

for some $m_+, m_- \geqslant 1$ with $m_+ + m_- = s - 1$. Let us consider the trace of $M_{r,s}$. From (10) we get

$$\begin{aligned}(m_+ - m_-)\sqrt{s} = \mathrm{Tr}(M_{r,s}) &= \sqrt{2}\sum_{n=1}^{s-1}\sin\left(\frac{rn^2\pi}{s}\right) \\ &= \sqrt{2}\sum_{n=1}^{(s-1)/2}\left(\sin\left(\frac{rn^2\pi}{s}\right) + \sin\left(\frac{r(s-n)^2\pi}{s}\right)\right) \\ &= \sqrt{2}\sum_{n=1}^{(s-1)/2}\left(\sin\left(\frac{rn^2\pi}{s}\right) - \sin\left(\frac{rn^2\pi}{s}\right)\right) = 0,\end{aligned}$$

hence $m_+ = m_-$ and the claim follows.

The second claim. An explicit computation shows that $(M_{2r,s}^2)_{n,m} = \frac{s}{2}(\delta_{n=m} - \delta_{n=s-m})$ so that by induction on s it is possible to prove that the characteristic polynomial of $M_{2r,s}$ is

$$\det\left(x\mathbb{I} - M_{2r,s}^2\right) = x^{(s-1)/2}(x - s)^{(s-1)/2}.$$

As a consequence the characteristic polynomial of $M_{2r,s}$ must be

$$\det(x\mathbb{I} - M_{2r,s}) = x^{(s-1)/2}(x - \sqrt{s})^{m_+}(x + \sqrt{s})^{m_-}$$

for some m_+, m_- with $m_+ + m_- = (s - 1)/2$. Let us consider the trace of $M_{2r,s}$. By Proposition 2 we get

$$\begin{aligned}(m_+ - m_-)\sqrt{s} = \mathrm{Tr}(M_{2r,s}) &= \sum_{n=1}^{s-1}\sin\left(\frac{2rn^2\pi}{s}\right) \\ &= \mathrm{Im}\, G(r, s) = \binom{r}{s}\sqrt{s}\ \delta_{s\equiv 3\ (4)}\end{aligned}$$

and the claim is proved. □

5. Eigenvalues of $M'_{\cdot,s}$

Theorem 8. *The characteristic polynomial of* $M'_{r,s}$ *is*

$$\det(x\mathbb{I} - M'_{r,s}) = x^{d_0} \prod_{\substack{d|s \\ (d,s/d)=1 \\ \mu(s/d)\neq 0}} (x^2 - d)^{(\psi(d)-\mu(d))/2},$$

with

$$d_0 := \phi(s) - \sum_{\substack{d|s \\ (d,s/d)=1 \\ \mu(s/d)\neq 0}} (\psi(d) - \mu(d)).$$

Analogously,

Theorem 9. *The characteristic polynomial of* $M'_{2r,s}$ *is*

$$\det(x\mathbb{I} - M'_{2r,s}) = x^{d_0} \prod_{\substack{d|s \\ (d,s/d)=1 \\ \mu(s/d)\neq 0}} (x - \sqrt{d})^{m_{d,+}} (x + \sqrt{d})^{m_{d,-}},$$

where $d_0 := \phi(s) - \frac{1}{2} \sum_{\substack{d|s \\ (d,s/d)=1 \\ \mu(s/d)\neq 0}} (\psi(d) - \mu(d))$ *and* $m_{d,\pm}$ *are the solutions of*

$$\begin{cases} m_{d,+} + m_{d,-} = \frac{1}{2}(\psi(d) - \mu(d)) \\ m_{d,+} - m_{d,-} = c_{r,s,d} \end{cases} \tag{11}$$

with

$$c_{r,s,d} = \begin{cases} \mu\left(\frac{s}{d}\right)\left(\frac{rs/d}{d}\right) & \text{if } s \text{ is squarefree}, d \equiv 3\ (4), \\ 0 & \text{otherwise}. \end{cases}$$

Remark 10. Since $\psi(1) - \mu(1) = 0$, 1 is never eigenvalue of $M'_{\cdot,s}$.

Remark 11. Using the multiplicativity of the function ψ it is easy to verify that when n is odd

$$\psi(n) - \mu(n) = \mu(n)(n-1) \bmod (4).$$

This fact shows that a "correction" term $c_{r,s,d}$ is necessary in order to (11) has integer solutions.

Remark 12. When s is an *odd* prime $M_{\cdot,s} = M'_{\cdot,s}$, therefore the conclusions of Theorems 8 and 9 have to accord to Theorem 7, as a simple check shows.

At last, we come back to the original problem of the invertibility of matrices $M_{\cdot,s}$ and $M'_{\cdot,s}$. Theorem 7 and the following corollary of Theorems 8 and 9 show that only

$M_{r,s}$ is invertible for every s and that (3) can be used to recover $H^a_{m,s}$ only when s is squarefree.

Corollary 13. $\det(M'_{2r,s}) = 0$ *and*

$$\det(M'_{r,s}) = \begin{cases} 0 & \text{if } s \text{ is not squarefree} \\ (-s)^{\frac{1}{2}(s-1)} & \text{if } s \text{ is prime} \\ \prod_{p|s} p^{\frac{1}{2}(p-2)\phi(s/p)} & \text{if } s \text{ is squarefree and not prime}, \end{cases}$$

where p runs on primes dividing s.

Proof. In Theorem 9 the exponent d_0 is always positive, hence $M'_{2r,s}$ is not invertible.

By Theorem 8 $\det M'_{r,s} \neq 0$ if and only if s is squarefree. In the last case, remembering that for every integer n, $\sum_{d|n} \mu(d) = \delta_{n=1}$ and $\sum_{d|n} \psi(d) = \phi(n)$, we get

$$\begin{aligned}\det(M'_{r,s}) &= \prod_{d|s} (-d)^{\frac{1}{2}(\psi(d)-\mu(d))} \\ &= (-1)^{\frac{1}{2}\sum_{d|s}(\psi(d)-\mu(d))} \prod_{p|s} p^{\frac{1}{2}\sum_{d|s/p}(\psi(pd)-\mu(pd))} \\ &= (-1)^{\frac{\phi(s)}{2}} \prod_{p|s} p^{\frac{1}{2}(\psi(p)\sum_{d|s/p}\psi(d)-\mu(p)\sum_{d|s/p}\mu(d))} \\ &= (-1)^{\frac{\phi(s)}{2}} \prod_{p|s} p^{\frac{1}{2}(\psi(p)\phi(s/p)-\mu(p)\delta_{s=p})}. \qquad \square\end{aligned}$$

We come now to the proof of Theorems 8 and 9. As first step we compute the matrix $M'^2_{\cdot,s}$.

Proposition 14. *Let r, s be coprime odd integers, $s > 1$. For every pair m, n coprime with s, $0 < m, n < s$, let $(M'^2_{\cdot,s})_{m,n}$ be the mth, nth entry of the matrix $M'^2_{\cdot,s}$, then*

$$\begin{aligned}\left(M'^2_{r,s}\right)_{m,n} = \sum_{d|s} \mu\left(\frac{s}{d}\right) \Big(& d\left(\delta_{m\equiv n(2d)} - \delta_{m\equiv -n(2d)}\right) \\ & + \delta_{m\not\equiv n(2)}\left(\delta_{m\not\equiv n(2d)} - \delta_{m\not\equiv -n(2d)}\right)\Big),\end{aligned}$$

$$\left(M'^2_{2r,s}\right)_{m,n} = \sum_{d|s} \mu\left(\frac{s}{d}\right) \frac{d}{2}\left(\delta_{m\equiv n(d)} - \delta_{m\equiv -n(d)}\right),$$

both independent of r.

Proof. Since for all integers l, s,

$$\delta_{(l,s)=1} = \sum_{d|(l,s)} \mu(d) = \sum_{d|s} \mu(d)\delta_{d|l},$$

for every function f we have

$$\sum_{\substack{l=1\\(l,s)=1}}^{s} f\left(\frac{l}{s}\right) = \sum_{l=1}^{s} \delta_{(l,s)=1} f\left(\frac{l}{s}\right) = \sum_{l=1}^{s}\sum_{d|s} \mu(d)\delta_{d|l} f\left(\frac{l}{s}\right)$$

$$= \sum_{d|s} \mu(d) \sum_{l=1}^{s} \delta_{d|l} f\left(\frac{l}{s}\right) = \sum_{d|s} \mu(d) \sum_{l=1}^{s/d} f\left(\frac{l}{s/d}\right),$$

so that changing $d \leftrightarrow s/d$ we obtain

$$\sum_{\substack{l=1\\(l,s)=1}}^{s} f\left(\frac{l}{s}\right) = \sum_{d|s} \mu(s/d) \sum_{l=1}^{d} f\left(\frac{l}{d}\right).$$

Using this identity we have

$$\begin{aligned}\left(M'^2_{r,s}\right)_{m,n} &= 2 \sum_{\substack{l=1\\(l,s)=1}}^{s} \sin\left(\frac{lrm\pi}{s}\right)\sin\left(\frac{lrn\pi}{s}\right)\\ &= \sum_{d|s} \mu(s/d) \sum_{l=1}^{d} \left(2\sin\left(\frac{lrm\pi}{d}\right)\sin\left(\frac{lrn\pi}{d}\right)\right)\\ &= \sum_{d|s} \mu(s/d) \sum_{l=0}^{d-1} \left(\cos\left(\frac{lr(m-n)\pi}{d}\right) - \cos\left(\frac{lr(m+n)\pi}{d}\right)\right)\\ &= \sum_{d|s} \mu(s/d) \sum_{l=0}^{d-1} \mathrm{Re}\left(\mathrm{e}^{\frac{lr(m-n)\pi\mathrm{i}}{d}} - \mathrm{e}^{\frac{lr(m+n)\pi\mathrm{i}}{d}}\right).\end{aligned}$$

The proof of the first claim is completed noting that for every $k, d \in \mathbb{N}$,

$$2d|k \Rightarrow \sum_{l=0}^{d-1} \mathrm{Re}\left(\mathrm{e}^{\frac{lk\pi\mathrm{i}}{d}}\right) = d,$$

$$2d\nmid k \Rightarrow \sum_{l=0}^{d-1} \mathrm{Re}\left(\mathrm{e}^{\frac{lk\pi\mathrm{i}}{d}}\right) = \mathrm{Re}\left(\frac{\mathrm{e}^{k\pi\mathrm{i}}-1}{\mathrm{e}^{\frac{k\pi i}{d}}-1}\right) = \mathrm{Re}\left(\frac{(-1)^k-1}{\mathrm{e}^{\frac{k\pi i}{2d}} - \mathrm{e}^{\frac{-k\pi\mathrm{i}}{2d}}}\,\mathrm{e}^{-\frac{k\pi\mathrm{i}}{2d}}\right)$$

$$= \mathrm{Re}\left(\frac{(-1)^k-1}{2\mathrm{i}\sin\frac{k\pi}{2d}}\,\mathrm{e}^{-\frac{k\pi\mathrm{i}}{2d}}\right) = \frac{1-(-1)^k}{2} = \delta_{k\equiv 1\ (2)}.$$

The second claim can be proved in a similar way. □

The proofs of the theorems are essentially equivalent but some important technical differences appear, hence we complete them separately.

5.1. Proof of Theorem 8

By Proposition 14 the entry $(M'^2_{r,s})_{m,n}$ is zero when $m \not\equiv n(2)$. As a consequence, there exists a permutation J such that

$$JM'^2_{r,s}J^{-1} = \begin{pmatrix} N_s & 0 \\ 0 & N_s \end{pmatrix}, \tag{12}$$

where N_s is a matrix of order $\frac{1}{2}\phi(s) \times \frac{1}{2}\phi(s)$ whose entries are

$$(N_s)_{m,n} := \sum_{d|s} \mu\left(\frac{s}{d}\right) d(\delta_{m\equiv n(d)} - \delta_{m\equiv -n(d)})$$
$$\text{with } 1 \leqslant m, n \leqslant s, \quad (mn, 2s) = 1.$$

Proposition 15. *Let $s > 1$ be an odd integer, let $D|s$ and let $f \in O_D$. Let v^f be the vector of $\mathbb{C}^{\phi(s)/2}$ whose entries are v^f_m with $(m, 2s) = 1$, $1 \leqslant m \leqslant s$, and whose value is $v^f_m = f(m)$. Then v^f is an eigenvector of N_s with eigenvalue $\kappa(D, s)$.*

Proof. It is sufficient to prove the claim when $f = \chi$, where χ is an odd primitive character modulo D. We have

$$\begin{aligned}\sum_n (N_s)_{m,n} v^\chi_n &= \sum_{\substack{n=1\\(n,2s)=1}}^{s} \sum_{d|s} \mu\left(\frac{s}{d}\right) d(\delta_{n\equiv m\ (d)} - \delta_{n\equiv -m\ (d)}) v^\chi_n \\ &= \sum_{d|s} \mu\left(\frac{s}{d}\right) d \sum_{\substack{n=1\\(n,2s)=1}}^{s} (\delta_{n\equiv m\ (d)} - \delta_{n\equiv -m\ (d)}) v^\chi_n \\ &= \sum_{d|s} \mu\left(\frac{s}{d}\right) d \left(\sum_{\substack{n=1\\(n,2s)=1\\n\equiv m\ (d)}}^{s} v^\chi_n - \sum_{\substack{n=1\\(n,2s)=1\\n\equiv -m\ (d)}}^{s} v^\chi_n \right) \\ &= \sum_{d|s} \mu\left(\frac{s}{d}\right) d \sum_{\substack{n=-s\\(n,2s)=1\\n\equiv m\ (d)}}^{s} \chi(n) = \sum_{d|s} \mu\left(\frac{s}{d}\right) d \sum_{\substack{n=1\\(n,s)=1\\n\equiv m\ (d)}}^{s} \chi(n).\end{aligned} \tag{13}$$

The restriction $n = m \bmod (d)$ can be eliminated using the orthogonality of the characters modulo d, i.e., the identity $\sum_{\eta \bmod d} \bar{\eta}(m)\eta(n) = \phi(d)\delta_{n\equiv m\ (d)}$, obtaining

$$\sum_n (N_s)_{m,n} v^\chi_n = \sum_{d|s} \mu\left(\frac{s}{d}\right) \frac{d}{\phi(d)} \sum_{\eta \bmod d} \bar{\eta}(m) \sum_{n=1}^{s} \widetilde{\chi\eta}(n),$$

where $\widetilde{\chi\eta}$ is the character modulo s which is induced by the character $\chi\eta$ (which is a character modulo l.c.m.(d, D).) The inner sum $\sum_{n=1}^{s} \widetilde{\chi\eta}(n)$ is not zero (and its value is $\phi(s)$) if and only if $D|d$ and η is induced by $\bar{\chi}$, since χ is primitive. Therefore,

$$\sum_n (N_s)_{m,n} v_n^{\chi} = \sum_{d:\, \substack{d|s \\ D|d}} \mu\left(\frac{s}{d}\right) \frac{d\phi(s)}{\phi(d)} \chi(m) = \kappa(D, s) v_m^{\chi}. \qquad \square$$

From Propositions 1 and 15 we get the following characterization of the eigenspaces of N_s.

Proposition 16. *Let T_d be the d-eigenspace of N_s. Then* $\dim T_d$ *is*

$$\begin{cases} \frac{1}{2}(\psi(d) - \mu(d)) & \textit{for } d \in \mathbb{N},\, d|s,\ |\mu(s/d)| = 1 \textit{ and } (d, s/d) = 1, \\ \frac{1}{2} \sum\limits_{\substack{d|s \\ \mu(s/d)=0 \\ (d,s/d)=1}} (\psi(d) - \mu(d)) + \frac{1}{2} \sum\limits_{\substack{d|s \\ (d,s/d)>1}} (\psi(d) - \mu(d)) & \textit{for } d = 0, \\ 0 & \textit{otherwise}. \end{cases}$$

In particular, $\ker N_s = \{0\}$ *if and only if s is squarefree*.

Proof. Evidently the vectors generated in Proposition 15 by different O_d spaces are linearly independent, therefore from Proposition 1 we get the lower-bounds

$$\dim T_0 = \dim \ker N_s \geqslant \sum_{\substack{d|s \\ \mu(s/d)=0 \\ (d,s/d)=1}} \dim O_d + \sum_{\substack{d|s \\ (d,s/d)>1}} \dim O_d,$$

and

$$\dim T_d \geqslant \dim O_d \quad \text{when } d|s,\ |\mu(s/d)| = 1,\ (d, s/d) = 1.$$

Adding these inequalities and using Proposition 5 we get

$$\begin{aligned} \frac{1}{2}\phi(s) &\geqslant \dim \ker N_s + \sum_{\substack{d|s \\ |\mu(s/d)|=1 \\ (d,s/d)=1}} \dim O_d \\ &\geqslant \sum_{\substack{d|s \\ \mu(s/d)=0 \\ (d,s/d)=1}} \dim O_d + \sum_{\substack{d|s \\ (d,s/d)>1}} \dim O_d + \sum_{\substack{d|s \\ |\mu(s/d)|=1 \\ (d,s/d)=1}} \dim O_d \\ &= \sum_{d|s} \dim O_d = \frac{1}{2} \sum_{d|s} (\psi(d) - \mu(d)) = \frac{1}{2}\phi(s). \end{aligned}$$

This inequality proves that there are no other eigenvalues and that the dimension of every eigenspace is that one stated in the claim. $\square$

A simple argument concludes the proof of the theorem. In fact, by (12) and the previous proposition we get that the eigenvalues of $M'^2_{r,s}$ are 0 and the integers d dividing s such that s/d is squarefree and coprime with d, with multiplicities d_0 (whose value is defined in the statement of the theorem) and $\psi(d) - \mu(d)$, respectively. It is important to recall that $d = 1$ is not an eigenvalue: its multiplicity is $\psi(1) - \mu(1) = 0$. As a consequence, the eigenvalues of $M'_{r,s}$ are 0 and $\pm\sqrt{d}$, where d is chosen as before. Let m_0 be the multiplicity of 0 and let $m_{d,+}$ and $m_{d,-}$ be those ones of $\sqrt{d}$ and $-\sqrt{d}$, respectively. From Proposition 16 (and (12)) we have $m_{+,d} + m_{d,-} = \psi(d) - \mu(d)$, so that

$$m_0 = \phi(s) - \sum_{\substack{d|s \\ (d,s/d)=1 \\ |\mu(s/d)|=1 \\ d>1}} (m_{+,d} + m_{d,-}) = \phi(s) - \sum_{\substack{d|s \\ (d,s/d)=1 \\ |\mu(s/d)|=1 \\ d>1}} (\psi(d) - \mu(d)) = d_0.$$

Moreover, from Proposition 4 we get

$$0 = \mathrm{Tr}(M'_{r,s}) = \sum_{\substack{d|s \\ (d,s/d)=1 \\ |\mu(s/d)|=1 \\ d>1}} (m_{d,+} - m_{d,-})\sqrt{d}. \tag{14}$$

Let us consider the integers d appearing in this equation. There is only one d which is a square, at most, and this fact happens if and only if s is not squarefree. For every other d appearing in (14) it is possible to find a prime p_d such that $p_d|d$ with odd order and $p_d\nmid d'$ if $d' \neq d$. As a consequence the numbers $\sqrt{d}$ are linearly $\mathbb{Q}$-independent so that (14) implies $m_{d,+} = m_{d,-}$. Since we know that $m_{d,+} + m_{d,-} = \psi(d) - \mu(d)$, we conclude that $m_{d,+} = m_{d,-} = \frac{1}{2}(\psi(d) - \mu(d))$ and the proof of Theorem 8 is completed.

5.2. *Proof of Theorem 9*

Proposition 17. *Let $s > 1$ be an odd integer let $D|s$ and let $f \in V_D$. Let v^f be the vector of $\mathbb{C}^{\phi(s)}$ whose entries are v^f_m with $(m, s) = 1$, $1 \leqslant m \leqslant s$ and whose value is $v^f_m = f(m)$. When $f \in E_D$, $v^f \in \ker M'^2_{2r,s}$ and when $f \in O_D$ then v^f belongs to the eigenspace of $M'^2_{2r,s}$ with eigenvalue $\kappa(D, s)$.*

Proof. It is sufficient to prove the claim when $f = \chi$, where χ is a primitive character modulo D. We have

$$\begin{aligned}\sum_n (M'^2_{2r,s})_{m,n} v^\chi_n &= \sum_{\substack{n=1 \\ (n,s)=1}}^{s} \sum_{d|s} \mu\left(\frac{s}{d}\right) \frac{d}{2} \left(\delta_{n\equiv m\ (d)} - \delta_{n\equiv -m\ (d)}\right) v^\chi_n \\ &= \sum_{d|s} \mu\left(\frac{s}{d}\right) \frac{d}{2} \sum_{\substack{n=1 \\ (n,s)=1}}^{s} \left(\delta_{n\equiv m\ (d)} - \delta_{n\equiv -m\ (d)}\right) v^\chi_n\end{aligned}$$

$$= \sum_{d|s} \mu\left(\frac{s}{d}\right) \frac{d}{2} \left(\sum_{\substack{n=1 \\ (n,s)=1 \\ n \equiv m\ (d)}}^{s} v_n^{\chi} - \sum_{\substack{n=1 \\ (n,s)=1 \\ n \equiv -m\ (d)}}^{s} v_n^{\chi} \right).$$

The inner sum is zero when χ is even, but for odd χ we get

$$\sum_n (M'^2_{2r,s})_{m,n} v_n^{\chi} = \sum_{d|s} \mu\left(\frac{s}{d}\right) d \sum_{\substack{n=1 \\ (n,s)=1 \\ n \equiv m\ (d)}}^{s} \chi(n)$$

which is the same term appearing in (13): the proof is completed by the same argument used there. □

From Propositions 1 and 17 we get the following characterization of the eigenspaces of $M'^2_{2r,s}$.

Proposition 18. *Let S_d be the d-eigenspace of $M'^2_{2r,s}$. Then* $\dim S_d$ *is*

$$\begin{cases} \frac{1}{2}(\psi(d) - \mu(d)) & \text{for } d \in \mathbb{N}, d|s, \\ & |\mu(s/d)| = 1 \\ & \text{and } (d, s/d) = 1, \\ \frac{\phi(s)}{2} + \frac{1}{2} \sum\limits_{\substack{d|s \\ \mu(s/d)=0 \\ (d,s/d)=1}} (\psi(d) - \mu(d)) + \frac{1}{2} \sum\limits_{\substack{d|s \\ (d,s/d)>1}} (\psi(d) - \mu(d)) & \text{for } d = 0, \\ 0 & \text{otherwise}. \end{cases}$$

In particular, $\dim\ker M'^2_{2r,s} \geqslant \phi(s)/2$, *with* $\dim\ker M'^2_{2r,s} = \phi(s)/2$ *if and only if s is squarefree.*

Proof. Evidently the vectors generated in Proposition 17 by different O_d and E_d spaces are linearly independent, therefore from Propositions 1 and 17 we get the lower-bounds

$$\dim S_0 = \dim\ker M'^2_{2r,s} \geqslant \sum_{d|s} \dim E_d + \sum_{\substack{d|s \\ \mu(s/d)=0 \\ (d,s/d)=1}} \dim O_d + \sum_{\substack{d|s \\ (d,s/d)>1}} \dim O_d,$$

and

$$\dim S_d \geqslant \dim O_d \quad \text{when } d|s, |\mu(s/d)| = 1, (d, s/d) = 1.$$

Adding these inequalities and using Proposition 5 we get

$$\phi(s) \geqslant \dim S_0 + \sum_{\substack{d|s \\ |\mu(s/d)|=1 \\ (d,s/d)=1}} \dim S_d \geqslant \frac{\phi(s)}{2} + \frac{1}{2} \sum_{d|s} (\psi(d) - \mu(d)) = \phi(s),$$

therefore there are no other eigenvalues and the dimension of every eigenspace is that one which is stated in the claim. □

Now we conclude the proof. The previous proposition shows that the eigenvalues of $M'^2_{2r,s}$ are 0 and the integers d dividing s such that s/d is squarefree and coprime with d, with multiplicities d_0 (the constant which is defined in Theorem 9) and $\psi(d)-\mu(d)$, respectively (note that $d=1$ is not an eigenvalue: its multiplicity is $\psi(1)-\mu(1)=0$.) As a consequence, the eigenvalues of $M'^2_{2r,s}$ are 0 and $\pm\sqrt{d}$, where d is chosen as before. Let m_0 be the multiplicity of 0 and let $m_{d,+}$ and $m_{d,-}$ be those ones of $\sqrt{d}$ and $-\sqrt{d}$, respectively. From Proposition 18 we have $m_{d,+}+m_{d,-}=(\psi(d)-\mu(d))/2$, so that

$$m_0=\phi(s)-\sum_{\substack{d|s\\(d,s/d)=1\\|\mu(s/d)|=1\\d>1}}(m_{+,d}+m_{d,-})=\phi(s)-\frac{1}{2}\sum_{\substack{d|s\\(d,s/d)=1\\|\mu(s/d)|=1\\d>1}}(\psi(d)-\mu(d))=d_0.$$

Moreover, from Proposition 4 we get

$$0=\mathrm{Tr}(M'_{r,s})-\mathrm{Tr}(M'_{r,s})=\sum_{\substack{d|s\\(d,s/d)=1\\|\mu(s/d)|=1\\d>1}}(m_{d,+}-m_{d,-}-c_{r,s,d})\sqrt{d}. \tag{15}$$

As for the proof of Theorem 8 we know that the numbers $\sqrt{d}$ appearing in (15) are $\mathbb{Q}$-linear independent, therefore system (11) is proved.

Acknowledgments

I wish to thank the anonymous referees whose accurate reading, suggestions and comments have considerably improved the presentation of these results.

References

[1] B.C. Berndt, R.J. Evans, The determination of Gauss sums, Bull. Amer. Math. Soc. (N.S.) 5 (2) (1981) 107–129.
[2] S. Clary, D.H. Mugler, Shifted Fourier matrices and their tridiagonal commutors, SIAM J. Matrix Anal. Appl. 24 (3) (2003) 809–821.
[3] H. Davenport, Multiplicative Number Theory, third ed., Springer-Verlag, New York, 2000 (revised and with a preface by Hugh L. Montgomery).
[4] B.W. Dickinson, K. Steiglitz, Eigenvectors and functions of the discrete Fourier transform, IEEE Trans. Acoust. Speech Signal Process. 30 (1) (1982) 25–31.
[5] H. Ehlich, Untersuchungen zur numerischen Fourieranalyse, Math. Z. 91 (1966) 380–420.
[6] W. Gautschi, Attenuation factors in practical Fourier analysis, Numer. Math. 18 (1971/72) 373–400.
[7] F.A. Grünbaum, The eigenvectors of the discrete Fourier transform: a version of the Hermite functions, J. Math. Anal. Appl. 88 (2) (1982) 355–363.

[8] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, second ed., Springer-Verlag, New York, 1990.
[9] V.B. Matveev, Intertwining relations between the Fourier transform, and discrete Fourier transform the related functional identities and beyond, Inverse Problems 17 (4) (2001) 633–657 (special issue to celebrate Pierre Sabatier's 65th birthday, Montpellier, 2000).
[10] P. Morton, On the eigenvectors of Schur's matrix, J. Number Theory 12 (1) (1980) 122–127.
[11] H. Rademacher, Lectures on Elementary Number Theory, A Blaisdell Book in the Pure and Applied Sciences, Blaisdell Publishing Co., Ginn and Co., New York, Toronto, London, 1964.
[12] I. Schur, Über die Gausschen Summen, Nach. Gessel. Göttingen Math—Phys. Klasse (1921) 147–153.
[13] G. Tenenbaum, Introduction to Analytic and Probabilistic Number Theory, in: Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.
[14] L.C. Washington, Introduction to Cyclotomic Fields, second ed., Springer-Verlag, New York, 1997.