involve
a journal of mathematics

The kernel of the matrix $[ij \pmod{n}]$ when n is prime

Maria I. Bueno, Susana Furtado, Jennifer Karkoska,
Kyanne Mayfield, Robert Samalis and Adam Telatovich

msp

2016 vol. 9, no. 2

INVOLVE 9:2 (2016)
dx.doi.org/10.2140/involve.2016.9.265

The kernel of the matrix $[ij \pmod n]$ when n is prime

Maria I. Bueno, Susana Furtado, Jennifer Karkoska, Kyanne Mayfield, Robert Samalis and Adam Telatovich

(Communicated by Kenneth S. Berenhaut)

In this paper, we consider the $n \times n$ matrix whose (i, j)-th entry is $ij \pmod n$ and compute its rank and a basis for its kernel (viewed as a matrix over the real numbers) when n is prime. We also give a conjecture on the rank of this matrix when n is not prime and give a set of vectors in its kernel, which is a basis if the conjecture is true. Finally, we include an application of this problem to number theory.

1. Introduction

When learning modular arithmetic, it is a natural exercise to consider the multiplication table modulo an integer n. This table can be seen as an $n \times n$ matrix whose entries are positive integers. A question in linear algebra, which is interesting by itself, is to determine the rank or, even better, a basis for the kernel, of this matrix over the real numbers.

In this paper, we denote by C_n the $n \times n$ matrix given by

$$C_n(i, j) = ij \pmod n, \quad i, j = 1, \dots, n, \tag{1}$$

where $C_n(i, j)$ denotes the (i, j)-th entry of C_n.

Using techniques from matrix analysis and analytic number theory, we find the rank and a basis for the kernel of C_n when n is prime. When n is composite, we give a conjecture on the rank of C_n and a set of vectors in the kernel of C_n that is a basis of the kernel if the conjecture is true.

Since the last row and column of C_n are both zero, the matrix H_n, obtained from C_n by deleting that row and that column, has the same rank as C_n. Moreover,

MSC2010: 15A03, 11M06, 11M20.
Keywords: rank of a matrix, kernel of a matrix, bisymmetric matrix.
Furtado completed this work within the activities of Centro de Estruturas Lineares e Combinatorias da Universidade de Lisboa. Bueno, Karkoska, Mayfield, Samalis, and Telatovich were supported by NSF grant DMS-0852065 for the REU program at UCSB.

it is easy to find a basis for the kernel of C_n from the kernel of H_n. Therefore, most of the paper will be focused on studying the kernel of H_n.

As an example, for $n = 5$, we have

$$H_5 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}.$$

The paper is organized as follows. In Section 2, we use a matrix theory approach to study the $(n-1) \times (n-1)$ matrix H_n. In particular, we give a block-diagonal matrix similar to H_n (Lemma 7) and use it to give a set of vectors in the kernel of H_n. This result allows us to obtain nontrivial lower and upper bounds for the rank of H_n for general n (Corollary 12). A conjecture for the exact value of this rank is also presented (Conjecture 16). In Section 3, we obtain the main result of the paper (Theorem 42) which describes the rank of the $n \times n$ matrix C_n when n is prime and gives a basis for its kernel. The proof of the rank result is done using techniques from character theory and analytic number theory. In Section 4, we present an application to number theory that motivated our work.

2. The kernel of the matrix H_n

We now present some properties of the matrix H_n for general n and use them to study the kernel of H_n. We first introduce some notation and recall some definitions.

We denote by $M_{n,m}$ the set of $n \times m$ matrices with entries in $\mathbb{R}$. We abbreviate $M_{n,n}$ to M_n.

We denote by R the exchange matrix (also called the flip-transpose of the identity matrix I) of appropriate size, that is,

$$R := \begin{bmatrix} 0 & \dots & 1 \\ \vdots & \iddots & \vdots \\ 1 & \dots & 0 \end{bmatrix}.$$

Note that $R^2 = I$.

Definition 1. Let $A \in M_n$.

- The matrix A is called *symmetric* if $A = A^T$.
- The matrix A is called *persymmetric* if $A = RA^T R$.
- The matrix A is called *centrosymmetric* if $A = RAR$.
- The matrix A is called *bisymmetric* (or *symmetric centrosymmetric*, or *doubly symmetric*) if it is symmetric and centrosymmetric.

Remark 2. If $A \in M_n$ is persymmetric, then RA is symmetric. Also, if A is symmetric and centrosymmetric (resp. persymmetric), then A is persymmetric (resp. centrosymmetric).

Note that $A \in M_n$ is bisymmetric if

$$A(i,j) = A(j,i) \quad \text{and} \quad A(i,j) = A(n+1-i, n+1-j), \quad i, j = 1, \dots, n.$$

This means that being bisymmetric is equivalent to being symmetric with respect to the main diagonal and being symmetric with respect to the antidiagonal. A look at H_5 shows that this matrix is bisymmetric.

Lemma 3. *Let $n \in \mathbb{N}$. The matrix $H_n \in M_{n-1}$ is bisymmetric.*

Proof. The matrix H_n is symmetric since $H_n(i,j) = ij \pmod n = H_n(j,i)$. Additionally, H_n is centrosymmetric since

$$(n-i)(n-j) \pmod n = ij \pmod n,$$

which implies that $H_n(i,j) = H_n(n-i, n-j)$. □

The following result follows from some well-known properties of bisymmetric matrices [Cantoni and Butler 1976, Lemma 2].

Lemma 4. *If n is odd, then H_n has the form*

$$H_n = \begin{bmatrix} A & RBR \\ B & RAR \end{bmatrix} \tag{2}$$

for some symmetric $A \in M_{(n-1)/2}$ and persymmetric $B \in M_{(n-1)/2}$.

If n is even, then H_n has the form

$$H_n = \begin{bmatrix} A & x & RBR \\ x^T & q & x^T R \\ B & Rx & RAR \end{bmatrix} \tag{3}$$

for some $q \in \mathbb{C}$, $x \in M_{(n-2)/2,1}$, symmetric $A \in M_{(n-2)/2}$ and persymmetric $B \in M_{(n-2)/2}$.

Next we give an explicit expression for the number q and the vector x in the block representation of H_n given in Lemma 4 when n is even.

Lemma 5. *If n is even, then the number q in (3) is given by*

$$\begin{cases} 0 & \text{if } n \equiv 0 \pmod 4, \\ \dfrac{n}{2} & \text{if } n \not\equiv 0 \pmod 4. \end{cases}$$

Proof. We have

$$q = H_n\left(\frac{n}{2}, \frac{n}{2}\right) = \frac{n}{2} \cdot \frac{n}{2} \pmod n.$$

If $n \equiv 0 \pmod 4$, then $n = 4k$ for some positive integer k. Thus,

$$\frac{n}{2} \cdot \frac{n}{2} \pmod n = kn \pmod n = 0.$$

If $n \not\equiv 0 \pmod 4$, then, since n is even, we know that $n = 4k+2$ for some positive integer k, and

$$\frac{n}{2} \cdot \frac{n}{2} \pmod n = kn + 2k + 1 \pmod n = 2k+1 = \frac{n}{2}. \qquad \square$$

Lemma 6. *If n is even, then the column vector x in (3) is given by*

$$x(i) = \begin{cases} \frac{n}{2} & \text{if } i \text{ is odd}, \\ 0 & \text{if } i \text{ is even}, \end{cases} \qquad i = 1, 2, \ldots, \frac{n-2}{2},$$

where $x(i)$ denotes the i-th component of x.

Proof. Note that x is located in the $(n/2)$-th column of H_n. Thus, $x(i) = H_n(i, n/2)$ for $i = 1, 2, \ldots, (n-2)/2$. If $i = 2k$ for some positive integer k, then

$$H_n\left(i, \frac{n}{2}\right) = kn \pmod n = 0.$$

Now, if $i = 2k+1$ for some positive integer k, then

$$H_n\left(i, \frac{n}{2}\right) = kn + \frac{n}{2} \pmod n = \frac{n}{2}. \qquad \square$$

Taking into account Lemma 4, we next obtain a symmetric block-diagonal matrix similar to H_n for all n. This result also follows from [Cantoni and Butler 1976, Lemma 3]. Observe that $A - RB$ and $A + RB$, where A and B are as in Lemma 4, are symmetric matrices since RB is symmetric by Remark 2.

Lemma 7. (1) *Suppose that n is odd and let H_n be expressed as in (2). Then,*

$$KH_nK^{-1} = \begin{bmatrix} A - RB & 0 \\ 0 & A + RB \end{bmatrix}, \quad \text{where } K = \begin{bmatrix} I & -R \\ I & R \end{bmatrix}.$$

(2) *Suppose that n is even and let H_n be expressed as in (3). Then,*

$$KH_nK^{-1} = \begin{bmatrix} A - RB & 0 & 0 \\ 0 & A + RB & \sqrt{2}x \\ 0 & \sqrt{2}x^T & q \end{bmatrix}, \quad \text{where } K = \begin{bmatrix} I & 0 & -R \\ I & 0 & R \\ 0 & \sqrt{2} & 0 \end{bmatrix}.$$

As a consequence of the previous result, the study of the kernel of the bisymmetric matrix H_n can be reduced to the study of the kernel of the diagonal blocks of the block-diagonal matrix similar to H_n given in Lemma 7. In fact, when n is odd, if $\{u_1, \ldots, u_j\}$ is a basis for the kernel of $A - RB$ and $\{u_{j+1}, \ldots, u_{j+k}\}$ is a basis for the kernel of $A + RB$, then $\{K^{-1}w_1, \ldots, K^{-1}w_{j+k}\}$ is a basis for the kernel of H_n, where $w_i = [u_i \ \ 0]^T \in M_{n-1,1}$ for $i \le j$, and $w_i = [0 \ \ u_i]^T \in M_{n-1,1}$ for $i > j$.

Analogously, when n is even, if $\{u_1, \dots, u_j\}$ is a basis for the kernel of $A - RB$ and $\{u_{j+1}, \dots, u_{j+k}\}$ is a basis for the kernel of

$$\begin{bmatrix} A+RB & \sqrt{2}x \\ \sqrt{2}x^T & q \end{bmatrix}, \tag{4}$$

then $\{K^{-1}w_1, \dots, K^{-1}w_{j+k}\}$ is a basis for the kernel of H_n, where each w_i is defined as before. Note that, if $n = 2$, the matrix $A - RB$ is empty.

In what follows, we denote by $\mathbb{A} + \mathbb{R}\mathbb{B}$ the symmetric matrix $A + RB$ if n is odd and

$$\begin{bmatrix} A+RB & 2x \\ 2x^T & 2q \end{bmatrix} \tag{5}$$

if n is even. Clearly, $\mathbb{A} + \mathbb{R}\mathbb{B} \in M_{\lfloor n/2 \rfloor}$. Note that v is in the kernel of the matrix (4) if and only if

$$\begin{bmatrix} I_{(n-2)/2} & 0 \\ 0 & \sqrt{2}/2 \end{bmatrix} v$$

is in the kernel of the matrix (5). In particular, the matrices (4) and (5) have the same rank.

Next we give an explicit expression for the symmetric matrix $\mathbb{A} + \mathbb{R}\mathbb{B}$.

Lemma 8. *The matrix $\mathbb{A} + \mathbb{R}\mathbb{B} \in M_{\lfloor n/2 \rfloor}$ is given by*

$$(\mathbb{A} + \mathbb{R}\mathbb{B})(i, j) = \begin{cases} 0 & \textit{if } n \textit{ divides } ij, \\ n & \textit{otherwise}, \end{cases} \qquad i, j = 1, \dots, \left\lfloor \frac{n}{2} \right\rfloor.$$

Proof. Recall that $A, B \in M_{\lfloor (n-1)/2 \rfloor}$. Suppose that $1 \le i, j \le \lfloor (n-1)/2 \rfloor$. We have

$$A(i, j) = H_n(i, j)$$

and

$$RB(i, j) = B\left(\left\lfloor \frac{n+1}{2} \right\rfloor - i, j\right) = H_n(n - i, j).$$

Thus, for $1 \le i, j \le \lfloor (n-1)/2 \rfloor$,

$$\begin{aligned} (\mathbb{A} + \mathbb{R}\mathbb{B})(i, j) &= H_n(i, j) + H_n(n - i, j) \\ &= ij \pmod n + (n - i)j \pmod n \\ &= ij \pmod n + (-ij) \pmod n, \end{aligned}$$

which implies the claim for the entry in position (i, j). If n is odd, the proof is complete. Now suppose that n is even. By Lemma 5,

$$(\mathbb{A} + \mathbb{R}\mathbb{B})\left(\frac{n}{2}, \frac{n}{2}\right) = 2q = \begin{cases} 0 & \text{if } n \equiv 0 \pmod 4, \\ n & \text{if } n \not\equiv 0 \pmod 4. \end{cases}$$

Since n divides $(n/2)^2$ if and only if $n \equiv 0 \pmod 4$, the result follows for $(i, j) = (n/2, n/2)$.

Now we consider the case $j = n/2$, where $1 \leq i \leq n/2 - 1$. By Lemma 6,

$$(\mathbb{A} + \mathbb{R}\mathbb{B})\left(i, \frac{n}{2}\right) = 2x(i) = \begin{cases} n & \text{if } i \text{ is odd,} \\ 0 & \text{if } i \text{ is even.} \end{cases}$$

Since n divides $in/2$ if and only if i is even, the result follows for the entries in positions $(i, n/2)$. Taking into account that $\mathbb{A} + \mathbb{R}\mathbb{B}$ is symmetric, the result also follows for the entries in positions $(n/2, j)$, where $1 \leq j \leq n/2 - 1$. $\square$

Next we compute the rank of $\mathbb{A} + \mathbb{R}\mathbb{B}$ in terms of the proper divisors of n. We call *a proper divisor of* n, where n is a positive integer, a positive divisor of n different from n. Note that any proper divisor of n is less than or equal to $\lfloor n/2 \rfloor$.

Lemma 9. *Let n be a positive integer and k be the number of proper divisors of n. Then*, $\operatorname{rank}(\mathbb{A} + \mathbb{R}\mathbb{B}) = k$.

Proof. Let $i \in \{1, \ldots, \lfloor n/2 \rfloor\}$. If $\gcd(i, n) = 1$, then n is not a divisor of ij for all $j = 1, \ldots, \lfloor n/2 \rfloor$. By Lemma 8, $(\mathbb{A} + \mathbb{R}\mathbb{B})(i, j) = n$ for all $j = 1, 2, \ldots, \lfloor n/2 \rfloor$.

If $\gcd(i, n) \neq 1$ and i has order m in $\mathbb{Z}_n$ (that is, m is the smallest possible integer such that $mi \equiv 0 \pmod n$), then, by Lemma 8, $(\mathbb{A} + \mathbb{R}\mathbb{B})(i, j) = 0$ if and only if $j = ms$ for some positive integer s. Moreover, the nonzero entries in the i-th row are equal to n. Thus, from the comments above, we conclude that there are at most k distinct rows in $\mathbb{A} + \mathbb{R}\mathbb{B}$, corresponding to the k proper divisors of n. Moreover, one of these rows has all entries equal to n, while the remaining have the first zero entry in distinct columns and have all the nonzero entries equal to n. Note that distinct proper divisors have distinct orders. By elementary row operations, it can be seen that these k rows are linearly independent, which proves the result. $\square$

Remark 10. When n is prime, Lemma 9 implies that $\operatorname{rank}(\mathbb{A} + \mathbb{R}\mathbb{B}) = 1$.

Another immediate consequence of Lemma 9 is given in the next corollary.

Corollary 11. *Let n be a positive integer and k be the number of proper divisors of n. Then*,

$$\dim(\ker(\mathbb{A} + \mathbb{R}\mathbb{B})) = \left\lfloor \frac{n}{2} \right\rfloor - k.$$

Since, from Lemma 7,

$$\operatorname{rank}(H_n) = \operatorname{rank}(A - RB) + \operatorname{rank}(\mathbb{A} + \mathbb{R}\mathbb{B}) \quad \text{and} \quad \operatorname{rank}(A - RB) \leq \left\lfloor \frac{n-1}{2} \right\rfloor,$$

from Lemma 9 we get the next result.

Corollary 12. *Let n be a positive integer and let k be the number of proper divisors of n. Then*,

$$k \leq \operatorname{rank}(H_n) \leq \left\lfloor \frac{n-1}{2} \right\rfloor + k.$$

Next we compute a basis for the kernel of $\mathbb{A}+\mathbb{R}\mathbb{B}$ when $n>2$. Note that when $n=2$, the kernel of $\mathbb{A}+\mathbb{R}\mathbb{B}$ only contains the zero vector by Corollary 11. We start with a technical lemma.

Lemma 13. *Let n be a positive integer. For each $j\in\{1,2,\ldots,\lfloor n/2\rfloor\}$, let $d_j=\gcd(j,n)$. Then, for $1\le i\le\lfloor n/2\rfloor$, we have $(\mathbb{A}+\mathbb{R}\mathbb{B})(i,j)=0$ if and only if $(\mathbb{A}+\mathbb{R}\mathbb{B})(i,d_j)=0$.*

Proof. Note that, from Lemma 8, the statement $(\mathbb{A}+\mathbb{R}\mathbb{B})(i,j)=0$ if and only if $(\mathbb{A}+\mathbb{R}\mathbb{B})(i,d_j)=0$ is equivalent to n divides ij if and only if n divides id_j.

Suppose that n divides ij. Then, there exists a positive integer k such that $nk=ij$. Since $\gcd(j,n)=d_j$, we have $d_j=jx+ny$ for some $x,y\in\mathbb{Z}$, $x\neq 0$. Thus,

$$nk=i\left(\frac{d_j-ny}{x}\right),$$

which implies $n(xk+iy)=id_j$ and, therefore, n divides id_j.

Suppose now that n divides id_j. Since d_j divides j, we have id_j divides ij and, therefore, n divides ij. □

We denote by e_i the vector of appropriate size whose entries are 0 except the entry in position i which is 1.

Theorem 14. *Let $n>2$. The set of vectors $u_j:=e_j-e_{d_j}\in M_{\lfloor n/2\rfloor,1}$, with $j\in\{1,\ldots,\lfloor n/2\rfloor\}$, where j is not a divisor of n and $d_j=\gcd(j,n)$, forms a basis for $\ker(\mathbb{A}+\mathbb{R}\mathbb{B})$.*

Proof. First we show that the vectors u_j are in the kernel of $\mathbb{A}+\mathbb{R}\mathbb{B}$. Note that, by the definition of u_j, the i-th entry of the vector $(\mathbb{A}+\mathbb{R}\mathbb{B})u_j$ is $(\mathbb{A}+\mathbb{R}\mathbb{B})(i,j)-(\mathbb{A}+\mathbb{R}\mathbb{B})(i,d_j)$. By Lemma 8, each entry of $\mathbb{A}+\mathbb{R}\mathbb{B}$ is either n or 0 and, by Lemma 13, $(\mathbb{A}+\mathbb{R}\mathbb{B})(i,j)=0$ if and only if $(\mathbb{A}+\mathbb{R}\mathbb{B})(i,d_j)=0$. This implies that $(\mathbb{A}+\mathbb{R}\mathbb{B})u_j=0$ for all u_j, as desired.

Next, we show that the vectors u_j form a linearly independent set. Let U be the matrix whose columns are the vectors u_j and let J be the set of integers in $\{1,\ldots,\lfloor n/2\rfloor\}$ that are not divisors of n. Notice that if $j_1,j_2\in J$, then $j_1\neq d_{j_2}$ since, if $j_1=d_{j_2}=\gcd(j_2,n)$, then j_1 would divide n. This implies that the submatrix of U formed by the rows indexed by J is a row permutation of the identity matrix of size $|J|$, which shows that U has full rank.

We have obtained a set of $|J|$ linearly independent vectors in the kernel of $\mathbb{A}+\mathbb{R}\mathbb{B}$. Since the largest proper divisor of n is less than or equal to $\lfloor n/2\rfloor$, we have $|J|=\lfloor n/2\rfloor-k$, where k is the number of proper divisors of n. By Corollary 11, the result follows. □

Example 15. Let $n=24$. Then $\dim(\ker(\mathbb{A}+\mathbb{R}\mathbb{B}))=5$ and the set J defined in the proof of Theorem 14 is given by $\{5,7,9,10,11\}$. A basis for $\ker(\mathbb{A}+\mathbb{R}\mathbb{B})$ is given by the vectors

$$\begin{bmatrix}-1\\0\\0\\0\\1\\0\\0\\0\\0\\0\\0\\0\end{bmatrix},\quad \begin{bmatrix}-1\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0\\0\end{bmatrix},\quad \begin{bmatrix}0\\0\\-1\\0\\0\\0\\0\\0\\1\\0\\0\\0\end{bmatrix},\quad \begin{bmatrix}0\\-1\\0\\0\\0\\0\\0\\0\\0\\1\\0\\0\end{bmatrix},\quad \begin{bmatrix}-1\\0\\0\\0\\0\\0\\0\\0\\0\\0\\1\\0\end{bmatrix}.$$

Though we could not find appropriate techniques from matrix theory to show it, numerical experiments in Matlab, in which the rank of H_n was computed for any n from 2 to 1000, suggest the following conjecture. Recall that $\operatorname{rank}(C_n) = \operatorname{rank}(H_n)$, where C_n is the matrix defined in (1).

Conjecture 16. *Let n be a positive integer and let k be the number of proper divisors of n. Then,*

$$\operatorname{rank}(C_n) = \operatorname{rank}(H_n) = \left\lfloor \frac{n-1}{2} \right\rfloor + k.$$

Clearly, the conjecture holds when $n = 2$. In the next section we prove the conjecture when n is prime. The result when n is not prime remains open.

Remark 17. Because of Lemmas 7 and 9, it follows that, if Conjecture 16 is true and $n > 2$, then $A - RB$ is a nonsingular matrix. Note that, if $n = 2$, the matrix $A - RB$ is empty and $\mathbb{A} + \mathbb{R}\mathbb{B}$ is nonsingular as well.

3. The rank of the matrix H_n when n is prime

In this section we compute the rank of the matrix H_n, when n is prime, using techniques from character theory and analytic number theory.

We start with some basic concepts and lemmas that will be used to obtain the main result.

Definition 18 (character [Apostol 1976, Section 6.5]). Let G be a group and let $\mathbb{C}$ denote the set of complex numbers. A function $f : G \to \mathbb{C}$ is called a character of G if

(i) f is a group homomorphism of G, that is, $f(g_1 g_2) = f(g_1) f(g_2)$ for all $g_1, g_2 \in G$; and

(ii) $f(g) \neq 0$ for some $g \in G$.

The set of characters of a finite group G is also a group with respect to the group operation of pointwise multiplication defined by $(f_1 \cdot f_2)(g) = f_1(g) f_2(g)$ [Apostol 1976, Section 6.6]. This group is denoted by $\hat{G}$. The identity element of $\hat{G}$ is the character f_I given by $f_I(g) = 1$ for all $g \in G$. The inverse of a character f is $\bar{f}$ given by $\bar{f}(g) = \overline{f(g)}$ for all $g \in G$, where $\overline{f(g)}$ is the complex conjugate of $f(g)$. The identity element of $\hat{G}$ is called the *principal character of* G, while the other characters are called *nonprincipal characters* of G. Note that any character of G maps the identity element of G to 1.

According to the next result, if f is a character of a finite group G, the range of a character of G lies on the unit circle. We recall that if G is a finite group with identity element e, then the *exponent of* G is the least positive integer k such that $g^k = e$ for all $g \in G$.

Proposition 19 [Apostol 1976, Theorem 6.7]. *Let G be a finite group with identity element e and let $f \in \hat{G}$. Then, $f(e) = 1$ and each function value $f(g)$ is an m-th root of unity, where m is the exponent of G.*

One may think that the set of characters of a group could potentially contain many functions. The next theorem gives the exact number of characters when the group is finite and abelian.

Proposition 20 [Apostol 1976, Theorem 6.8]. *If G is a finite abelian group, then $|\hat{G}| = |G|$.*

In particular, if G is a finite cyclic group of order n (in which case the exponent of G equals the order of G) and g is a generator of G, then the n characters of G are determined by sending g to the different n-th roots of unity in $\mathbb{C}$.

Example 21. Let G be the additive group $\mathbb{Z}_4$. Then, there exist four characters f_1, f_2, f_3, f_4 of G and each character value is in the set $\{1, -1, i, -i\}$, the 4th roots of unity. Suppose that f_1 is the principal character and f_2, f_3, f_4 are defined by $f_2(1) = -1$, $f_3(1) = i$ and $f_4(1) = -i$. Note that, since 1 is a generator of G and characters are group homomorphisms, f_2, f_3, f_4 are well-defined. We give the range of the characters of G through a 4×4 matrix A whose entry $A(i, j)$ is given by $f_i(g_j)$, where $g_1 = 0$, $g_2 = 1$, $g_3 = 2$, and $g_4 = 3$:

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \\ 1 & -i & -1 & i \end{bmatrix}.$$

The following concept will be key in the proof of our main results.

Definition 22 (group matrix [Chan et al. 1998]). Let G be a finite group of order n. Fix an enumeration $\{g_1, \ldots, g_n\}$ of the elements of G. For every complex-valued function α on G, the matrix A_α given by $A_\alpha(i, j) = \alpha(g_i g_j^{-1})$ is called *a group matrix associated to* α.

Example 23. Let G be the additive group $\mathbb{Z}_4$ and let f_2 be the character defined in Example 21. Then, the following matrix is a group matrix associated to f_2:

$$A_{f_2} = \begin{bmatrix} 1 & -i & i & -1 \\ -1 & 1 & -i & i \\ i & -1 & 1 & -i \\ -i & i & -1 & 1 \end{bmatrix}.$$

In what follows, we let p denote a prime number. Next we show that the rank of H_p can be computed by finding the rank of a group matrix. In particular, the next lemma states that the matrix H_p can be obtained by permuting some columns of a group matrix associated with a real-valued function on the multiplicative group $\mathbb{Z}_p^\times$ consisting of the units of $\mathbb{Z}_p$.

Lemma 24. *Let p be a prime number. Let $\alpha : \mathbb{Z}_p^\times \to \mathbb{N}$ be given by $\alpha(\bar{m}) = m$, where $\bar{m}$ denotes the equivalence class mod p of $m \in \{1, 2, \dots, p-1\}$. Then, H_p is a column permutation of the group matrix A_α associated to α.*

Proof. First recall that, since p is a prime number, the group $\mathbb{Z}_p^\times$ is a cyclic group under multiplication. Let $\bar{g}$, where $g \in \{1, 2, \dots, p-1\}$, be a generator for $\mathbb{Z}_p^\times$ and consider the enumeration of $\mathbb{Z}_p^\times$ given by $\{\overline{g^{\sigma(1)}}, \overline{g^{\sigma(2)}}, \dots, \overline{g^{\sigma(p-1)}}\}$, where σ is a permutation of $\{1, 2, \dots, p-1\}$ such that $g^{\sigma(i)} = i$. Then,

$$A_\alpha(i, j) = \alpha(\overline{g^{\sigma(i)}}\,\overline{g^{-\sigma(j)}}) = ij^{-1} \pmod{p}.$$

Let π be the permutation of $\{1, 2, \dots, p-1\}$ such that $\pi(j) = j^{-1}$. Now consider the matrix $\widetilde{A_\alpha}$ obtained from A_α by permuting its columns as follows: column j of $\widetilde{A_\alpha}$ is column $\pi(j) = j^{-1}$ of A_α. Then, $\widetilde{A_\alpha} = H_p$ is obtained by permuting the columns of A_α and the result follows. □

The previous lemma implies that $\operatorname{rank}(H_p) = \operatorname{rank}(A_\alpha)$.

We next characterize the eigenvalues of a group matrix of a finite abelian group, associated to an injective function, and show that it is diagonalizable, implying that its rank is the number of its nonzero eigenvalues. For this purpose, we present the next lemma which gives the spectrum of a group matrix associated to an integer-valued injective function in terms of the values of the characters of G at an element of the group ring $\mathbb{Z}[G]$, when G is a finite abelian group. Note that any character in the character group of G can be extended by linearity to a complex-valued function on $\mathbb{Z}[G]$.

Lemma 25 [Chan et al. 1998; Jungnickel 1993, Theorem 7.7.4]. *Let G be a finite abelian group and α an injective function from G to $\mathbb{N}$. Let $a = \sum_{g \in G} \alpha(g) g \in \mathbb{Z}[G]$. Then, the group matrix A_α associated to α is diagonalizable and its spectrum is the set $\{f(a) : f \in \hat{G}\}$.*

Since A_α is diagonalizable, we can compute the rank of A_α by counting the number of eigenvalues distinct from zero. Thus, $\operatorname{rank}(A_\alpha) = |\{f \in \hat{G} : f(a) \neq 0\}|$.

Remark 26. Taking into account Lemmas 24 and 25, in order to compute $\operatorname{rank}(H_p)$, it is enough to determine the number of characters f in the character group of $\mathbb{Z}_p^\times$ such that $\sum_{i=1}^{p-1} i f(\bar{i}) \neq 0$.

Here, it becomes convenient to work with the so-called Dirichlet characters whose definition we give below.

Definition 27 (Dirichlet character [Apostol 1976, Section 6.8]). Let $n \in \mathbb{N}$ and f be any character of $\mathbb{Z}_n^\times$. The function $\chi : \mathbb{N} \to \mathbb{C}$ given by

$$\chi(m) = \begin{cases} f(\bar{m}) & \text{if } n \text{ and } m \text{ are relatively prime,} \\ 0 & \text{if } n \text{ and } m \text{ are not relatively prime} \end{cases}$$

is called the *Dirichlet character modulo n induced by f*. The Dirichlet character induced by the principal character is called the *principal Dirichlet character modulo n*. A Dirichlet character modulo n that is not the principal character is called *nonprincipal*.

It is easy to see that Dirichlet characters modulo n are completely multiplicative and periodic with period n [Apostol 1976, Theorem 6.15]; that is, if χ is a Dirichlet character, then

- $\chi(x+n) = \chi(x)$ for all $x \in \mathbb{N}$;
- $\chi(xy) = \chi(x)\chi(y)$ for all $x, y \in \mathbb{N}$.

Note that the number of Dirichlet characters modulo n equals the order of $\mathbb{Z}_n^\times$ since, by Proposition 20, the number of characters of a finite abelian group equals its cardinality.

Example 28. The following table displays the Dirichlet characters for $n = 5$. We obtain four functions since $\mathbb{Z}_5$ contains 4 units. We only give the values of the functions on the set $\{1, \dots, 5\}$ since these Dirichlet characters are periodic functions of period 5:

x	1	2	3	4	5
$\chi_1(x)$	1	1	1	1	0
$\chi_2(x)$	1	-1	-1	1	0
$\chi_3(x)$	1	i	$-i$	-1	0
$\chi_4(x)$	1	$-i$	i	-1	0

Definition 29 (primitive Dirichlet character [Apostol 1976, Section 8.7]). If χ is a Dirichlet character modulo n, we say that χ is primitive if for every proper divisor d of n, there exists an integer a such that $a \equiv 1 \pmod d$, $\gcd(a, n) = 1$, and $\chi(a) \neq 1$.

Example 30. Consider the Dirichlet characters modulo 5, given in Example 28. The only proper divisor of 5 is 1. Note that χ_1 is not primitive since $\chi_1(a) = 1$ whenever $\gcd(a, n) = 1$. However, the rest of the Dirichlet characters are primitive since $\chi_i(2) \neq 1$ for $i = 2, 3, 4$.

The observations in the previous example can be generalized as follows.

Lemma 31 [Apostol 1976, Theorems 8.13 and 8.14]. *The principal Dirichlet character modulo n is not primitive. Moreover, if n is prime, all nonprincipal Dirichlet characters modulo n are primitive.*

Definition 32 (admissible Dirichlet character). Let χ be a Dirichlet character modulo n. We say that χ is *admissible* if

$$\sum_{i=1}^{n-1} i\chi(i) \neq 0.$$

Note, the principal Dirichlet character modulo p is admissible since $\sum_{i=1}^{p-1} i \neq 0$. Taking into account Remark 26, we obtain the following.

Remark 33. If p is prime, the rank of H_p is equal to the number of admissible Dirichlet characters modulo p.

In order to see which Dirichlet characters are admissible, we need some well-known results from the theory of Dirichlet L-functions.

Definition 34 (Dirichlet L-function [Apostol 1976, Sections 11 and 12]). Let χ be a Dirichlet character modulo n and $s \in \mathbb{C}$ with real part greater than 1. The associated Dirichlet L-series is the absolutely convergent series given by

$$L(s, \chi) = \sum_{i=1}^{\infty} \frac{\chi(i)}{i^s}.$$

If χ is nonprincipal, $L(s, \chi)$ is a complex-valued function in s that can be analytically extended to an entire function on the whole complex plane [Apostol 1976, Theorem 12.5]. This function is called a Dirichlet L-function and is also denoted by $L(s, \chi)$.

The following is a well-known result in analytic number theory.

Lemma 35 [Apostol 1976, Thm. 12.20]. *If χ is a nonprincipal Dirichlet character modulo n, then*

$$L(0, \chi) = -\frac{1}{n} \sum_{i=1}^{n-1} i\chi(i).$$

Remark 36. The admissible Dirichlet characters modulo p, where p is prime, are exactly the principal Dirichlet character and the nonprincipal Dirichlet characters such that $L(0, \chi) \neq 0$.

In order to determine when $L(0, \chi) \neq 0$, we introduce the functional equation for Dirichlet L-functions.

Let $\bar{\chi}$ denote the complex conjugate of the Dirichlet character χ.

Lemma 37 (functional equation [Apostol 1976, Theorem 12.11]). *Let χ be a primitive Dirichlet character modulo n. Then, for all $s \in \mathbb{C}$, we have*

$$L(1-s, \chi) = \frac{n^{s-1}\Gamma(s)}{(2\pi)^s}\big(e^{-\pi i s/2} + \chi(-1)e^{\pi i s/2}\big)G(1, \chi)L(s, \bar{\chi}),$$

where $\Gamma(s)$ is the Gamma function and $G(1, \chi) = \sum_{r=1}^{n} \chi(r)e^{2\pi i r/n}$ is the Gauss sum associated with χ.

The following are well-known results in analytic number theory.

Lemma 38 [Apostol 1976, Theorem 8.15]. *Let χ be a primitive Dirichlet character modulo n. Then, $G(1, \chi) \neq 0$.*

Lemma 39 [Apostol 1976, Section 7.3]. *Let χ be a nonprincipal Dirichlet character modulo n. Then, $L(1, \chi)$ is finite and nonzero.*

The next result gives necessary and sufficient conditions for a Dirichlet character modulo p to be admissible.

Lemma 40. *Let $p > 2$ be a prime number and consider the primitive $(p-1)$-th root of unity $w = e^{2\pi i/(p-1)}$. Let $\bar{g}$ be a generator of $\mathbb{Z}_p^\times$ and let f_k be the character of $\mathbb{Z}_p^\times$ defined by $f_k(\bar{g}) := w^{k-1}$, with $k = 1, \dots, p-1$. Let $\chi_1, \dots, \chi_{p-1}$ be the Dirichlet characters modulo p induced by $f_1, \dots, f_k$, respectively. Then, for $k = 2, \dots, p-1$, we have χ_k is admissible if and only if k is even.*

Proof. Since $\bar{g}$ is a generator of $\mathbb{Z}_p^\times$, we have $g^{p-1} \equiv 1 \pmod p$ and $g^s \neq 1 \pmod p$ for $s = 1, \dots, p-2$. Thus, $g^{(p-1)/2} \equiv -1 \pmod p$. So, for $k = 2, \dots, p-1$, we have $\chi_k(-1) = \chi_k(g^{(p-1)/2}) = (w^{(p-1)/2})^{k-1} = (-1)^{k-1}$. Therefore, $\chi_k(-1) = -1$ if k is even and $\chi_k(-1) = 1$ if k is odd. Since p is prime and χ_k is nonprincipal, χ_k is primitive by Lemma 31. By Lemma 37,

$$L(0, \chi_k) = \frac{1}{2\pi}\big(-i + \chi_k(-1)i\big)G(1, \chi_k)L(1, \overline{\chi_k}).$$

Note that if χ_k is a nonprincipal Dirichlet character, then $\bar{\chi}$ is also nonprincipal. Taking into account Lemmas 38 and 39, it follows that, if k is even, $L(0, \chi_k) \neq 0$; if k is odd, $L(0, \chi_k) = 0$. Now the result follows from Remark 36. □

We can now give the rank of the matrix H_p when $p > 2$ is a prime number.

Lemma 41. *Let $p > 2$ be a prime number. Then,* $\operatorname{rank}(H_p) = (p+1)/2$.

Proof. By Lemma 40, we have that the nonprincipal Dirichlet characters modulo p $\chi_2, \chi_4, \dots, \chi_{p-1}$ are admissible, while $\chi_3, \chi_5, \dots, \chi_{p-2}$ are not admissible. Since, by Remark 36, χ_1 is admissible, the result follows taking into account Remark 33. □

Observe that, by Lemma 41, we have that Conjecture 16 is true when $n > 2$ is prime. Then, by Remark 17, Lemma 7, and Theorem 14, we can obtain a basis for the kernel of H_p when $p > 2$ is prime (note that when $p = 2$, the kernel of H_p is $\{0\}$). From this basis for the kernel of H_p, we can easily obtain a basis for the kernel of C_p, the $p \times p$ matrix whose (i, j)-th entry is $ij \pmod p$.

Theorem 42. *Let $p > 2$ be a prime number and $C_p \in M_p$ be defined by $C_p(i, j) = ij \pmod p$. Let K be as in Lemma 7. Let $u_j := e_j - e_1 \in M_{(p-1)/2,1}$ and $w_j = [0_{(p-1)/2}, u_j, 0]^T \in M_{p,1}$, with $j = 2, \ldots, (p-1)/2$. Then, the set of vectors $\{K^{-1}w_2, \ldots, K^{-1}w_{(p-1)/2}, e_p\}$ is a basis for the kernel of C_p. In particular,* $\operatorname{rank}(C_p) = (p+1)/2$.

4. Application

We now present a number theoretic application of the problem we have considered in this paper. This application, which motivated our work, appears in the context of the study of Stickelberger relations on class groups of group rings.

Let G be a finite abelian group and let n be the order of G. Fix a primitive n-th root of unity z. Then, for each $g \in G$ and $f \in \hat{G}$, there is a unique integer r, with $1 \le r \le n$, such that $f(g) = z^r$. We therefore can define the function

$$\langle \cdot , \cdot \rangle : G \times \hat{G} \to \mathbb{Q}/\mathbb{Z}$$

given by

$$\langle g, f \rangle = \left\{ \frac{r}{n} \right\},$$

where $\{r/n\}$ denotes the fractional part of r/n.

Note that the group rings $\mathbb{Q}[G]$ and $\mathbb{Q}[\hat{G}]$ are $\mathbb{Q}$-vector spaces with dimension $|G| = |\hat{G}|$, and G and $\hat{G}$ are bases for $\mathbb{Q}[G]$ and $\mathbb{Q}[\hat{G}]$, respectively. Thus, we may extend the function above via linearity to

$$\langle \cdot , \cdot \rangle : \mathbb{Q}[G] \times \mathbb{Q}[\hat{G}] \to \mathbb{Q}$$

defined by

$$\left\langle \sum_{g \in G} c_g g, \sum_{f \in \hat{G}} c_f f \right\rangle = \sum_{g \in G} \sum_{f \in \hat{G}} c_g c_f \langle g, f \rangle,$$

where $c_g, c_f \in \mathbb{Q}$. Now consider the function h: $\mathbb{Q}[\hat{G}] \to \mathbb{Q}[G]$ given by

$$h(a) = \sum_{g \in G} \langle g, a \rangle g \quad \text{for any } a \in \mathbb{Q}[\hat{G}]. \tag{6}$$

We may view h as a linear map between two $\mathbb{Q}$-vector spaces of dimension $|G|$. An interesting problem, which motivated our work, is the study of the kernel of h.

When the group G is cyclic (and, therefore, isomorphic to $\mathbb{Z}_n$ for some n), we can determine explicitly the matrix representation of h as the following lemma states.

Lemma 43. *Let G be the additive group $\mathbb{Z}_n$ and g be a generator of G. Let $\hat{G} = \{f_1, f_2, \ldots, f_n\}$, where $f_i(g) = z^{i-1}$ and z is a primitive n-th root of unity. Then, the matrix representation R_n of h in the bases $\beta_1 = \{f_2, f_3, \ldots, f_n, f_1\}$ and $\beta_2 = \{g, g^2, \ldots, g^{n-1}, e\}$ is given by*

$$R_n(i, j) = \left\{\frac{ij}{n}\right\} = \frac{ij \pmod n}{n}, \quad i, j = 1, 2, \ldots, n.$$

Proof. For $i, j = 1, \ldots, n-1$, since $f_{j+1}(g^i) = z^{ij}$, the (i, j)-th entry of R_n is given by

$$\langle g^i, f_{j+1}\rangle = \left\{\frac{ij}{n}\right\} = \frac{ij \pmod n}{n}.$$

Since $f_j(e) = 1 = z^0$, we have $\langle e, f_j\rangle = 0$ for $j = 1, \ldots, n$, which implies that the last row of R_n is zero. Since $f_1(g^i) = 1 = z^0$, we have $\langle g^i, f_1\rangle = 0$ for $i = 1, \ldots, n$, and, then, the last column of R_n is zero. Thus, the claim follows. □

Note that

$$R_n = \frac{1}{n} C_n = \frac{1}{n}\begin{bmatrix} H_n & 0 \\ 0 & 0 \end{bmatrix}.$$

Finally, we observe that, although the function h given in (6) is defined between $\mathbb{Q}$-vector spaces, the determination of the kernel and rank of the matrix representation of h can be done by considering it as a matrix over the real numbers.

Acknowledgement

We would like to thank the anonymous referee for the time spent reading our paper and for the suggestions to improve its presentation.

References

[Apostol 1976] T. M. Apostol, *Introduction to analytic number theory*, Springer, New York, 1976. MR 55 #7892 Zbl 0335.10001

[Cantoni and Butler 1976] A. Cantoni and P. Butler, "Eigenvalues and eigenvectors of symmetric centrosymmetric matrices", *Linear Algebra and Appl.* **13**:3 (1976), 275–288. MR 53 #476 Zbl 0326.15007

[Chan et al. 1998] W.-K. Chan, Y.-C. Chan, and M.-K. Siu, "Minimal rank of abelian group matrices", *Linear and Multilinear Algebra* **44**:3 (1998), 277–285. MR 99j:15002 Zbl 0960.15003

[Jungnickel 1993] D. Jungnickel, *Finite fields: Structure and arithmetics*, Bibliographisches Institut, Mannheim, 1993. MR 94g:11109 Zbl 0779.11058

Received: 2014-10-14 Revised: 2015-04-13 Accepted: 2015-04-16

mbueno@math.ucsb.edu
Mathematics Department and College of Creative Studies, The University of California, Santa Barbara, Santa Barbara, CA 93106-3080, United States

sbf@fep.up.pt
CEAFEL, Faculdade de Economia, Universidade do Porto, 4200-464 Porto, Portugal

karkoj@rpi.edu
Applied Mathematics Department, Rensselaer Polytechnic Institute, Troy, NY 12180, United States

mayfield13@up.edu
Fast Enterprises LLC, Madison, WI 53704, United States

robsamalis@gmail.com
Department of Mathematics, University of Georgia, Athens, GA 30602, United States

aet156@psu.edu
Department of Mathematics, Pennsylvania State University, State College, PA 16803, United States

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2016 is US $160/year for the electronic version, and $215/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2016 vol. 9 no. 2