International Journal of Pure and Applied Mathematics
Volume 32 No. 2 2006, 199-208

SPECTRA ANALYSIS OF THE MATRIX DD', D THE DIRICHLET MATRIX

H.K. Terzidis[1], P. Tzekis[2 §]

[1,2]Department of Mathematics
School of Sciences
Technological Educational Institution of Thessaloniki
P.O. Box 14561, Thessaloniki, GR-541 01, GREECE
[2]e-mail: tzekis@math.auth.gr

Abstract: The aim of this work is to study the spectra analysis of the matrix $DD\prime$, D the Dirichlet matrix. First we prove that the Dirichlet matrix is unitary. Then, we prove that the matrix $G = DD'$, D the Dirichlet matrix, is symmetrical and orthogonal and we find its eigenvalues. In last, we study the spectra analysis of the matrix G.

AMS Subject Classification: 11C20, 11T24
Key Words: Dirichlet characters, Dirichlet matrix, specra analysis

1. Introduction

Let n is a prime number p, so the reduced residue system (mod$p$), coincides with the set $\{1, 2, ..., p-1\}$. From these numbers, the primitive roots g(mod$p$), are those numbers from which the sequence $\{1, g, g^2, ..., g^{p-2}\}$, constitutes a permutation of the sequence $\{1, 2, ..., p-1\}$. Primitive roots exist iff n has the form $1, 2, 4, p^k$ or $2p^k$, where p is a prime number ($\neq 2$) and k is a positive integer. If n has primitive root g then the integers $g, g^2, ..., g^{\varphi(n)} \equiv 1$ constitutes a reduced residue system (mod$n$). In this case if a is an arbitrary integer, prime to n, then exists a unique integer k, $1 \leq k \leq \varphi(n)$, such that $a \equiv g^k$(mod$n$). This integer is the *index* of a as for the base g(mod$n$).

Define now the Adelian group $G = \left\{\overline{1}, \overline{2}, ..., \overline{p-1}\right\}$ of the reduced residue system (mod$p$), where p is a prime number. If g is a primitive root (mod$p$)

Received: September 1, 2006

§Correspondence author

and $\beta(n)$ is the index of n as for the base g, when $\overline{n}$ is an item of G, i.e. $n = g^{\beta(n)}(\mathrm{mod}\, p)$, with $1 \leq \beta(n) \leq p-1$, then the functions which are defined from the relations

$$x_m(n) = e^{2\pi i m\beta(n)/(p-1)}, \quad n \neq 0(\mathrm{mod}\, p)\,,$$

$$x_m(n) = 0, \quad n \equiv 0(\mathrm{mod}\, p)\,,$$

with $m = 1, 2, ..., p-1$, constitute the Dirichlet characters (mod$p$), with main character in this case the function x_{p-1}. In general, let us consider a primitive root g(mod$p$), where p is a prime number ($\neq 2$) which is also a primitive root (modp^a) for $a \geq 1$. Let $\beta(n)$ is the index of the integer n, with $(n, p) = 1$, as for the base g (modp^a), i.e. $\beta(n)$ is the unique defined integer for which $n \equiv g^{\beta(n)}$ (modp^a), with $1 \leq \beta(n) \leq \varphi(p^a)$. The functions which are defined from the relations

$$x_m(n) = e^{2\pi i m\beta(n)/\phi(p^\alpha)}, \quad n \neq 0(\mathrm{mod}\, p)\,,$$

$$x_m(n) = 0, \quad n \equiv 0(\mathrm{mod}\, p)\,,$$

with $m = 1, 2, ..., \phi(p^\alpha)$, is complete multiplicative and periodical with period p^a. Consequently, these functions are Dirichlet characters (modp^a), with main character the function $x_{\phi(p^\alpha)}$. But from the relation $n = g^{\beta(n)}$, results for $n = g$, that $g = g^{\beta(g)}$ and so $\beta(g) = 1$. Thus,

$$x_m(g) = e^{2\pi i m/\phi(p^\alpha)}$$

for $m = 1, 2, ..., \varphi(p^a)$ and so the characters $x_1, x_2, ..., x_{\varphi(p^a)}$ take different values in g. Consequently, these characters are distinct and therefore are the Dirichlet characters (modp^a). This analysis holds also in the case where $p = 2$, with $a = 1$ and 2, whereas it is not true for $a \geq 3$, because in this case the number 2^a has not a primitive root, so it is required a different approach.

Let now μ a number with a primary analysis

$$\mu = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}\,,$$

where $p_1, p_2, ..., p_k$ are prime odd numbers, different one from each other. If x_{ij} is a Dirichlet character (mod$p_i^{a_i}$), $i = 1, 2, ..., k$, $j = 1, 2, ..., \varphi(p_i^{a_i})$, then the product

$$x_{1j}x_{2j}...x_{kj} = x_j$$

is a Dirichlet character (modμ). Because the count of the characters x_{ij}, $i = 1, 2, ..., k$, $j = 1, 2, ..., \varphi(p_i^{a_i})$, for a specific i is $\varphi(p_i^{a_i})$, implied that while every x_{ij} runs the $\varphi(p_i^{a_i})$ characters (mod$p_i^{a_i}$), the set of the characters x_j is

$$\phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k}) = \phi(\mu)\,.$$

2. Eigenvalues of the Matrix DD', D the Dirichlet Matrix

Let the matrix

$$D = \frac{1}{\sqrt{p-1}} \left\{ w^{m\beta(n)} \right\} ,$$

$m, n = 1, 2, ..., p-1$, where p is a prime number, $w = e^{2\pi i/p-1}$ and $\beta(n)$ is the index of n as for a primitive root $g\,(\text{mod} p)$, i.e. $n = g^{\beta(n)}$.

We name the matrix D Dirichlet matrix and the transformation which has as matrix, for the usual base of the n-d space, this matrix, Dirichlet transform.

Proposition 1. *The Dirichlet matrix is unitary.*

Proof. The conjucate transpose matrix $D^T = \overline{D'}$ of the matrix D is

$$D^T = \overline{D'} = \frac{1}{\sqrt{p-1}} \left\{ w^{-n\beta(m)} \right\} ,$$

$m, n = 1, 2, ..., p-1$ and so,

$$D \cdot D^T = \frac{1}{p-1} \left\{ \sum_{k=1}^{p-1} w^{(m-n)\beta(k)} \right\} .$$

But

$$\sum_{k=1}^{p-1} w^{(m-n)\beta(k)} == 1 + w^{(m-n)} + w^{2(m-n)} + ... + w^{(p-2)(m-n)} =$$

$$= \frac{w^{(m-n)(p-1)} - 1}{w^{(m-n)} - 1} = \begin{cases} 0 , & m - n \neq 0(\text{mod}(p-1)) , \\ p-1 , & m - n = 0(\text{mod}(p-1)) , \end{cases}$$

and then $D \cdot D^T = I_n$. So, $D^T = D^{-1}$ and D is unitaty.

Let now find the eigenvalues of the matrix $G = DD'$. □

Proposition 2. *The matrix $G = DD'$ is symmetrical and orthognonal with eigenvalues ± 1.*

Proof. Let D' is the transpose of the matrix D. Then

$$G = DD' = D \cdot D = \frac{1}{p-1} \left\{ \sum_{k=1}^{p-1} w^{(m+n)\beta(k)} \right\} , \quad m, n = 1, 2, ..., p-1 .$$

But

$$\sum_{k=1}^{p-1} w^{(m+n)\beta(k)} = \frac{w^{(m+n)(p-1)} - 1}{w^{(m+n)} - 1}$$

$$= \begin{cases} 0\,, & m+n \neq 0(\mathrm{mod}(p-1))\,, \\ p-1\,, & m+n = 0(\mathrm{mod}(p-1))\,, \end{cases}$$

and then

$$G = DD' = \begin{pmatrix} 0 & 0 & . & 1 & 0 \\ . & . & 1 & 0 & . \\ 0 & 1 & . & . & . \\ 1 & 0 & . & . & 0 \\ 0 & 0 & . & 0 & 1 \end{pmatrix}.$$

So, the matrix G is symmetrical because $G' = G$. Therefore, because $GG' = I$, implies that $G^{-1} = G = G'$ and then the matrix G is orthognonal with eigenvalues ± 1. □

Let now the characteristic polynomial of the matrix G, $|G - \lambda I|$.

Proposition 3. *The multiplicity of the eigenvalue $\lambda_1 = 1$ of the matrix G is $k+1$ when $N = 2k$ or $N = 2k+1$ while the multiplicity of the eigenvalue $\lambda_2 = -1$ is $k-1$, when $N = 2k$ and k, when $N = 2k+1$.*

Proof. If $N = 2k+1$ the primary and secondary diagonal have common element, otherwise they have not. For this reason we split the proof in two cases:

1. For $N = 2k$ the factor $1 - \lambda$ appears twice in the primary diagonal of the matrix $G_{2k} - \lambda I$ and we have:

$$|G_{2k} - \lambda I| = \begin{vmatrix} -\lambda & 0 & 0 & . & 1 & 0 \\ 0 & -\lambda & 0 & . & . & 0 \\ . & . & 1-\lambda & . & . & . \\ 0 & 1 & . & -\lambda & . & 0 \\ 1 & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1-\lambda \end{vmatrix}$$

$$= (1-\lambda) \begin{vmatrix} -\lambda & 0 & 0 & . & . & 1 \\ 0 & -\lambda & 0 & . & 1 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & . & 1-\lambda & . & 0 \\ . & . & . & . & . & . \\ 1 & 0 & . & . & 0 & -\lambda \end{vmatrix}$$

$$= (1-\lambda)\begin{vmatrix} -\lambda & 0 & 0 & . & . & . & 0 & 1 \\ 0 & -\lambda & 0 & 0 & . & . & 1 & 0 \\ . & . & . & . & . & . & . & . \\ 0 & 0 & . & -\lambda & 0 & 1 & . & 0 \\ 0 & 0 & . & . & 1-\lambda & 0 & . & 0 \\ 0 & 0 & . & . & 0 & -\lambda+\frac{1}{\lambda} & . & 0 \\ . & . & . & . & . & . & . & . \\ 0 & 0 & . & . & . & 0 & 0 & -\lambda+\frac{1}{\lambda} \end{vmatrix}$$

$$= (1-\lambda)^2(-\lambda)^{k-1}(-\lambda+\frac{1}{\lambda})^{k-1} = (-1)^{k-1}\lambda^{k-1}(1-\lambda)^2\frac{(1-\lambda^2)^{k-1}}{\lambda^{k-1}}$$
$$= (-1)^{k-1}(-1)^{k-1}(\lambda-1)^2(\lambda-1)^{k-1}(\lambda+1)^{k-1}$$
$$= (-1)^{2(k-1)}(\lambda-1)^{k+1}(\lambda+1)^{k-1} = (\lambda-1)^{k+1}(\lambda+1)^{k-1}\,.$$

Let X is the vector $X = (x_1x_2...x_{k-1}x_kx_{k+1}...x_{2k})'$. For $\lambda = 1$ the system $(G_{2k}-I)X = 0$ has the solution

$$x_1 = 1,\quad x_{k+1} = 1,\quad -x_2 + x_{2k} = 0,\quad -x_3 + x_{2k+1} = 0, ...,\ x_3 - x_{2k-1} = 0$$

and $x_2 - x_{2k} = 0$, and for $\lambda = -1$ the system $(G_{2k}+I)X = 0$ has the solution

$$x_1 = x_{k+1} = 0,\quad x_2 + x_{2k} = 0,\quad x_3 + x_{2k-1} = 0, \dots .$$

Then, for $n = 2k$ and for $\lambda = 1$ the matrix G, has the eigenvectors

$$(1,0,....,0,0)',\quad (\overbrace{0,0,...,0,}^{k}1,0,...,0)',\quad (0,1,0,...,0,1)',$$
$$(0,0,1,...,1,0)',...,(0,0,...,1,0,1,...,0)'\ ,$$

with count $k+1$, and for $\lambda = -1$ has the eigenvectors

$$(0,-1,0,...,0,1)',(0,0,-1,...,1,0)',...,(0,0,...,-1,0,1,...,0)'$$

with count $k-1$.

2. For $N = 2k+1$ the factor $1-\lambda$ appears once in the primary diagonal of the matrix $G_{2k+1} - \lambda I$ and we have:

$$|G_{2k+1} - \lambda I| = \begin{vmatrix} -\lambda & 0 & 0 & . & 1 & 0 \\ 0 & -\lambda & 0 & . & . & 0 \\ . & . & -\lambda & . & . & . \\ 0 & 1 & . & -\lambda & . & 0 \\ 1 & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1-\lambda \end{vmatrix}$$

$$
= (1-\lambda)\begin{vmatrix} -\lambda & 0 & 0 & . & . & 1 \\ 0 & -\lambda & 0 & . & 1 & 0 \\ . & . & . & . & . & . \\ 0 & . & -\lambda & 1 & . & 0 \\ 0 & . & 1 & -\lambda & . & 0 \\ . & . & . & . & . & . \\ 1 & 0 & . & . & . & \lambda \end{vmatrix}
$$

$$
= (1-\lambda)\begin{vmatrix} -\lambda & 0 & 0 & . & . & . & 0 & 1 \\ 0 & -\lambda & 0 & . & . & 0 & 1 & 0 \\ . & . & . & . & . & . & . & . \\ 0 & 0 & . & -\lambda & 1 & 0 & . & 0 \\ 0 & 0. & . & 0 & -\lambda+\frac{1}{\lambda} & 0 & . & 0 \\ . & . & . & . & . & . & . & . \\ 0 & 0 & . & . & . & . & 0 & -\lambda+\frac{1}{\lambda} \end{vmatrix}
$$

$$
== (1-\lambda)(-\lambda)^k(-\lambda+\frac{1}{\lambda})^k = (-1)^{k+1}\lambda^k(\lambda-1)\frac{(1-\lambda^2)^k}{\lambda^k}
$$

$$
= (-1)^{2k+1}(\lambda-1)^{k+1}(\lambda+1)^k = -(\lambda-1)^{k+1}(\lambda+1)^k\,.
$$

Let X is the vector $X = (x_1 x_2 ... x_{2k+1})$. For $\lambda = 1$ the system $(G_{2k+1} - I)X = 0$ has the solution

$$
x_1 = 1,\ -x_2 + x_{2k+1} = 0,\ -x_3 + x_{2k} = 0, ..., x_2 - x_{2k+1} = 0\,,
$$

and for $\lambda = -1$ the system $(G_{2k+1} + I)X = 0$ has the solution

$$
x_1 = 1,\ x_2 + x_{2k+1} = 0,\ x_3 + x_{2k} = 0, \ldots.
$$

Then, for $n = 2k+1$ and for $\lambda = 1$ the matrix G, has the eigenvectors

$$
(1,0,...,0,0)',\ (0,1,0,...,0,1)',\ (0,0,1,...,1,0)', ..., (0,0,...,1,1,...,0)'\,,
$$

with count $k+1$, and for $\lambda = -1$ has the eigenvectors

$$
(0,-1,0,...,0,1)',\ (0,0,-1,...,1,0)', ..., (0,0,...,-1,1,...,0)'\,,
$$

with count k.

Summarising, we can see for N odd or even, the multiplicity of the eigenvalues $\lambda_1 = 1$ and $\lambda_2 = -1$ as well as the characteristic polynomial of G_N in the schema below:

	$\lambda = 1$	$\lambda = -1$	$\lvert G - \lambda I \rvert$
$N = 2k$	$k+1$	$k-1$	$(\lambda-1)^{k+1}(\lambda+1)^{k-1}$
$N = 2k+1$	$k+1$	k	$-(\lambda-1)^{k+1}(\lambda+1)^{k}$

3. Spectra Analysis of the Matrix DD', D the Dirichlet Matrix

Let an n-square matrix A such that its minimal polynomial $m(t)$ has the form

$$m(t) = (t-\lambda_1)(t-\lambda_2)\dots(t-\lambda_\mu)\ ,$$

where $\lambda_1, \lambda_2, \dots, \lambda_\mu$ are the distinct eigenvalues of A. In this case, the space K^n is the direct sum of its subspaces $\mathrm{Ker}(A-\lambda_i I)$, for $i = 1, 2, \dots, \mu$, and the spectra analysis of the matrix A is

$$A = \lambda_1 P_1 + \lambda_2 P_2 + \dots + \lambda_\mu P_\mu\ ,$$

where $P_1, P_2, \dots, P_\mu$ are the projection matrices, which they project an arbitrary vector of K^n, to its above subspaces.

Now we have

$$\frac{1}{m(t)} = \frac{1}{\prod\limits_{i=1}^{\mu}(t-\lambda_i)} = \sum_{i=1}^{\mu}\frac{a_i}{t-\lambda_i} = \frac{\sum\limits_{j=1}^{\mu}\{a_j \prod\limits_{\substack{i=1\\ j\neq i}}^{\mu}(t-\lambda_i)\}}{\prod\limits_{i=1}^{\mu}(t-\lambda_i)}\ ,$$

and then

$$a_j = \frac{1}{\prod\limits_{\substack{i=1\\ j\neq i}}^{\mu}(\lambda_j-\lambda_i)}, \quad j = 1, 2, \dots, \mu\ ,$$

and if

$$g_j(t) = \prod_{\substack{i=1\\ j\neq i}}^{\mu}(t-\lambda_i) \text{ and } \beta_j(t) = a_j g_j(t), \quad j = 1, 2, .., \mu\ ,$$

we can rewrite the $1/m(t)$ as

$$\frac{1}{m(t)} = \frac{\sum\limits_{j=1}^{\mu}\beta_j(t)}{\prod\limits_{i=1}^{\mu}(t-\lambda_i)}\ .$$

In such a case, the projection matrices P_j, $j = 1, 2, .., \mu$ are given from the relations

$$P_j = \beta_j(A) = \frac{\prod\limits_{\substack{i=1\\ i\neq j}}^{\mu}(A-\lambda_i I)}{\prod\limits_{\substack{i=1\\ i\neq j}}^{\mu}(\lambda_j-\lambda_i)}, \quad j = 1, 2, \dots, \mu\ .$$

Let now the matrix A be the matrix G (which is equal to G^{-1}) of order n. In this case, because for each n, the distinct eigenvalues of G and G^{-1} are $\lambda_1 = 1, \lambda_2 = -1$ respectively, implied that the space K^n it is analyzed for each n, to the direct sum of its subspaces

$$Ker\,(G - \lambda_i I)\,, \quad i = 1, 2$$

which are orthogonal to each other. In fact, if u and v are arbitrary vectors of the subspaces of K^n that corresponds to the eigenvalues of G, λ_1 and λ_2, will be

$$Du = \lambda_1 u \;\text{ and }\; Dv = \lambda_2 v\,.$$

Therefore we will have

$$< Du, Dv >=< \lambda_1 u, \lambda_2 v >= \lambda_1 < u, \lambda_2 v >= \lambda_i \lambda_2 < u, v > \;.$$

But it is

$$< Du, Dv >=< u, v >\,,$$

so

$$< u, v > (\lambda_1 \lambda_2 - 1) = 0\,.$$

But for $\lambda_1 = 1, \lambda_2 = -1$ is $\lambda_1 \lambda_2 - 1 \neq 0$. So, $< u, v >= 0$, and so its true that the subspaces are orthogonal to each other.

After all these, the spectra analysis of the matrix $G = DD'$ is $G = P_1 - P_2$, where

$$P_1 = \frac{(G - \lambda_2 I)}{(\lambda_1 - \lambda_2)} \;\text{ and }\; P_2 = \frac{(G - \lambda_1 I)}{(\lambda_2 - \lambda_1)}\,,$$

$$P_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 & . & 1 & 0 \\ 0 & 1 & . & . & 0 \\ . & 1 & . & . & . \\ 1 & . & . & . & . \\ 0 & 0 & 0 & . & 2 \end{pmatrix} \;\text{ and }\; P_2 = -\frac{1}{2}\begin{pmatrix} -1 & 0 & . & 1 & 0 \\ 0 & -1 & . & . & 0 \\ . & 1 & . & . & . \\ 1 & . & . & . & . \\ 0 & 0 & 0 & . & 0 \end{pmatrix}.$$

Let now v is a vector of K^n. Because $G^2 v = Iv = v$ and because $I = P_1 + P_2$ we have that

$$v = P_1 v + P_2 v \;\text{ and }\; Gv = G_1 v - G_2 v\,.$$

The eigenvectors $P_1 v$ and $P_2 v$ are eigenvectors of G, which correspond to the eigenvalues 1 and -1, because

$$G(P_1 v) = (P_1 - P_2)(P_1 v) = P_1^2 v - P_1 P_2 v = P_1 v \;\text{ and }\; G(P_2 v) = -P_2 v\,.$$

So, because $v = P_1v + P_2v$ and $Gv = G_1v - G_2v$, it follows that if we multiply an arbitrary vector v of R^n with G, the vector is reflected as for the direction, who detemined from the eigenvector of G, which corresponds to its eigenvalue 1. So, if $a = (a_1, a_2, ..., a_N)$ is a vector of R^N, we will have

$$Ga' = (a_{N-1}, a_{N-2}, ..., a_2, a_1|a_N)' \quad \text{and} \quad aG = (a_{N-1}, a_{N-2}, ..., a_2, a_1|a_N) \ .$$

References

[1] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer Verlang, New York (1976).

[2] R. Crandall, *Mathematica for the Sciences*, Addisson Wesley (1995).

[3] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, 5-th Edition, Clarendon, Oxford (1979).

[4] Hewlett Packard Co, *Spectrum Analysis*, AN 63 and AN 63A, Palo Alto, CA (1965).

[5] H. Hsu, *Fourier Analysis*, Simon and Schuster (1970).

[6] J.H. McClellan, C.M. Rader, *Number theory in Digital Signal Processing*, Prentice Hall, Englewood Clifs, NJ (1979).

[7] A. Papoulis, *Signal Analysis*, McGraw Hill (1977).

[8] M.R. Schroeder, *Number Theory in Science and Communication*, Springer Verlag, New York (1984).

[9] H. Terzidis, G. Danas, The spectral analysis of the periods of the inverses of integers, *Jour. Inst. Maths. and Comp. Sciences (Comp. Sc. Ser.)*, **10**, No. 1 (1999), 61-69.

[10] H. Terzidis, G. Danas, The systems of primitive roots. The degree and rank of prime numbers, *Intern. J. Computer Math.*, **73** (1999), 469-478.

[11] H. Terzidis, G. Danas, The spectral analysis of the discrete Fourier transform, *Handronic Journal*, **24** (2001), 225-240.

[12] H. Terzidis, G. Danas, The periods of the inverses of integers, *NNTDM*, **8**, No. 1 (2002), 1-20.

[13] H. Terzidis, P. Tzekis, Fourier transform of the sequences of the primitive roots of the prime numbers, *Acad. Op. Int. J.*, **18** (2006).