ACTA ARITHMETICA
115.3 (2004)

Determinants of Legendre symbol matrices

by

Robin Chapman (Exeter)

1. Introduction. When studying lattices constructed from quadratic residue codes and their generalizations, the author needed to prove that $\det N_p = \pm 1$ where p is an odd prime and N_p is the $\frac{1}{2}(p+1)$ by $\frac{1}{2}(p+1)$ matrix with entries

$$(N_p)_{j,k} = \begin{cases} \dfrac{1}{2}\left[1 - \left(\dfrac{k-j+(p-1)/2}{p}\right)\right] & \text{if } 1 \le j \le \frac{1}{2}(p-1), \\ 1 & \text{if } j = \frac{1}{2}(p+1). \end{cases}$$

Here $\left(\frac{t}{p}\right)$ denotes the Legendre symbol of t modulo p. The argument was to show that this integer matrix was nonsingular modulo every prime, and proving this used properties of quadratic residue codes over finite fields. The author was then led into investigating the minors of the matrix N_p and the sign of $\det N_p$. We report the results of this investigation here.

The northwest and northeast minors of N can be easily derived from the $\frac{1}{2}(p-1)$ by $\frac{1}{2}(p-1)$ matrix $C_p(x)$ with (j,k)-entry $x + \left(\frac{j+k-1}{p}\right)$ where x is an indeterminate. It is convenient to consider $C_p(x)$ in tandem with the $\frac{1}{2}(p+1)$ by $\frac{1}{2}(p+1)$ matrix $C_p^*(x)$ with (j,k)-entry $x + \left(\frac{j+k-1}{p}\right)$. Corollary 3 to Theorem 2 below gives the values of $\det C_p(x)$ and $\det C_p^*(x)$. The proof of Theorem 2 involves analogues of quadratic residue codes defined over the complex numbers.

A preliminary section fixes notation and proves the basic properties of complex quadratic residue codes. The proof of the main theorem follows. After this we consider some other determinants evaluable by the same method, including that of a matrix D_p closely related to N_p defined above. Finally we make some remarks comparing and contrasting other determinant evaluations in the literature.

The author wishes to thank the many mathematicians who have commented on this problem to him, notably Roland Bacher, Neil Sloane and

2000 *Mathematics Subject Classification*: Primary 11C20.

especially Benne de Weger who helped to simplify his original arguments greatly, and also Bill Hart for pointing out various errors in earlier versions.

2. Quadratic residue codes over $\mathbb{C}$. We require some preliminaries on quadratic residue codes over $\mathbb{C}$. These will be defined by analogy with the quadratic residue codes over finite fields used in the theory of error-correcting codes.

Fix an odd prime p and let $\mathcal{A} = \mathbb{C}[T]/\langle T^p - 1\rangle$. We may identify this quotient ring with the vector space $\mathbb{C}^p$ with the polynomial $\sum_{j=0}^{p-1} a_j T^j$ corresponding to the vector $(a_0, \ldots, a_{p-1})$.

Let $\zeta = \exp(2\pi i/p)$ be a primitive pth root of unity and let

$$\boldsymbol{\mu} = \{\zeta^j : 0 \le j < p\}$$

denote the group of all pth roots of unity in $\mathbb{C}$. Define $\boldsymbol{\mu}^+$ as the set of $\zeta^j \in \boldsymbol{\mu}$ with $\left(\frac{j}{p}\right) = 1$ and $\boldsymbol{\mu}^-$ as the set of $\zeta^j \in \boldsymbol{\mu}$ with $\left(\frac{j}{p}\right) = -1$. Thus $\boldsymbol{\mu}$ is the disjoint union of $\boldsymbol{\mu}^+$, $\boldsymbol{\mu}^-$ and $\{1\}$. Note that

$$\boldsymbol{\mu}^+ = \left\{\zeta^{k^2} : 1 \le k \le \tfrac{1}{2}(p-1)\right\}, \quad \{1\} \cup \boldsymbol{\mu}^+ = \left\{\zeta^{k^2} : 0 \le k \le \tfrac{1}{2}(p-1)\right\}.$$

Let

$$\tau_p = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta^j.$$

This Gauss sum satisfies $\tau_p^2 = (-1)^{(p-1)/2} p$; indeed

$$\tau_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

a result due to Gauss, [1, Chapter 5, Section 4, Theorem 7]. Moreover

$$\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta^{jk} = \left(\frac{k}{p}\right) \tau_p$$

for all integers k. For $p \equiv 3 \pmod 4$ let h_{-p} denote the class number of the quadratic field $\mathbb{Q}(i\sqrt{p})$, and for $p \equiv 1 \pmod 4$ let h_p denote the class number of the quadratic field $\mathbb{Q}(\sqrt{p})$ and ε_p denote its fundamental unit satisfying $\varepsilon_p > 1$.

If $f \in \mathcal{A}$, it is meaningful to write $f(\eta)$ for $\eta \in \boldsymbol{\mu}$. Define

$$\mathcal{Q} = \{f \in \mathcal{A} : f(\eta) = 0 \text{ for all } \eta \in \boldsymbol{\mu}^-\}.$$

Equivalently $\mathcal{Q}$ is the set of $(a_0, \ldots, a_{p-1}) \in \mathbb{C}^p$ with $\sum_{j=0}^{p-1} a_j \eta^j = 0$ for all $\eta \in \boldsymbol{\mu}^-$. We regard $\mathcal{Q}$ as our complex analogue of a quadratic residue code. Clearly $\mathcal{Q}$ is an ideal of $\mathcal{A}$, with dimension $\frac{1}{2}(p+1)$ over $\mathbb{C}$, and is generated by

$$G(T) = \prod_{\eta \in \boldsymbol{\mu}^-} (T - \eta) = T^{(p-1)/2} + \sum_{j=0}^{(p-3)/2} g_j T^j.$$

Considered as a vector subspace of $\mathbb{C}^p$, $\mathcal{Q}$ is generated by the rows of the $\frac{1}{2}(p+1)/2$ by p matrix

$$\Gamma = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{(p-3)/2} & 1 & 0 & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{(p-5)/2} & g_{(p-3)/2} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & g_0 & g_1 & g_2 & \cdots & 1 \end{pmatrix}.$$

We shall require some examples of polynomials in $\mathcal{Q}$. Let

$$F = \tau_p + \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) T^j, \qquad U = \sum_{j=0}^{p-1} T^j.$$

For $\eta = \zeta^k \in \boldsymbol{\mu}$,

$$F(\eta) = \tau_p + \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta^{jk} = \tau_p + \left(\frac{k}{p}\right) \tau_p = \begin{cases} \tau_p & \text{if } \eta = 1, \\ 2\tau_p & \text{if } \eta \in \boldsymbol{\mu}^+, \\ 0 & \text{if } \eta \in \boldsymbol{\mu}^-, \end{cases}$$

and

$$U(\eta) = \begin{cases} p & \text{if } \eta = 1, \\ 0 & \text{if } \eta \in \boldsymbol{\mu}^+ \cup \boldsymbol{\mu}^-, \end{cases}$$

so that $F, U \in \mathcal{Q}$.

We now prove a lemma concerning the evaluation of size $\frac{1}{2}(p+1)$ determinants by means of evaluating polynomials at roots of unity. Let M be an r by p matrix each row of which lies in $\mathcal{Q}$. Then these rows correspond to polynomials $f_1, \ldots, f_r \in \mathcal{A}$. Define an r by $\frac{1}{2}(p+1)$ matrix $\Phi(M)$ by

$$\Phi(M)_{j,k} = f_j(\zeta^{k^2}) \quad (1 \le j \le \tfrac{1}{2}(p+1),\ 0 \le k \le \tfrac{1}{2}(p-1)).$$

When $r = \frac{1}{2}(p+1)$ the matrix $\Phi(M)$ is square and so has a determinant.

LEMMA 1. *Let M be a $\frac{1}{2}(p+1)$ by p matrix all of whose rows lie in $\mathcal{Q}$. Then*

$$\det M' = \frac{\det \Phi(M)}{\det \Phi(\Gamma)}$$

where M' is the matrix consisting of the last $\frac{1}{2}(p+1)$ columns of M.

Proof. By hypothesis, $M = A\Gamma$ for some matrix A. Hence $M' = A\Gamma'$ where Γ' is the matrix consisting of the last $\frac{1}{2}(p+1)$ columns of Γ. But Γ' is lower triangular with all diagonal entries equal to 1, and so $\det M' = \det A$.

Let $\mathbf{v}_\eta = (1, \eta, \eta^2, \dots, \eta^{p-1})^{\mathrm{t}}$ and $\mathbf{w}_\eta = (1, \eta, \eta^2, \dots, \eta^{(p-1)/2})^{\mathrm{t}}$ for $\eta \in \boldsymbol{\mu}$. Since the rows of Γ are cyclic shifts of the first row, it follows that

$$\Gamma \mathbf{v}_\eta = G(\eta)\mathbf{w}_\eta.$$

For $\eta \in \{1\} \cup \boldsymbol{\mu}^+$, $G(\eta) \neq 0$. Let V be the matrix with columns $\mathbf{v}_{\zeta^{k^2}}$ for $0 \le k \le \frac{1}{2}(p+1)$. The columns of ΓV are then the vectors $G(\zeta^{k^2})\mathbf{w}_{\zeta^{k^2}}$ for $0 \le k \le \frac{1}{2}(p+1)$, which are linearly independent (by the nonsingularity of a Vandermonde matrix). Now $MV = \Phi(M)$, $\Gamma V = \Phi(\Gamma)$ and $M = A\Gamma$. Hence $\Phi(M) = A\Gamma V = A\Phi(\Gamma)$. As $\Phi(\Gamma)$ is nonsingular we conclude that

$$\det M' = \det A = \frac{\det \Phi(M)}{\det \Phi(\Gamma)}. \ \blacksquare$$

The matrix $\Phi(\Gamma)$ is a Vandermonde matrix multiplied by a diagonal matrix, and so has determinant

$$\prod_{\eta \in \{1\} \cup \boldsymbol{\mu}^+} G(\eta) \cdot \prod_{0 \le j < k \le (p-1)/2} (\zeta^{k^2} - \zeta^{j^2}).$$

3. The main theorem. We now state and prove the main theorem. Recall that $C_p(x)$ and $C_p^*(x)$ are the square matrices of sizes $\frac{1}{2}(p-1)$ and $\frac{1}{2}(p+1)$ with (j,k)-entry $x + \binom{j+k-1}{p}$. It is plain that $\det C_p(x)$ and $\det C_p^*(x)$ are linear polynomials in the indeterminate x.

We evaluate $\det C_p(x)$ and $\det C_p^*(x)$ by introducing a square matrix $M_p(x,y)$ of size $\frac{1}{2}(p+1)$ containing a further indeterminate y. Its entries are

$$M_p(x,y)_{j,k} = \begin{cases} x + \left(\dfrac{j+k-1}{p}\right) & \text{if } 1 \le j+k-1 < p, \\ x + y & \text{if } j+k-1 = p. \end{cases}$$

The only entry in $M_p(x,y)$ containing y is that in the lower right corner. As $M_p(x,0) = C_p^*(x)$ and as deleting the last row and last column of $M_p(x,y)$ yields $C_p(x)$, it follows that

$$\det M_p(x,y) = \det C_p^*(x) + y \det C_p(x).$$

Since $M_p(x,y)$ is a polynomial with integer coefficients, to evaluate $\det C_p(x)$ and $\det C_p^*(x)$ it suffices to calculate $M_p(x,y)$ for some irrational value of y, and it turns out that the Gauss sum τ_p is a particularly convenient choice.

THEOREM 2. *Let $p \ge 5$ be prime. If $p \equiv 3 \pmod 4$ then*

$$\det M_p(x,y) = 2^{(p-1)/2}(1 - xy).$$

If $p \equiv 1 \pmod 4$ then

$$\det M_p(x, \sqrt{p}) = (-1)^{(p-1)/4} 2^{(p-1)/2} (1 + x\sqrt{p}) \varepsilon_p^{-h_p}.$$

Proof. Define a $\frac{1}{2}(p+1)$ by p matrix $N_p(x,y)$ as follows:

$$(N_p(x,y))_{i,j} = \begin{cases} \left(\dfrac{j-i}{p}\right) + x & \text{if } j \neq i, \\ x+y & \text{if } j = i. \end{cases}$$

The key observation here is that $M_p(x,y)$ is essentially the submatrix $N'_p(x,y)$ formed by taking the last $(p+1)/2$ columns of $N_p(x,y)$. In detail, if $p \equiv 1 \pmod 4$ then $M_p(x,y)$ is the left-right reflection of $N'_p(x,y)$ and if $p \equiv 3 \pmod 4$ then $M_p(x,y)$ is the left-right reflection of $-N'_p(-x,-y)$. Thus

$$\det M_p(x,y) = \begin{cases} (-1)^{(p-1)/4} \det N'_p(x,y) & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{(p+1)/4} \det N'_p(-x,-y) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

We evaluate $\det N'_p(x,\tau_p)$ by using Lemma 1.

Regard the rows of $N_p(x,\tau_p)$ as elements of $\mathcal{A} \cong \mathbb{C}^p$. The polynomial corresponding to the $(k+1)$th row $(0 \le k \le \frac{1}{2}(p-1))$ is

$$F_k(T) = \tau_p T^k + \sum_{j=1}^{p-1-k} \left(\frac{j}{p}\right) T^{k+j} + \sum_{j=p-k}^{p-1} \left(\frac{j}{p}\right) T^{k+j-p} + x \sum_{j=0}^{p-1} T^j.$$

In the ring $\mathcal{A}$ this equals $T^k F(T) + xU(T)$. As $\mathcal{Q}$ is an ideal of $\mathcal{A}$ and $F, U \in \mathcal{Q}$, we have $F_k \in \mathcal{Q}$.

By Lemma 1,

$$\det N'_p(x,\tau_p) = \frac{\det \Phi(N_p(x,\tau_p))}{\det \Phi(\Gamma)}.$$

The entries of the matrix $\Phi(N_p(x,\tau_p))$ are

$$F_j(\zeta^{k^2}) = \zeta^{jk^2}(F(\zeta^{k^2}) + xU(\zeta^{k^2}))$$

for $0 \le j,k \le \frac{1}{2}(p-1)$ while those of $\Phi(\Gamma)$ are $\zeta^{jk^2} G(\zeta^{k^2})$. Thus each column of $\Phi(N_p(x,\tau_p))$ is a scalar multiple of the corresponding column of $\Phi(\Gamma)$ and we conclude that

$$(*) \qquad \det N'_p(x,\tau_p) = \prod_{\eta \in \{1\} \cup \boldsymbol{\mu}^+} \frac{F(\eta) + xU(\eta)}{G(\eta)} = \frac{F(1)+px}{G(1)} \prod_{\eta \in \boldsymbol{\mu}^+} \frac{F(\eta)}{G(\eta)}.$$

The numerator of $(*)$ is

$$(F(1)+px) \prod_{\eta \in \boldsymbol{\mu}^+} F(\eta) = (\tau_p + px)(2\tau_p)^{(p-1)/2}.$$

The denominator of $(*)$ is

$$G(1) \prod_{j=1}^{(p-1)/2} G(\zeta^{j^2}) = \prod_{\eta \in \boldsymbol{\mu}^-} (1-\eta) \cdot \prod_{j=1}^{(p-1)/2} \prod_{\eta \in \boldsymbol{\mu}^-} (\zeta^{j^2} - \eta)$$

$$= \prod_{\eta\in\boldsymbol{\mu}^-}(1-\eta)\cdot\prod_{j=1}^{(p-1)/2}\prod_{\eta\in\boldsymbol{\mu}^-}\zeta^{j^2}(1-\eta\zeta^{-j^2}).$$

Now

$$\sum_{j=1}^{(p-1)/2} j^2 = \frac{p}{6}\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) = p\left(\frac{p^2-1}{24}\right).$$

As long as $p\geq 5$, $(p^2-1)/24$ is an integer and so $\prod_{j=1}^{(p-1)/2}\zeta^{j^2}=1$. Consequently,

$$\prod_{\eta\in\{1\}\cup\boldsymbol{\mu}^+} G(\eta) = \prod_{\eta'\in\{1\}\cup\boldsymbol{\mu}^+}\prod_{\eta\in\boldsymbol{\mu}^-}(1-\eta/\eta').$$

To proceed further, we divide into cases according to the congruence class of p modulo 4. Let Q and N denote the sets of quadratic residues and quadratic nonresidues of p in $\{1,\dots,p-1\}$.

Suppose first that $p\equiv 3 \pmod 4$ (and that $p>3$). Note that $\tau_p^2=-p$. In this case -1 is a quadratic nonresidue modulo p. Then

$$\prod_{\eta\in\{1\}\cup\boldsymbol{\mu}^+} G(\eta) = \prod_{j\in N}(1-\zeta^j)\cdot\prod_{j\in N,\,k\in Q}(1-\zeta^{j-k}).$$

It is an easy exercise to show that if $a\in Q$ then ζ^a appears $(p+1)/4$ times as ζ^{j-k} for $j\in N$ and $k\in Q$ and if $a\in N$ then ζ^a appears $(p-3)/4$ times as ζ^{j-k} for $j\in N$ and $k\in Q$. Hence

$$\prod_{\eta\in\{1\}\cup\boldsymbol{\mu}^+} G(\eta) = \prod_{a=1}^{p-1}(1-\zeta^a)^{(p+1)/4} = p^{(p+1)/4}$$

and so

$$\begin{aligned}\det N_p'(x,\tau_p) &= \frac{2^{(p-1)/2}(\tau_p+px)\tau_p(-p)^{(p-3)/4}}{p^{(p+1)/4}}\\ &= (-1)^{(p+1)/4}2^{(p-1)/2}(1-x\tau_p).\end{aligned}$$

Thus

$$\det M_p(-x,-\tau_p) = (-1)^{(p+1)/4}\det N_p'(x,\tau_p) = 2^{(p-1)/2}(1-x\tau_p),$$

and so

$$\det M_p(x,y) = 2^{(p-1)/2}(1-xy).$$

Suppose now that $p\equiv 1 \pmod 4$. In this case -1 is a quadratic residue modulo p. Then

$$\prod_{\eta\in\{1\}\cup\boldsymbol{\mu}^+} G(\eta) = \prod_{j\in N}(1-\zeta^j)\cdot\prod_{j\in N,\,k\in Q}(1-\zeta^{j-k}).$$

It is an easy exercise to show, for all a not divisible by p, that ζ^a appears $(p-1)/4$ times as ζ^{j-k} for $j \in N$ and $k \in Q$. Hence

$$\prod_{\eta \in \{1\} \cup \boldsymbol{\mu}^+} G(\eta) = \prod_{j \in N} (1-\zeta^j) \cdot \prod_{a=1}^{p-1} (1-\zeta^a)^{(p-1)/4} = p^{(p-1)/4} \prod_{j \in N} (1-\zeta^j).$$

As a consequence of the analytic class number formula [1, Chapter 5, Section 4, Theorem 2],

$$\prod_{j \in N} (1-\zeta^j) = \varepsilon_p^{h_p} \sqrt{p}.$$

It follows that

$$\det N'_p(x,y) = \frac{2^{(p-1)/2} (\sqrt{p})^{(p-1)/2} (\sqrt{p} + xp)}{p^{(p-1)/4} \varepsilon_p^{h_p} \sqrt{p}} = 2^{(p-1)/2} (1 + x\sqrt{p}) \varepsilon_p^{-h_p}.$$

Consequently,

$$\begin{aligned} \det M_p(x, \sqrt{p}) &= (-1)^{(p-1)/4} \det N'_p(x, \sqrt{p}) \\ &= (-1)^{(p-1)/4} 2^{(p-1)/2} (1 + x\sqrt{p}) \varepsilon_p^{-h_p}. \ \blacksquare \end{aligned}$$

We can now evaluate $\det C_p(x)$ and $\det C_p^*(x)$. To state the results for $p \equiv 1 \pmod 4$, we write $\varepsilon_p^{h_p} = \alpha_p + \beta_p \sqrt{p}$ where $\alpha_p, \beta_p \in \mathbb{Q}$.

COROLLARY 3. *Let $p \geq 5$ be prime. If $p \equiv 3 \pmod 4$ then*

$$\det C_p(x) = -2^{(p-1)/2} x, \quad \det C_p^*(x) = 2^{(p-1)/2}.$$

If $p \equiv 1 \pmod 4$ then

$$\begin{aligned} \det C_p(x) &= (-1)^{(p-1)/4} 2^{(p-1)/2} (\beta_p - \alpha_p x), \\ \det C_p^*(x) &= (-1)^{(p-1)/4} 2^{(p-1)/2} (p\beta_p x - \alpha_p). \end{aligned}$$

Proof. Note that $\det M_p(x,y) = \det C_p^*(x) + y \det C_p(x)$.

Suppose first that $p \equiv 3 \pmod 4$. Then

$$\det M_p(x,y) = 2^{(p-1)/2} (1 - xy)$$

and so

$$\det C_p(x) = -2^{(p-1)/2} x, \quad \det C_p^*(x) = 2^{(p-1)/2}.$$

Now suppose that $p \equiv 1 \pmod 4$. As ε_p has norm -1 and h_p is odd [4, Chapter XI, Theorems 4 and 6], $\varepsilon_p^{-h_p} = -\alpha_p + \beta_p \sqrt{p}$ and so

$$\det M_p(x, \sqrt{p}) = (-1)^{(p-1)/4} 2^{(p-1)/2} [(p\beta_p x - \alpha_p) + (\beta_p - \alpha_p x)\sqrt{p}\,]$$

or

$$\det M_p(x,y) = (-1)^{(p-1)/4} 2^{(p-1)/2} [(p\beta_p x - \alpha_p) + (\beta_p - \alpha_p x) y].$$

Hence

$$\det C_p(x) = (-1)^{(p-1)/4}2^{(p-1)/2}(\beta_p - \alpha_p x),$$
$$\det C_p^*(x) = (-1)^{(p-1)/4}2^{(p-1)/2}(p\beta_p x - \alpha_p). \blacksquare$$

4. Related determinants. We first consider a related determinant which was evaluated, up to sign, in [3]. We re-evaluate this and determine the sign.

For each odd prime p we define a matrix D_p as follows. The matrix D_p is square of size $\frac{1}{2}(p+1)$ and its entries are given by

$$(D_p)_{i,j} = \begin{cases} \left(\dfrac{j-i+(p-1)/2}{p}\right) & \text{if } j \le (p-1)/2, \\ 1 & \text{if } j = (p+1)/2. \end{cases}$$

In brief, D_p is the same as the matrix $N_p'(0,y)$ of Theorem 2 except that its final row consists entirely of ones (thus eliminating the dependence on y). We shall show that $\det D_p = \pm 2^{(p-1)/2}$ where the plus sign is taken if $p \equiv 1 \pmod 4$ and where the sign depends on a class number when $p \equiv 3 \pmod 4$. (This matrix D_p may be readily transformed by row and column operations into the matrix denoted by N_p in the introduction).

We need a lemma on class numbers, which surely must be well known, but for which we lack a reference.

LEMMA 4. *Let p be a prime congruent to 3 modulo 4 with $p > 3$. Then*

$$\prod_{j=1}^{(p-1)/2} (1 - \zeta^{j^2}) = -(-1)^{(h_{-p}-1)/2} i\sqrt{p}.$$

Proof. Let P denote this product. Then

$$|P|^2 = \prod_{k=1}^{p-1}(1-\zeta^k) = p$$

so we only need to prove that $P/|P| = -(-1)^{(h_{-p}-1)/2}i$. Now

$$P = \prod_{j=1}^{(p-1)/2} (1-\zeta^{4j^2}) = \prod_{j=1}^{(p-1)/2} (-\zeta^{2j^2})(\zeta^{2j^2} - \zeta^{-2j^2})$$
$$= \prod_{j=1}^{(p-1)/2} (-2i\zeta^{2j^2}) \sin(4\pi j^2/p).$$

Hence

$$P/|P| = (-i)^{(p-1)/2}(-1)^a \prod_{j=1}^{(p-1)/2} \zeta^{2j^2}$$

where a is the number of integers k in the open interval $(p/2, p)$ for which $\left(\frac{2k}{p}\right) = 1$. Now

$$\prod_{j=1}^{(p-1)/2} \zeta^{2j^2} = \zeta^{p(p^2-1)/12} = 1$$

and so

$$P/|P| = -(-1)^{a+(p-3)/4} i.$$

Let a_+ be the number of integers $k \in (p/2, p)$ with $\left(\frac{k}{p}\right) = 1$ and a_- be the number of integers $k \in (p/2, p)$ with $\left(\frac{k}{p}\right) = -1$. Then $a_+ + a_- = \frac{1}{2}(p-1)$ and, by the analytic class number formula,

$$a_- - a_+ = \left(2 - \left(\frac{2}{p}\right)\right) h_{-p}$$

[1, Chapter 5, Section 4, Theorem 4].

When $p \equiv 3 \pmod 8$, $\left(\frac{2}{p}\right) = -1$ and then $a = a_-$ and $a_- - a_+ = 3h_{-p}$. As $\frac{1}{4}(p-3)$ is even, $P/|P| = -(-1)^a i$. Now $2a = 3h_{-p} + \frac{1}{2}(p-1) \equiv 1 - h_{-p} \pmod 4$ and so

$$P/|P| = -(-1)^{(1-h_{-p})/2} i = -(-1)^{(h_{-p}-1)/2} i.$$

When $p \equiv 7 \pmod 8$, $\left(\frac{2}{p}\right) = 1$ and then $a = a_+$ and $a_- - a_+ = h_{-p}$. As $\frac{1}{4}(p-3)$ is odd, $P/|P| = (-1)^a i$. Now $2a = -h + \frac{1}{2}(p-1) \equiv 3 - h \pmod 4$ and so

$$P/|P| = (-1)^{(3-h_{-p})/2} i = (-1)^{(h_{-p}-3)/2} i = -(-1)^{(h_{-p}-1)/2} i.$$

Hence in all cases

$$P = -(-1)^{(h_{-p}-1)/2} i\sqrt{p}. \quad \blacksquare$$

We now state and prove the evaluation of $\det D_p$.

THEOREM 5. *Let p be a prime with $p \geq 5$. If $p \equiv 1 \pmod 4$ then*

$$\det D_p = 2^{(p-1)/2}.$$

If $p \equiv 3 \pmod 4$ then

$$\det D_p = (-1)^{(p+1)/4+(h_{-p}-1)/2} 2^{(p-1)/2}.$$

Proof. We use a similar argument to the proof of Theorem 2. We omit details resembling those in the earlier proof.

Let R be the $\frac{1}{2}(p+1)$ by p matrix with entries

$$(R)_{i,j} = \begin{cases} \left(\dfrac{j-i}{p}\right) & \text{if } j \leq (p-1)/2 \text{ and } i \neq j, \\ \tau_p & \text{if } j \leq (p-1)/2 \text{ and } i = j, \\ 1 & \text{if } j = (p+1)/2, \end{cases}$$

so that D_p is formed by the last $\frac{1}{2}(p+1)$ columns of R. The first $\frac{1}{2}(p-1)$ rows of R correspond to the polynomials $F(T)$, $TF(T), \dots, T^{(p-1)/3}F(T) \in \mathcal{Q}$ and the last to $U(T) \in \mathcal{Q}$. By Lemma 1,

$$\det D_p = \frac{\det \Phi(R)}{\det \Phi(\Gamma)}.$$

The bottom row of $\Phi(R)$ is $(p, 0, \dots, 0)$ while the entries in the other rows are $\zeta^{jk^2}F(\zeta^{k^2})$ for $0 \le j \le \frac{1}{2}(p-3)$ and $0 \le k \le \frac{1}{2}(p-1)$. Thus

$$\det \Phi(R) = (-1)^{(p-1)/2} p \det S \prod_{k=1}^{(p-1)/2} F(\zeta^{k^2})$$

where S is the size $\frac{1}{2}(p-1)$ Vandermonde matrix with second row entries ζ^{k^2} for $1 \le k \le \frac{1}{2}(p-1)$. From the proof of Theorem 2 it follows that

$$\det \Phi(\Gamma) = \det T \prod_{k=0}^{(p-1)/2} G(\zeta^{k^2})$$

where T is the size $\frac{1}{2}(p+1)$ Vandermonde matrix with second row entries ζ^{k^2} for $1 \le k \le \frac{1}{2}(p+1)$.

As $\tau_p^2 = (-1)^{(p-1)/2}p$ and $F(1) = \tau_p$ it follows from the formula for the Vandermonde determinant that

$$\det D_p = \tau_p \prod_{\eta \in \{1\} \cup \boldsymbol{\mu}^+} \frac{F(\eta)}{G(\eta)} \cdot \prod_{\eta \in \boldsymbol{\mu}^+} \frac{1}{\eta - 1}.$$

The product $\prod_{\eta \in \{1\} \cup \boldsymbol{\mu}^+} F(\eta)/G(\eta)$ was, in effect, computed in the proof of Theorem 2 (in the case $x = 0$):

$$\prod_{\eta \in \{1\} \cup \boldsymbol{\mu}^+} \frac{F(\eta)}{G(\eta)} = \begin{cases} 2^{(p-1)/2} \varepsilon_p^{-h_p} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{(p+1)/4} 2^{(p-1)/2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Now

$$\prod_{\eta \in \boldsymbol{\mu}^+} (\eta - 1) = (-1)^{(p-1)/2} \prod_{j=1}^{(p-1)/2} (1 - \zeta^{j^2}).$$

When $p \equiv 1 \pmod 4$ then

$$\prod_{j=1}^{(p-1)/2} (1 - \zeta^{j^2}) = \varepsilon_p^{-h_p} \sqrt{p}$$

and so $\det D_p = 2^{(p-1)/2}$.

When $p \equiv 3 \pmod 4$ then

$$\prod_{j=1}^{(p-1)/2} (1-\zeta^{j^2}) = -(-1)^{(h_p-1)/2} i\sqrt{p}$$

and so $\det D_p = (-1)^{(h_p-1)/2+(p+1)/4} 2^{(p-1)/2}$. ∎

We now consider matrices related to those in Theorem 2, but differing in the final row.

Define a $\frac{1}{2}(p+1)$ by $\frac{1}{2}(p+1)$ matrix $M_p^{(r)}(x,y)$, where $0 \le r \le \frac{1}{2}(p-1)$, as follows:

$$M_p^{(r)}(x,y)_{j,k} = \begin{cases} \left(\dfrac{j+k-1}{p}\right) + x & \text{if } 1 \le j \le \frac{1}{2}(p-1), \\ \left(\dfrac{r+j+k-1}{p}\right) + x & \text{if } j = \frac{1}{2}(p+1) \text{ and } k \ne \frac{1}{2}(p+1) - r, \\ x+y & \text{if } j = \frac{1}{2}(p+1) \text{ and } k = \frac{1}{2}(p+1) - r. \end{cases}$$

Note that $M_p^{(0)}(x,y)_{j,k} = M_p(x,y)$ and as a polynomial in y, $\det M_p^{(r)}(x,y)$ is linear. Again to calculate $M_p^{(p)}(x,y)$ it suffices to calculate $M_p^{(r)}(x,\tau_p)$.

THEOREM 6. *Let p be an odd prime. Then*

$$\det M_p^{(r)}(x,\tau_p) = \mathcal{H}_r M_p(x,\tau_p)$$

where $\mathcal{H}_r$ is the homogeneous symmetric function of $\frac{1}{2}(p+1)$ variables evaluated on the elements of $\{1\} \cup \boldsymbol{\mu}^+$.

Proof. Define a matrix $N_p^{(r)}(x,y)$ as follows: $N_p^{(r)}(x,y)$ has $(p+1)/2$ rows and p columns, and

$$(N_p^{(r)}(x,y))_{i,j} = \begin{cases} \left(\dfrac{j-i}{p}\right) + x & \text{if } i \le \frac{1}{2}(p-1) \text{ and } j \ne i, \\ x+y & \text{if } j = i \le \frac{1}{2}(p-1), \\ \left(\dfrac{j-i-r}{p}\right) + x & \text{if } i = \frac{1}{2}(p-1) \text{ and } j \ne \frac{1}{2}(p-1) + r, \\ x+y & \text{if } i = \frac{1}{2}(p-1) \text{ and } j = \frac{1}{2}(p-1) + r. \end{cases}$$

Then $M_p^{(r)}(x,y)$ is essentially the submatrix $N_p'^{(r)}(x,y)$ formed by taking the last $(p+1)/2$ columns of $N_p^{(r)}(x,y)$. In detail, if $p \equiv 1 \pmod 4$ then $M_p^{(r)}(x,y)$ is the left-right reflection of $N_p'^{(r)}(x,y)$ and if $p \equiv 3 \pmod 4$ then $M_p^{(r)}(x,y)$ is the left-right reflection of $-N_p'^{(r)}(-x,-y)$. Thus

$$\det M_p^{(r)}(x,y) = \begin{cases} (-1)^{(p-1)/4} \det N_p'^{(r)}(x,y) & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{(p+1)/4} \det N_p'^{(r)}(-x,-y) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

We evaluate $\det N_p'^{(r)}(x,\tau_p)$ by using Lemma 1.

Regard the rows of $N_p^{(r)}(x,\tau_p)$ as elements of $\mathcal{A}\cong\mathbb{C}^p$. The polynomial corresponding to the $(k+1)$th row $(0\le k\le\frac12(p-3))$ is

$$F_k(T)=\tau_pT^k+\sum_{j=1}^{p-1-k}\left(\frac{j}{p}\right)T^{k+j}+\sum_{j=p-k}^{p-1}\left(\frac{j}{p}\right)T^{k+j-p}+x\sum_{j=0}^{p-1}T^j,$$

which equals $T^kF(T)+xU(T)$ in $\mathcal{A}$. Also $F_k\in\mathcal{Q}$. The polynomial corresponding to the bottom row is $F_{(p-1)/2+r}\in\mathcal{Q}$.

By Lemma 1,

$$\det N_p'^{(r)}(x,\tau_p)=\frac{\det\Phi(N_p^{(r)}(x,\tau_p))}{\det\Phi(\Gamma)}.$$

The entries of the matrix $\Phi(N_p^{(r)}(x,\tau_p))$ are

$$F_j(\zeta^{k^2})=\zeta^{jk^2}(F(\zeta^{k^2})+xU(\zeta^{k^2}))$$

for $0\le j\le\frac12(p-3)$, $0\le k\le\frac12(p-1)$ and

$$F_j(\zeta^{k^2})=\zeta^{(j+r)k^2}(F(\zeta^{k^2})+xU(\zeta^{k^2}))$$

for $j=\frac12(p-1)$, $0\le k\le\frac12(p-1)$.

We are concerned with

$$\frac{\det N_p'^{(r)}(x,\tau_p)}{\det N_p'^{(0)}(x,\tau_p)}=\frac{\det\Phi(N_p^{(r)}(x,\tau_p))}{\det\Phi(N_p^{(0)}(x,\tau_p))}=\frac{\det V_r}{\det V_0}$$

where V_0 is the size $\frac12(p+1)$ Vandermonde matrix with second row entries ζ^{k^2} for $1\le k\le\frac12(p-1)$ and V_r is the same as the matrix V_0 save that in the final row the entries $\zeta^{((p-1)/2)k^2}$ are replaced by $\zeta^{((p-1)/2+r)k^2}$.

Such quotients are special cases of Schur functions as studied in the theory of symmetric functions. In our case [6, Ch. I, §3, (3.9)] we have

$$\frac{\det V_r}{\det V_0}=H_r(1,\zeta,\zeta^{2^2},\dots,\zeta^{((p-1)/2)^2})=\mathcal{H}_r$$

where H_r denotes the homogeneous symmetric function in $\frac12(p+1)$ variables. This completes the proof. ∎

To evaluate $\mathcal{H}_r$ in the above theorem for small values of r, it is convenient to express H_r in terms of the power sum symmetric functions S_r defined by

$$S_r(x_1,\dots,x_{(p+1)/2})=x_1^r+\cdots+x_{(p+1)/2}^r$$

as

$$S_r(1,\zeta,\zeta^{2^2},\dots,\zeta^{(p-1)/2})=1+\sum_{\eta\in\boldsymbol{\mu}^+}\eta^r=\frac12\left(1+\left(\frac{r}{p}\right)\tau_p\right)$$

if $0<r<p$.

As

$$H_1 = S_1, \quad 2H_2 = S_1^2 + S_2, \quad 6H_3 = S_1^3 + 3S_1S_2 + 2S_3,$$

we have

$$\frac{\det V_1}{\det V_0} = \frac{1+\tau_p}{2},$$
$$\frac{\det V_2}{\det V_0} = \frac{(1+\tau_p)^2}{4} + \frac{1+\left(\frac{2}{p}\right)\tau_p}{2},$$
$$\frac{\det V_3}{\det V_0} = \frac{(1+\tau_p)^3}{8} + \frac{(1+\tau_p)\left(1+\left(\frac{2}{p}\right)\tau_p\right)}{4} + \frac{1+\left(\frac{3}{p}\right)\tau_p}{2}.$$

To simplify these further requires splitting into cases according to the residue classes of p modulo 8 and 12 and so on.

5. Further remarks. The matrices dealt with here have size $\frac{1}{2}(p \pm 1)$. Determinants of similarly defined matrices of size $p-1$ have been calculated by Lehmer and Carlitz.

Lehmer [5] computes the determinants of matrices with entries $a+b\left(\frac{j}{p}\right)+c\left(\frac{k}{p}\right)+d\left(\frac{jk}{p}\right)$ and $c+\left(\frac{\alpha+j+k}{p}\right)$ $(1 \le j,k \le p-1)$. In each case he is able to explicitly determine the eigenvalues of these matrices.

Carlitz [2] studies the determinant of the matrices with entries $c+\chi(\alpha+j+k)$ and $c+\chi(j-k)$ $(1 \le j,k \le p-1)$ with χ an arbitrary Dirichlet character of conductor p. His method is to write such matrices as submatrices of size p circulant matrices. He is able to explicitly compute the eigenvalues of these matrices in terms of roots of unity.

It is unlikely that the methods employed by these authors can be extended to compute our determinants. In general our matrices have eigenvalues which do not lie in extensions of the rationals with soluble Galois group. In particular `MAPLE` calculations showed that the Galois group of the characteristic polynomial of $C_p^*(\tau_p)$ over $\mathbb{Q}(\tau_p)$ is insoluble for $p = 13$, $p = 17$ and $p = 19$. In view of this it is optimistic to expect explicit formulas for the eigenvalues of such matrices.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.

[2] L. Carlitz, *Some cyclotomic matrices*, Acta Arith. 5 (1959), 293–308.

[3] R. Chapman, *Steinitz classes of unimodular lattices*, European J. Combin. 25 (2004), 487–493.

[4] H. Cohn, *A Second Course in Number Theory*, John Wiley & Sons, 1962.

[5] D. H. Lehmer, *On certain character matrices*, Pacific J. Math. 6 (1956), 491–499.
[6] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, Clarendon Press, 1979.

Department of Mathematics
University of Exeter
Exeter, EX4 4QE, UK
E-mail: rjc@maths.ex.ac.uk

Received on 7.10.2003
and in revised form on 29.3.2004 (4643)