On Gauss sums and Vandermonde matrices

K. Motose


この研究から派生した研究の方向で、今後この方向に研究を進めたいと考えている。

June 2003 本瀬香
On Gauss sums and Vandermonde matrices

Kaoru Motose

We set $\zeta = e^{\frac{2\pi}{p}}$ and $\omega = e^{\frac{2\pi}{p}}$ for an odd prime $p$. Let $\chi$ be a linear character of the multiplicative group $F^*$ of a prime field $F$ of characteristic $p$. We consider Gauss sums $g(\chi) = \sum_{t \in F^*} \zeta^t \chi(t)$, the following Vandermonde matrices $A$ and character vectors $\chi$ defined by

$$A = \begin{pmatrix}
\zeta & \zeta^2 & \cdots & \zeta^{p-1} \\
\zeta^2 & \zeta^4 & \cdots & \zeta^{2(p-1)} \\
\vdots & \vdots & \ddots & \vdots \\
\zeta^{p-1} & \zeta^{2(p-1)} & \cdots & \zeta^{(p-1)^2}
\end{pmatrix}, \quad \chi = \begin{pmatrix}
\chi(1) \\
\chi(2) \\
\vdots \\
\chi(p-1)
\end{pmatrix}$$

The purpose of this paper is to show that discriminant $|A|^2$ of a cyclotomic polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$ are essential in the proof of quadratic reciprocity, and determinant $|A|$ and trace of $A$ are closely related to the quadratic Gaussian sums. We shall begin from the following easy and important result.

**Lemma 1.**

1. $A\chi = g(\chi)\bar{\chi}$.

2. $A^2 = pJ - K$ and $\bar{A}A = pI - K$ where $I$ is the identity matrix, $\bar{A}$ is the complex conjugate of $A$,

$$J = \begin{pmatrix} 0 & 1 \\ \vdots & \vdots \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad K = \begin{pmatrix} 1 & \cdots & 1 \\ 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}.$$

3. $A^2\chi = p\chi(-1)\bar{\chi}$ and $\bar{A}A\chi = p\chi$. Hence, we obtain the usual formulas $g(\chi)g(\bar{\chi}) = \chi(-1)p$ and $|g(\chi)|^2 = p$. 

1
Proof.

1. We have the assertion from \( \chi(k)(\sum_{t=1}^{p-1} \zeta^{kt}\chi(t)) = g(\chi) \).

2. Since \( \sum_{t=1}^{p-1} \zeta^{kt} = -1 \) or \( p - 1 \) according as \( k \not\equiv 0 \mod p \) or \( k \equiv 0 \mod p \), we can see our equations.

3. The equations \( K\chi = 0 \) and \( J\chi = \chi(-1)\chi \) follow from \( \sum_{t\in F^*} \chi(t) = 0 \) and \( \chi(-1)\chi(p - k) = \chi(k) \), respectively. Thus we have our assertions.

Remark.

1. Lemma 1 can be generalized for an odd integer \( p \) and a Dirichlet character \( \chi \) with the conductor \( p \).

2. The value \( |A|^2 \) is the discriminant of a cyclotomic polynomial \( x^{p-1} + \cdots + x + 1 \) and it plays an important role in Theorem 1.

3. We should remark that trace of \( A \) is \( g(\eta) - 1 \). This fact is well known but it will be proved in the proof of Theorem 2.

The proof 1 in Theorem 1 is only depend on \( |A|^2 \).

**Theorem 1** (Quadratic reciprocity). Let \( p \) and \( q \) be distinct odd primes and let \( \left( \frac{a}{p} \right) \) be a Legendre symbol. Then

\[
\left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left( \frac{p}{q} \right).
\]

Proof 1.

\[
|A|^2 = |A^2| = |pJ - K| = \begin{vmatrix}
-1 & -1 & \cdots & p - 1 \\
-1 & -1 & \cdots & -1 \\
\vdots & \vdots & \ddots & \vdots \\
p - 1 & -1 & \cdots & -1
\end{vmatrix} = (-1)^{\frac{p-1}{2}p^{p-2}}
\]

Hence we have the next equation since \( p - 2 \) is odd.

\[
|A|^{p-1} = |A^2|^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2} \frac{q-1}{2} (p^{q-1})^{p-2}} \equiv (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left( \frac{p}{q} \right) \mod q.
\]
Let \( A^{(k)} = (\zeta_{stk}) \) be the matrix of \( k \)-th powers of all entries in \( A \), let \( r \) be a primitive root of \( p \), and let \( \sigma_r \) be a cyclic odd permutation \((1, c_1, \ldots, c_{p-2})\) where \( c_k \equiv r^k \mod p \). Then we have

\[
|A^{(r)}| = \text{sgn}(\sigma_r)|A| = -|A|.
\]

Thus, setting \( r^s \equiv q \mod p \), we can see

\[
|A|^q \equiv |A(q)| = |A^{(r^s)}| = (-1)^s|A| = \left(\frac{q}{p}\right)|A| \mod q\mathbb{Z}[\zeta].
\]

We product \( |A| \) on both sides of the above equation and divide by the integer \( |A|^2 \not\equiv 0 \mod q \). Then we have

\[
\left(\frac{q}{p}\right) \equiv |A|^{q-1} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \mod q.
\]

**Proof 2.** We set \( \eta(a) = \left(\frac{a}{p}\right) \). We can see from \( A^2\eta = \eta(-1)p\eta \) that

\[
A^{q-1}\eta = (A^2)^{\frac{q-1}{2}}\eta = (\eta(-1)p)^{\frac{q-1}{2}}\eta \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)\eta \mod q\eta.
\]

We have from the next equation that \( \eta(q) \equiv g(\eta)^{q-1} \mod q \) since \( g(\eta)^2 = g(\eta)g(\eta) = \eta(-1)p \not\equiv 0 \mod q \).

\[
\eta(q)g(\eta)^q = \eta(q)(\sum_{t \in F} \zeta_t\eta(t))^q \equiv \eta(q) \sum_{t \in F} \zeta^{q^t}\eta(t) = g(\eta) \mod q\mathbb{Z}[\zeta].
\]

Hence it follows from \( A\eta = g(\eta)\eta \) that

\[
A^{q-1}\eta = g(\eta)^{q-1}\eta \equiv \eta(q)\eta = \left(\frac{q}{p}\right)\eta \mod q\eta.
\]

**Lemma 2.** We set \( \omega = e^{\frac{2\pi}{p}} \). Then we have

1. \[
\prod_{p > s > t \geq 1} \omega^{s+t} = (-1)^{\frac{p-1}{2}}
\]

2. \[
\left\{ \prod_{k=1}^{p-1}2\sin\left(\frac{\pi k}{p}\right) \right\}^2 = \prod_{k=1}^{p-1}2\sin\left(\frac{\pi k}{p}\right) = p
\]

3. \[
\prod_{p > s > t \geq 1} \sin\left(\frac{(s-t)\pi}{p}\right) = p^{\frac{p-1}{2}}\sqrt{p}
\]
Proof.

1. First, we shall show that

\[
\sum_{p>s>t \geq 1} (s+t) = \sum_{s=2}^{p-1} \sum_{t=1}^{s-1} (s+t) = \sum_{s=2}^{p-1} \left\{ s(s-1) + \frac{s(s-1)}{2} \right\} = \frac{3^{p-2}}{2} \sum_{s=1}^{p-1} (s^2 + s) = \frac{p(p-1)(p-2)}{2}
\]

Thus we have the next equation since \( p \) is odd.

\[
\sum_{p>s>t \geq 1} \omega^{s+t} = \omega^{\frac{p(p-1)(p-2)}{4}} = \left( (-1)^{p-2} \right)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}
\]

2. Setting \( \omega = e^{\frac{i\pi}{p}} \) and \( x = 1 \) in \( x^{p-1} + x^{p-2} + \cdots + 1 = \prod_{k=1}^{p-1} (x - \zeta^k) \)
we have the next equation because \( \sin\left(\frac{\pi(p-k)}{p}\right) = \sin\left(\frac{\pi}{p}k\right) \).

\[
p = \prod_{k=1}^{p-1} (1 - \zeta^k) = \prod_{k=1}^{p-1} (1 - \omega^{2k}) = \prod_{k=1}^{p-1} \omega^k (\omega^{-k} - \omega^k)
\]

\[
= \omega^{p \frac{p-1}{2}} (-1)^{p-1} \prod_{k=1}^{p-1} (\omega^k - \omega^{-k}) = (-1)^{\frac{p-1}{2}} \prod_{k=1}^{p-1} 2i \sin\left(\frac{\pi k}{p}\right)
\]

\[
= i^{p-1} p^{p-1} \prod_{k=1}^{p-1} 2 \sin\left(\frac{\pi k}{p}\right) = \prod_{k=1}^{p-1} 2 \sin\left(\frac{\pi k}{p}\right) = \left( \prod_{k=1}^{p-1} 2 \sin\left(\frac{\pi k}{p}\right) \right)^2
\]

3. Noting \( \sin\left(\frac{\pi(p-k)}{p}\right) = \sin\left(\frac{\pi}{p}k\right) \), we can see from the assertion 2 that

\[
\prod_{p>s>t \geq 1} 2 \sin\left(\frac{(s-t)\pi}{p}\right)
\]

\[
= \{ 2 \sin\left(\frac{\pi}{p}\right) \} \cdot \{ 2 \sin\left(\frac{(p-2)\pi}{p}\right) \cdots 2 \sin\left(\frac{\pi}{p}\right) \} \cdot \{ 2 \sin\left(\frac{2\pi}{p}\right) 2 \sin\left(\frac{\pi}{p}\right) \} \cdot \{ 2 \sin\left(\frac{(p-3)\pi}{p}\right) \cdots 2 \sin\left(\frac{\pi}{p}\right) \} \cdot \{ 2 \sin\left(\frac{p-3}{p}\pi\right) \cdots 2 \sin\left(\frac{\pi}{p}\right) \} \cdot \{ 2 \sin\left(\frac{p-1}{p}\pi\right) \cdots 2 \sin\left(\frac{\pi}{p}\right) \} \cdot \{ 2 \sin\left(\frac{\pi}{p}\right) \} \cdot \{ 2 \sin\left(\frac{p+1}{p}\pi\right) \} \cdots \{ 2 \sin\left(\frac{\pi}{p}\right) \} \cdot \{ 2 \sin\left(\frac{p-1}{p}\pi\right) \} \cdot \{ 2 \sin\left(\frac{\pi}{p}\right) \} \cdot \{ 2 \sin\left(\frac{p-3}{p}\pi\right) \} \cdot \{ 2 \sin\left(\frac{\pi}{p}\right) \} \cdot \{ 2 \sin\left(\frac{\pi}{p}\right) \} \cdot \{ 2 \sin\left(\frac{\pi}{p}\right) \} = p^{\frac{p-3}{2}} \sqrt{p}
\]
**Theorem 2.** Let $\eta$ be quadratic character of the multiplicative group $F^*$ of a prime field $F$ of characteristic $p$. Then we have

$$g(\eta) = \sum_{k=0}^{p-1} \zeta^{k^2} = i \frac{(p-1)^2}{4} \sqrt{p}.$$ 

**Proof.** Let $\epsilon, \eta, \chi_1, \bar{\chi}_1, \ldots, \chi_{\frac{p-3}{2}}, \bar{\chi}_{\frac{p-3}{2}}$ be the all distinct linear characters of $F^*$ where $\epsilon$ is the trivial character and $\eta$ is the quadratic character. Then $A\epsilon = -\epsilon$, $A\eta = g(\eta)\eta$ and for a linear character $\chi$ with $\chi \neq \bar{\chi}$,

$$A(\chi, \bar{\chi}) = (\chi, \bar{\chi}) \begin{pmatrix} 0 & g(\chi) \\ g(\chi) & 0 \end{pmatrix}$$

by $A\chi = g(\chi)\bar{\chi}$. Considering the canonical form $X^{-1}AX$ by the character table $X = (\epsilon, \eta, \chi_1, \bar{\chi}_1, \ldots, \chi_{\frac{p-3}{2}}, \bar{\chi}_{\frac{p-3}{2}})$, we obtain

$$\sum_{k=1}^{p-1} \zeta^{k^2} = \text{trace of } A = -1 + g(\eta) \quad \text{and}$$

$$|A| = -g(\eta) \prod_{k=1}^{\frac{p-3}{2}} (-g(\chi_k)g(\bar{\chi}_k)) = -g(\eta) \prod_{k=1}^{\frac{p-3}{2}} (-\chi_k(-1)p)$$

$$= (-1)^{\frac{p-3}{2}} (1+2+\cdots+\frac{p-3}{2}) \frac{p-3}{2} g(\eta)$$

$$= (-1)^{\frac{p-1}{2}} \frac{(p-1)(p-3)}{8} \frac{p-3}{2} \frac{p}{2} g(\eta) = i^{\frac{p-1}{2}} \frac{(p-1)(p-3)}{4} \frac{p-3}{2} g(\eta)$$

$$= i^{\frac{p-1}{4}} \frac{p}{2} \frac{p-3}{2} g(\eta).$$

On the other hand, we have from the definition of $A$ and Lemma 2.

$$|A| = \zeta \zeta^2 \cdots \zeta^{p-1} \prod_{s>t} (\zeta^s - \zeta^t) = \zeta^{\frac{(p-1)}{2}} \prod_{s>t} (\omega^{2s} - \omega^{2t})$$

$$= \prod_{s>t} \omega^{s+t}(\omega^{s-t} - \omega^{-(s-t)}) = (-1)^{\frac{p-1}{2}} 2i \sin \frac{(s-t)\pi}{p}$$

$$= i^{\frac{p-1}{4}} \frac{(p-1)(p-3)}{2} \prod_{s>t} 2 \sin \frac{(s-t)\pi}{p} = i^{\frac{p-1}{2}} \frac{p}{2} \frac{p-3}{2} \sqrt{p}.$$

Hence we have our assertion from

$$i^{\frac{p-1}{4}} \frac{p}{2} \frac{p-3}{2} g(\eta) = |A| = i^{\frac{p-1}{2}} \frac{p}{2} \frac{p-3}{2} \sqrt{p}.$$
REFERENCES


Kaoru Motose

Department of Mathematical Systems Science
Faculty of Science and Technology
Hirosaki University,
Hirosaki 036-8561, Japan

E-mail address: skm@cc.hirosaki-u.ac.jp