On Gauss sums and Vandermonde matrices

K. Motose

Bull. Fac. Sci. Techn. Hirosaki Univ. 2(2003), In press

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 $\zeta = e^{\frac{2\pi i}{p}}$ and $\omega = e^{\frac{\pi i}{p}}$ for an odd prime p. Let χ 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 $\boldsymbol{\chi}$ defined by

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

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 Gauss sums. We shall begin from the following easy and important result.

Lemma 1.

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

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

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

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 $k \not\equiv 0 \bmod p$ or $k \equiv 0 \bmod p$, we can see our equations.

3. The equations $K\boldsymbol{\chi} = 0$ and $J\boldsymbol{\chi} = \chi(-1)\boldsymbol{\chi}$ 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 χ 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 $\left(\frac{q}{p}\right)$ 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.

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

Hence we have the next equation since $p-2$ is odd.

$$|A|^{q-1} = |A^2|^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(p^{\frac{q-1}{2}})^{p-2} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \bmod q.$$

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 σ_r be a cyclic odd permutation $(1, c_1, \ldots, c_{p-2})$ where $c_k \equiv r^k \bmod p$. Then we have

$$|A^{(r)}| = \mathrm{sgn}(\sigma_r)|A| = -|A|.$$

Thus, setting $r^s \equiv q \bmod p$, we can see

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

We product $|A|$ on both sides of the above equation and divide by the integer $|A|^2 \not\equiv 0 \bmod q$. 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 $A^2\boldsymbol{\eta} = \eta(-1)p\boldsymbol{\eta}$ that

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

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

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

Hence it follows from $A\boldsymbol{\eta} = g(\eta)\boldsymbol{\eta}$ that

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

Lemma 2. We set $\omega = e^{\frac{\pi i}{p}}$. Then we have

1. $\prod_{p>s>t\geq 1}\omega^{s+t} = (-1)^{\frac{p-1}{2}}$
2. $\{\prod_{k=1}^{\frac{p-1}{2}} 2\sin(\frac{\pi k}{p})\}^2 = \prod_{k=1}^{p-1} 2\sin(\frac{\pi k}{p}) = p$
3. $\prod_{p>s>t\geq 1}\sin(\frac{(s-t)\pi}{p}) = p^{\frac{p-3}{2}}\sqrt{p}$

Proof.

1. First, we shall show that

$$\begin{aligned}\sum_{p>s>t\geq 1}(s+t) &= \sum_{s=2}^{p-1}\sum_{t=1}^{s-1}(s+t)=\sum_{s=2}^{p-1}\{s(s-1)+\frac{s(s-1)}{2}\}\\ &= \frac{3}{2}\sum_{s=1}^{p-2}(s^2+s)=\frac{p(p-1)(p-2)}{2}\end{aligned}$$

Thus we have the next equation since p is odd.

$$\sum_{p>s>t\geq 1}\omega^{s+t}=\omega^{\frac{p(p-1)(p-2)}{2}}=((-1)^{p-2})^{\frac{p-1}{2}}=(-1)^{\frac{p-1}{2}}$$

2. Setting $\omega=e^{\frac{\pi i}{p}}$ 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 $\sin(\frac{\pi(p-k)}{p})=\sin(\frac{\pi k}{p})$.

$$\begin{aligned}p &= \prod_{k=1}^{p-1}(1-\zeta^k)=\prod_{k=1}^{p-1}(1-\omega^{2k})=\prod_{k=1}^{p-1}\omega^k(\omega^{-k}-\omega^k)\\ &= \omega^{\frac{p(p-1)}{2}}(-1)^{p-1}\prod_{k=1}^{p-1}(\omega^k-\omega^{-k})=(-1)^{\frac{p-1}{2}}\prod_{k=1}^{p-1}2i\sin(\frac{\pi k}{p})\\ &= i^{p-1}i^{p-1}\prod_{k=1}^{p-1}2\sin(\frac{\pi k}{p})=\prod_{k=1}^{p-1}2\sin(\frac{\pi k}{p})=(\prod_{k=1}^{\frac{p-1}{2}}2\sin(\frac{\pi k}{p}))^2\end{aligned}$$

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

$$\begin{aligned}&\prod_{p>s>t\geq 1}2\sin(\frac{(s-t)\pi}{p})\\ &= \{2\sin(\frac{\pi}{p})\}\cdot\{2\sin(\frac{(p-2)\pi}{p})\cdots 2\sin(\frac{\pi}{p})\}\cdot\\ &\quad \{2\sin(\frac{2\pi}{p})2\sin(\frac{\pi}{p})\}\cdot\{2\sin(\frac{(p-3)\pi}{p})\cdots 2\sin(\frac{\pi}{p})\}\cdot\\ &\quad \{2\sin(\frac{\frac{p-3}{2}\pi}{p})\cdots 2\sin(\frac{\pi}{p})\}\cdot\{2\sin(\frac{\frac{p+1}{2}\pi}{p})\cdots 2\sin(\frac{\pi}{p})\}\cdot\\ &\quad \{2\sin(\frac{\frac{p-1}{2}\pi}{p})\cdots 2\sin(\frac{\pi}{p})\}\\ &= p^{\frac{p-3}{2}}\sqrt{p}\end{aligned}$$

Theorem 2. *Let η be quadratic character of the multiplicative group F^* of a prime field F of characteristic p. Then we have*

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

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 ϵ is the trivial character and η is the quadratic character. Then $A\boldsymbol{\epsilon} = -\boldsymbol{\epsilon}$, $A\boldsymbol{\eta} = g(\eta)\boldsymbol{\eta}$ and for a linear character χ with $\chi \neq \bar{\chi}$,

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

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

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

$$\begin{aligned} |A| &= -g(\eta) \prod_{k=1}^{\frac{p-3}{2}} (-g(\chi_k) g(\bar{\chi}_k)) = -g(\eta) \prod_{k=1}^{\frac{p-3}{2}} (-\chi_k(-1)p) \\ &= -(-1)^{\frac{p-3}{2}} (-1)^{1+2+\cdots+\frac{p-3}{2}} p^{\frac{p-3}{2}} g(\eta) \\ &= (-1)^{\frac{p-1}{2}} (-1)^{\frac{(p-1)(p-3)}{8}} p^{\frac{p-3}{2}} g(\eta) = i^{p-1+\frac{(p-1)(p-3)}{4}} p^{\frac{p-3}{2}} g(\eta) \\ &= i^{\frac{p^2-1}{4}} p^{\frac{p-3}{2}} g(\eta) \end{aligned}$$

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

$$\begin{aligned} |A| &= \zeta\zeta^2 \cdots \zeta^{p-1} \prod_{s>t} (\zeta^s - \zeta^t) = \zeta^{\frac{p(p-1)}{2}} \prod_{s>t} (\omega^{2s} - \omega^{2t}) \\ &= \prod_{s>t} \omega^{s+t} (\omega^{s-t} - \omega^{-(s-t)}) = (-1)^{\frac{p-1}{2}} \prod_{s>t} 2i \sin(\frac{(s-t)\pi}{p}) \\ &= i^{p-1} i^{\frac{(p-1)(p-2)}{2}} \prod_{s>t} 2\sin(\frac{(s-t)\pi}{p}) = i^{\frac{p(p-1)}{2}} p^{\frac{p-3}{2}} \sqrt{p}. \end{aligned}$$

Hence we have our assertion from

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

References

[1] R. Lidl and H. Niederwriter, *Finite fields,* Encyclopedia of Mathematics and Applications, **20**, Cambridge University Press, London, 1984.

Kaoru Motose
Department of Mathematical System Science
Faculty of Science and Technology
Hirosaki University,
Hirosaki 036-8561, Japan
E-mail address: skm@cc.hirosaki-u.ac.jp