On the pure Jacobi Sums *

Shigeki Akiyama

Let p be an odd prime and $\mathbf{F}_q$ be the field of $q = p^2$ elements. We consider the Jacobi sum over $\mathbf{F}_q$;

$$J(\chi, \psi) = \sum_{x \in \mathbf{F}_q} \chi(x)\psi(1-x),$$

where χ, ψ is a non trivial character of $\mathbf{F}_q^{\times}$, whose value at 0 is defined to be 0. It is well known that the absolute value of $J(\chi, \psi)$ is $\sqrt{q} = p$, when $\chi\psi$ is not principal. According to [11], [9], call the Jacobi sum $J(\chi, \psi)$ pure if $J(\chi, \psi)/p$ is a root of unity.

Let $\mathrm{ord}(\chi)$ be the order of χ in $\widehat{\mathbf{F}_q^{\times}}$. From now on in this paper, we assume that $\mathrm{ord}(\psi) = 2$ and $\mathrm{ord}(\chi) = n \geq 3$. This special type of Jacobi sums play an important role in evaluating the argument of Gauss sum:

$$G(\chi) = \sum_{x \in \mathbf{F}_q} \chi(x)\zeta_p^{\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(x)},$$

where ζ_p is a primitive p-th root of unity (see [3], [4]). Moreover, recently the rationality of this Jacobi sum is used to characterize the irreducible module of the Terwilliger algebras of cyclotomic association schemes (see [10]).

In this note, we prove

Theorem. $J(\chi, \psi)$ is pure if and only if one of the the following four conditions holds:

1. n is a divisor of $p+1$
2. $n = 2(p-1)/k$ with an odd integer k
3. $n = 24$ and $p \equiv 17, 19 \pmod{24}$
4. $n = 60$ and $p \equiv 41, 49 \pmod{60}$

*Only for the private copy. See Acta Arith. Vol.75, no.2 (1996), 97 – 104, for the exact published version.

Further, $J(\chi, \psi) = \pm p$ in all four cases.

There are a lot of results concerning the determination of Gauss and Jacobi sums. See eg. [3], [4], [8]. A nice historical survey is found in [5]. Same type of "purity" problem for the case of Gauss sums are treated in [1], [13], [2], [7], [9], [11]. But it seems that this type of concrete result on Jacobi sums is not known. Although the essential tool to prove the Theorem is the theorem of Stickelberger, the argument of "only if" part of the proof is elementary and rather complicated. The author feels somewhat curious that this simple result is derived by such brute force method.

We first see

Proposition. Let $S_1 = \{x \in (\mathbf{Z}/n\mathbf{Z})^\times : x \equiv i \pmod{\mathrm{n}} \quad \text{for} \quad i \in [1, n/2) \cap \mathbf{Z}\}$, and $S_2 = (\mathbf{Z}/n\mathbf{Z})^\times \setminus S_1$. Then $J(\chi, \psi)$ is pure if and only if there exist an element $x \in S_1$ so that $xS_1 = S_1$ and $p \equiv -x \pmod{\mathrm{n}}$ holds.

Proof. By using the Theorem of Hasse-Davenport (see Theorem 5.1 of [12]) and the well known result of the sign determination of Gauss sums of order 2 for the prime field F_p, it is shown that $G(\psi) = (-1)^{(p+1)/2}p$. The theorem of Stickelberger (see Theorem 2.2 of [12]) reads, $J(\chi, \psi)/p = \pm G(\chi)/G(\chi\psi)$ is a unit of the integer ring of $\mathbf{Q}(\zeta_n)$ if and only if

$$\{\frac{a}{n}\} + \{\frac{pa}{n}\} = \{\frac{a}{n} + \frac{1}{2}\} + \{p(\frac{a}{n} + \frac{1}{2})\} \quad \text{for all } a \text{ with } \ (a, n) = 1.$$

Here $\{x\} = x - [x]$ and $[x]$ is the greatest integer not exceeds x. As p is odd, we have to check the conditions only for $a \in S_1$, because the condition is symmetric with respect to $a \leftrightarrow n - a$. Thus we choose a with $1 \leq a \leq n/2$ and $(a, n) = 1$. Then we have

$$\frac{a}{n} + \{\frac{pa}{n}\} = \frac{a}{n} + \frac{1}{2} + \{\frac{pa}{n} + \frac{1}{2}\} \quad \text{for} \quad a \in S_1. \tag{1}$$

Note that the condition depends only on $p \bmod n$. We see that (1) is equivalent to $\{pa/n\} \in [1/2, 1)$ for $a \in S_1$. Put $p = ny - x$ with integers x, y. Then we see $x \bmod n \in S_1$ and $\{xa/n\}$ must lie in the interval [0,1/2). Noting that $|J(\chi, \psi)| = p$ and $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ is an abelian extention, $J(\chi, \psi)/p$ is a root of unity under these conditions. This shows the assertion. $\square$

Remark. Consider the Jacobi sum on the general finite field $\mathbf{F}_q$ with $q = p^f$, for a while. Then, similarly as in the above proof, we can easily show that, if the extention degree f is odd, then there are no χ that $J(\chi, \psi)/\sqrt{q}$ is a root of unity. Our Theorem concerned the first non trivial case.

The sufficiency of the conditions of the Theorem follows immediately. Because

- $1 \times S_1 = S_1 \longleftrightarrow$ Condition 1.
- $n \equiv 0 \pmod 4$ and $(n/2-1)S_1 = S_1 \longleftrightarrow$ Condition 2.
- If $n = 24$ and $S_1 = \{\tilde{1}, \tilde{5}, \tilde{7}, \widetilde{11}\}$, then $\tilde{5}S_1 = S_1$ and $\tilde{7}S_1 = S_1 \longleftrightarrow$ Condition 3.
- If $n = 60$ and $S_1 = \{\tilde{1}, \tilde{7}, \widetilde{11}, \widetilde{13}, \widetilde{17}, \widetilde{19}, \widetilde{23}, \widetilde{29}\}$, then $\widetilde{11}S_1 = S_1$ and $\widetilde{19}S_1 = S_1 \longleftrightarrow$ Condition 4.

Here we denote by $\tilde{x}$, the coset $x \pmod{\mathrm{n}}$. Our next task is to show that $J(\chi,\psi)$ is real in the above four cases. The first two cases are handled easily.

Lemma 1. We have $J(\chi,\psi) = \pm p$ when n is a divisor of $p+1$ or $n = 2(p-1)/k$ with an odd integer k.

Proof. We see

$$J(\chi,\psi) = \sum_{x \in \mathbf{F}_q} \chi(x^p)\psi(1-x^p) = \sum_{x \in \mathbf{F}_q} \chi^p(x)\psi^p(1-x) = J(\chi^p,\psi) \tag{2}$$

If $p \equiv -1 \pmod{\mathrm{n}}$ then

$$J(\chi^p,\psi) = J(\overline{\chi},\psi) = \overline{J(\chi,\psi)}$$

This shows the first case. For the second case, we have $p-1 \equiv nk/2 \equiv n/2 \pmod{\mathrm{n}}$ and $\chi^{p-1} = \chi^{n/2} = \psi$, as $n = \mathrm{ord}(\chi)$. By using (2) and $\psi(-1) = 1$, we have

$$\begin{aligned} J(\chi,\psi) &= \sum_{x \in \mathbf{F}_q} \chi^p(x)\psi(1-x) = \sum_{x \in \mathbf{F}_q} \chi(x)\psi(x(1-x)) \\ &= \sum_{x \in \mathbf{F}_q^\times} \overline{\chi(x)}\psi(x^{-1}(1-x^{-1})) = \sum_{x \in \mathbf{F}_q} \overline{\chi(x)}\psi(x-1) \\ &= \overline{J(\chi,\psi)} \end{aligned}$$

This shows the assertion. □

The case $n = 24$ was already proved in [4]. We show this directly for the convenience of the reader.

Lemma 2. We have $J(\chi,\psi) = \pm p$ when $n = 24$ and $p \equiv 17, 19 \pmod{24}$.

Proof. We have already shown that $J(\chi,\psi)/p$ is a root of unity of the field $\mathbf{Q}(\zeta_{24})$. Let σ_k be the element of $\mathrm{Gal}(\mathbf{Q}(\zeta_{24})/\mathbf{Q})$ with $\sigma_k(\zeta_{24}) = \zeta_{24}^k$. Then we have

$$\sigma_{11}(J(\chi,\psi)) = \sigma_{11}(G(\chi)G(\psi)/G(\chi^{13})) = G(\overline{\chi^{13}})G(\psi)/G(\overline{\chi}) = J(\chi,\psi).$$

This shows that $J(\chi,\psi)/p$, the 24-th root of unity, is invariant under σ_{11}. This shows the assertion. $\square$

The first manuscript of this note does not contain the next proof of Lemma 3, which is essentially due to Mieko Yamada. The author tried in vain to do this. She also informed me that more general assertion concerning Lemma 1,2 and 3 is presented in [10] and the detailed version of it will contain its proof.

Lemma 3. We have $J(\chi,\psi)=\pm p$ when $n=60$ and $p\equiv 41,49 \pmod{60}$.

Proof. Similarly as in Lemma 2, we see $\sigma_{29}(J(\chi,\psi)) = (J(\chi,\psi))$. Thus $J(\chi,\psi)\in\mathbf{Q}(\sqrt{-1})$ and $J(\chi,\psi)/p$ is equal to ±1 or $\pm\sqrt{-1}$. Note that

$$(J(\chi,\psi))^5 \equiv J(\chi^5,\psi) \pmod{5}. \tag{3}$$

As $\mathrm{ord}(\chi^5)=12$, we see that there exist rational integers C, D with $p=C^2+D^2$ and

$$J(\chi^5,\psi) = -(C+D\sqrt{-1})^2,$$

by Theorem 4.8 and 4.10 of [4]. We easily see that $CD\equiv 0 \pmod{5}$ as $p\equiv\pm1 \pmod{5}$. This shows the assertion. $\square$.

Remark. There is a remaining problem to determine the sgn of $J(\chi,\psi)$ when it is real. See [4], for the first three cases of the Theorem. If $n=60$ and $p\equiv 41,49 \pmod{60}$, the congruence relation (3) and Theorem 4.8 and 4.10 of [4] is enough to determine the sgn ambiguity of $J(\chi,\psi)$. Summing up, we have

$$J(\chi,\psi) = \begin{cases} p, & \text{for the case 1 and 3} \\ (-1)^{(p+1)/2}p, & \text{for the case 2} \\ \pm\left(\frac{p}{3}\right)p, & \text{for the case 4.} \end{cases}$$

Here $\pm$ of the last case is $+$ (resp. $-$) when $A\equiv 0 \pmod{5}$ (resp. $\not\equiv$), with a positive odd integer A, which is uniquely determined by $p=A^2+B^2$.

Now we show the necessity of the conditions of the Theorem. For the convenience, we identify the element of S_1 (resp. S_2) with the integer in $[1,n/2)$ (resp. $[n/2,n)$) in the later proof.

Lemma 4. Besides the case 1 of the Theorem, if $J(\chi,\psi)$ is pure then $n=\mathrm{ord}(\chi)$ is divisible by 4.

Proof. Assume n is odd and $a\neq 1$ is an integer with $aS_1=S_1$. Choose an integer $i\geq 1$ such that $n/2^{i+1}<a\leq n/2^i$. Then $a\neq 1$ implies $1\leq n/2^{i+1}$. Thus $2^i\in S_1$ and $2^ia\in S_2$

which contradicts with $aS_1 = S_1$. Thus by using the proposition, n must be even. Now if $n = 2m$ and m is odd, then similarly we choose $a \in S_1$ and an integer i. Noting that a is odd, we have

$$a(\frac{n}{2} - 2^i) \equiv \frac{n}{2} - 2^i a \pmod{n}.$$

We see $n/2 - 2^i \in S_1$ and $n/2 - 2^i a \in S_2$, which contradicts with $aS_1 = S_1$. □

The next step is the prototype of our following arguments, which seems somewhat curious at first glance.

Lemma 5. Besides the case 1 or 2 of the Theorem, if n is divisible by 8 and $n > 14^2$, then $J(\chi, \psi)$ is not pure.

Proof. Let

$$T(a, b) = \{x \in (\mathbf{Z}/n\mathbf{Z})^\times : x \equiv i \pmod{\text{n}} \quad \text{for} \;\; i \in [a, b) \cap \mathbf{Z}\}$$

and define

$$T_i = T\left(\frac{(i-1)n}{4}, \frac{in}{4}\right) \quad (i = 1, 2, 3, 4).$$

We identify the element of T_i with the integer in $[(i-1)n/4, in/4)$. Let $n = 2^e m$ $(e \geq 3)$ and m is odd. Consider a vector;

$$(A, B, C, D) = \left(\frac{n}{2^e} + 2^i, \quad \frac{n}{2^e} + 2^{i+1}, \quad \frac{n}{2^e} + \frac{n}{4} + 2^i, \quad \frac{n}{2^e} + \frac{n}{4} + 2^{i+1}\right) \quad \text{for } i \geq 1.$$

Assume that $2^{i+4} \leq n$, which implies A, B, C and $D \in S_1$. As $n/2$ is even, the condition $aS_1 = S_1$ is equivalent to $(n/2 - a)S_1 = S_1$ and $n/2 - a$ also lies in S_1. Thus if $J(\chi, \psi)$ is pure, we may assume $a \in [1, n/4)$ and $aS_1 = S_1$. We first treat the case $a \in [8, n/4)$. Let $i \geq 1$ be an integer such that $a \in [n/2^{i+2}, n/2^{i+1})$. (We can choose i which satisfies $2^{i+4} \leq n$ in this case.) Then we have $aA \in T_1$ and $aB \in T_2$. In fact, $B - A = 2^i$ and $2^i a \pmod{\text{n}}$ has an representative in $[n/4, n/2) \cap \mathbf{Z}$. Thus if aA $(\in S_1)$ lies in T_2 then aB must be in S_2. Noting a is odd, we classify in two cases:

1. If $a \equiv 1 \pmod{4}$ then
$$aD \equiv \frac{n}{4} + aB \pmod{n}$$
which implies $aD \in T_3$.
2. If $a \equiv 3 \pmod{4}$ then
$$aC \equiv \frac{3n}{4} + aA \pmod{n}$$
which implies $aC \in T_4$.

Therefore when $a \in [8, n/4)$, we have shown that, contradicting with the assumption, that aA, aB, aC and aD can not lies in S_1 simultaneously.

It remains the case $a \in [1, 7]$. The value 1 corresponds to the case 1 or 2 of the Theorem. (Remember that we used the reflection $a \leftrightarrow n/2 - a$). Thus the only remaining case is $a = 3, 5$ and 7. But this case is easily handled because if $aS_1 = S_1$ then $a^2 S_1 = S_1$ and $n/4 > 7^2$ implies $a^2 \in [8, n/4)$. $\square$

Lemma 6. Besides the case 1 or 2 of the Theorem, if $n > 10^2$ and $n = 4m$ and $(m, 3) = 1$ then $J(\chi, \psi)$ is not pure.

Proof. In this case, consider a vector;

$$(A, B, C) = \left(\frac{n}{4} + 2^i, \quad \frac{n}{4} + 2^{i+1}, \quad \frac{n}{4} + 3 \cdot 2^i\right) \quad \text{for } i \geq 1.$$

As A, B and C must be in S_1, we assume $3 \cdot 2^{i+2} \leq n$. Using the reflection $a \leftrightarrow n/2 - a$, we may choose $a \in [1, n/4)$. First we assume that $a \in [6, n/4)$ and $aS_1 = S_1$. Choose the integer i by $a \in [n/2^{i+2}, n/2^{i+1})$. Then by the same argument as Lemma 5, we have $aA \in T_1$ and $aB \in T_2$. Thus we have $aC \in S_2$, which is a contradiction. The case $a = 3$ and 5 is handled similarly. $\square$

In the following, we proceed similarly. In other words, we first choose four elements in S_1. Then we show that the a-multiple of these elements can not lies in S_1 simultaneously. The later arguments become a little bit complicated, especially in Lemma 8.

Lemma 7. Besides the case 1 or 2 of the Theorem, if $n > 46^2$ and $n = 4m$ and m is odd and not square free, then $J(\chi, \psi)$ is not pure.

Proof. Let q be an odd prime and m is divisible by q^2. In this case, we take a vector;

$$(A, B, C, D) = \left(\frac{n}{4q} + 2^i, \quad \frac{n}{4q} + 2^{i+1}, \quad \frac{n}{4q} + \frac{kn}{2q} + 2^i, \quad \frac{n}{4q} + \frac{kn}{2q} + 2^{i+1}\right) \quad \text{for } i \geq 1.$$

Here k is a positive integer smaller than $3q/4$, which is taken suitably later. Assume that $3 \cdot 2^{i+4} \leq n$. Then we have

$$\frac{n}{4q} + \frac{kn}{2q} + 2^{i+1} \leq \frac{n}{12} + \frac{3n}{8} + 2^{i+1} \leq \frac{n}{2}.$$

Thus A, B, C and D are contained in S_1. We first prove the case $a \in [24, n/4)$. Choose k so that

$$\frac{1}{4} \leq \{\frac{ak}{2q}\} \leq \frac{3}{4} \tag{4}$$

holds. This is possible. In fact, let $l \in [q/2, 3q/2) \cap \mathbf{Z}$ and solve the congruence for x:

$$ax \equiv l \pmod{2q} \text{ and } x \in [1, 2q] \cap \mathbf{Z}.$$

Define

$$k(l) = \left(\begin{array}{ll} x & \text{for } x \leq q \\ 2q - x & \text{for } x > q \end{array} \right. \tag{5}$$

Then (4) is satisfied for $k = k(l)$. It is easily shown that the number of distinct $k(l)$ is $(q+1)/2$. So $k = k(l)$ can be taken smaller than, say, $3q/4$. Noting $3 \cdot 2^{i+4} \leq n$ and $a \geq 24$, we can choose the integer i by $a \in [n/2^{i+2}, n/2^{i+1})$. Then, similarly to Lemma 5, we can easily check that $aA \in T_1$ and $aB \in T_2$. By (4), we have $akn/2q \in T_2 \cup T_3$. We classify in two cases. If $akn/2q \in T_2$ then $aD \in S_2$. And if $akn/2q \in T_3$ then $aC \in S_2$. This completes the proof for $a \in [24, n/4)$. Finally we treat the remaining case $a \leq 23$. If $23 \geq a \geq 5$, then $a^2 S_1 = S_1$ and $24 < a^2 < n/4$, we can prove these cases. If $a = 3$ then consider $27 S_1 = S_1$. $\square$

Lemma 8. Besides the case 1 or 2 of the Theorem, if $n > 70^2$ and $n = 12m$ and $(m, 6) = 1$ and m has a prime factor greater than 6, then $J(\chi, \psi)$ is not pure.

Proof. Let q be the greatest prime factor of q. We assume $(n/q, q) = 1$, in light of Lemma 7. In this case, we take a vector;

$$(A, B, C, D) = \left(\frac{n}{12} \pm 2^{i+1}, \quad \frac{n}{12} \pm 3 \cdot 2^i, \quad A + \frac{kn}{2q}, \quad B + \frac{kn}{2q} \right) \quad \text{for } i \geq 1.$$

The sgn $\pm$ of A and B are defined by

$$\frac{n}{12} \pm 2^{i+1} \not\equiv 0 \pmod{3}.$$

Here k is a positive integer smaller than $3q/4$, which is chosen later. Assume that $3^2 \cdot 2^{i+3} \leq n$. Then we see that A, B, C and D are in $[1, n/2)$. Moreover we see $A, B \in S_1$ and C, D are coprime with 6. But, in this case, C, D may be divisible by q. Let $l \in [q/2, 3q/2) \cap \mathbf{Z}$ and $k(l)$ be the an integer defined by (5) in Lemma 7. Then there exist $(q+1)/2$ choices of $k(l)$. As $q \geq 7$, we can take $[q/4] + 3$ different $k(l)$ values. Then there exist at least three $k = k(l)$ such that both (4) and $k \leq 3q/4$ holds. Thus we can choose $k = k(l)$ so that $C, D \in S_1$. (Here we used the fact $(n/q, q) = 1$.) Now consider the case $a \in [36, n/2)$, and take an integer i by $a \in [n/2^{i+2}, n/2^{i+1})$. Similarly, as in Lemma 7, we see that aA, aB, aC and aD can not lies in S_1 simultaneously. Finally we consider the case $a \leq 35$. If $a \in [7, 35]$ then $a^2 \in [36, n/4)$. If $a = 5$ then $5^3 S_1 = S_1$ and $5^3 \in [36, n/4)$. This completes the proof. $\square$

Proof of the Theorem. By using the proposition, very suitable for numerical calculations, we can easily check the assertion of the Theorem for $n \leq 70^2$. Combining Lemma 4,5,6 and 7, if n is counter example of Theorem 1, we see $n = 12m$ and $(m, 6) = 1$ with a square free integer m. Now in scope of Lemma 8, the greatest prime factor of m is 5, which yields the case 4 of the Theorem. This completes the proof.

Acknowledgments.

I am very grateful to Yoshio Mimura and Akihiro Munemasa, who showed me this problem and the computational phenomena, which is now explained for the time being. Thanks are also due to Mieko Yamada who kindly permitted me to include her proof of Lemma 3 in this article. And I would like to express my best gratitude to my colleague, Teruo Takeuchi, whom I discussed and enjoyed with. The essential part of the proof of Lemma 4 is due to him.

References

[1] S. Chowla, On Gaussian sums., Proc. Nat. Acad. Sci. U.S.A. **48** (1962) 1127-1128.

[2] L. D. Baumert, W. H. Mills and R. L. Ward, Uniform cyclotomy., J. of Number Theory **14**, no. 1 (1982) 67-82.

[3] B. C. Berndt and R. J. Evans, Sums of Gauss, Jacobi, Jacobsthal., J. of Number Theory **11**, no.3 (1979) 349-398.

[4] B. C. Berndt and R. J. Evans, Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer., Illinois J. of Math. **23**, no.3 (1979) 374-437.

[5] B. C. Berndt and R. J. Evans, The determination of Gauss Sums., Bull. Amer. Math. Soc. (N. S.) **5**, no.2 (1981) 107-129.

[6] B. C. Berndt and R. J. Evans, Corrigendum to "The determination of Gauss Sums"., Bull. Amer. Math. Soc. (N. S.) **7**, no.2 (1982) 441.

[7] R. J. Evans, Generalization of a Theorem of Chowla on Gaussian sums., Houston J. Math. **3**, no.3 (1977) 343-349.

[8] R. J. Evans, Resolution of sign ambiguities in Jacobi and Jacobsthal sums., Pacific J. Math. **81**, no. 1 (1979) 71 - 80.

[9] R. J. Evans, Pure Gauss sums over finite fields, Mathematika **28**, no. 2 (1981) 239 -248.

[10] T. Ito, H. Ishibashi, A. Munemasa and M. Yamada, The Terwilliger algebra of cyclotomic schemes and rationality of Jacobi Sums., abstracts of the conference on Algebraic Combinatorics, Fukuoka (1993), 43-44.

[11] D. S. Kubert and S. Lang, Independence of Modular Units on Tate Curves, Math. Ann. **240** (1979) 191-201.

[12] S. Lang, Cyclotomic fields I and II, Graduate text in Math. **121**, Springer (1990).

[13] L. Mordell, On a cyclotomic resolvent, Arch. Math. **13** (1962) 486-487.

SHIGEKI AKIYAMA

Faculty of Science
Niigata University
Niigata, 950-21, Japan
email: akiyama@geb.ge.niigata-u.ac.jp