COLLOQUIUM MATHEMATICUM

VOL. 73 1997 NO. 2

ON RATIONALITY OF JACOBI SUMS

BY

KATSUMI SHIRATANI AND MIEKO YAMADA (FUKUOKA)

1. Introduction. Let p be an odd prime and $q = p^f$, where f is a positive integer. Let $\mathrm{GF}(q)$ be the finite field of q elements. The character group of the multiplicative group $\mathrm{GF}(q)^\times$ is generated by the Teichmüller character ω, and is cyclic of order $q-1$.

Let $\eta \in \langle\omega\rangle$ be a nonprincipal character. For any character $\chi \in \langle\omega\rangle$ different from the principal character ω^0 and from the character η we consider the Jacobi sum

$$J(\chi,\eta) = \sum_{x\in \mathrm{GF}(q)-\{0,1\}} \chi(x)\eta(1-x).$$

We consider the problem of obtaining precise conditions to ensure that $J(\chi,\eta)$ belongs to the rational number field $\mathbb{Q}$. This problem seems to be of interest in itself and has an application. Indeed, it is related to a question in algebraic combinatorics. The Jacobi sum $J(\chi,\eta)$ with the quadratic character $\eta = \omega^{\frac{q-1}{2}}$ belongs to $\mathbb{Q}$ if and only if the T-submodule of the Terwilliger algebra obtained from a cyclotomic scheme with class 2 is reducible [4].

In this paper we treat only the case where the character η is the quadratic character $\omega^{\frac{q-1}{2}}$. Namely we determine conditions on χ and q ensuring that $J(\chi,\eta)$ belongs to the rationals $\mathbb{Q}$, in the case $f=2$:

Suppose $q=p^2$ and $1\le i\le p^2-1$. Then $J(\omega^{-i},\omega^{\frac{p^2-1}{2}})$ is rational if and only if $i=(p-1)k$ $(k=1,2,\ldots,p)$, or $i=\frac{p+1}{2}k$ $(k=1,3,\ldots,2(p-1)-1)$, or ω^{-i} is of order 24 and $p\equiv 17,19 \pmod{24}$, or ω^{-i} is of order 60 and $p\equiv 41,49 \pmod{60}$ (1).

We can discuss the problem in the general case by the same method.

1991 *Mathematics Subject Classification*: 11T24.

(1) One of the authors has recently received a reprint of a paper by S. Akiyama, *On the pure Jacobi sums*, Acta Arith. 75 (1996), 97–104. The authors have found that the same result is independently obtained there with a completely different proof. The authors had already announced the result in a symposium of RIMS at Kyoto University held in November 1994.

We turn to the case where q is arbitrary. It is known [7] that Jacobi sums can be factored into Gauss sums in the sense that

$$J(\chi,\eta)=\frac{g(\chi)g(\eta)}{g(\chi\eta)}. \tag{1}$$

Here we define the Gauss sum $g(\chi)$ for any $\chi\in\langle\omega\rangle$, as usual, as follows:

$$g(\chi)=\sum_{x\in\mathrm{GF}(q)^\times}\chi(x)\zeta_p^{s(x)},$$

where ζ_p denotes a fixed primitive pth root of unity and $s(x)$ means the trace of x with respect to $\mathrm{GF}(q)/\mathrm{GF}(p)$.

Now, we embed the Gauss sum $g(\omega^{-i})\in\mathbb{Q}(\zeta_p,\zeta_{q-1})$ $(0\le i\le q-2)$ into the p-adic field $\mathbb{Q}_p(\zeta_p,\zeta_{q-1})$ over the p-adic rational number field $\mathbb{Q}_p$, where ζ_{q-1} denotes a primitive $(q-1)$th root of unity. Then we have the Gross–Koblitz formula [5]

$$g(\omega^{-i})=-\varpi^{s_p(i)}\prod_{l=0}^{f-1}\mathit{\Gamma}_p\bigg(\frac{p^l i}{q-1}-\sum_{j=1}^{l}i_{f-j}p^{l-j}\bigg). \tag{2}$$

Here $s_p(i)=\sum_{j=0}^{f-1}i_j$ means the sum of the coefficients of the canonical p-adic expansion of i, namely $i=i_0+i_1p+\ldots+i_{f-1}p^{f-1}$ with $0\le i_j\le p-1$, and ϖ denotes a prime element in the field $\mathbb{Q}_p(\zeta_p)$ such that $\varpi=\sqrt[p-1]{-p}$, $\varpi\equiv\zeta_p-1 \pmod{(\zeta_p-1)^2}$. The function $\mathit{\Gamma}_p(x)$ is the p-adic gamma function. For example, we see for $\eta=\omega^{-\frac{q-1}{2}}$ that

$$g(\omega^{-\frac{q-1}{2}})=-\varpi^{\frac{p-1}{2}f}\mathit{\Gamma}_p\big(\tfrac12\big)^f.$$

In the sequel, for the sake of convenience, we call the product appearing in the Gross–Koblitz formula the *gamma product part* and $\varpi^{s_p(i)}$ the *ϖ-part* of the Gauss sum $g(\omega^{-i})$.

2. A formulation in the general case. The condition $J(\omega^{-i},\omega^{\frac{q-1}{2}})\in\mathbb{Q}$ is equivalent to $J(\omega^{-i},\omega^{\frac{q-1}{2}})\in\mathbb{Z}$, the ring of rational integers, because $J(\omega^{-i},\omega^{\frac{q-1}{2}})$ is an algebraic integer. This condition yields easily $f\equiv 0 \pmod 2$, in view of $|J(\omega^{-i},\omega^{\frac{q-1}{2}})|=\sqrt{q}$ and the formula (1).

Next, as $J(\omega^{-i},\omega^{\frac{q-1}{2}})\in\mathbb{Z}$ is left fixed by the element σ_{-1} in the Galois group $G(\mathbb{Q}(\zeta_{q-1},\zeta_p))/\mathbb{Q}(\zeta_p))$, which is defined by $\sigma_{-1}(\zeta_{q-1})=\zeta_{q-1}^{-1}$, $\sigma_{-1}(\zeta_p)=\zeta_p$, we have by the equality (1),

$$\frac{g(\omega^{-i})}{g(\omega^{-i+\frac{q-1}{2}})}=\frac{g(\omega^{i})}{g(\omega^{i+\frac{q-1}{2}})}. \tag{3}$$

Then, comparing the ϖ-parts of both sides we see at once that

$$s_p(i)-s_p(j)=s_p(q-1-i)-s_p(q-1-j),$$

where we put $\omega^{-j} = \omega^{-i+\frac{q-1}{2}}$ with $1 \le j \le q-2$. Hence we have $s_p(i) = s_p(j)$. In the case $1 \le i < \frac{q-1}{2}$ this gives $s_p(i) = s_p\big(i + \frac{q-1}{2}\big)$, and in the case $\frac{q-1}{2} < i \le q-2$ this gives $s_p(i) = s_p\big(i - \frac{q-1}{2}\big)$ from the equality $s_p(q-1-i) + s_p(i) = f(p-1)$.

In the former case this can be rewritten as

$$s_p(i) + s_p\left(\frac{q-1}{2} - i\right) = f(p-1),$$

and this means that the canonical p-adic expansion $i = i_0 + i_1 p + \ldots + i_{f-1}p^{f-1}$ has just $\frac{f}{2}$ coefficients not smaller than $\frac{p-1}{2}$.

Moreover, for $f \equiv 0 \pmod 2$ we see

$$g(\omega^{-\frac{q-1}{2}}) = (-1)^{1+\frac{f}{2}\frac{p-1}{2}} p^{\frac{f}{2}}. \tag{4}$$

Hence, $J(\omega^{-i}, \omega^{\frac{q-1}{2}}) \in \mathbb{Z}$ means necessarily that its absolute value is $p^{\frac{f}{2}}$. From this and (1), (4) we conclude that

$$g(\omega^{-i}) = \pm g(\omega^{-i+\frac{q-1}{2}}).$$

Conversely, if this equality holds together with $f \equiv 0 \pmod 2$, we see readily that $J(\omega^{-i}, \omega^{\frac{q-1}{2}}) = \pm p^{\frac{f}{2}} \in \mathbb{Z}$. In the sequel we may assume $1 \le i < \frac{q-1}{2}$, because we can take $q-1-i$ instead of i if necessary. Thus we have the following:

THEOREM 1. *It is necessary and sufficient for* $J(\omega^{-i}, \omega^{\frac{q-1}{2}}) \in \mathbb{Q}$ *that we have* $f \equiv 0 \pmod 2$, $s_p(i) = s_p\big(i + \frac{q-1}{2}\big)$ *and*

$$\prod_{l=0}^{f-1} \Gamma_p\left(\frac{p^l i}{q-1} - \sum_{j=1}^{l} i_{f-j}p^{l-j}\right)$$
$$= \pm \prod_{l=0}^{f-1} \Gamma_p\left(\frac{p^l\big(i+\frac{q-1}{2}\big)}{q-1} - \sum_{j=1}^{l}\left(i + \frac{q-1}{2}\right)_{f-j} p^{l-j}\right).$$

3. The case $f = 2$. In what follows we treat only the case $f = 2$. In this case the condition can be simply expressed as follows.

For $1 \le i < \frac{p^2-1}{2}$, let $i = i_0 + i_1 p$ be the canonical expansion of i. Then the equality in Theorem 1 states that for $\frac{p-1}{2} < i_0 \le p-1, 0 \le i_1 < \frac{p-1}{2}$ we have

$$\Gamma_p\left(\frac{i_0 + i_1 p}{p^2-1}\right)\Gamma_p\left(\frac{i_1 + i_0 p}{p^2-1}\right) = \pm \Gamma_p\left(\frac{i_0 + i_1 p}{p^2-1} + \frac{1}{2}\right)\Gamma_p\left(\frac{i_1 + i_0 p}{p^2-1} - \frac{1}{2}\right). \tag{5}$$

We immediately get two systems of trivial solutions of this equation, namely solutions with the integers i that satisfy

$$\frac{i_0 + i_1 p}{p^2-1} = 1 - \frac{i_1 + i_0 p}{p^2-1} \quad \text{or} \quad \frac{i_0 + i_1 p}{p^2-1} = \frac{i_1 + i_0 p}{p^2-1} - \frac{1}{2}.$$

The former follows from the norm relation $\Gamma_p\big(\frac{i_1+i_0p}{p^2-1}\big)\Gamma_p\big(1-\frac{i_1+i_0p}{p^2-1}\big)=\pm 1$, which is explained below. Hence in the range $1\le i<p^2-1$ we obtain

THEOREM 2. *For* $i=(p-1)k$ $(k=1,\ldots,p)$ *or* $i=\frac{p+1}{2}k$ $(k=1,3,\ldots,2(p-1)-1)$ *we have* $J(\omega^{-i},\omega^{\frac{p^2-1}{2}})\in\mathbb{Z}$.

In order to find all nontrivial solutions we explain the distribution relation of Gauss sums. The equality $g(\omega^{-i})=\pm g(\omega^{-i+\frac{q-1}{2}})$ in question is a relation between Gauss sums. Hence it follows necessarily only from the norm relations, the Davenport–Hasse relations and the 2-torsion relations of Gauss sums, because the Davenport–Hasse distribution of the Gauss sums is the universal odd distribution up to 2-torsion relations [6]–[9]. The equality $g(\omega^{-i})=\pm g(\omega^{-i+\frac{q-1}{2}})$ is equivalent to $g(\omega^{-i})^2=g(\omega^{-i+\frac{q-1}{2}})^2$, thus this equality comes only from the norm relations and the Davenport–Hasse relations. It is also known that the norm relations and the Davenport–Hasse relations of Gauss sums can be obtained from the norm relations and the distribution relations of the p-adic gamma function $\Gamma_p(x)$ together with consideration of the ϖ-parts by making use of the Gross–Koblitz formula. The norm relations of $\Gamma_p(x)$ in the case of odd p are as follows [5]:

$$\Gamma_p(x)\Gamma_p(1-x)=(-1)^{1+u(-x)}\qquad\text{for any } x\in\mathbb{Z}_p,$$

where $u(-x)\in\mathbb{Z}$ denotes the unique integer satisfying $u(-x)\equiv -x \pmod p$, $0\le u(-x)\le p-1$.

The distribution relations of $\Gamma_p(x)$ are expressed as follows. Let m be any natural number prime to p. Then

$$\frac{\prod_{h=0}^{m-1}\Gamma_p\big(\frac{x+h}{m}\big)}{\Gamma_p(x)\prod_{h=1}^{m-1}\Gamma_p\big(\frac{h}{m}\big)}=m^{u(-x)}(m^{1-p})^{\frac{1}{p}(u(-x)+x)}\tag{6}$$

for any $x\in\mathbb{Z}_p$ [5]. This is called the *m-multiplication formula*.

Now, if d denotes the order of the character ω^{-i}, the equality $g(\omega^{-i})=\pm g(\omega^{-i+\frac{p^2-1}{2}})$ is left fixed by any $\varphi(d)$ automorphisms of the Galois group $G(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ of the extension $\mathbb{Q}(\zeta_d)/\mathbb{Q}$, where ζ_d means a primitive dth root of unity.

By setting

$$\frac{i_0+i_1p}{p^2-1}=\frac{\alpha}{d},\qquad \frac{i_1+i_0p}{p^2-1}=\frac{\beta}{d},\qquad (\alpha,d)=(\beta,d)=1,$$

namely $i_0=\frac{1}{d}(\beta p-\alpha)$, $i_1=\frac{1}{d}(\alpha p-\beta)$, where $\alpha p\equiv\beta \pmod d$, $\beta p\equiv\alpha$ (mod d), the equality (5) can be rewritten as

$$\Gamma_p\Big(\frac{\alpha}{d}\Big)\Gamma_p\Big(\frac{\beta}{d}\Big)=\pm\Gamma_p\Big(\frac{\alpha}{d}+\frac{1}{2}\Big)\Gamma_p\Big(\frac{\beta}{d}-\frac{1}{2}\Big).\tag{7}$$

Furthermore, α and β satisfy

$$0<\frac{\alpha}{d}<\frac{1}{2}\quad\text{and}\quad\frac{1}{2}<\frac{\beta}{d}<1. \tag{8}$$

From the invariance property mentioned above, the equality (7) is simply equivalent to

$$\Gamma_p\left(\frac{1}{d}\right)\Gamma_p\left(\frac{\beta}{d}\right)=\pm\Gamma_p\left(\frac{1}{d}+\frac{1}{2}\right)\Gamma_p\left(\frac{\beta}{d}-\frac{1}{2}\right), \tag{9}$$

where $\beta\equiv p \pmod d$, $\frac{1}{d}<\frac{\beta}{d}-\frac{1}{2}<\frac{\beta}{d}<\frac{1}{d}+\frac{1}{2}$.

First we assume that the equality (9) (or (7)) holds. Under this assumption we prove several lemmas.

LEMMA 1. *Denote the order of ω^{-i} by d. If ω^{-i} gives a nontrivial solution, namely the equality* (7) *holds for ω^{-i}, then d is divisible by* 4.

Proof. The order of $\chi\eta=\omega^{-i+(p^2-1)/2}$ is d or $2d$ when d is even or odd respectively. Therefore, we can suppose that d is odd by taking $\chi\eta$ instead of χ if necessary. Then $\sigma_2:\zeta_d\to\zeta_d^2$ is an element of the Galois group $G(\mathbb{Q}(\zeta_d)/\mathbb{Q})$. Let n be the minimal positive integer such that $2^n\equiv 1 \pmod d$. From the assumption and letting σ_2 operate repeatedly on the Davenport–Hasse relation

$$g(\chi)^2=\pm g(\chi)g(\chi\eta)=\pm\chi(2^{-2})g(\eta)g(\chi^2),$$

we obtain

$$g(\chi)=g(\chi^{2^n})=\pm p^{-(2^n-1)}g(\chi)^{2^n}. \tag{10}$$

By the Gross–Koblitz formula we then have

$$g(\chi)^{2^n}=-(\varpi^{\frac{\alpha+\beta}{d}(p-1)})^{2^n}\left(\Gamma_p\left(\frac{\alpha}{d}\right)\Gamma_p\left(\frac{\beta}{d}\right)\right)^{2^n}.$$

Comparing the ϖ-parts of both sides of (10) we have

$$\varpi^{\frac{\alpha+\beta}{d}(p-1)}=\pm(-\varpi^{\frac{\alpha+\beta}{d}(p-1)})^{2^n}p^{-(2^n-1)}.$$

This yields $\frac{\alpha+\beta}{d}=1$. By virtue of the norm relation of $\Gamma_p(x)$ this means that ω^{-i} is a trivial solution. Consequently, d is divisible by 4.

As mentioned before, since the equality is a relation between Gauss sums, it comes from the norm relations and the distribution relations of the p-adic gamma function. It is equivalent to obtain the simultaneous solutions of the equality (9) and the distribution relations (6). Thus, if the equality (9) or (7) has a simultaneous solution with the m-multiplication formula for some positive integer m prime to p, then we call the equality (9) *m-reducible*. Then the equality holds if and only if there exists an odd prime l such that l

divides d exactly once and the equality is l-reducible. Namely, if the equality is m-reducible for some m, then it has to be l-reducible for some odd prime l.

Using these definitions we have

LEMMA 2. *Assume that ω^{-i} gives a nontrivial solution of the equality* (9) *and this is l-reducible for an odd prime divisor l of d. Then l is equal to* 3 *or* 5. *Furthermore, the equality holds only when $d = 24$ and $p \equiv 17, 19 \pmod{24}$ or $d = 60$ and $p \equiv 41, 49 \pmod{60}$.*

Proof. We distinguish two cases according as $p - 1 \equiv 0 \pmod{l}$ or $p + 1 \equiv 0 \pmod{l}$.

Case 1: $p + 1 \equiv 0 \pmod{l}$. As $(p - 1, l) = 1$, the denominator of $\frac{\beta}{d} - \frac{1}{d} \equiv \frac{p-1}{d} \pmod{1}$ is divisible by l. From the above, it must be equal to l.

Now we put

$$\frac{\beta}{d} - \frac{1}{d} = \frac{h}{l}, \quad (h, l) = 1, \quad 0 < h < l.$$

The left-hand side of the equality (9) appears in the numerator of the following distribution relation:

$$\frac{\prod_{x=0}^{l-1} \Gamma_p\big(\frac{1}{d} + \frac{x}{l}\big)}{\Gamma_p\big(\frac{l}{d}\big) \prod_{x=1}^{l-1} \Gamma_p\big(\frac{x}{l}\big)} = l^{u(-\frac{l}{d})} \big(l^{1-p}\big)^{\frac{1}{p}(u(-\frac{l}{d}) + \frac{l}{d})}. \tag{11}$$

Similarly the right-hand side of (9) appears in the numerator of the distribution relation

$$\frac{\prod_{x=0}^{l-1} \Gamma_p\big(\frac{\beta}{d} - \frac{1}{2} + \frac{x}{l}\big)}{\Gamma_p\big(\frac{l\beta}{d} - \frac{l}{2}\big) \prod_{x=1}^{l-1} \Gamma_p\big(\frac{x}{l}\big)} = l^{u(-\frac{l\beta}{d} + \frac{l}{2})} \big(l^{1-p}\big)^{\frac{1}{p}(u(-\frac{l\beta}{d} + \frac{l}{2}) + \frac{l\beta}{d} - \frac{l}{2})}. \tag{12}$$

Exactly one fraction, say $\frac{1}{d} + \frac{m}{l}$, in the numerator of (11) has the denominator $\frac{d}{l}$. Then $\frac{1}{d} + \frac{m}{l} = \frac{1}{d}(1 + \frac{dm}{l}) \equiv 0 \pmod{\frac{l}{d}}$. The other $l-1$ fractions have the denominator d. We first consider the fraction $\frac{1}{d} + \frac{j}{l}$ $(0 \le j < h, j \ne m)$. Letting the automorphism $\sigma_p : \zeta_d \to \zeta_d^p$ operate on the Gauss sums, we have

$$p\left(1 + \frac{d}{l}j\right) \equiv \beta + \frac{d}{l}pj \equiv \beta - \frac{d}{l}j \equiv 1 + \frac{d}{l}(h - j) \pmod{d}.$$

This means that $\Gamma_p\big(\frac{1}{d} + \frac{j}{l}\big)\Gamma_p\big(\frac{1}{d} + \frac{h-j}{l}\big)$ is the gamma product part of the Gauss sum $g(\chi\xi_l)$, where ξ_l denotes a character of order l. Since an element of the Galois group $G(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ maps $g(\chi)$ to $g(\chi\xi_l)$ and the equality is left fixed by this automorphism, the fractions $\frac{1}{d} + \frac{j}{l}$ and $\frac{1}{d} + \frac{h-j}{l}$ satisfy the condition (8), namely one of them is less than $\frac{1}{2}$ and the other is greater than $\frac{1}{2}$.

Next we consider the fractions $\frac{1}{d} + \frac{h+j}{l}$ $(0 < j < l - h, j \ne m)$. Letting

σ_p operate on the Gauss sums, we have

$$p\left(1+\frac{d}{l}(h+j)\right) \equiv \beta+\frac{d}{l}p(h+j) \equiv 1+\frac{d}{l}h-\frac{d}{l}(h+j) \equiv 1+\frac{d}{l}(l-j) \pmod{d}.$$

This means that $\Gamma_p\big(\frac{1}{d}+\frac{h+j}{l}\big)\Gamma_p\big(\frac{1}{d}+\frac{l-j}{l}\big)$ is also the gamma product part of a Gauss sum. Hence $\frac{1}{d}+\frac{h+j}{l}$ and $\frac{1}{d}+\frac{l-j}{l}$ must also satisfy the condition (8), but both numbers are greater than $\frac{1}{2}$.

Therefore $h=l-1$ or $h=l-2$, and $m=l-1$. But the case $h=l-2$ and $m=l-1$ does not occur. Indeed, when we take $j=\frac{l-1}{2}$, the product $\Gamma_p\big(\frac{1}{d}+\frac{1}{l}\frac{l-1}{2}\big)\Gamma_p\big(\frac{1}{d}+\frac{1}{l}\big(l-2-\frac{l-1}{2}\big)\big)$ is the gamma product part of a Gauss sum. But the fractions $\frac{1}{d}+\frac{1}{l}\frac{l-1}{2}$ and $\frac{1}{d}+\frac{1}{l}\big(l-2-\frac{l-1}{2}\big)$ do not satisfy the condition (8), as

$$\frac{1}{d}+\frac{1}{l}\frac{l-1}{2}<\frac{1}{2} \quad \text{and} \quad \frac{1}{d}+\frac{1}{l}\left(l-2-\frac{l-1}{2}\right)<\frac{1}{2}.$$

Hence $h=l-1$. We see that $m=\frac{1}{2}(l-1)$ and $\beta=1+\frac{d}{l}(l-1)$. Since the $l-1$ values of the gamma function in the numerator of (11) (also (12)) are the gamma product parts of certain $\frac{l-1}{2}$ Gauss sums, and an element of $G(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ maps $g(\chi)$ to those $\frac{l-1}{2}$ Gauss sums, and the equality is left fixed by these automorphisms, the distribution relations (11), (12) give rise to the relation

$$\Gamma_p\left(\frac{l}{d}\right)\Gamma_p\left(\frac{1}{2}-\frac{1}{d}+\frac{1}{2l}\right)=\pm\Gamma_p\left(\frac{l}{d}+\frac{1}{2}\right)\Gamma_p\left(\frac{1}{2l}-\frac{1}{d}\right). \tag{13}$$

Since $\frac{1}{2l}-\frac{1}{d}\equiv\frac{1}{d}\big(\frac{d}{2l}-1\big)\equiv 0 \pmod{\frac{l}{d}}$, we obtain $\frac{d}{2l}\equiv 1 \pmod{l}$. Therefore the order d can be written as $d=2l(kl+1)$ for some odd integer k.

Assume that $kl\equiv 1 \pmod 4$. If l is not equal to 5, we put $x=\frac{1}{2}(kl+5)$. Then by letting the automorphism $\sigma_{\frac{1}{2}(kl+5)}:\zeta_d\to\zeta_d^{\frac{1}{2}(kl+5)}$ operate on the Gauss sum $g(\chi)$, we have

$$\begin{aligned}\beta x &= (1+2(lk+1)(l-1))\frac{1}{2}(kl+5)\\ &\equiv \frac{1}{2}(-2l-2l(k-1)-1)(kl+5)\\ &\equiv kl^2-\frac{9}{2}kl+l-\frac{5}{2} \pmod{d}.\end{aligned}$$

The condition (8) is not satisfied except for $l=3$ as

$$kl^2-\frac{9}{2}kl+l-\frac{5}{2}<\frac{d}{2}=kl^2+l.$$

When $kl\equiv 3 \pmod 4$ and $l\neq 3$, by letting the automorphism $\sigma_{\frac{1}{2}(kl+3)}:\zeta_d\to\zeta_d^{\frac{1}{2}(kl+3)}$ operate on the Gauss sum $g(\chi)$, we see that (8) is not satisfied.

Now we assume $l = 3$. Then $d = 18k + 6$ and $\beta = 12k + 5$. If $k \equiv 1 \pmod 4$ and $k > 1$, we put $x = \frac{1}{2}(3k+7)$. Then by letting the automorphism $\sigma_{\frac{1}{2}(3k+7)} : \zeta_d \to \zeta_d^{\frac{1}{2}(3k+7)}$ operate on the Gauss sum $g(\chi)$, we have

$$\beta x = \frac{1}{2}(3k+7)(12k+5) \equiv 7k+5+\frac{1}{2}(k+1) \pmod d,$$
$$7k+5+\frac{1}{2}(k+1) < 9k+3 = \frac{d}{2}.$$

This contradicts (8).

If $k \equiv 3 \pmod 4$, we see that βx is also less than $\frac{1}{2}$ by letting the automorphism $\sigma_{\frac{1}{2}(3k-11)}$ for $k > 3$ operate on the Gauss sum. In two cases $l = 3$, $k = 1$ and $l = 3$, $k = 3$, we can verify easily that for every positive integer c such that $(c, d) = 1$, one of $\frac{c}{d}$ and $\frac{\beta c}{d}$ is less than $\frac{1}{2}$ and the other is greater than $\frac{1}{2}$.

We treat the case $l = 5$ similarly. Assume $k > 1$. Then, operating by $\sigma_{\frac{1}{2}(5k-7)} : \zeta_d \to \zeta_d^{\frac{1}{2}(5k-7)}$ if $k \equiv 1 \pmod 4$ and by $\sigma_{\frac{1}{2}(5k+3)} : \zeta_d \to \zeta_d^{\frac{1}{2}(5k+3)}$ if $k \equiv 3 \pmod 4$ respectively, we get the same contradiction. However, the condition (8) is satisfied in the case $k = 1$.

Consequently, we have the solutions $d = 24$, $\beta = 17$, and $d = 60$, $\beta = 41$, and $d = 60$, $\beta = 49$.

Case 2: $p - 1 \equiv 0 \pmod l$. As $(p+1, l) = 1$, the denominator of $\frac{3}{2} - \frac{\beta}{d} - \frac{1}{d} \equiv \frac{3}{2} - \frac{p+1}{d} \pmod 1$ is divisible by l, hence it must be equal to l. As above, we have quite similarly the solutions $d = 24$, $\beta = 19$, and $d = 60$, $\beta = 41$, and $d = 60$, $\beta = 49$.

From Lemmas 1 and 2 we obtain

THEOREM 3. *It is necessary and sufficient for* $J(\omega^{-i}, \omega^{\frac{p^2-1}{2}}) \in \mathbb{Q}$, *except for the trivial solutions, that the character* ω^{-i} *is of order* 24 *for* $p \equiv 17, 19 \pmod{24}$ *or the character* ω^{-i} *is of order* 60 *for* $p \equiv 41, 49 \pmod{60}$.

Proof. Assume that the equality (7) or (9) holds. From the above lemmas, the order d is equal to 24 or 60, and $p \equiv 17, 19 \pmod{24}$ or $p \equiv 41, 49 \pmod{60}$.

Conversely, let d be equal to 24 or 60, and $p \equiv 17, 19 \pmod{24}$ or $p \equiv 41, 49 \pmod{60}$, respectively. When $d = 24$ and $p \equiv 17 \pmod{24}$, from the norm relations together with the distribution relations of $\Gamma_p(x)$, we have

$$\frac{\Gamma_p\left(\frac{1}{24}\right)\Gamma_p\left(\frac{9}{24}\right)\Gamma_p\left(\frac{17}{24}\right)}{\Gamma_p\left(\frac{1}{8}\right)\Gamma_p\left(\frac{1}{3}\right)\Gamma_p\left(\frac{2}{3}\right)} = 3^{u(-\frac{1}{8})}(3^{1-p})^{\frac{1}{p}(u(-\frac{1}{8})+\frac{1}{8})} = 1$$

and

$$\frac{\Gamma_p\left(\frac{5}{24}\right)\Gamma_p\left(\frac{13}{24}\right)\Gamma_p\left(\frac{21}{24}\right)}{\Gamma_p\left(\frac{5}{8}\right)\Gamma_p\left(\frac{1}{3}\right)\Gamma_p\left(\frac{2}{3}\right)} = 3^{u(-\frac{5}{8})}(3^{1-p})^{\frac{1}{p}(u(-\frac{5}{8})+\frac{5}{8})} = 1,$$

hence we obtain the equality

$$\Gamma_p\left(\frac{1}{24}\right)\Gamma_p\left(\frac{17}{24}\right) = \pm\Gamma_p\left(\frac{5}{24}\right)\Gamma_p\left(\frac{13}{24}\right).$$

When $d = 60$ and $p \equiv 41 \pmod{60}$, from the norm relations together with the two distribution relations, we easily get

$$\frac{\Gamma_p\left(\frac{1}{60}\right)\Gamma_p\left(\frac{21}{60}\right)\Gamma_p\left(\frac{41}{60}\right)}{\Gamma_p\left(\frac{1}{20}\right)} = \pm\frac{\Gamma_p\left(\frac{11}{60}\right)\Gamma_p\left(\frac{31}{60}\right)\Gamma_p\left(\frac{51}{60}\right)}{\Gamma_p\left(\frac{11}{20}\right)}.$$

By making use of the distribution relation of 5-multiplication

$$\frac{\Gamma_p\left(\frac{1}{20}\right)\Gamma_p\left(\frac{5}{20}\right)\Gamma_p\left(\frac{9}{20}\right)\Gamma_p\left(\frac{13}{20}\right)\Gamma_p\left(\frac{17}{20}\right)}{\Gamma_p\left(\frac{1}{4}\right)\Gamma_p\left(\frac{1}{5}\right)\Gamma_p\left(\frac{2}{5}\right)\Gamma_p\left(\frac{3}{5}\right)\Gamma_p\left(\frac{4}{5}\right)} = 5^{u(-\frac{1}{4})}(5^{1-p})^{\frac{1}{p}(u(-\frac{1}{4})+\frac{1}{4})} = 1,$$

we see that

$$\Gamma_p\left(\frac{1}{60}\right)\Gamma_p\left(\frac{41}{60}\right) = \pm\Gamma_p\left(\frac{11}{60}\right)\Gamma_p\left(\frac{31}{60}\right).$$

This completes the proofs for sufficiency in the cases treated.

In the other cases, where $d = 24$ and $p \equiv 19 \pmod{24}$ or $d = 60$ and $p \equiv 49 \pmod{60}$, the sufficiency can be proved in a similar way.

It should be noted that the condition in Theorem 3 is sufficient in any general case where the problem is considered in $\mathrm{GF}(p^f)$ with $f \equiv 0 \pmod 2$. If a character ω^{-i} of order d is a solution of the equality, then the induced character $\omega^{-i} \circ N_{\mathrm{GF}(p^f)/\mathrm{GF}(p^2)}$ of $\mathrm{GF}(p^f)^\times$, which is of the same order d, also satisfies the equality

$$\left(\Gamma_p\left(\frac{1}{d}\right)\Gamma_p\left(\frac{\beta}{d}\right)\right)^{\frac{f}{2}} = \pm\left(\Gamma_p\left(\frac{1}{d}+\frac{1}{2}\right)\Gamma_p\left(\frac{\beta}{d}-\frac{1}{2}\right)\right)^{\frac{f}{2}},$$

where $p \equiv \beta \pmod d$ and $N_{\mathrm{GF}(p^f)/\mathrm{GF}(p^2)}$ means the norm with respect to $\mathrm{GF}(p^f)/\mathrm{GF}(p^2)$.

This equality amounts just to one of the Davenport–Hasse relations for Gauss sums. Thus we see that the condition in Theorem 3 is still sufficient in any general case with $f \equiv 0 \pmod 2$.

REFERENCES

[1] R. F. Coleman, *The Gross–Koblitz formula*, Adv. Stud. Pure Math. 12 (1987), 21–52.

[2] H. Davenport und H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. 172 (1935), 151–182.

[3] M. Ishibashi, H. Sato and K. Shiratani, *On the Hasse invariants of elliptic curves*, Kyushu J. Math. 48 (1994), 307–321.

[4] T. Ito, H. Ishibashi, A. Munemasa and M. Yamada, *The Terwilliger algebras of cyclotomic schemes and rationality of Jacobi sums*, in: Algebraic Combinatorics (Fukuoka 1993), 43–44.

[5] N. Koblitz, *p-adic Analysis: a Short Course on Recent Works*, Cambridge University Press, Cambridge, 1980.

[6] C. G. Schmidt, *Die Relationenfaktorgruppen von Stickelberger-Elementen und Kreiszahlen*, J. Reine Angew. Math. 315 (1980), 60–72.

[7] L. G. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, 1982.

[8] K. Yamamoto, *On a conjecture of Hasse concerning multiplicative relations of Gaussian sums*, J. Combin. Theory 1 (1966), 476–489.

[9] —, *The gap group of multiplicative relationships of Gaussian sums*, Sympos. Math. 15 (1975), 427–440.

Graduate School of Mathematics
Kyushu University
Fukuoka 812, Japan
E-mail: siratani@math.kyushu-u.ac.jp
yamada@math.kyushu-u.ac.jp

Received 24 September 1996