Indian J. pure appl. Math., **12**(7) : 804-806, July 1981

A CONGRUENCE RELATION BETWEEN THE COEFFICIENTS OF THE JACOBI SUM

J. C. PARNAMI, M. K. AGRAWAL AND A. R. RAJWADE
Mathematics Department, Panjab University, Chandigarh 160014

(*Received* 10 *December* 1980)

Let $J(a, b) = \Sigma\, \chi^a(v)\, \chi^b(v+1)$ be the Jacobi function where χ is a character modulo the odd prime l. The congruence $J \equiv -1 \pmod{(1-\zeta)^2}$ is well known (where $\zeta = e^{2\pi i/l}$). We improve this to $J \equiv -1 \pmod{(1-\zeta)^3}$. Further write $J(a, b) = a_1\zeta + \ldots - a_{l-1}\zeta^{l-1}$ $(a_j \in \mathbb{Z})$. The relations

$$\Sigma\, a_k \equiv -1,\ \Sigma\, k a_k \equiv 0,\ \Sigma\, k^3 a_k \equiv 0,\ \Sigma\, k^4 a_k \equiv 0 \pmod{l}$$

are well known. We prove a new relation viz. if $l > 7$ then

$$\Sigma\, k^6 a_k + 10\,(\Sigma\, k^3 a_k)^2 \equiv 0 \pmod{l}.$$

Let F_q be the finite field of q elements where $q = p^\alpha$ is a power of an odd prime $p \equiv 1 \pmod{l}$ (l an odd prime). Let γ be a generator of F_q^* and let $\zeta = e^{2\pi i/l}$. Define the lth power character χ on F_q by

$$\chi(\gamma) = \zeta, \quad \chi(0) = 0.$$

The Jacobi sum is then defined by

$$J(a, b) = \sum_{v \in F_q} \chi^a(v)\, \chi^b(v+1).$$

(Here the integers a, b only matter modulo l). Write

$$J(a, b) = a_1\zeta + \ldots + a_{l-1}\zeta^{l-1} (a_i \in \mathbb{Z}). \qquad \ldots(1)$$

Let $a, b, a+b \not\equiv 0 \pmod{l}$. The following results are classical and well known [see Dickson (1935)], at least for the case $q = p$:

$$J \cdot \bar{J} = p^\alpha \qquad \ldots(2)$$

$$J \equiv -1 \pmod{(1-\zeta)^2}. \qquad \ldots(3)$$

We shall first prove the following:

Proposition 1 — For $l \geqslant 5$ we have $J \equiv -1 \pmod{(1-\zeta)^3}$.

PROOF : Let $F(x) = a_1x + a_2x^2 + \ldots + a_{l-1}x^{l-1}$

$$= b_0 + b_1(x-1) + \ldots + b_{l-1}(x-1)^{l-1},$$

so that by (1), $J = F(\zeta)$, $\bar{J} = F(\zeta^{-1})$. By (3), $b_0 + 1 \equiv 0 \pmod{(1-\zeta)}$ and so $b_0 + 1 \equiv 0 \pmod{l}$. Consequently $b_1 \equiv 0 \pmod{(1-\zeta)}$ and so $\equiv 0 \pmod{l}$. By (2), therefore,

$$(-1 + b_2(\zeta - 1)^2 + \ldots + b_{l-1}(\zeta - 1)^{l-1})(-1 + b_2(\zeta^{-1} - 1)^2 + \ldots + b_{l-1}(\zeta^{-1} - 1)^{l-1}) \equiv 1 \pmod{(\zeta - 1)^{l-1}}, \text{ since } (l) = (\zeta - 1)^{l-1}. \quad \ldots(4)$$

This gives

$$b_2(1 + \zeta^{-2}) \equiv 0 \pmod{(\zeta - 1)}$$

since $l - 1 > 3$ and so $b_2 \equiv 0 \pmod{l}$.

Thus

$$b_0 \equiv -1, b_1 \equiv 0, b_2 \equiv 0 \text{ (modulo } l). \quad \ldots(5)$$

It follows that

$$J \equiv -1 \pmod{(1-\zeta)^3}.$$

This proves Proposition 1.

In addition to (5) the following lemma gives two more congruence relations amongst the coefficients b_j.

Lemma — For $l > 7$, we have

(i) $3b_3 + 2b_4 \equiv 0 \pmod{l}$;

(ii) $60b_3 + 60b_4 + 30b_5 + 12b_6 + 6b_3^2 \equiv 0 \pmod{l}$.

PROOF: By (4) and (5) we have

$$(-1 + b_3(\zeta - 1)^3 + b_4(\zeta - 1)^4 + b_5(\zeta - 1)^5 + b_6(\zeta - 1)^6 + \ldots) \times (-1 - \zeta^{-3}b_3(\zeta - 1)^3 + \zeta^{-4}b_4(\zeta - 1)^4 - \zeta^{-5}b_5(\zeta - 1)^5 + \zeta^{-6}b_6(\zeta - 1)^6 + \ldots) \equiv 1 \pmod{(\zeta - 1)^7} \text{ (since } l - 1 \geqslant 7).$$

Hence

$$b_3(-1 + \zeta^{-3}) + b_4(\zeta - 1)(-1 - \zeta^{-4}) + b_5(\zeta - 1)^2(-1 + \zeta^{-5}) + b_6(\zeta - 1)^3(-1 - \zeta^{-6}) - b_3^2(\zeta - 1)^3\zeta^{-3} \equiv 0 \pmod{(\zeta - 1)^4}.$$

Now let

$$p(x) = b_3(-1 + x^{l-3}) + b_4(x-1)(-1 - x^{l-4}) + b_5(x-1)^2(-1 + x^{l-5}) + b_6(x-1)^3(-1 - x^{l-6}) - b_3^2(x-1)^3 x^{l-3}.$$

Then

$$p(\zeta) \equiv 0 \pmod{(\zeta - 1)^4} \qquad \ldots(6)$$

Further write $p(x) = c_0 + c_1(x-1) + c_2(x-1)^2 + \ldots$, so that, by (6) we have

$$c_0 + c_1(\zeta - 1) + c_2(\zeta - 1)^2 + c_3(\zeta - 1)^3 \equiv 0 \pmod{(\zeta - 1)^4}.$$

This gives successively $c_0 \equiv 0$, $c_1 \equiv 3$, $c_2 \equiv 0$, $c_3 \equiv 0$ (modulo l), i.e. $p(1) \equiv 0$, $p'(1) \equiv 0$, $\frac{1}{2}p''(1) \equiv 0$, $\frac{1}{6}p'''(1) \equiv 0$ (modulo l). Hence by the definition of $p(x)$ we get $0 \equiv 0$, $-3b_3 - 2b_4 \equiv 0$, $12b_3 + 8b_4 \equiv 0$ and $-60b_3 - 60b_4 - 30b_5 - 12b_6 - 6b_3^2 \equiv 0$ (modulo l). This proves the Lemma.

Now using the fact that $b_j = (1/j!)\, F^{(j)}(1) = (1/j!) \sum k(k-1) \ldots (k-j+1)\, a_k$ our relations in (5) and (i) of Lemma immediately give the following well-known congruence relations amongst the coefficients a_j:

$$\sum a_k \equiv -1, \quad \sum k a_k \equiv 0, \quad \sum k^2 a_k \equiv 0, \quad \sum k^4 a_k \equiv 0 \text{ (modulo } l).$$

Futher (ii) of our Lemma, as above, gives our main result viz. the following:

Proposition 2 — For $l > 7$, we have $\sum k^6 a_k + 10(\sum k^3 a_k)^2 \equiv 0 \pmod{l}$.

Reference

Dickson, L. E. (1935). Cyclotomy and trinomial congruences. *Trans. Am. math. Soc.*, **37**, 363–80.