

STANISLAV JAKUBEC

Note on the jacobi sum $J(\chi, \chi)$

Journal de Théorie des Nombres de Bordeaux, tome 7, n° 2 (1995),
p. 461-471

http://www.numdam.org/item?id=JTNB_1995__7_2_461_0

© Université Bordeaux 1, 1995, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Note on the Jacobi sum $J(\chi, \chi)$.

par STANISLAV JAKUBEC

Notation

$$\zeta_l = \cos \frac{2\pi}{l} + i \sin \frac{2\pi}{l}$$

$$\zeta_p = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$$

$$m = \frac{l-1}{2}$$

χ - the Dirichlet character modulo p , $\chi(x) = \zeta_l^{\text{ind}(x)}$

$J(\chi, \chi) = \sum_{x+y=1} \chi(x)\chi(y)$ - Jacobi sum

$$\tau(\chi) = \sum_{x=1}^{p-1} \chi(x)\zeta_p^x \text{ - Gaussian sum}$$

Recall that $\tau(\chi) \in K\mathbf{Q}(\zeta_l)$, where $K \subset \mathbf{Q}(\zeta_p)$ and $[K : \mathbf{Q}] = l$.

Introduction

Let $J(\chi, \chi)$ be the Jacobi sum, $J(\chi, \chi) \in \mathbf{Q}(\zeta_l)$. It is well known that $J(\chi, \chi)\overline{J(\chi, \chi)} = p$, and one easily proves that

$$J(\chi, \chi) \equiv \overline{\chi}(4) \pmod{2}.$$

The main aim of this paper is to solve the problem: When is $J(\chi, \chi)$ up to association and conjugation uniquely determined by the solution of the equation

$$X\overline{X} = p, X \in \mathbf{Z}(\zeta_l), X \equiv 1 \pmod{2}?$$

We give a complete solution in cases $l = 11, 19$.

On the basis of this result, the following question is answered:

When is the prime 2 an 11-th resp. a 19-th power modulo p if p is not representable by the quadratic form $x^2 + 11y^2$, resp. $x^2 + 19y^2$.

We shall now present a survey of results obtained by solving the problem when the prime 2 is an l -th power modulo p .

Jacobi has given necessary and sufficient conditions for primes $q < 37$ to be cubes modulo primes $p \equiv 1 \pmod{3}$. For example, he proves the following

PROPOSITION 1. *2 is a cube modulo p if and only if $L \equiv 0 \pmod{2}$, where*

$$4p = L^2 + 27M^2,$$

$$L \equiv 1 \pmod{3}.$$

Emma Lehmer [2] finds the following result:

PROPOSITION 2. *Let $p \equiv 1 \pmod{5}$ be a prime. Then 2 is a fifth power modulo p if and only if $x \equiv 0 \pmod{2}$, where (x, u, v, w) is one of the exactly four solutions (x, u, v, w) , $(x, -u, -v, w)$, $(x, v, -u, -w)$, $(x, -v, u, -w)$ of the diophantine system (Dickson):*

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2,$$

$$xw = v^2 - 4uv - u^2,$$

$$x \equiv 1 \pmod{5}.$$

P.A. Leonard and K.S. Williams [4] prove the following

PROPOSITION 3. *Let $p \equiv 1 \pmod{7}$ be a prime. Then 2 is a seventh power modulo p if and only if $x_1 \equiv 0 \pmod{2}$, where $(x_1, x_2, \dots, x_6)$ is one of the exactly six non-trivial solutions of the diophantine system of equations*

$$(i) \quad 72p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2),$$

$$(ii) \quad 12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 + 24x_2x_3 - 24x_2x_4 + 48x_3x_4 + 98x_5x_6 = 0,$$

$$(iii) \quad 12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 + 48x_2x_3 + 24x_2x_4 + 24x_3x_4 + 490x_5x_6 = 0,$$

$$(iv) \quad x_1 \equiv 1 \pmod{7}.$$

P.A. Leonard, B.C. Mortimer and K.S. Williams [3] prove the following

PROPOSITION 4. *Let $p \equiv 1 \pmod{11}$ be a prime. Then 2 is an eleventh power modulo p if and only if a certain condition involving solutions of a very complicated diophantine system holds (the exact statement may be seen in [3]).*

J.C. Parnami, M.K. Agrawal and A.R. Rajwade [5] have the following

PROPOSITION 5. *Let $p \equiv 1 \pmod{l}$. Then 2 is an l -th power modulo p if and only if*

$$a_1 + a_2 + \cdots + a_{l-1} \equiv 0 \pmod{2},$$

where $(a_1, a_2, \dots, a_{l-1})$ is one of the exactly $l-1$ solutions of the diophantine system of equations

$$(i) \quad p = \sum_{i=1}^{l-1} a_i^2 - \sum_{i=1}^{l-1} a_i a_{i+1},$$

$$(ii) \quad \sum_{i=1}^{l-1} a_i a_{i+1} = \sum_{i=1}^{l-1} a_i a_{i+2} = \cdots = \sum_{i=1}^{l-1} a_i a_{i+l-1},$$

$$(iii) \quad p \text{ does not divide } \prod_{\lambda(2k) > k} \sigma_k \left(\sum_{i=1}^{l-1} a_i \zeta_l^i \right),$$

where $\lambda(n)$ is the least non-negative residue of n modulo l , and σ_k is the automorphism $\zeta_l \rightarrow \zeta_l^k$,

$$(iv) \quad 1 + a_1 + \cdots + a_{l-1} \equiv 0 \pmod{l},$$

$$(v) \quad a_1 + 2a_2 + \cdots + (l-1)a_{l-1} \equiv 0 \pmod{l}.$$

Now let $X\overline{X} = p$, and let $J(\chi, \chi)$ be associated with the number X , i.e. $J(\chi, \chi) = \varepsilon X$, where ε is a unit of the field $\mathbf{Q}(\zeta_l)$. Then

$$J(\chi, \chi) \overline{J(\chi, \chi)} = p = \varepsilon \overline{\varepsilon} X \overline{X}$$

implies $\varepsilon \overline{\varepsilon} = 1$ and hence $\varepsilon = (-\zeta_l)^n$. So we have

$$J(\chi, \chi) = (-\zeta_l)^n X.$$

Let 2 be a primitive root modulo l . Consider a residue class field $\mathbf{Z}(\zeta_l)/(2)$ of the degree $f = l-1$ over $\mathbf{Z}/2\mathbf{Z}$. Let g be a generator of the multiplicative group $(\mathbf{Z}(\zeta_l)/(2))^*$ of the field $\mathbf{Z}(\zeta_l)/(2)$ such that there holds $\varphi(g) = g^2$, where φ is a generator of the Galois group $G(\mathbf{Q}(\zeta_l)/\mathbf{Q})$.

LEMMA 1. Every unit ε of the field $\mathbf{Q}(\zeta_l)$ is a $\frac{2^m+1}{l}$ -th power in the group $(\mathbf{Z}(\zeta_l)/(2))^*$, $m = \frac{l-1}{2}$.

Proof. Let $\varepsilon \equiv g^n \pmod{2}$. It is necessary to prove that $\frac{2^m+1}{l} | n$. Consider the unit $\varepsilon_1 = \prod_{i=0}^{m-1} \varphi^i(\varepsilon)$. Then $\varepsilon_1 \cdot \bar{\varepsilon}_1 = N(\varepsilon) = 1$, hence ε_1 must be a root of 1, therefore $\varepsilon_1^{2^l} = 1$. Further,

$$1 = \varepsilon_1^{2^l} = \prod_{i=0}^{m-1} \varphi^i(\varepsilon)^{2^l} \equiv \prod_{i=0}^{m-1} \varphi^i(g^n)^{2^l} \equiv \prod_{i=0}^{m-1} g^{2^{nl} \cdot 2^i} \equiv g^{2^{ln}(2^m-1)} \pmod{2}.$$

It follows that $2ln(2^m - 1) \equiv 0 \pmod{2^{l-1} - 1}$, and therefore $n \equiv 0 \pmod{\frac{2^m+1}{l}}$. $\square$

LEMMA 2. Let 2 be a primitive root modulo l . For a natural number a , $0 < a \leq l-1$ the following identity holds

$$a \frac{2^{l-1} - 1}{l} = \sum_{n=1}^{l-1} \left[\frac{2n}{l} \right] 2^{r_n}$$

(the decomposition into binary system), where $r_n \equiv l - 2 - \text{ind}(n) + \text{ind}(a) \pmod{l-1}$, $0 \leq r_n < l-1$, and $\text{ind}(x)$ is the index of the element x in the group $(\mathbf{Z}/l\mathbf{Z})^*$ under the base 2, i.e. $2^{\text{ind}(x)} \equiv x \pmod{l}$.

Proof. The lemma can be readily proved when the rational number $\frac{a}{l}$ is expressed in the binary system, $\frac{a}{l} = \sum_{n=1}^{\infty} a_n 2^{-n}$.

LEMMA 3. The factorisation of the Jacobi sum $J(\chi, \chi)$ into prime divisors of the field $\mathbf{Q}(\zeta_l)$ is $J(\chi, \chi) \approx \prod_{n=1}^{l-1} \sigma_{\frac{1}{n}}(\mathfrak{p})^{[\frac{2n}{l}]}$, where $\mathfrak{p}$ is a prime divisor of the field $\mathbf{Q}(\zeta_l)$, $\mathfrak{p} | p$, and $\sigma_{\frac{1}{n}}$ is an automorphism $\sigma_{\frac{1}{n}}(\zeta_l) = \zeta_l^{\frac{1}{n}}$.

Proof. According to [1],

$$J(\chi, \chi) = \frac{\tau(\chi)\tau(\chi)}{\tau(\chi^2)}.$$

The factorisation $J(\chi, \chi) \approx \prod_{n=1}^{l-1} \sigma_{\frac{1}{n}}(\mathfrak{p})^{[\frac{2n}{l}]}$ is obtained using the factorisation of the Gaussian sum into prime divisors of the field $K\mathbf{Q}(\zeta_l)$. $\square$

Consider a divisor $A = \prod_{i=0}^{l-2} \varphi^i(\mathfrak{p})^{j_i}$, where $j_i = 0; 1$, and define

$$\Psi\left(\prod_{i=0}^{l-2} \varphi^i(\mathfrak{p})^{j_i}\right) = \sum_{i=0}^{l-2} j_i 2^i.$$

LEMMA 4. *The factorisation $A = \prod_{i=0}^{l-2} \varphi^i(\mathfrak{p})^{j_i}$ is a conjugation of the factorisation $J(\chi, \chi) = \prod_{n=1}^{l-1} \sigma_{\frac{1}{n}}(\mathfrak{p}) \left[\frac{2n}{l}\right]$ if and only if $\Psi\left(\prod_{i=0}^{l-2} \varphi^i(\mathfrak{p})^{j_i}\right) = a \frac{2^{l-1}-1}{l}$, where $0 < a \leq l-1$.*

Proof. Let A be a conjugation of $J(\chi, \chi)$. Then $A = J(\chi^s, \chi^s)$ for some s . If $s \equiv \frac{k}{2} \pmod{l}$, then we can write

$$\begin{aligned} J_s &= J_{\frac{k}{2}} \approx \prod_{n=1}^{l-1} \sigma_{\frac{1}{n}}(\mathfrak{p})^{\left[\frac{2n}{l}\right]} = \prod_{n=1}^{l-1} \varphi^{\text{ind}(\frac{1}{n} \cdot \frac{k}{2})}(\mathfrak{p})^{\left[\frac{2n}{l}\right]} \\ \Psi\left(\prod_{n=1}^{l-1} \varphi^{\text{ind}(\frac{1}{n} \cdot \frac{k}{2})}(\mathfrak{p})^{\left[\frac{2n}{l}\right]}\right) &= \sum_{n=1}^{l-1} \left[\frac{2n}{l}\right] 2^{\text{ind}(\frac{1}{n} \cdot \frac{k}{2})} = \\ &= \sum_{n=1}^{l-1} \left[\frac{2n}{l}\right] \cdot 2^{l-1-\text{ind}(n)+\text{ind}(k)-1} = k \frac{2^{l-1}-1}{l} \quad (\text{by Lemma 2}). \end{aligned}$$

2. Conversely, let $\Psi\left(\prod_{i=0}^{l-2} \varphi^i(\mathfrak{p})^{j_i}\right) = a \frac{2^{l-1}-1}{l}$, $0 < a \leq l-1$.

By Lemma 2,

$$a \frac{2^{l-1}-1}{l} = \sum_{n=1}^{l-1} \left[\frac{2n}{l}\right] 2^{r_n} = \Psi\left(\prod_{n=1}^{l-1} \varphi^{\text{ind}(\frac{1}{n} \cdot \frac{a}{2})}(\mathfrak{p})^{\left[\frac{2n}{l}\right]}\right) = \sum_{i=0}^{l-2} j_i \cdot 2^i.$$

Since the expansion of a number in the binary system is uniquely determined, Lemma 4 is proved. $\square$

For $\mathfrak{p}|p$, denote by $h_{\mathfrak{p}}$ the least natural number such that a principal divisor $\mathfrak{p}^{h_{\mathfrak{p}}} = (\alpha)$.

THEOREM 1. *Let 2 be a primitive root modulo l , and let $\alpha \equiv g^M \pmod{2}$, where $(M, \frac{2^m+1}{l}) = 1$.*

If

$$X \in \mathbf{Z}(\zeta_l), \quad X\overline{X} = p, \quad X \equiv 1 \pmod{2},$$

then X is, up to association and conjugation, equal to the Jacobi sum $J(\chi, \chi)$.

Proof. According to Lemma 1, the choice of a generator α of the principal divisor $\mathfrak{p}^{h_p} = (\alpha)$ is not substantial.

Suppose the factorisation of X into prime divisors of the field $\mathbf{Q}(\zeta_l)$ is

$$X \approx \prod_{i=0}^{l-2} \varphi^i(\mathfrak{p})^{j_i}.$$

It is necessary to prove that this factorisation is a conjugate of the factorisation $J(\chi, \chi)$.

Clearly

$$X^{h_p} \approx \prod_{i=0}^{l-2} \varphi^i(\mathfrak{p}^{h_p})^{j_i} \approx \prod_{i=0}^{l-2} \varphi^i(\alpha)^{j_i},$$

hence

$$X^{h_p} = \varepsilon \prod_{i=0}^{l-2} \varphi^i(\alpha)^{j_i},$$

where ε is a unit of the field $\mathbf{Q}(\zeta_l)$.

But $\varepsilon\overline{\varepsilon} = 1$ implies $\varepsilon = (-\zeta_l)^s$, and therefore

$$X^{h_p} = (-\zeta_l)^s \prod_{i=0}^{l-2} \varphi^i(\alpha)^{j_i}.$$

From $X \equiv 1 \pmod{2}$ we obtain

$$\begin{aligned} 1 &\equiv (-\zeta_l)^s \prod_{i=0}^{l-2} \varphi^i(\alpha)^{j_i} \equiv (-\zeta_l)^s \prod_{i=0}^{l-2} \varphi^i(g^M)^{j_i} \equiv (-\zeta_l)^s \prod_{i=0}^{l-2} g^{M j_i \cdot 2^i} \equiv \\ &\equiv (-\zeta_l)^s g^{M \sum_{i=0}^{l-2} j_i 2^i} \pmod{2}. \end{aligned}$$

Since $\zeta_l \equiv -\zeta_l \pmod{2}$, we have

$$g^{Ml \sum_{i=0}^{l-2} j_i 2^i} \equiv 1 \pmod{2},$$

hence

$$lM \sum_{i=0}^{l-2} j_i 2^i \equiv 0 \pmod{2^{l-1} - 1}.$$

Consequently

$$M \sum_{i=0}^{l-2} j_i 2^i \equiv 0 \pmod{\frac{2^{l-1} - 1}{l}}. \quad (1)$$

It is easy to prove that the condition $X\overline{X} = p$ gives

$$\sum_{i=0}^{l-2} j_i 2^i \equiv 0 \pmod{2^m - 1}. \quad (2)$$

From the congruences (1) and (2), using the assumption $(M, \frac{2^m+1}{l}) = 1$ and the fact that $(2^m - 1, 2^m + 1) = 1$, we obtain the congruences

$$\sum_{i=0}^{l-2} j_i 2^i \equiv 0 \pmod{\frac{2^{l-1} - 1}{l}}, \quad (3)$$

hence

$$\sum_{i=0}^{l-2} j_i 2^i = a \frac{2^{l-1} - 1}{l}.$$

From $X\overline{X} = p$, it follows that $j_i \leq 1$, and this implies $a \leq l - 1$. Due to Lemma 4, Theorem 1 is proved. $\square$

Remark. If $(M, \frac{2^m+1}{l}) = d > 1$, then instead of the congruence (3) we get the congruence

$$\sum_{i=0}^{l-2} j_i 2^i \equiv 0 \pmod{\frac{2^{l-1} - 1}{ld}}.$$

It can be proved that this congruence has always the solution $(j_0, j_1, \dots, j_{l-2})$ which is not corresponding to the conjugates of the Jacobi sum $J(\chi, \chi)$.

The question of whether for p with $d > 1$ the Jacobi sum $J(\chi, \chi)$ can be uniquely determined transforms in the question, for which j_i the divisor

$$\prod_{i=0}^{l-2} \varphi^i(p)^{j_i},$$

is principal.

COROLLARY 1. *Let 2 be a primitive root modulo l , and let the class number of the field $\mathbf{Q}(\zeta_l)$ be equal to 1. Then the Jacobi sum $J(\chi, \chi)$ is uniquely determined, up to association and conjugation, from the solution of the equation $X\bar{X} = p, X \equiv 1 \pmod{2}, X \in \mathbf{Z}(\zeta_l)$ if and only if $(M, \frac{2^m+1}{l}) = 1$.*

Proof. This follows from the preceding Remark, because in such a case, every divisor is principal.

EXAMPLE 1. $l = 5, \frac{2^m+1}{l} = \frac{2^2+1}{5} = 1$. It follows that for all p one has $d = 1$, hence the Jacobi sum $J(\chi, \chi)$ is uniquely determined, up to association and conjugation, by the solution of the equation $X\bar{X} = p, X \equiv 1 \pmod{2}, X \in \mathbf{Z}(\zeta_l)$.

EXAMPLE 2. $l = 11, \frac{2^m+1}{l} = \frac{2^5+1}{11} = 3; l = 19, \frac{2^m+1}{l} = \frac{2^9+1}{19} = 27$.

It is easy to see, that if we want to answer the question, for which primes p is the Jacobi sum $J(\chi, \chi)$ uniquely determined, up to association and conjugation, by the solution of the equation $X\bar{X} = p, X \equiv 1 \pmod{2}, X \in \mathbf{Z}(\zeta_l)$, then we must know for which primes p the number α , where $N(\alpha) = p$, is a third power in the group $(\mathbf{Z}(\zeta_l)/(2))^*$. This question is solved in the following lemma.

LEMMA 5. *Let 2 be a primitive root modulo $l \equiv 3 \pmod{4}$, $p|p$, and $p^{h_p} = \alpha$.*

Then α is a third power in the group $(\mathbf{Z}(\zeta_l)/(2))^$ if and only if $p^{h_p} = x^2 + ly^2$, where x, y are not simultaneously divisible by p .*

Proof. By Lemma 1, the choice of a generator α of the principal divisor p^{h_p} is not substantial.

Consider the product

$$\beta = \prod_{(\frac{z}{l})=1} \sigma_z(\alpha), \text{ hence } \beta \in \mathbf{Q}(\sqrt{-l}).$$

Let

$$\beta = a' \sum_{(\frac{z}{l})=1} \zeta_l^z + b' \sum_{(\frac{z}{l})=1} \zeta_l^{-z}, \quad a', b' \in \mathbf{Z},$$

and let $\alpha \equiv g^r \pmod{2}$, where $r \equiv 0 \pmod{3}$,

$$\beta = \prod_{(\frac{z}{l})=1} \sigma_z(\alpha) \equiv \prod_{i=0}^{\frac{l-3}{2}} g^{r \cdot 2^i} \equiv g^{r \frac{2^{l-1}-1}{3}} \equiv 1 \pmod{2}.$$

So we have $a' \equiv b' \equiv 1 \pmod{2}$.

Hence

$$\begin{aligned}\beta &= a' \sum_{\left(\frac{z}{l}\right)=1} \zeta_l^z + b' \sum_{\left(\frac{z}{l}\right)=1} \zeta_l^{-z} = a' \frac{-1 + \sqrt{-l}}{2} + b' \frac{-1 - \sqrt{-l}}{2} \\ &= a + b\sqrt{-l}, \quad a, b \in \mathbf{Z},\end{aligned}$$

therefore

$$\beta \bar{\beta} = p^{h_p} = a^2 + lb^2.$$

Let conversely $p^{h_p} = a^2 + lb^2$. Put

$$\begin{aligned}a + b\sqrt{-l} &= a' \frac{-1 + \sqrt{-l}}{2} + b' \frac{-1 - \sqrt{-l}}{2} = \\ &= (b - a) \frac{-1 + \sqrt{-l}}{2} + (-a - b) \frac{-1 - \sqrt{-l}}{2}.\end{aligned}$$

This implies $a' \equiv b' \equiv 1 \pmod{2}$, hence

$$\beta = a' \sum_{\left(\frac{z}{l}\right)=1} \zeta_l^z + b' \sum_{\left(\frac{z}{l}\right)=1} \zeta_l^{-z} \equiv 1 \pmod{2}.$$

Let $\mathfrak{p}|\beta$. Then since β is invariant on σ_z , where $\left(\frac{z}{l}\right) = 1$, we set that $\sigma_z(\mathfrak{p})|\beta$.

But if $\left(\frac{n}{l}\right) = -1$, then $\sigma_n(\mathfrak{p})$ does not divide β (in the opposite case we would get $p|\beta$, hence a contradiction).

It implies

$$\beta \approx \prod_{\left(\frac{z}{l}\right)=1} \sigma_z(\mathfrak{p})^{h_p},$$

therefore

$$1 \equiv \beta \equiv (-\zeta_l)^s \prod_{\left(\frac{z}{l}\right)=1} \sigma_z(\mathfrak{p})^{h_p} \equiv (-\zeta_l)^s g^{r \frac{2^{l-1}-1}{3}} \pmod{2},$$

and

$$g^{lr \frac{2^{l-1}-1}{3}} \equiv 1 \pmod{2}.$$

From this we finally obtain

$$lr \frac{2^{l-1}-1}{3} \equiv 0 \pmod{2^{l-1}-1} \text{ which implies } r \equiv 0 \pmod{3}.$$

□

THEOREM 2. Let $l = 11; 19$, and let $p \equiv 1 \pmod{l}$, $4p = A^2 + lB^2$. The Jacobi sum $J(\chi, \chi)$ is uniquely determined, up to conjugation and association, by the solution of

$$X\overline{X} = p, \quad X \in \mathbf{Z}(\zeta_l), \quad X \equiv 1 \pmod{2},$$

if and only if $A \equiv B \equiv 1 \pmod{2}$.

Proof. The proof follows from Lemma 5 and Corollary 1. $\square$

By Proposition 5 and Theorem 2, we come to the following

THEOREM 3. Let $l = 11; 19$, and let $p \equiv 1 \pmod{l}$, $4p = A^2 + lB^2$, $A \equiv B \equiv 1 \pmod{2}$. Then 2 is an l -th power modulo p if and only if

$$a_1 \equiv a_2 \equiv \cdots \equiv a_{l-1} \equiv 1 \pmod{2},$$

where $(a_1, a_2, \dots, a_{l-1})$ is one of the exactly $l-1$ solutions of the diophantine system of equations

$$(i) \quad p = \sum_{i=1}^{l-1} a_i^2 - \sum_{i=1}^{l-1} a_i a_{i+1}, \quad .$$

$$(ii) \quad \sum_{i=1}^{l-1} a_i a_{i+1} = \sum_{i=1}^{l-1} a_i a_{i+2} = \cdots = \sum_{i=1}^{l-1} a_i a_{i+l-1},$$

$$(iv) \quad 1 + a_1 + \cdots + a_{l-1} \equiv 0 \pmod{l},$$

$$(v) \quad a_1 + 2a_2 + \cdots + (l-1)a_{l-1} \equiv 0 \pmod{l}.$$

Remark. As we can see, Theorem 2 enables us to remove condition (iii) of Proposition 5.

REFERENCES

- [1] H. HASSE, *Vorlesungen über Zahlentheorie*, Berlin 1950.
- [2] E. LEHMER, *The quintic character of 2 and 3*, *Duke math. J.* **18** (1951), 11–18.
- [3] P. A. LEONARD, B. C. MORTIMER and K. S. WILLIAMS, *The eleventh power character of 2*, *Crelle* **286/287** (1976), 213–222.

- [4] P. A. LEONARD and K. S. WILLIAMS, *The septic character of 2, 3, 5 and 7*, Pacific J. Math. **52** (1974), 143–147.
- [5] J. C. PARNAMI, M. K. AGRAWAL and A. R. RAJWADE, *Criterion for 2 to be l -th power*, Acta Arithmetica **43** (1984), 361–364.

Stanislav JAKUBEC
Mathematical Institute
of Slovak Academy of Sciences
Stefanikova 49
814 73 Bratislava
Slovakia