Acta Mathematica et Informatica Universitatis Ostraviensis

Stanislav Jakubec

Criterion for 3 to be eleventh power

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 3 (1995), No. 1, 37--(43)

Persistent URL: `http://dml.cz/dmlcz/120492`

Terms of use:

© University of Ostrava, 1995

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* `http://project.dml.cz`

Criterion for 3 to be eleventh power

STANISLAV JAKUBEC

Abstract. In this paper we prove a criterion for 3 to be an 11th power modulo p in the case when p is not representable by the quadratic form $x^2 + 11y^2$.

1991 Mathematics Subject Classification: Primary 11R18

The solution of the question when 3 is the lth power modulo a prime p for prime l goes back to Jacobi who solved the case $l = 3$ in [3]. The solution for $l = 5$ was given by E. Lehmer in [5].

Proposition 1. *3 is a quintic residue of a prime $p = 30n + 1$ if and only if the equations*

$$16p = x^2 + 450b^2 + 450c^2 + 1125d^2, \qquad xd = c^2 - b^2 - 4bc$$

have a solution, and of the prime $p = 30n + 11$, if and only if the equations

$$16p = 81a^2 + 450b^2 + 450c^2 + 125w^2, \qquad aw = c^2 - b^2 - 4bc$$

have a solution in common.

For $l = 7$ the solution was given by P. A. Leonard and K. S. Williams in [6], where the following theorem was proved.

Proposition 2. *3 is a seventh power modulo p if and only if $x_5 \equiv x_6 \equiv 0 \pmod 3$, where $(x_1, x_2, x_3, x_4, x_5, x_6)$ is one of the six nontrivial solutions of diophantine equations*

$$\begin{gathered}
72p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + x_6^2) \\
12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 + 24x_2x_3 - 24x_2x_4 + \\
+48x_3x_4 + 98x_5x_6 = 0 \\
12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 + 28x_1x_6 + 48x_2x_3 + \\
+24x_2x_4 24x_3x_4 + 490x_5x_6 = 0 \\
x_1 \equiv 1 \pmod 7
\end{gathered}$$

More work has been done on the question when q is an l-th power modulo p by various authors, for instance the cases $l = 7$, $q = 2, 3$ have been treated somewhat differently by Alderson [1], the case $p \equiv 1 \pmod l$ has been considered by Ankeny

[2], the case $q = l$ by Ankeny [2] and Muskat [7] and the cases $l = 5$, $q \leq 19$ by Williams [9].

To attack this problem for $l = 11$, we shall use some results from the papers [4] and [8].

Let χ be the Dirichlet character modulo p

$$\chi(x) = \zeta_l^{\text{ind}(x)},$$

and $J(\chi, \chi)$ the Jacobi sum

$$J(\chi, \chi) = \sum_{x+y=1} \chi(x)\chi(y).$$

The starting point of our solution of the problem when 3 is an 11^{th} power is the following result of J. C. Parnami, M. K. Agrawal and A. R. Rajwade proved in [8]:

Proposition 3. *Let $p \equiv 1 \pmod{l}$, then 2 is an l-th power modulo p if and only if*

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

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

$$\begin{array}{ll} (i) & p = \sum_{i=1}^{l-1} a_i^2 - \sum_{i=1}^{l-1} a_i a_{i+1}, \\ (ii) & \sum_{i=1}^{l-1} a_i a_{i+1} = \sum_{i=1}^{l-1} a_i a_{i+2} = \ldots = \sum_{i=1}^{l-1} a_i a_{i+l-1}, \\ (iii) & p \text{ does not divide } \prod_{\lambda(2k)>k} \sigma_k \left(\sum_{i=1}^{l-1} a_i \zeta_l^i \right), \end{array}$$

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

$$\begin{array}{ll} (iv) & 1 + a_1 + \ldots + a_{l-1} \equiv 0 \pmod{l}, \\ (v) & a_1 + 2a_2 + \ldots + (l-1)a_{l-1} \equiv 0 \pmod{l}. \end{array}$$

Note now that each solution $(a_1, a_2, \ldots, a_{l-1})$ of this system corresponds to the Jacobi sum

$$J(\chi^s, \chi^s) = a_1\zeta_l + a_2\zeta_l^2 + \ldots + a_{l-1}\zeta_l^{l-1},$$

for some $s = 1, 2, \ldots, l-1$. For, let

$$X = a_1\zeta_l + a_2\zeta_l^2 + \ldots + a_{l-1}\zeta_l^{l-1},$$

then the conditions (i), (ii) guarantee that

$$X\overline{X} = p.$$

Further let $\mathfrak{p}$ be a prime divisor of the field $\mathbf{Q}(\zeta_l)$, $\mathfrak{p}|p$. The condition (iii) guarantees that

$$\mathfrak{p}|X \text{ if and only if} \mathfrak{p}|J(\chi^s, \chi^s),$$

for some $s = 1, 2, \ldots, l-1$.

Hence, the conditions (i), (ii), (iii) guarantee the existence of s and of a unit $\varepsilon \in \mathbf{Q}(\zeta_l)$, such that

$$J(\chi^s, \chi^s) = \varepsilon X.$$

The conditions (iv), (v) guarantee that $\varepsilon = 1$, hence

$$J(\chi^s, \chi^s) = X.$$

The most peculiar of the conditions (i), (ii), (iii), (iv), (v) is (iii).

In [4] the following result is proved

Proposition 4. *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 conjugativity and associativity, by the solution*

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

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

On the basis of this proposition, the condition (iii) can be now replaced by the condition

$$(iii)' \qquad a_1\zeta_l + a_2\zeta_l^2 + \ldots + a_{l-1}\zeta_l^{l-1} \equiv \zeta_l^m \pmod{2}.$$

Let

$$\alpha = \zeta_{11} + \zeta_{11}^3 + \zeta_{11}^4 + \zeta_{11}^5 + \zeta_{11}^9,$$

then

$$\alpha\overline{\alpha} = 3.$$

Our main result is

Theorem . *Let p be a prime $4p = A^2 + 11B^2$, $A \equiv B \equiv 1 \pmod{2}$. The prime 3 is an 11th pover modulo p if and only if*

$$a_1\zeta_{11} + a_2\zeta_{11}^2 + \ldots + a_{10}\zeta_{11}^{10} \equiv (-\zeta_{11})^w \pmod{\alpha},$$

for some $w \in \mathbf{N}$, where

$$\begin{array}{cc}
(i) & p = \sum_{i=1}^{10} a_i^2 - \sum_{i=1}^{10} a_i a_{i+1}, \\
(ii) & \sum_{i=1}^{10} a_i a_{i+1} = \sum_{i=1}^{10} a_i a_{i+2} = \ldots = \sum_{i=1}^{10} a_i a_{i+10}, \\
(iii)' & a_1\zeta_{11} + a_2\zeta_{11}^2 + \ldots + a_{10}\zeta_{11}^{10} \equiv \zeta_{11}^m \pmod{2}, \\
(iv) & 1 + a_1 + \ldots + a_{10} \equiv 0 \pmod{11}, \\
(v) & a_1 + 2a_2 + \ldots + 10a_{10} \equiv 0 \pmod{11}.
\end{array}$$

Let q, p, l be primes, $p \equiv 1 \pmod{l}$ $q \neq p$, q and let K be a subfield of t field $\mathbf{Q}(\zeta_p)$, $[K:\mathbf{Q}] = l$. Let

$$\beta_1 = \mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}(\zeta_p), \qquad \beta_i = \sigma^{i-1}(\beta_1), \qquad \text{for} \qquad i = 1, 2 \ldots, l.$$

Lemma 1. *Let $n, m \in \mathbf{N}$, $n \not\equiv m \pmod{l}$.*

If q is a lth power modulo p, then

$$Tr_{\mathbf{Q}(\zeta_p)/K}(\beta_1^{q^n+q^m}) \equiv -\frac{p-1}{l} + p \pmod{q}.$$

If q is not a lth power modulo p, then

$$Tr_{\mathbf{Q}(\zeta_p)/K}(\beta_1^{q^n+q^m}) \equiv -\frac{p-1}{l} \pmod{q}.$$

Proof: If q is lth power modulo p, then

$$\beta_1^q \equiv \beta_1 \pmod{q},$$

and hence

$$\mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}(\beta_1^{q^n+q^m}) \equiv \mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}(\beta_1^2) \pmod{q}.$$

The assertion follows from the equality

$$\mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}(\beta_1^2) = -\frac{p-1}{l} + p.$$

If q is not a lth power modulo p then

$$\beta_1^q \equiv \beta_s \pmod{q},$$

for some s,$s \neq 1$.

Hence

$$\mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}(\beta_1^{q^n+q^m}) \equiv \mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}(\beta_s\beta_t) \pmod{q}, \qquad s \neq t.$$

Because $s \neq t$, the following equality holds

$$\mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}(\beta_s\beta_t) = -\frac{p-1}{l}.$$

Lema 1 is proved. [

If

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

is the Gauss sum, then the identity

$$\zeta_l\tau(\chi) + \zeta_l^2\tau(\chi^2) + \ldots + \zeta_l^{l-1}\tau(\chi^{l-1}) = 1 + l\beta_s,$$

is true for some $s = 1, 2, \ldots, l$.

It follows that

$$\begin{aligned}
&\mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}(\beta_1^{q^n+q^m}) = \\
&= \mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}\left(\frac{\zeta_l\tau(\chi) + \zeta_l^2\tau(\chi^2) + \ldots + \zeta_l^{l-1}\tau(\chi^{l-1}) - 1}{l}\right)^{q^n+q^m} \equiv \\
&\equiv \frac{1}{l^{q^n+q^m}}\mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}(\zeta_l^{q^n}\tau(\chi)^{q^n} + \zeta_l^{2q^n}\tau(\chi^2)^{q^n} + \ldots + \zeta_l^{(l-1)q^n}\tau(\chi^{l-1})^{q^n} - \\
&(\zeta_l^{q^m}\tau(\chi)^{q^m} + \zeta_l^{2q^m}\tau(\chi^2)^{q^m} + \ldots + \zeta_l^{(l-1)q^m}\tau(\chi^{l-1})^{q^m} - 1) \pmod q.
\end{aligned}$$

Let d be an integer such that

$$q^n + dq^m \equiv 0 \pmod l,$$

then

$$\tau(\chi)^{q^n}\tau(\chi^d)^{q^m} \in \mathbf{Q}(\zeta_l).$$

and we have the equality

$$\begin{aligned}
&\mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}(\zeta_l^{q^n}\tau(\chi)^{q^n} + \zeta_l^{2q^n}\tau(\chi^2)^{q^n} + \ldots + \zeta_l^{(l-1)q^n}\tau(\chi^{l-1})^{q^n} - 1) \\
&(\zeta_l^{q^m}\tau(\chi)^{q^m} + \zeta_l^{2q^m}\tau(\chi^2)^{q^m} + \ldots + \zeta_l^{(l-1)q^m}\tau(\chi^{l-1})^{q^m} - 1) = \\
&= \mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}(1 + \mathrm{Tr}_{\mathbf{Q}(\zeta_l)/\mathbf{Q}}(\tau(\chi)^{q^n}\tau(\chi^d)^{q^m}).
\end{aligned}$$

Thus we proved the next lemma.

Lemma 2. *A prime q is a lth power modulo p if and only if*

$$\frac{l}{l^{q^n+q^m}}(1 + Tr_{\mathbf{Q}(\zeta_l)/\mathbf{Q}}(\tau(\chi)^{q^n}\tau(\chi^d)^{q^m}) \equiv -\frac{p-1}{l} + p \pmod q.$$

Proof of the Theorem: We have

$$\tau(\chi)^2\tau(\chi^9) = pJ(\chi,\chi).$$

Take $n = 1, m = 2$ in the above, then $d = 7$.

If σ is the automorphism with $\sigma(\zeta_{11}) = \zeta_{11}^2$ then

$$\tau(\chi)^3\tau(\chi^7)^9 = pJ(\chi,\chi)\sigma J(\chi,\chi)\sigma^7 J(\chi,\chi)^4\sigma^8 J(\chi,\chi)^2\sigma^9 J(\chi,\chi),$$

The field $\mathbf{Z}(\zeta_{11})/(\alpha)$ is of the characteristic 3 and

$$[\mathbf{Z}(\zeta_{11})/(\alpha) : \mathbf{Z}/3\mathbf{Z}] = 5.$$

Clearly

$$\begin{aligned}
\sigma J(\chi,\chi)\sigma^6 J(\chi,\chi) &= \sigma J(\chi,\chi)\overline{\sigma J(\chi,\chi)} = p, \\
\sigma^7 J(\chi,\chi)\sigma^2 J(\chi,\chi) &= \sigma^7 J(\chi,\chi)\overline{\sigma^7 J(\chi,\chi)} = p, \\
\sigma^9 J(\chi,\chi)\sigma^4 J(\chi,\chi) &= \sigma^9 J(\chi,\chi)\overline{\sigma^9 J(\chi,\chi)} = p.
\end{aligned}$$

Substituing into (1) we get

$$\tau(\chi)^3\tau(\chi^7)^9 = p^7 J(\chi,\chi)\sigma^6 J(\chi,\chi)^{-1}\sigma^2 J(\chi,\chi)^{-4}\sigma^8 J(\chi,\chi)^2\sigma^4 J(\chi,\chi)^{-1}.$$

It is easy to see that

$$\begin{aligned}
\sigma^6 J(\chi,\chi) &\equiv J(\chi,\chi)^9 \pmod{\alpha},\\
\sigma^2 J(\chi,\chi) &\equiv J(\chi,\chi)^{81} \pmod{\alpha},\\
\sigma^8 J(\chi,\chi) &\equiv J(\chi,\chi)^3 \pmod{\alpha},\\
\sigma^4 J(\chi,\chi) &\equiv J(\chi,\chi)^{27} \pmod{\alpha}.
\end{aligned}$$

By substitution into (1) we have

$$\tau(\chi)^3\tau(\chi^7)^9 \equiv p^7 J(\chi,\chi)^{-352} \equiv p^7 J(\chi,\chi)^{132} \pmod{\alpha}.$$

The order of the multiplicative group of the field $\mathbf{Z}(\zeta_{11})/(\alpha)$ is equal to $3^5 - 1 = 242$.

It is easy to see

$$J(\chi,\chi)^{132} \equiv \zeta_{11}^w \pmod{\alpha}.$$

Using Lemma 2 we see that 3 is an 11th power modulo p if and only if

$$J(\chi,\chi)^{132} \equiv 1 \pmod{\alpha}.$$

This congruence holds if and only if

$$J(\chi,\chi) \equiv (-\zeta_{11})^s \pmod{\alpha},$$

for some $s = 1, 2, \ldots, 22$ and Theorem 1 is proved. □

References

[1] Alderson, H. P., *On the septimic character of 2 and 3*, Proc. Camb. Phil. Soc. **74** (1973), 421–433.

[2] Ankeny, N. C., *Criterion for rth power residuacity*, Pacific J. Math. **10** (1960), 1115–1124.

[3] Jacobi, C. G. J., *De residuis cubicis commentatio numerosa*, J. für Reine und Angew. Math. **2** (1827), 66–69.

[4] Jakubec, S., *Note on the Jacobi sum*, Seminaire de theorie des nombres de Bordeaux **to appear** (1994), .

[5] Lehmer, E., *The quintic character of 2 and 3*, Duke Math. J. **18** (1951), 11–18.

[6] Leonard, P. A., Williams, K. S., *The septic character of 2, 3, 5 and 7*, Pacific J. Math. **52** (1974), 143–147.

[7] Muskat, J. B., *On the solvalibility of* $x^e \equiv e \pmod p$, Pacific J. Math. **14** (1964), 257–260.

[8] Parnami, J. C., Agrawal, M. K., Rajwade, A. R., *Criterion for 2 to be l-th power*, Acta Arith. **43** (1984), 361–364.

[9] Williams, K. S., *Explicit criteria for quintic residuacity*, Math. Comp. **30** (1974), 1–6.

Address: S. Jakubec, Matematický ústav SAV; Štefánikova 49; 814 73 Bratislava; Slovakia