Stanislav Jakubec
Note on the congruences $2^{p-1} \equiv 1 \pmod{p^2}$, $3^{p-1} \equiv 1 \pmod{p^2}$, $5^{p-1} \equiv 1 \pmod{p^2}$

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 6 (1998), No. 1, 115--120

Persistent URL: http://dml.cz/dmlcz/120522

Terms of use:

© University of Ostrava, 1998

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
Note on the congruences $2^{p-1} \equiv 1 \pmod{p^2}$, $3^{p-1} \equiv 1 \pmod{p^2}$, $5^{p-1} \equiv 1 \pmod{p^2}$.

Stanislav Jakubec

Abstract: This paper studies the solvability of congruences from the title, and distribution of numbers \( z \in H_i \), where \( H_i \) are cosets of group \((\mathbb{Z}/p^2\mathbb{Z})^*\) by a subgroup \( H_0 \) of index \( p \) for \( i = 0, 1, \ldots, p - 1 \).

Key Words: Wieferich congruence

Mathematics Subject Classification: Primary 11R18

Introduction

Let \( p \) be a prime \( p > 5 \) and let \( H_0 \) be a subgroup of the group \((\mathbb{Z}/p^2\mathbb{Z})^*\) of the index \( p \) and let \( H_i = (1 + ip)H_0 \) be cosets for \( i = 0, 1, \ldots, p - 1 \). The group \( G \) is defined in Definition 3 such that \( G = H_0 \) or \( G = (\mathbb{Z}/p^2\mathbb{Z})^* \), (Theorem 2).

The aim of this paper is to prove the following theorem.

**Theorem 1.** Suppose that \( G \neq (\mathbb{Z}/p^2\mathbb{Z})^* \). Then there holds

(i) $2^{p-1} \equiv 1 \pmod{p^2}$ if and only if

\[
\sum_{z \in H_i, \; z < \frac{p^2}{2}} 1 \equiv \frac{p^2 - 1}{8} \pmod{2}, \text{ for } i = 0, 1, \ldots, p - 1.
\]

(ii) $3^{p-1} \equiv 1 \pmod{p^2}$ if and only if

\[
\sum_{z \in H_i, \; \frac{z^2}{p^2} < z < \frac{p^2}{2}} 1 \equiv r \pmod{2}, \text{ for } i = 0, 1, \ldots, p - 1,
\]

where \((-1)^r = \left( \frac{3}{p} \right)\).

(iii) $5^{p-1} \equiv 1 \pmod{p^2}$ if and only if

\[
\sum_{z \in H_i, \; \frac{z^2}{p^2} < z < 2\frac{p^2}{2}} 1 \equiv r \pmod{2}, \text{ for } i = 0, 1, \ldots, p - 1,
\]
where \((-1)^r = \left(\frac{5}{p}\right).\)

By the computation it was verified that \(G \neq (\mathbb{Z}/p^2\mathbb{Z})^*\) for \(p < 50000.\)

Unless the contrary is stated, we shall always suppose that \(n\) is a positive integer and \(p, l\) are odd primes with \(\varphi(p^n) \equiv 0 \pmod{l}\), \(\mathbb{Z}\) is the ring of integers while \(\mathbb{Z}^+\) is the set of positive integers.

\(H_0\) will stand for the (uniquely determined) subgroup of the group \((\mathbb{Z}/p^n\mathbb{Z})^*\) of index \(l\).

The cosets of \((\mathbb{Z}/p^n\mathbb{Z})^*\) will be denoted by \(H_i, i \in \{0, 1, 2, ..., l-1\}\).

**Definition 1.** A subset \(T_i\) of a coset \(H_i\) will be called a semisystem (in \(H_i\)) if for each \(x \in H_i\) exactly one of the residue classes \(x, -x\) belongs to \(T_i\). Clearly

\[
\#T_i = \frac{\#H_0}{2} = \frac{\varphi(p^n)}{2l} = \frac{(p-1)p^{n-1}}{2l},
\]

for every semisystem \(T_i\).

**Definition 2.** Given a positive integer \(a\) coprime to \(p\) and a semisystem \(T_i\) for some \(i \in I\), let

\[
g(a, i) = \sum_{z \in T_i} \left( \left\lfloor \frac{az}{p^n} \right\rfloor + \left\lfloor \frac{z}{p^n} \right\rfloor \right), \text{ for } a \text{ odd} \tag{1}
\]

\[
g(a, i) = \sum_{z \in T_i} \left( \left\lfloor \frac{2az}{p^n} \right\rfloor + \left\lfloor \frac{2z}{p^n} \right\rfloor \right), \text{ for } a \text{ even} \tag{2}
\]

**Proposition 1.** Let \(i \in I, a \in \mathbb{Z}^+, (a, p) = 1\). The number \(g(a, i) \pmod{2}\) does not depend on the system of representatives of the group \((\mathbb{Z}/p^n\mathbb{Z})^*\) and on the choice of the semisystem \(T_i\).

**Definition 3.** Denote by \(G\) the set of all \(a \in (\mathbb{Z}/p^n\mathbb{Z})^*\) such that \(g(a, i) \equiv g(a, j) \pmod{2}\) for all \(i, j \in I\).

Note that \(1 \in G\) and thus \(G\) is non-empty.

**Proposition 2.** Let \(a \in G\). If \(a \equiv a' \pmod{p^n}\), then \(g(a, i) \equiv g(a', i) \pmod{2}\) for all \(i \in I\).

**Proof.** In the case \(a \equiv a' \pmod{2}\) the proposition is evident. Therefore suppose that \(a \equiv 1 \pmod{2}\) and \(a' \equiv 0 \pmod{2}\).

In order to prove the proposition we will prove the congruence

\[
\sum_{z \in T_i} \left( \left\lfloor \frac{az}{p^n} \right\rfloor + \left\lfloor \frac{z}{p^n} \right\rfloor \right) \equiv \sum_{z \in T_i} \left( \left\lfloor \frac{2az}{p^n} \right\rfloor + \left\lfloor \frac{2z}{p^n} \right\rfloor \right) \pmod{2}. \tag{3}
\]

To do this write \(a' = a + kp^n, k \in \mathbb{Z}\). Then

\[
\sum_{z \in T_i} \left( \left\lfloor \frac{2a'z}{p^n} \right\rfloor + \left\lfloor \frac{2z}{p^n} \right\rfloor \right) = \sum_{z \in T_i} \left( \left\lfloor \frac{2(a + kp^n)z}{p^n} \right\rfloor + \left\lfloor \frac{2z}{p^n} \right\rfloor \right) =
\]
Note on the congruences $2^{p-1} \equiv 1 \pmod{p^2}$, $3^{p-1} \equiv 1 \pmod{p^2}$, $5^{p-1} \equiv 1 \pmod{p^2}$.

\[
\sum_{z \in T_i} \left( \left[ \frac{2az}{p^n} \right] + \left[ \frac{2z}{p^n} \right] \right) + 2k \sum_{z \in T_i} z \equiv \sum_{z \in T_i} \left( \left[ \frac{2az}{p^n} \right] + \left[ \frac{2z}{p^n} \right] \right) \pmod{2},
\]

\[
\sum_{z \in T_i} \left( \left[ \frac{2az}{p^n} \right] + \left[ \frac{2z}{p^n} \right] \right) \equiv \sum_{z \in T_i} \left( \left[ \frac{az'}{p^n} \right] + \left[ \frac{z'}{p^n} \right] \right) \pmod{2}.
\]

The assumption $a \in G$ yields

\[
\sum_{z' \in 2T_i} \left( \left[ \frac{az'}{p^n} \right] + \left[ \frac{z'}{p^n} \right] \right) \equiv \sum_{z \in T_i} \left( \left[ \frac{az}{p^n} \right] + \left[ \frac{z}{p^n} \right] \right) \pmod{2},
\]

and (3) follows.

**Proposition 3.** The set $G$ is a subgroup of the group $(\mathbb{Z}/p^n\mathbb{Z})^\star$.

**Proof.** It is sufficient to prove that $ab \in G$ for $a, b \in G$.

In view of Proposition 2 we may suppose that $a, b$ are odd. Then

\[
\sum_{z \in T_i} \left( \left[ \frac{az}{p^n} \right] + \left[ \frac{z}{p^n} \right] \right) \equiv \sum_{z \in T_i} \left( \left[ \frac{az}{p^n} \right] + \left[ \frac{bz}{p^n} \right] + \left[ \frac{z}{p^n} \right] \right) \equiv
\]

\[
\sum_{z \in T_i} \left( \left[ \frac{az}{p^n} \right] + \left[ \frac{z}{p^n} \right] \right) + \sum_{z \in T_i} \left( \left[ \frac{bz}{p^n} \right] + \left[ \frac{z}{p^n} \right] \right) \equiv
\]

\[
\sum_{z \in T_i} \left( \left[ \frac{az}{p^n} \right] + \left[ \frac{z}{p^n} \right] \right) \pmod{2}.
\]

In other words, the parity of the sum

\[
\sum_{z \in T_i} \left( \left[ \frac{az}{p^n} \right] + \left[ \frac{z}{p^n} \right] \right),
\]

does not depend on the choice of $i \in I$, and consequently $ab \in G$ as desired.

The following theorem shows that we have only two possibilities for the group $G$ defined in Definition 3.

**Theorem 2.** For group $G$ we have either $G = H_0$ or $G = (\mathbb{Z}/p^n\mathbb{Z})^\star$.

**Proof.** In view of Proposition 3 it suffices to prove that $H_0 \subset G$. Let $z_1 \equiv 1 \pmod{2}$ be a generator of the group $H_0$. By the Proposition 3 it is sufficient to prove that $z_1 \in G$.

Let $b \in H_i$. If $m = \phi(p^n) - 1$ and for $j = 0, 1, 2, ..., m$ we put $b_j$ to be equal the residue of $bz_1^j \pmod{p^n}$, then $T_i = \{b_0, b_1, ..., b_m\}$ is a semisystem.

$b_j \equiv bz_1^j \pmod{p^n} 0 < b_j < p^n$ for $j = 0, 1, 2, ..., m$.

Since $b_j < p^n$, we have in turn

\[
\sum_{j=0}^{m} \left( \left[ \frac{z_1b_j}{p^n} \right] + \left[ \frac{b_j}{p^n} \right] \right) = \sum_{j=0}^{m} \left[ \frac{z_1b_j}{p^n} \right].
\]
\[
\sum_{j=0}^{m} \left[ \frac{z_1 b_j}{p^n} \right] = \frac{1}{p^n} (z_1 b_0 - b_1 + z_1 b_1 - b_2 + \ldots + z_1 b_m - b_{m+1}) = \\
= \frac{1}{p^n} [(z_1 - 1)(b_0 + b_1 + \ldots + b_m) + b_0 - b_{m+1}].
\]

It is easy to see that \( z_1^{m+1} \equiv -1 \pmod{p^n} \) and thus \( b_{m+1} = p^n - b \). This implies that

\[
\sum_{j=0}^{m} \left[ \frac{z_1 b_j}{p^n} \right] = \\
= \frac{1}{p^n} [(z_1 - 1)(b_0 + b_1 + \ldots + b_m) + 2b - p^n] \equiv 1 \pmod{2}.
\]

Note that the sum is independent on the choice of \( i \), therefore

\[
\sum_{\ell \in T_i} \left( \left[ \frac{z_1 z}{p^n} \right] + \left[ \frac{z}{p^n} \right] \right) \equiv 1 \pmod{2},
\]

for all \( i \in I \). \( \Box \)

From now on we will denote \( \zeta = \cos \frac{2\pi}{p^n} + i \sin \frac{2\pi}{p^n} \).

Let \( L = \mathbb{Q}(\zeta + \zeta^{-1}) \), \( K \subset L \), \( [K : \mathbb{Q}] = l \).

Given \( a \in (\mathbb{Z}/p^n\mathbb{Z})^* \), let \( \gamma_a \) be a cyclotomic unit of the field \( L \) defined by

\[
\gamma_a = 1 + \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} + \cdots + \zeta^{\frac{p^n}{2} - 1} + \zeta^{-\frac{p^n}{2}} = \frac{\sin \frac{2\pi a}{p^n}}{\sin \frac{\pi}{p^n}}, \text{ for a odd} \tag{4}
\]

\[
\gamma_a = \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} + \cdots + \zeta^{\frac{p^n}{2}} + \zeta^{-\frac{p^n}{2}} = \frac{\sin \frac{2\pi a}{p^n}}{\sin \frac{\pi}{p^n}}, \text{ for a even} \tag{5}
\]

Denote by \( \varepsilon_a^{(i)} \), \( i \in I \), that conjugate of unit \( \varepsilon_a = N_{L/K}(\gamma_a) \) for which

\[
\varepsilon_a^{(i)} = \prod_{\ell \in T_i} \frac{\sin \frac{2\pi a}{p^n}}{\sin \frac{\pi}{p^n}}, \text{ for a odd}
\]

\[
\varepsilon_a^{(i)} = \prod_{\ell \in T_i} \frac{\sin \frac{2\pi a}{p^n}}{\sin \frac{2\pi}{p^n}}, \text{ for a even}
\]

The behavior of the function \( \sin x \) implies that the sign of \( \varepsilon_a^{(i)} \) is \((-1)^{g(a, i)}\).

We have proved following propositions:

**Proposition 4.** Let \( a \in (\mathbb{Z}/p^n\mathbb{Z})^* \). Then \( a \in G \) if and only if the unit \( \varepsilon_a \) is totally positive or totally negative.

**Proposition 5.** \( G = (\mathbb{Z}/p^n\mathbb{Z})^* \) if and only if for all \( a \in (\mathbb{Z}/p^n\mathbb{Z})^* \) the units \( \varepsilon_a^{(i)} \) are totally positive or totally negative.
Note on the congruences \( 2^{p-1} \equiv 1 \pmod{p^2}, 3^{p-1} \equiv 1 \pmod{p^2}, 5^{p-1} \equiv 1 \pmod{p^2} \).

**Theorem 3.** Let \( a \in (\mathbb{Z}/p^n\mathbb{Z})^* \). Then \( \varepsilon_a = \pm 1 \) if and only if \( a \in H_0 \). Moreover, if \( a \in H_0 \) then \( \varepsilon_a = \left( \frac{a}{p} \right) \).

**Proof.** Let \( \gamma'_a \) be the cyclotomic unit of the field \( \mathbb{Q}(\zeta) \) defined by
\[
\gamma'_a = 1 + \zeta + \zeta^2 + \cdots + \zeta^{a-1} = \frac{1 - \zeta^a}{1 - \zeta}.
\]

Let \( \gamma_a \) be the cyclotomic unit of the field \( L \) defined by equalities (4),(5).

An easy calculation shows that
\[
N_{\mathbb{Q}(\zeta)/K}(\gamma'_a) = N_{L/K}(\gamma_a)^2.
\]

Hence \( \varepsilon_a = \pm 1 \) if and only if \( N_{\mathbb{Q}(\zeta)/K}(\gamma'_a) = 1 \),
\[
N_{\mathbb{Q}(\zeta)/K}(\frac{1 - \zeta^a}{1 - \zeta}) = 1,
\]
if and only if
\[
N_{\mathbb{Q}(\zeta)/K}(1 - \zeta) = N_{\mathbb{Q}(\zeta)/K}(1 - \zeta^a).
\]

Denote by \( \sigma \) the automorphism of the field \( Q(\zeta) \) for which \( \sigma(\zeta) = \zeta^a \)
\[
N_{\mathbb{Q}(\zeta)/K}(1 - \zeta) = N_{\mathbb{Q}(\zeta)/K}(1 - \zeta^a),
\]
if and only if
\[
N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta) = \sigma N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta),
\]
\[
N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta) = p \text{ implies } N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta) \not\in \mathbb{Q}.
\]

Since the extension \( K/\mathbb{Q} \) is of prime degree, the field \( K \) has only trivial subfields. Hence \( N_{\mathbb{Q}(\zeta)/K}(1 - \zeta) \) is primitive element of the field \( K \).

On the other hand \( \sigma N_{\mathbb{Q}(\zeta)/K}(1 - \zeta) = N_{\mathbb{Q}(\zeta)/K}(1 - \zeta) \).

This implies that the automorphism \( \sigma \) fixes all elements of the field \( K \). Therefore \( a \in H_0 \).

It remains to prove that if \( a \in H_0 \), then \( \varepsilon_a = \left( \frac{a}{p} \right). \) Since \( \gamma_a \equiv a \pmod{1 - \zeta} \)
then \( N_{L/K}(\gamma_a) \equiv a^{\#H_0} \pmod{1 - \zeta} \). However \( a^{\#H_0} \equiv \left( \frac{a}{p} \right) \pmod{p} \) and the proof is finished. \( \square \)

Now we shall prove Theorem 1. Because \( G = H_0 \) by Proposition 4 and Theorem 3 the unit \( \varepsilon_a \) is totally positive or totally negative if and only if \( a \in H_0 \). In all cases take \( \mathcal{T}_i = \left\{ z | z \in H_i, z < \frac{p^2}{2} \right\} \). Clearly \( a \in H_0 \) if and only if \( a^{p-1} \equiv 1 \pmod{p^2} \).

(i) Because \( 2 + p^2 \) is odd we have
\[
\sum_{z \in H_i, z < \frac{p^2}{2}} \left( \left\lfloor \frac{(2 + p^2)z}{p^2} \right\rfloor + \left\lfloor \frac{2z}{p^2} \right\rfloor \right) \equiv \sum_{z \in H_i, z < \frac{p^2}{2}} z \pmod{2}.
\]
(ii) In this case we have
\[
\sum_{\substack{z \in H_1 \\ z < p^{1/2}}} \left( \frac{4z}{p^2} \right) + \left( \frac{2z}{p^2} \right) \equiv \sum_{\substack{z \in H_1 \\ z^2 < p^{1/2}}} 1 \pmod{2}.
\]
An analogous procedure gives the proof in the remaining cases. Theorem 3 yields that the corresponding sums correspond with the Legendre symbol \( \left( \frac{2}{p} \right), \left( \frac{3}{p} \right), \left( \frac{5}{p} \right) \).

References

Author's address: Matematicky ústav SAV, Štefánikova 49, 814 73 Bratislava, Slovakia

Received: February 23, 1998