**Notes on Number Theory and Discrete Mathematics**
**Print ISSN 1310–5132, Online ISSN 2367–8275**
**2026, Volume 32, Number 2, 269–280**
**DOI: 10.7546/nntdm.2026.32.2.269-280**

# Simpler congruences for Jacobi sum $J(1,1)_{49}$ of order 49

**Ishrat Jahan Ansari** [1], **Vikas Jadhav** [2] **and Devendra Shirolkar** [3]

[1] Department of Mathematics, M.C.E. Society's Abeda Inamdar Senior College,
Savitribai Phule Pune University
Research Scholar, Sir Parshurambhau College
Pune, Maharashtra, India
e-mail: ishrat1984@gmail.com

[2] Department of Mathematics, Nowrosjee Wadia College
Pune, Maharashtra, India
e-mail: svikasjadhav@gmail.com

[3] Savitribai Phule Pune University
Pune, Maharashtra, India
e-mail: dshirolkar@gmail.com

**Received:** 9 May 2025 **Revised:** 3 March 2026
**Accepted:** 16 April 2026 **Online First:** 24 April 2026

**Abstract:** Congruences of order $l^2$ (with $l$ an odd prime) were obtained by D. Shirolkar and S. A. Katre [15]. In this paper we determine congruence of Jacobi sums $J(1,1)_{49}$ of order $49$ over a field $\mathbb{F}_p$. We also show that simpler congruences hold for $J(1,1)_{49}$ in the case of artiad and hyperartiad primes.

**Keywords:** Jacobi sums, Cyclotomic numbers, Congruences, Dickson–Hurwitz sums.
**2020 Mathematics Subject Classification:** 11T22, 11T24.

# 1 Introduction

For a positive integer $e \geq 2$, the Jacobi sums of order $e$ are algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta_e)$, where $\zeta_e = \exp(2\pi i/e)$. These are defined in the set up of a finite field $\mathbb{F}_q$ with $q = p^r$ where $q \equiv 1 \pmod{e}$, $p$ prime. Jacobi sums are important in the theory of cyclotomy and their congruences have been studied by many authors. Earlier authors [2] obtained congruences in the set up of $\mathbb{F}_p$, $p \equiv 1 \pmod{e}$ and later authors [5] considered $q = p^r \equiv 1 \pmod{e}$.

1. It is well known that ([2] and [13]) the Jacobi sums of odd prime order $l$, $J(1,j)_l \equiv -1 \pmod{(1-\zeta_l)^2}$. This congruence also holds $\pmod{(1-\zeta_l)^3}$ ([7] and [14]).
2. Congruence of Jacobi sums of order $2l$ ($l$ odd prime) were obtained by V. V. Acharya, S. A. Katre [1]. They showed that
   $J(1,n)_{2l} \equiv -\zeta^{m(n+1)} \pmod{(1-\zeta_l)^2}$, where $n$ is an odd integer such that $1 \leq n \leq 2l-3$ and $m = \mathrm{ind}_\gamma 2$ where $\gamma$ is generator of $\mathbb{F}_q^*$.
3. A congruence of Jacobi sum $J(1,1)_9$ of order 9 was obtained by S. A. Katre and Rajwade [8]. They showed that $J(1,1)_9 \equiv -1 - (\mathrm{ind}_\gamma 3)(1-\omega) \pmod{(1-\zeta_9)^4}$ where $\omega = {\zeta_9}^3$ and $\gamma$ is generator of $\mathbb{F}_q^*$.
4. Congruences of order $l^2$ ($l$ odd prime) were obtained by D. Shirolkar and S. A. Katre. Refer to Theorem and Remarks following [15]. They showed that
$$J(1,n)_{l^2} \equiv \begin{cases} -1 + \sum_{i=3}^{l} c_{i,n}(\zeta-1)^i \pmod{(1-\zeta)^{l+1}}, & \text{if } \gcd(l,n) = 1, \\ -1 \pmod{(1-\zeta)^{l+1}}, & \text{if } \gcd(l,n) = l, \end{cases}$$
   where $1 \leq n \leq l^2 - 1$.
5. If $k$ is an odd power $> 3$, then $J(i,j)_k \equiv -1 \pmod{(1-\zeta_k)^3}$ (see [6]).
   R. J. Evans [5] generalised this result to all $k > 2$ by elementary methods getting sharper congruences in some cases, especially when $k > 8$ is a power of 2.

The purpose of this paper is to apply the general result of D. Shirolkar and S. A. Katre [15] to the case $l = 7$ and to show that, for septic artiad and septic hyperartiad primes $p$, the corresponding determining congruence for the Jacobi sum $J(1,1)_{49}$ simplifies considerably.

# 2 Preliminaries

Let $e$ be a positive integer $\geq 2$ and $q = p^r \equiv 1 \pmod{e}$, $p$ prime. Let $\mathbb{F}_q$ be a finite field with $q$ elements. Write $p^r = q = ef + 1$. Let $\zeta$ be a complex primitive $e$th root of unity. If $\gamma$ is a generator of $\mathbb{F}_q^*$, then define the multiplicative character $\chi : \mathbb{F}_q \to \mathbb{Q}(\zeta)$ by $\chi(\gamma) = \zeta$, $\chi(0) = 0$. Given a generator $\gamma$ of $\mathbb{F}_q^*$ define the Jacobi sum $J(i,j)_e$ by

$$J(i,j) = J(i,j)_e = \sum_{v \in \mathbb{F}_q} \chi^i(v)\chi^j(1+v), \ 0 \leq i,j \leq e-1.$$

Here $\chi^0(0) = 0$. Also, $i$ and $j$ can be considered modulo $e$, with the understanding that $\chi^i(0) = 0$ for any integer $i$. Note that $J(i,j)_e \in \mathbb{Z}[\zeta]$, the ring of integers of $\mathbb{Q}(\zeta)$.

A variation of the Jacobi sum is defined as

$$J(\chi^i, \chi^j)_e = \sum_{v \in \mathbb{F}_q} \chi^i(v)\chi^j(1-v),\ 0 \le i, j \le e-1.$$

Observe that $J(i,j)_e = \chi^i(-1)J(\chi^i, \chi^j)_e$. When $q = 2^r$, $\chi^i(-1) = \chi^i(1) = 1$ and both the Jacobi sums coincide. Otherwise, $\chi^i(-1) = (-1)^{if}$ and hence the two Jacobi sums differ at most in sign. For multiplicative characters $\chi$ and $\psi$ on $\mathbb{F}_q$, $J(\chi, \psi)$ can be analogously defined.

In the following theorem, we state some standard results about Jacobi sums.

**Theorem 2.1** (Elementary properties of Jacobi sums)**.**

1) *If $i$ and $j$ are congruent to $0$ modulo $e$, then $J(\chi^i, \chi^j)_e = q - 2$.*
2) *If exactly one of $i$ and $j$ is congruent to $0$ modulo $e$, then $J(\chi^i, \chi^j)_e = -1$.*
3) *If $i$ is nonzero modulo $e$ and $i + j$ is congruent to $0$ modulo $e$, then $J(\chi^i, \chi^j)_e = -\chi^i(-1)$.*
4) $J(\chi^i, \chi^j)_e = J(\chi^j, \chi^i)_e = \chi^i(-1)J(\chi^{-i-j}, \chi^i)_e$.
5) *If $e$ does not divide $i, j$ and $i + j$, then* $\mid J(\chi^i, \chi^j)_e \mid = \sqrt{q}$.

*Proof.* See [2] for the case $q = p$, and [16] for $q = p^r$. □

**Remark**: If $f$ is even or $q = 2^r$, then $J(i,j)_e = J(\chi^i, \chi^j)_e$, so (4) gives $J(i,j)_e = J(j,i)_e = J(-i-j, j)_e = J(j, -i-j)_e = J(-i-j, i)_e = J(i, -i-j)_e$. In particular $J(i,i)_e = J(-2i, i)_e = J(i, -2i)_e$.

# 3 Cyclotomy

Let $\gamma$, $\zeta$ and $\chi$ be as in Section 2. For $0 \le i, j \le e-1$ ($i, j \pmod e$), define the $e^2$ cyclotomic numbers $(i,j)_e$ by $(i,j)_e$ = Cardinality$(X_{ij})$ where

$$\begin{aligned} X_{ij} &= \{v \in \mathbb{F}_q \mid \chi(v) = \zeta^i, \chi(v+1) = \zeta^j\} \\ &= \{v \in \mathbb{F}_q - \{0, -1\} \mid \mathrm{ind}_\gamma v \equiv i \pmod e,\ \mathrm{ind}_\gamma(v+1) \equiv j \pmod e\}. \end{aligned}$$

We state below some basic properties of the cyclotomic numbers. (See [3] for $q = p$, [16]). For $q = p^r$,

$$\begin{aligned} (i,j)_e &= (i',j')_e \quad \text{if } i \equiv i' \text{ and } j \equiv j' \pmod e. \\ (i,j)_e &= (e-i, j-i)_e \\ &= \begin{cases} (j,i)_e, & \text{if } f \text{ is even or } q = 2^r, \\ (j + \frac{1}{2}e, i + \frac{1}{2}e)_e, & \text{otherwise.} \end{cases} \end{aligned}$$

Thus if $f$ is even or $q = 2^r$, $r \ge 2$, then

$$\begin{aligned} (i,j)_e &= (j,i)_e = (i-j, -j)_e = (j-i, -i)_e \\ &= (-i, j-i)_e = (-j, i-j)_e. \end{aligned} \tag{1}$$

The $e^2$ Jacobi sums and the $e^2$ cyclotomic numbers are related by

$$\sum_i \sum_j \zeta^{-(ai+bj)} J(i,j)_e = e^2(a,b)_e, \tag{2}$$

and

$$\sum_i \sum_j (i,j)_e \zeta^{ai+bj} = J(a,b)_e. \tag{3}$$

Jacobi sums and cyclotomic numbers are related to Dickson–Hurwitz sums. These are defined for $i, j \pmod e$ by (for $q = p$, see [2])

$$B(i,j) = B(i,j)_e = \sum_{h=0}^{e-1} (h, i-jh)_e. \tag{4}$$

They satisfy the relation $B(i,j)_e = B(i, e-j-i)_e$. Also,

$$B(i,0)_e = \begin{cases} f-1, & \text{if } i = 0, \\ f, & \text{if } 1 \le i \le e-1. \end{cases} \tag{5}$$

and

$$\sum_{i=0}^{e-1} B(i,j)_e = q-2. \tag{6}$$

Dickson–Hurwitz sums and Jacobi sums $J(\chi, \chi^j)_e$ are related by (for $q = p$, see [2])

$$\chi^j(-1) J(\chi, \chi^j)_e = \chi^j(-1)\chi(-1) J(1,j)_e = \sum_{i=0}^{e-1} B(i,j)_e \zeta^i. \tag{7}$$

Hence if $f$ is even or $q = 2^r$, then $J(1,j)_e = \sum_{i=0}^{e-1} B(i,j)_e \zeta^i$.

# 4 Congruences of Jacobi sums $J(1,n)_{l^2}$ of order $l^2$

The determining congruences of Jacobi sums $J(1,\ n)_{l^2}$ of order $l^2$ have been studied by Devendra Shirolkar and S. A. Katre [15]. This congruence is in the terms of linear combination of cyclotomic numbers of order $l$. Their work generalises the work of R. J. Evans [5]. We state their important result for ready reference.

**Lemma 4.1.** *Let $l > 3$ be a prime and $1 \le n \le l^2 - 1$. Write $n = dl + n'$ where $1 \le n' \le l-1$ . For $1 \le h \le l-1$, let*

$$\lambda_h = \lambda_h(n) \quad = \quad \left[\frac{n'h}{l}\right] + \left[\frac{-h(n'+1)}{l}\right],$$

*and $1 \le h, k \le l-1$, $h \ne k$, let*

$$\lambda_{h,k} = \lambda_{h,k}(n) = \left[\frac{h+n'k}{l}\right] + \left[\frac{k+n'h}{l}\right] + \left[\frac{n'k-h(n'+1)}{l}\right] + \left[\frac{n'h-k(n'+1)}{l}\right] + \left[\frac{k-h(n'+1)}{l}\right] + \left[\frac{h-k(n'+1)}{l}\right].$$

*For a given $n$, $\lambda_{h,k}$ depends only on the class of six elements (cf.* (1)*) to which $(h,k)_l$ belongs. Define*

$$S(n) := \sum_{t=0}^{l-1}\sum_{j=0}^{l-1} tB(lt+j,n)_{l^2}.$$

*Then*

$$S(n) \equiv \sum_{h=1}^{l-1}\lambda_h(h,0)_l + \sum_{c}\lambda_{h,k}(h,k)_l \pmod{l}$$

*where $\sum_c$ is taken over a set of representatives of classes of six elements of cyclotomic numbers of order $l$, obtained with respect to* (1)*. Furthermore $S(n) \equiv 0 \pmod{l}$ if gcd $(l,n) = l$.*

*Proof.* See [15]. □

**Theorem 4.1.** *Let $l > 3$ be a prime and $p^r = q \equiv 1 \pmod{l^2}$. If $1 \le n \le l^2 - 1$, then a (determining) congruence for $J(1,n)_{l^2}$ for a finite field $\mathbb{F}_q$ is given by*

$$J(1,n)_{l^2} \equiv \begin{cases} -1 + \sum_{i=3}^{l} c_{i,n}(\zeta-1)^i \pmod{(1-\zeta)^{l+1}}, & \text{if } \gcd(l,n) = 1, \\ -1 \pmod{(1-\zeta)^{l+1}}, & \text{if } \gcd(l,n) = l, \end{cases}$$

*where for $3 \le i \le l-1$, $c_{i,n} = \sum_{u=i}^{l-1}\binom{u}{i}B(u,n')_l$ and $c_{l,n} = S(n)$ is given by Lemma 4.1.*

*Proof.* See [15]. □

# 5 Cyclotomic numbers of order 7

There are 49 cyclotomic numbers of order 7. Of these, only twelve distinct cyclotomic numbers of order 7 are sufficient to determine the remaining (see Equation (1)). If $p \equiv 1 \pmod{7}$, the Diophantine system of Leonard and Williams is given by (see [10]):

$$\begin{aligned} 72p &= 2{x_1}^2 + 42({x_2}^2 + {x_3}^2 + {x_4}^2) + 343({x_5}^2 + 3{x_6}^2), \\ 12{x_2}^2 - 12{x_4}^2 + 147{x_5}^2 - 441{x_6}^2 + 56x_1x_6 + 24x_2x_3 - 24x_2x_4 + 48x_3x_4 + 98x_5x_6 &= 0, \\ 12{x_5}^2 - 12{x_4}^2 + 49{x_5}^2 - 147{x_6}^2 + 28x_1x_5 + 28x_1x_6 + 48x_2x_3 + 24x_3x_4 + 490x_5x_6 &= 0. \end{aligned}$$

$x_1 \equiv 1 \pmod 7$ has six non-trivial solutions satisfying $x_1 \equiv 1 \pmod 7$ in addition to the two trivial solutions $(-6t, \pm 2u, \pm 2u, \mp 2u, 0, 0)$ where $t$ is given uniquely and $u$ is given ambiguously by $p = t^2 + 7u^2$, $t \equiv 1 \pmod 7$. If $X_1 = (x_1, x_2, x_3, x_4, x_5, x_6)$ is one of the non-trivial solutions, then the other five non-trivial solutions are (see [10]):

$$\begin{aligned}
X_2 &= (x_1, x_3, -x_4, x_2, -\frac{1}{2}(x_5 + 3x_6), \frac{1}{2}(x_5 - x_6)),\\
X_3 &= (x_1, x_4, -x_2, x_3, -\frac{1}{2}(x_5 - 3x_6), -\frac{1}{2}(x_5 + x_6)),\\
X_4 &= (x_1, -x_4, x_2, -x_3, -\frac{1}{2}(x_5 - 3x_6), -\frac{1}{2}(x_5 + x_6)),\\
X_5 &= (x_1, -x_3, x_4, x_2, -\frac{1}{2}(x_5 + 3x_6), \frac{1}{2}(x_5 - x_6)),\\
X_6 &= (x_1, -x_2, -x_3, -x_4, x_5, x_6).
\end{aligned}$$

For a suitable choice of solution of the above Diophantine system, the cyclotomic numbers of order 7 are given by (see [11]):

$$\begin{aligned}
49(0,0) &= p - 20 - 12t + 3x_1\\
588(0,1) &= 12p - 72 + 24t + 168u - 6x_1 + 84x_2 - 42x_3 + 147x_4 + 147x_6\\
588(0,2) &= 12p - 72 + 24t + 168u - 6x_1 + 84x_3 + 42x_4 - 294x_6\\
588(0,3) &= 12p - 72 + 24t - 168u - 6x_1 + 42x_2 + 84x_4 - 147x_5 + 147x_6\\
588(0,4) &= 12p - 72 + 24t + 168u - 6x_1 - 42x_2 - 84x_4 - 147x_5 + 147x_6\\
588(0,5) &= 12p - 72 + 24t - 168u - 6x_1 - 84x_3 - 42x_4 - 294x_6\\
588(0,6) &= 12p - 72 + 24t - 168u - 6x_1 - 84x_2 + 42x_3 + 147x_5 + 147x_6\\
588(1,2) &= 12p + 12 + 24t + 8x_1 - 196x_5\\
588(1,3) &= 12p + 12 - 60t - 84u - 6x_1 + 42x_2 + 42x_3 - 42x_4\\
588(1,4) &= 12p + 12 + 24t + 8x_1 + 98x_5 - 294x_6\\
588(1,5) &= 12p + 12 - 60t + 84u - 6x_1 - 42x_2 - 42x_3 + 42x_4\\
588(2,4) &= 12p + 12 + 24t + 8x_1 + 98x_5 + 294x_6
\end{aligned} \tag{8}$$

Also, if $J(1,1)_7 = \sum_{i=0}^{6} c_i\zeta^i = \sum_{i=0}^{6} B(i,1)_7\zeta^i$ is a Jacobi sum of order 7, then for a suitable choice of solution of the above Diophantine system, the integers $c_1, c_2, \ldots, c_6$ are given by (see [11]):

$$\begin{aligned}
12c_1 &= -2x_1 + 6x_2 + 7x_5 + 21x_6\\
12c_2 &= -2x_1 + 6x_3 + 7x_5 - 21x_6\\
12c_3 &= -2x_1 + 6x_4 - 14x_5\\
12c_4 &= -2x_1 - 6x_4 - 14x_5\\
12c_5 &= -2x_1 - 6x_3 + 7x_5 - 21x_6\\
12c_6 &= -2x_1 - 6x_2 + 7x_5 + 21x_6
\end{aligned} \tag{9}$$

# 6 Congruences of Jacobi sum $J(1,1)_{49}$ of order 49

Let $p \equiv 1 \pmod{49}$ be a prime and $\zeta$ be primitive 49-th root of unity in $\mathbb{Q}(\zeta)$. Then from Theorem 4.1 the determining congruences for Jacobi sum $J(1,1)_{49}$ of order 49 are given as:

$$J(1,1)_{49} \equiv -1 + \sum_{i=3}^{7} c_{i,1}(\zeta-1)^i \pmod{(1-\zeta)^8}$$

where $c_{i,1}$ are defined in Theorem 4.1. Let $q = 7f+1$ ($f$ even) be a prime. Then the Jacobi sum $J(1,1)_7$ in terms of the Dickson–Hurwitz sums $B(i,1)_7$, $(0 \le i \le 6)$ is given in (7). These Dickson–Hurwitz sums of order 7 in terms of solutions of the Diophantine system are given by P. A. Leonard and K. S. Williams (see [11]):

$$\begin{aligned}
84B(0,1)_7 &= 12x_1 + 12p - 24\\
84B(1,1)_7 &= -2x_1 + 42x_2 + 49x_5 + 147x_6 + 12p - 24\\
84B(2,1)_7 &= -2x_1 + 42x_3 + 49x_5 - 147x_6 + 12p - 24\\
84B(3,1)_7 &= -2x_1 + 42x_4 - 98x_5 + 12p - 24\\
84B(4,1)_7 &= -2x_1 - 42x_4 - 98x_5 + 12p - 24\\
84B(5,1)_7 &= -2x_1 - 42x_3 + 49x_5 - 147x_6 + 12p - 24\\
84B(6,1)_7 &= -2x_1 - 42x_3 + 49x_5 + 147x_6 + 12p - 24
\end{aligned} \tag{10}$$

Therefore,

$$\begin{aligned}
c_{1,1} &= (\frac{6p - x_1 - 12}{2}) - (\frac{x_4 + 3x_3 + 5x_2}{2})\\
c_{2,1} &= (\frac{5}{3})(\frac{6p - x_1 - 12}{2}) - 3(\frac{x_4 + 3x_3 + 5x_2}{2}) + (\frac{28x_5 + 42x_6}{6})\\
c_{3,1} &= (\frac{5}{3})(\frac{6p - x_1 - 12}{2}) - 3(\frac{3x_4 + 10x_3 + 20x_2}{2}) + (\frac{105x_6 + 70x_5}{6})\\
c_{4,1} &= (\frac{6p - x_1 - 12}{2}) - (\frac{x_4 - 5x_3 - 15x_2}{2}) + (\frac{35x_6 + 21x_5}{2})\\
c_{5,1} &= (\frac{2}{6})(\frac{6p - x_1 - 12}{2}) - (\frac{x_3 + 6x_2}{2}) + (\frac{105x_6 + 49x_5}{12})\\
c_{6,1} &= (\frac{2}{42})(\frac{6p - x_1 - 12}{2}) - (\frac{9x_3 + 14x_2}{28}) + (\frac{21x_6 + 7x_5}{12})
\end{aligned} \tag{11}$$

Using equation (8) and Lemma 4.1.

$$c_{7,1} = -(\frac{2}{14})(\frac{6p - x_1 - 12}{2}) + (\frac{2}{14})(\frac{3x_3 + 5x_2}{2}) + (\frac{7x_5 - 5x_4}{28}).$$

We observe that as $x_1 \equiv 1 \pmod 7$ and $p \equiv 1 \pmod 7$ therefore, $\dfrac{6p - x_1 - 12}{2} \equiv 0 \pmod 7$.

## 6.1 Congruence of Jacobi sum $J(1,1)_{49}$ for artiad and hyperartiad primes

Lloyd Tanner (see [17]) came across some special primes while studying Jacobi sums in the field of $5^{th}$ root of unity in the field $\mathbb{F}_p$ where $p = 10f + 1$. He observed that, when Jacobi sums corresponding to these primes were expanded so that the sum of their coefficients is $-1$, the coefficients of Jacobi sums are congruent modulo 5. He called these primes artiad primes.

Later in 1985, Emma Lehmer gave a characterization of such primes (see [9]). She showed that in case of $p = 10f + 1$ artiads are those primes for which the Fibonacci root $\theta = \frac{(1+\sqrt{5})}{2}$ is a solution to the congruence $x^2 - x - 1 \equiv 0 (\mathrm{mod}\ p)$ is a quintic residue. She also defined hyperartiads as primes for which 5 and the Fibonacci roots are quintic residues modulo $p$.

Emma Lehmer (see [9]) further extended the notion of artiad and hyperartiad primes to $p = 14s + 1$, defining the septic artiad and septic hyperartiad primes. She showed that when $\theta$ is replaced by $2\cos(\frac{2\pi}{7}) = \zeta + \zeta^{-1}$ the septic artiad and septic hyperartiad is defined as follows: The prime $p = 14s + 1$ for which all solutions of congruence $x^3 + x^2 - 2x - 1 \equiv 0 \pmod{p}$ are seventh power residues is an artiad prime.

Septic hyperartiad primes are septic artiad primes for which 7 is a seventh power residue.

Here, we state the characterization of septic artiad primes and septic hyperartiad primes obtained by Emma Lehmer for reference.

We reformulate these definitions for the prime $p$, $p = 14s+1$, in terms of $x_1, x_2, \ldots, x_6$. This enables us to determine simpler congruences that hold for Jacobi sum $J(1,1)_{49}$ of order 49 for the artiad and hyperartiad case.

**Lemma 6.1.** *Let $p \equiv 1 \pmod 7$, and let $J(1,1)_7 = \sum_{i=0}^{6} c_i \zeta^i$ be the Jacobi sum of order 7, normalized by $\sum_{i=0}^{6} c_i = -1$ and $\theta_k = \zeta^k + \zeta^{-k}$ be the roots of the congruence $x^3 + x^2 - 2x - 1 \equiv 0 \pmod p$. Fix a generator $\gamma$ of $\mathbb{F}_p^*$. Then, for $k = 1, 2, 3$, $\mathrm{ind}_\gamma(\theta_k) \equiv k\big(c_{3k} - c_{7-3k}\big) (\mathrm{mod}\ 7)$, where the subscripts are taken modulo 7.*

*Proof.* (see [9]) □

**Theorem 6.1** (Septic artiads)**.** *Let $p = 14s + 1$. The three roots of the congruence $x^3 + x^2 - 2x - 1 \equiv 0 (\mathrm{mod}\ p)$ are seventh power residues modulo $p$ if and only if $c_k \equiv c_{7-k} \pmod 7$, $k = 1, 2, 3$, where the coefficients $c_i$ are defined by the Jacobi sum of order 7. Primes satisfying this condition will be called* septic artiads.

*Proof.* (see [9]) □

The notion of septic hyperartiad primes is given by the following theorem.

**Theorem 6.2** (Septic hyperartiads)**.** *Let $p$ be a septic artiad prime, has 7 as a seventh power residue modulo $p$ if and only if $(0,\ k) \equiv (0,\ 7 - k) (\mathrm{mod}\ 7)$ for $k = 1, 2, 3$.*

*Proof.* See [9]. □

**Lemma 6.2.** *$p = 14s + 1$ is an artiad prime if and only if $x_2 \equiv x_3 \equiv x_4 \equiv 0 \pmod 7$.*

*Proof.* Let $p = 14s + 1$ be an artiad prime. Then from the work of Emma Lehmer (see [9], Section 5, Theorem 5), $c_k \equiv c_{7-k} \pmod 7$, $k = 1, 2, 3$. Using (9) we get, $x_2 \equiv x_3 \equiv x_4 \equiv 0 \pmod 7$.

Conversely, suppose $p = 14s + 1$ with $x_2 \equiv x_3 \equiv x_4 \equiv 0 \pmod 7$ and $x_1 \equiv 1 (\mathrm{mod}\ 7)$. From (9) we obtain $c_k \equiv c_{7-k} \pmod 7$, $k = 1, 2, 3$. Therefore, $p$ is an artiad prime. □

**Lemma 6.3.** *$p = 14s + 1$ is a hyperartiad prime if and only if $p$ is an artiad prime and for a generator $\gamma$ of ${\mathbb{F}_p}^*$ $\mathrm{ind}_\gamma 7 \equiv 0 \pmod 7$.*

*Proof.* J.B. Muskat has given the expression for $\mathrm{ind}_\gamma 7$ in terms of cyclotomic numbers of order 7 as (see [12], Section 1, Theorem 1),

$$\mathrm{ind}_\gamma 7 \equiv (\frac{p-1}{2}) - \sum_{h=0}^{6}(h,0)_7 h \pmod 7. \tag{12}$$

Let $p$ be a hyperartiad prime (hence, an artiad, as well). Then $(0,h)_7 \equiv (0,7-h)_7 \pmod 7$ (see the work of Emma Lehmer [9], Section 5, Theorem 6). Hence by (13) we get, $\mathrm{ind}_\gamma 7 \equiv 0 \pmod 7$.

Conversely, suppose $p = 14s + 1$ is an artiad prime and $\mathrm{ind}_\gamma 7 \equiv 0 \pmod 7$. Then using (12) we get, $\sum_{h=0}^{e-1}(h,0)_7 h \equiv 0 \pmod 7$. Hence $(0,h)_7 \equiv (0,7-h)_7 \pmod 7$ for $h = 1,2,3$. Therefore, from the work of Emma Lehmer (see ( [15], Theorem 6), $p$ is a hyperartiad prime. □

**Lemma 6.4.** *$p = 14s + 1$ is an artiad prime if and only if $c_{1,1} \equiv c_{2,1} \equiv c_{3,1} \equiv c_{4,1} \equiv c_{5,1} \equiv 0 \pmod 7$, $12c_{6,1} \equiv (\frac{4}{7})^{\frac{6p-x_1-12}{2}} \pmod 7$, $4c_{7,1} - 4\mathrm{ind}_\gamma 7 \equiv -12c_{6,1} + x_5 \pmod 7$.*

*Proof.* Let $p = 14s + 1$ be an artiad prime. Then by Lemma 6.2 and Equation (11), we get $c_{1,1} \equiv c_{2,1} \equiv c_{3,1} \equiv c_{4,1} \equiv c_{5,1} \equiv 0 \pmod 7$ (being $x_1 \equiv 1 \pmod 7$).
From Equation (11)

$$12c_{6,1} = \frac{12p - 2x_1 - 24}{7} + (-21x_6 + 7x_5 - x_2)$$

Hence,

$$12c_{6,1} \equiv \frac{4}{7}(\frac{6p - x_1 - 12}{2}) \pmod 7.$$

Now we have $28\mathrm{ind}_\gamma 7 \equiv x_2 - 19x_3 - 18x_4 \pmod{49}$ (see [16] Corollary 2, Equation 8).
Hence

$$4\mathrm{ind}_\gamma 7 \equiv (\frac{x_2 - 19x_3 - 18x_4}{7}) \pmod 7.$$

Using Equation (11),

$$28c_{7,1} = -(12p - 7x_5 + 5x_4 - 6x_3 - 10x_2 - 2x_1 - 24).$$

Therefore,

$$28c_{7,1} - 28\mathrm{ind}_\gamma 7 \equiv -12p + 2x_1 + 24 + 9x_2 + 25x_3 + 13x_4 + 7x_5 \pmod{49}$$

and we get

$$4c_{7,1} - 4\mathrm{ind}_\gamma 7 \equiv -12c_{6,1} + x_5 \pmod 7.$$

Conversely, suppose $c_{1,1} \equiv c_{2,1} \equiv c_{3,1} \equiv c_{4,1} \equiv c_{5,1} \equiv 0 \pmod 7$, $12c_{6,1} \equiv \frac{4}{7}(\frac{6p-x_1-12}{2}) \pmod 7$, $4c_{7,1} - 4\mathrm{ind}_\gamma 7 \equiv -12c_{6,1} + x_5 \pmod 7$.

Using equation (11) we get

$$\begin{aligned} 4x_4 + x_3 + 3x_2 &\equiv 0 \pmod 7 \\ 5x_4 + 5x_3 - 4x_2 &\equiv 0 \pmod 7 \\ 4x_4 + 5x_3 - x_2 &\equiv 0 \pmod 7 \\ x_3 &\equiv 6x_2 \pmod 7 \end{aligned} \tag{13}$$

Hence, $x_2 \equiv x_3 \equiv x_4 \equiv 0 \pmod 7$. Therefore, using Lemma 6.2 $p$ is an artiad prime. □

**Lemma 6.5.** *$p = 14s + 1$ is a hyperartiad prime if and only if $c_{1,1} \equiv 0 \pmod 7$, $c_{2,1} \equiv 0 \pmod 7$, $c_{3,1} \equiv 0 \pmod 7$, $c_{4,1} \equiv 0 \pmod 7$, $c_{5,1} \equiv 0 \pmod 7$, $12c_{6,1} \equiv (\frac{4}{7})^{\frac{6p-x_1-12}{2}} \pmod 7$, $4c_{7,1} \equiv -12c_{6,1} + x_5 \pmod 7$.*

*Proof.* Apply Lemma 6.2 and Lemma 6.3. □

**Theorem 6.3.** (1) *$p$ is an artiad prime if and only if*

$$J(1,1)_{49} \equiv -1 + c_{6,1}(\zeta - 1)^6 + (-3c_{6,1} + \mathrm{ind}_\gamma 7 + 2x_5)(\zeta - 1)^7 \pmod{(1-\zeta)^8}.$$

(2) *$p$ is a hyperartiad prime if and only if*

$$J(1,1)_{49} \equiv -1 + c_{6,1}(\zeta - 1)^6 + (-3c_{6,1} + 2x_5)(\zeta - 1)^7 \pmod{(1-\zeta)^8}.$$

*Proof.* (1) We have $J(1,1)_{49} \equiv -1 + \sum_{i=3}^{7} c_{i,1}(\zeta - 1)^i \pmod{(1-\zeta)^8}$.

Let $p$ be an artiad prime then by Lemma 6.4 $c_{1,1} \equiv c_{2,1} \equiv c_{3,1} \equiv c_{4,1} \equiv c_{5,1} \equiv 0 \pmod 7$. Therefore,

$$J(1,1)_{49} \equiv -1 + c_{6,1}(\zeta - 1)^6 + c_{7,1}(\zeta - 1)^7 \pmod{(1-\zeta)^8}.$$

From Lemma 6.4 $c_{7,1} \equiv -3c_{6,1} + \mathrm{ind}_\gamma 7 + 2x_5 \pmod 7$. Hence,

$$J(1,1)_{49} \equiv -1 + c_{6,1}(\zeta - 1)^6 + (-3c_{6,1} + \mathrm{ind}_\gamma 7 + 2x_5)(\zeta - 1)^7 \pmod{(1-\zeta)^8}.$$

Suppose $J(1,1)_{49} \equiv -1 + c_{6,1}(\zeta - 1)^6 + (-3c_{6,1} + \mathrm{ind}_\gamma 7 + 2x_5)(\zeta - 1)^7 \pmod{(1-\zeta)^8}$. Therefore, $c_{1,1} \equiv c_{2,1} \equiv c_{3,1} \equiv c_{4,1} \equiv c_{5,1} \equiv 0 \pmod 7$. Repeating the arguments as in Lemma 6.4 we get, $x_2 \equiv x_3 \equiv x_4 \equiv 0 \pmod 7$ and hence $p$ is an artiad prime.

(2) If $p$ is a hyperartiad prime, then it is an artiad prime. By part(1)

$$J(1,1)_{49} \equiv -1 + c_{6,1}(\zeta - 1)^6 + (-3c_{6,1} + \mathrm{ind}_\gamma 7 + 2x_5)(\zeta - 1)^7 \pmod{(1-\zeta)^8}.$$

As $p$ is a hyperartiad prime from Lemma 6.3 $\mathrm{ind}_\gamma 7 \equiv 0 \pmod 7$. Therefore

$$J(1,1)_{49} \equiv -1 + c_{6,1}(\zeta - 1)^6 + (-3c_{6,1} + 2x_5)(\zeta - 1)^7 \pmod{(1-\zeta)^8}.$$

Suppose $J(1,1)_{49} \equiv -1 + c_{6,1}(\zeta - 1)^6 + (-3c_{6,1} + 2x_5)(\zeta - 1)^7 \pmod{(1-\zeta)^8}$. Therefore, $c_{1,1} \equiv c_{2,1} \equiv c_{3,1} \equiv c_{4,1} \equiv c_{5,1} \equiv 0 \pmod 7$. Repeating the argument as in Lemma (6.4) we get, $x_2 \equiv x_3 \equiv x_4 \equiv 0 \pmod 7$ and hence $p$ is an artiad prime. Again by Lemma 6.4 $12c_{6,1} \equiv (\frac{4}{7})^{\frac{6p-x_1-12}{2}} \pmod 7$ and $4c_{7,1} - 4\mathrm{ind}_\gamma 7 \equiv -12c_{6,1} + x_5 \pmod 7$. But as $c_{7,1} \equiv -3c_{6,1} + 2x_5 \pmod 7$, hence $\mathrm{ind}_\gamma 7 \equiv 0 \pmod 7$. Apply Lemma 6.5 $p$ is a hyperartiad prime. □

**Example 1** (Septic artiad prime)**.** *Take artiad prime* $p = 15570437 \equiv 1(\mathrm{mod}\ 49)$*,* $\gamma = 5$ *we get,* $\mathrm{ind}_5 7 = 6454989 \equiv 3(\mathrm{mod}\ 7)$ *and* $c_{1,1} \equiv c_{2,1} \equiv c_{3,1} \equiv c_{4,1} \equiv c_{5,1} \equiv 0\ (\mathrm{mod}\ 7)$*,* $c_{6,1} = 448558 \equiv 0\ (\mathrm{mod}\ 7)$ *and* $c_{7,1} = -6891133$*.* $c_{7,1} \equiv 3\ (\mathrm{mod}\ 7)$*, also using Lemma 6.4 we get* $x_5 \equiv 0\ (\mathrm{mod}\ 7)$*. Thus, Theorem 6.3 holds.*

**Example 2** (Septic hyperartiad prime)**.** *Take hyperartiad prime* $p = 876611 \equiv 1(\mathrm{mod}\ 49)$*,* $\gamma = 2$ *we get,* $\mathrm{ind}_2 7 = 694323 \equiv 0\ (\mathrm{mod}\ 7)$ *and* $c_{1,1} \equiv c_{2,1} \equiv c_{3,1} \equiv c_{4,1} \equiv c_{5,1} \equiv 0\ (\mathrm{mod}\ 7)$*,* $c_{6,1} = 1,537,589,240,299 \equiv 0\ (\mathrm{mod}\ 7)$ *and* $c_{7,1} = 8,071,253,483,167 \equiv 0\ (\mathrm{mod}\ 7)$*, also using Lemma 6.5 we get* $x_5 \equiv 0\ (\mathrm{mod}\ 7)$*. Thus, Theorem 6.3 holds.*

# References


[1] Acharya, V. V., & Katre, S. A. (1995). Cyclotomic numbers of orders $2l$, $l$ an odd prime. *Acta Arithmetica*, 69(1), 51–74.

[2] Dickson, L. E. (1935). Cyclotomy and trinomial congruences. *Transactions of the American Mathematical Society*, 37, 363–380.

[3] Dickson, L. E. (1935). Cyclotomy, higher congruences, and Waring's problem. *American Journal of Mathematics*, 57, 391–424.

[4] Dickson, L. E. (1935). Cyclotomy when $e$ is composite. *Transactions of the American Mathematical Society*, 38, 187–200.

[5] Evans, R. J. (1998). Congruences for Jacobi sums. *Journal of Number Theory*, 71, 109–120.

[6] Ihara, Y. (1986). Profinite braid groups, Galois representations, and complex multiplications. *Annals of Mathematics*, 123(1), 43–106.

[7] Iwasawa, K. (1975). A note on Jacobi sums. *Symposia Mathematica*, 15, 447–459.

[8] Katre, S. A., & Rajwade, A. R. (1983). On the Jacobsthal sum $\phi_9(a)$ and the related sum $\psi_9(a)$. *Mathematica Scandinavica*, 53, 193–202.

[9] Lehmer, E. (1966). Artiads characterized. *Journal of Mathematical Analysis and Applications*, 15(1), 118–131.

[10] Leonard, P. A., & Williams, K. S. (1974). A Diophantine system of Dickson. *Rendiconti della Classe di Scienze Fisiche, Matematiche e Naturali dell'Accademia Nazionale dei Lincei*, 56(2), 145–150.

[11] Leonard, P. A., & Williams, K. S. (1975). The cyclotomic numbers of order 7. *Proceedings of the American Mathematical Society*, 51, 295–300.

[12] Muskat, J. B. (1964). On the solvability of $x^e \equiv e\ (\mathrm{mod}\ p)$. *Pacific Journal of Mathematics*, 14(1), 257–260.

[13] Parnami, J. C., Agrawal, M. K., & Rajwade, A. R. (1982). Jacobi sums and cyclotomic numbers for a finite field. *Acta Arithmetica*, 41, 1–13.

[14] Parnami, J. C., Agrawal, M. K., & Rajwade, A. R. (1981). A congruence relation between the coefficients of the Jacobi sum. *Indian Journal of Pure and Applied Mathematics*, 12(7), 804–806.

[15] Shirolkar, D., & Katre, S. A. (2011). Jacobi sums and cyclotomic numbers of order $l^2$. *Acta Arithmetica*, 33–49.

[16] Storer, T. (1967). *Cyclotomy and Difference Sets*. Markham, Chicago.

[17] Tanner, Lloyd H. W. L. (1892–1893). On complex primes formed with fifth roots of unity. *Proceedings of the London Mathematical Society*, 24, 223–262.