Original Article

Available online at
www.bpasjournals.com

Bulletin of Pure and Applied Sciences.
Vol. 38E (Math & Stat.), No.1, 2019. P.466-470
Print version ISSN 0970 6577
Online version ISSN 2320 3226
DOI: 10.5958/2320-3226.2019.00050.X

COMPUTATION OF JACOBI SUMS AND CYCLOTOMIC NUMBERS WITH REDUCED COMPLEXITY

Md. Helal Ahmed[1,*], Jagmohan Tanti[2]

Authors Affiliation:
[1]Department of Mathematics, Central University of Jharkhand, Ranchi, Jharkhand 835205, India.
E-mail: ahmed.helal@cuj.ac.in
[2] Department of Mathematics, Central University of Jharkhand, Ranchi, Jharkhand 835205, India.
E-mail: jagmohan.t@gmail.com

***Corresponding Author:**
Md. Helal Ahmed, Department of Mathematics, Central University of Jharkhand, Ranchi, Jharkhand 835205, India.

E-mail: ahmed.helal@cuj.ac.in

Received on 21.01.2019, Revised on 06.05.2019, Accepted on 28.05.2019

Abstract:
Jacobi sums and cyclotomic numbers are the important objects in number theory. The determination of all the Jacobi sums and cyclotomic numbers of order e is merely intricate to compute. This paper presents the lesser numbers of Jacobi sums and cyclotomic numbers which are enough for the determination all Jacobi sums and the cyclotomic numbers of a particular order.

Keywords: Character; Cyclotomic numbers; Jacobi sums; Finite fields; Cyclotomic polynomial.

2010 Mathematics Subject Classification: Primary: 11T24, Secondary: 11T22.

1. INTRODUCTION

For $e \in Z^+ \geq 2$, in a finite field, a Jacobi sum of order e mainly depends on two parameters. Therefore, these values can be naturally assembled into a matrix of order e. As illustrated in [1], Jacobi sums could be used for estimating the number of integral solutions to congruences such as $x^3 + y^3 \equiv 1 \pmod{p}$. These estimates play a key role in the development of the Weil's conjecture [2]. Jacobi sums were also utilized by Adleman, Pomerance, Rumely [3] for primality testing.

Let $e \geq 2$ be an integer, p a prime, $q = p^r, r \in Z^+$ and $q \equiv 1 \pmod{e}$. One writes $q = ek + 1$ for some positive integer k. Let F_q be a finite field of q elements and γ be a generator of the cyclic group F_q^*. For a primitive e-th root $\zeta_e$of unity, define a multiplicative character χ_e of order e on F_q^* by $\chi_e(\gamma) = \zeta_e$. We now extend χ_e to a map from F_q to $Q(\zeta_e)$ by taking $\chi_e(0) = 0$. For $0 \leq i, j \leq e - 1$, the Jacobi sum of order e is defined by

$$J_e(i,j) = \sum_{v \in F_q} \chi_e^i(v)\chi_e^j(v+1).$$

For $0 \leq a, b \leq e - 1$, the cyclotomic numbers $(a,b)_e$ of order e is defined as follows:

$$(a,b)_e := \#\{v \in F_q \mid \chi_e(v) = \zeta_e^a,\ \chi_e(v+1) = \zeta_e^b\}$$

$$= \#\{v \in F_q \setminus \{0,-1\} | ind_\gamma(v) \equiv a \ (\text{mod } e),\ ind_\gamma(v+1) \equiv b \ (\text{mod } e)\}.$$

The Jacobi sums $J_e(i,j)$ and the cyclotomic numbers $(a,b)_e$ are well connected by the following relations [4, 5]:

$$\textstyle\sum_a \sum_b (a,b)_e \zeta_e^{ai+bj} = J_e(i,j), \tag{1.1}$$

$$\textstyle\sum_i \sum_j \zeta_e^{-(ai+bj)} J_e(i,j) = e^2 (a,b)_e. \tag{1.2}$$

For more information about the properties of Jacobi sums and cyclotomic numbers, one may refer to [4, 5, 6]. Cyclotomic numbers are one of the most important objects in number theory. These numbers have been extensively used in cryptography, coding theory and other branches of information theory. Thus determination of cyclotomic numbers, so called cyclotomic number problem, of different orders is one of the basic problems in number theory. Complete solutions to cyclotomic number problem for $e = 2-6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 18, 20, 22, l, 2l, l^2$ with l an odd prime have been investigated by many authors [5, 6, 7].

The problem of determining Jacobi sums and cyclotomic numbers has been treated by many authors since the age of Gauss. Jacobi sums and cyclotomic numbers are interrelated, which is shown in (1.1) and (1.2). The problem of cyclotomic numbers of prime order l in the finite field F_q, $q = p^r$, $p \equiv 1 \ (\text{mod } l)$ has been investigated by Katre ans Rajwade [7] in terms of arithmetic characterization of Jacobi sums of prime order l. Later, Acharya and Katre [6] induced some additional condition and solved the cyclotomic problem twice for a prime in terms of the coefficients of Jacobi sums of orders l and $2l$. Recently, Shirolkar and Katre [5] solved the cyclotomic problem of order l^2 in terms of the coefficients of Jacobi sums of orders l and l^2.

The question of determining all Jacobi sums of orders e in terms of lesser number of Jacobi sums has also been taken by many authors such as Parnami, Agrawal and Rajwade [8]. Similar kind of arguments for cyclotomic numbers can also be given. In this paper, we give a list of fewer cyclotomic numbers (respectively Jacobi sums) of order e which qualifies to determine all cyclotomic numbers (respectively Jacobi sums) of order e. We exhibit an explicit case with $e = 3$.

2. MAIN RESULTS

2.1. Computation of Cyclotomic Numbers of order e. The following result is a sort of optimization of the cyclotomic number problem.

Theorem 2.1. The number of cyclotomic numbers $(\mathrm{a},\mathrm{b})_\mathrm{e}$ required for the determination of all the cyclotomic numbers of order e is equal to $e + (e-1)(e-2)/6$, if $6|(e-1)(e-2)$, otherwise $e + \lceil (e-1)(e-2)/6 \rceil + 1$.

Proof. Recall from the properties of cyclotomic numbers [4, 5, 6], if k is even or $q = 2^r$, then $(a,b)_e = (b,a)_e = (a-b,-b)_e = (b-a,-a)_e = (-a,b-a)_e = (-b,a-b)_e$, (2.1)

otherwise

$$(a,b)_e = (b+\tfrac{e}{2}, a+\tfrac{e}{2})_e = (\tfrac{e}{2}+a-b,-b)_e = (\tfrac{e}{2}+b-a,\tfrac{e}{2}-a)_e = (-a,b-a)_e = (\tfrac{e}{2}-b,a-b)_e. \tag{2.2}$$

Thus by (2.1) and (2.2) partition cyclotomic numbers $(a,b)_e$ of order e into group of classes. The expression (2.1) splits the problem into two cases:

Case 1: $2|k \ / \ q = 2^r$ and $3 \nmid e$: In this case, $(0,0)_e$ forms singleton class, $(-a,0)_e, (a,a)_e, (0,-a)_e$ form classes of three elements where $1 \le a \le e-1 \ (\text{mod } e)$ and rest $(e^2 - 3e + 2)$ of the cyclotomic numbers form classes of six elements. Therefore the total number of distinct cyclotomic number classes is equal to $1 + (e-1) + (e^2 - 3e + 2)/6 = e + (e-1)(e-2)/6$.

Case 2: $2|k \ / \ q = 2^r$ and $3|e$ with $e = 3x$ for some $x \in Z^+$: In this situation, $(0,0)_e$ form singleton class, $(-a,0)_e$, $(a,a)_e, (0,-a)_e$ form classes of three elements where $1 \le a \le e-1 \ (\text{mod } e)$, $(x,2x)_e, (2x,x)_e$ which are grouped into classes of two elements and rest $(e^2 - 3e)$ of the cyclotomic numbers form classes of six elements. Therefore the total number of distinct cyclotomic number classes is equal to $1 + 1 + (e-1) + (e^2 - 3e)/6 = e + \lceil (e-1)(e-2)/6 \rceil + 1$.

Again the expression (2.2) splits the problem into two cases:

Case 3: $2 \nmid k$ & $q \neq 2^r$ and $3 \nmid e$: In this case, $(0, \frac{e}{2})_e$ form singleton class, $(0, a)_e$, $(a + \frac{e}{2}, \frac{e}{2})_e$, $(\frac{e}{2} - a, -a)_e$ form classes of three elements where $0 \leq a \neq \frac{e}{2} \leq e - 1 \pmod e$ and rest $(e^2 - 3e + 2)$ of the cyclotomic numbers form classes of six elements. Therefore the total number of distinct cyclotomic number classes is equal to $1 + (e - 1) + (e^2 - 3e + 2)/6 = e + (e - 1)(e - 2)/6$.
Case 4: $2 \nmid k$ & $q \neq 2^r$ and $3|e$: (it implies that $e = 6x$ for some $x \in Z^+$). Here cyclotomic number $(0, \frac{e}{2})_e$ form singleton class, $(0, a)_e$, $(a + \frac{e}{2}, \frac{e}{2})_e$, $(\frac{e}{2} - a, -a)_e$ form classes of three elements where $0 \leq a \neq \frac{e}{2} \leq e - 1 \pmod e$, $(2x, x)_e$, $(x + \frac{e}{2}, 2x + \frac{e}{2})_e$ which are grouped into classes of two elements and rest $(e^2 - 3e)$ of the cyclotomic numbers form classes of six elements. Thus the total number of distinct cyclotomic number classes is equal to $1 + 1 + (e - 1) + (e^2 - 3e)/6 = e + \lceil (e - 1)(e - 2)/6 \rceil + 1$.
Therefore, the number of cyclotomic numbers required for the determination of all the cyclotomic numbers for $e \geq 2$, is equal to $e + (e - 1)(e - 2)/6$, if $6|(e - 1)(e - 2)$, otherwise $e + \lceil (e - 1)(e - 2)/6 \rceil + 1$.

□

Remark 2.1. For the determination all the Jacobi sums $J_e(i, j)$of order e, it is sufficient to determine exactly $e + (e - 1)(e - 2)/6$ numbers of cyclotomic numbers of order e, if $(e - 1)(e - 2)$ is completely divisible by 6, otherwise $e + \lceil (e - 1)(e - 2)/6 \rceil + 1$.

2.2 Computation of Jacobi sums of order e.

Theorem 2.2. The number of Jacobi sums $J_e(i, j)$ required for the determination of all the Jacobi sums of order e is equal to $e + (e - 1)(e - 2)/6$, if $6|(e - 1)(e - 2)$, otherwise $\mathrm{e} + \lceil (\mathrm{e} - 1)(\mathrm{e} - 2)/6 \rceil + 1$.
Proof. From the properties of Jacobi sums [4, 5, 6], if k is even or $q = 2^r$, then

$$J_e(i, j) = J_e(j, i) = J_e(-i - j, i) = J_e(i, -i - j) = J_e(j, -i - j) = J_e(-i - j, j), \quad (2.3)$$

otherwise

$$(-1)^{ik} J_e(i, j) = (-1)^{jk} J_e(j, i) = (-1)^{jk} J_e(-i - j, i) = (-1)^{jk} J_e(i, -i - j) = (-1)^{ik} J_e(j, -i - j) = (-1)^{ik} J_e(-i - j, j).$$

These above expressions partition the Jacobi sums $J_e(i, j)$ of order e into group of classes. It is clear that Jacobi sums matrix is always symmetric and if k is even or $q = 2^r$, the entries of the Jacobi sums matrix differ atmost by sign. Let us consider the expression (2.3). It splits the problem into three cases:
Case 1: $i = j$: In this case, Jacobi sums of order e partition into classes of singleton and three elements. If $3i \equiv 0 \pmod e$ form singleton class i.e. $J_e(i, i)$, otherwise form classes of three elements i.e. $J_e(i, i) = J_e(i, -2i) = J_e(-2i, i)$.
Case 2: $i = 0$ and $i \neq j$: In this situation, Jacobi sums of order e partition into classes of three and six elements. If $2j \equiv 0 \pmod e$ form classes of three elements i.e. $J_e(0, j) = J_e(j, 0) = J_e(-j, j)$, otherwise form classes of six elements i.e. $J_e(0, j) = J_e(j, 0) = J_e(-j, j) = J_e(j, -j) = J_e(-j, 0) = J_e(0, -j)$.
Case 3: $i \neq 0$ and $i \neq j$: Again in this case, Jacobi sums of order e partition into classes of three and six elements. If $i + 2j \equiv 0 \pmod e$ form classes of three elements i.e. $J_e(i, j) = J_e(j, i) = J_e(-i - j, j)$, otherwise form classes of six elements i.e. $J_e(i, j) = J_e(j, i) = J_e(-i - j, i) = J_e(i, -i - j) = J_e(j, -i - j) = J_e(-i - j, j)$.
Thus, it is clear by above cases, for the determination of all the Jacobi sums for $e \geq 2$, it is enough to determine $e + (e - 1)(e - 2)/6$, numbers of Jacobi sums if $6|(e - 1)(e - 2)$, otherwise $e + \lceil (e - 1)(e - 2)/6 \rceil + 1$.

□

Remark 2.2. For the determination all the cyclotomic numbers $(a, b)_e$ of order e, it is sufficient to determine exactly $e + (e - 1)(e - 2)/6$ numbers of Jacobi sums $J_e(i, j)$ of order e, if $6|(e - 1)(e - 2)$, otherwise $e + \lceil (e - 1)(e - 2)/6 \rceil + 1$.
Here we give an example for optimization of computation for determination of Jacobi sums and cyclotomic numbers respectively of order 3.

Example 1. Let us choose a number q that satisfies $q = p^r \equiv 1 \pmod 3$, where p prime and $r \in Z^+$. Assume that $q = 7$. The number of cyclotomic numbers required for the determination of all the cyclotomic numbers of order 3 is shown in the Table 1.

Table 1:

(a,b)	b		
a	0	1	2
0	(0,0)	(0,1)	(0,2)
1	(0,1)	(0,2)	(1,2)
2	(0,2)	(1,2)	(0,1)

For the determination of all the Jacobi sums of order 3 over F_7, we need to determine only four cyclotomic numbers out of nine cyclotomic numbers, which are $(0,0)_3$, $(0,1)_3$, $(0,2)_3$ and $(1,2)_3$. For the determination of above cyclotomic numbers, applying the formula [9], we get $(0,0)_3 = 0$, $(0,1)_3 = 0$, $(0,2)_3 = 1$ and $(1,2)_3 = 1$ w.r.t. the generator 3 of F_7, which is shown in matrix A.

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Apply the relation (1.1) for the determination of $J_3(i,j)$, where $0 \le i,j \le 2$,

$$J_3(i,j) = \zeta_3^{2j} + \zeta_3^{i+j} + \zeta_3^{i+2j} + \zeta_3^{2i} + \zeta_3^{2i+j}.$$

On substituting the values of i and j, and employing the cyclotomic polynomial of order 3, which is $\zeta_3^2 + \zeta_3 + 1$, we get $J_3(0,0) = 5 = q - 2$, $J_3(0,1) = -1$, $J_3(0,2) = -1$, $J_3(1,0) = -1$, $J_3(1,2) = -1$, $J_3(2,0) = -1$, $J_3(2,1) = -1$, $J_3(1,1) = -3\zeta_3 - 1$ and $J_3(2,2) = 3\zeta_3 + 1$.

Conversely, the number of Jacobi sums required for the determination all the Jacobi sums of order 3 is shows in Table 2.

Table 2:

(a,b)	b		
a	0	1	2
0	(0,0)	(0,1)	(0,1)
1	(0,1)	(1,1)	(0,1)
2	(0,1)	(0,1)	(2,2)

Now, for the determination of all the cyclotomic numbers of order 3 of F_7 in terms of Jacobi sums of order 3, we need to determine only four Jacobi sums of order 3 out of nine Jacobi sums of order 3, these are $J_3(0,0)$, $J_3(0,1)$, $J_3(1,1)$ and $J_3(2,2)$. Now, for the determination of $(a,b)_3$, where $0 \le a,b \le 2$, apply the relation (1.2). On substituting the values of $J_3(0,0)$, $J_3(0,1)$, $J_3(1,1)$ and $J_3(2,2)$, we get $(0,0)_3 = 0$, $(0,1)_3 = 0$, $(0,2)_3 = 1$, $(1,0)_3 = 0$, $(1,1)_3 = 1$, $(1,2)_3 = 1$, $(2,0)_3 = 1$, $(2,1)_3 = 1$ and $(2,2)_3 = 0$.

3. CONCLUSION

We expect that the calculated number of cyclotomic numbers and Jacobi sums are the minimal for the determination of cyclotomic numbers and Jacobi sums, as lesser than this has not been seen in the literature.

ACKNOWLEDGEMENT

The authors are thankful to the Central University of Jharkhand, Ranchi, India for providing the research support.

REFERENCES

[1]. Ireland, K. and Rosen, M. (1990). A Classical Introduction to Modern Number Theory, Second edition, Springer, New York.

[2]. Weil, A. (1949). Number of solutions of equations in a finite field, *Bull. Amer. Math. Soc.*, 55, 497-508.

[3]. Adleman, L., Pomerance, C. and Rumely, R. (1983). On distinguishing prime numbers from composite numbers, *Ann. of Math.*, 117, 173-206.

[4]. Berndt, B.C., Evans, R.J. and Williams, K.S. (1998). Gauss and Jacobi Sums, John Wiley and Sons Inc., A Wiley-Interscience Publication, New York.

[5]. Shirolkar, D. and Katre, S.A. (2011). Jacobi sums and cyclotomic numbers of order l^2, *Acta Arith.*, 147, 33-49.

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

[7]. Katre, S.A. and Rajwade, A.R. (1985). Complete solution of the cyclotomic problem in F_q for any prime modulus $l, q = p^\alpha, p \equiv 1 \pmod{l}$, *Acta Arith.*, 45, 183-199.

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

[9]. Dickson, L.E. (1935). Cyclotomy, Higher Congruences and Waring's problem, *Amer. J. Math.*, 57, 391-424.